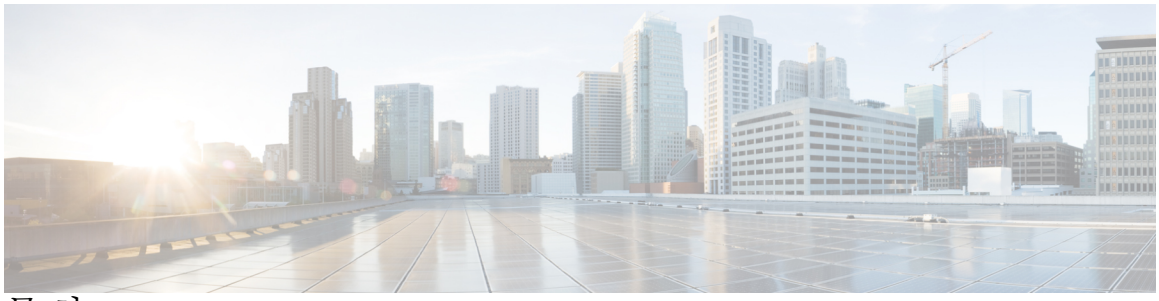
CLI Book 3: Cisco ASA Series VPN CLI 구성 가이드, 9.9

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883



목 차

가이드 정보

다음 주제에서는 이 가이드를 사용하는 방법을 설명합니다.

문서 목적

이 설명서는 CLI(Command Line Interface) 을 사용하여 ASA(Adaptive Security Appliance)에서 VPN을 구성하는 작업을 지원하기 위해 제공됩니다. 여기서는 모든 기능을 다루기보다는 가장 대표적인 구성 시나리오에 대해서만 설명합니다.

웹 기반 GUI 애플리케이션인 ASDM(Adaptive Security Device Manager)을 사용하여 ASA를 구성하고 모니터링할 수도 있습니다. ASDM에는 몇 가지 일반적인 구성 시나리오를 안내하는 구성 마법사와 특수한 시나리오에 대한 온라인 도움말이 포함되어 있습니다.

이 설명서는 Cisco ASA 시리즈에 적용됩니다. 이 가이드에서 "ASA"라는 용어는 별도로 지정하지 않는 한, 일반적으로 지원되는 모델에 적용됩니다.

관련 문서

자세한 내용은 http://www.cisco.com/go/asadocs에서 Navigating the Cisco ASA Series Documentation(Cisco ASA Series 설명서 찾기)을 참조하십시오.

문서 표기 규칙

이 문서는 다음 텍스트 표기, 표시 및 경고 규칙을 따릅니다.

가이드 정보

텍스트 표기 규칙

표기 규칙	표시
boldface	명령, 키워드, 버튼 레이블, 필드 이름 및 사용자 입력 텍스트는 **boldface**에 나타납니다. 메뉴 기반 명령의 경우, 명령에 대한 전체 경로가 표시됩니다.
기울임꼴	제공하는 값에 대한 변수는 기울임꼴 서체로 표시됩니다. 기울임꼴 유형은 문서 제목 및 일반적인 강조 시에도 사용됩니다.
monospace	시스템에 표시되는 터미널 세션 및 정보는 monospace 유형으로 표시됩니다.
{x | y | z}	필수 대체 키워드는 중괄호로 묶어 세로 선으로 구분합니다.
[ ]	대괄호로 묶인 요소는 선택적 요소입니다.
[x | y | z]	선택적 대체 키워드는 대괄호로 묶어 세로 선으로 구분합니다.
[ ]	시스템 프롬프트에 대한 기본 응답은 대괄호 안에도 표시됩니다.
< >	비밀번호와 같이 인쇄할 수 없는 문자는 꺾쇠괄호 안에 표시됩니다.
!, #	코드 라인 시작 부분에 있는 느낌표(!) 또는 숫자 기호(#)는 코멘트 행을 나타냅니다.

독자 알림

이 문서에서는 독자에게 알리기 위해 다음 사항을 사용합니다.

참고 독자가 주목해야 하는 내용을 의미합니다. 참고에는 유용한 제안이나 해당 설명서에서 다루지 않는 자료에 대한 참조 정보가 포함됩니다.

팁 다음 정보가 문제를 해결하는 데 도움이 된다는 것을 의미합니다.

주의 독자가 유의해야 하는 내용임을 의미합니다. 장비 손상이나 데이터 손실이 발생할 수 있으므로 주의해야 한다는 내용이 포함됩니다.

간편한 방법 설명한 작업이 시간을 절약함을 의미합니다. 단락에서 설명한 작업을 수행함으로써 시간을 절약할 수 있습니다.

경고! 독자에게 경고하는 내용을 의미합니다. 이러한 상황에서는 신체 상해로 이어질 수 있는 작업을 수행해야 할 수 있습니다.

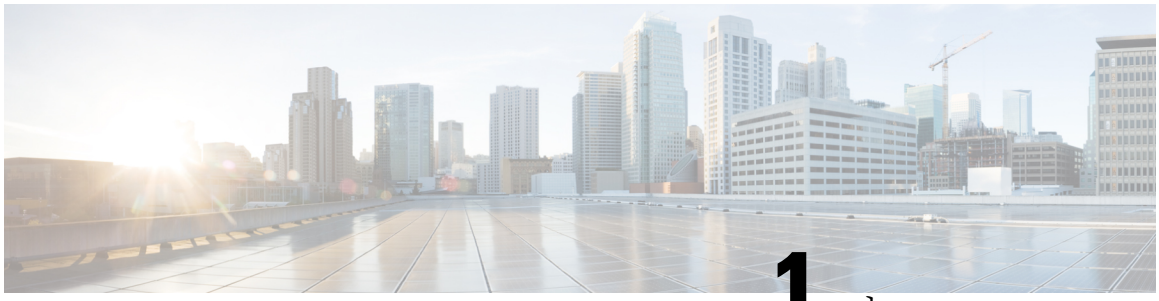
문서 가져오기 및 서비스 요청 제출

문서 가져오기, Cisco BST(Bug Search Tool) 사용, 서비스 요청 제출, 추가 정보 수집에 대한 자세한 내용은 Cisco 제품 설명서의 새로운 사항을 참조하십시오.

신규 및 수정된 Cisco 기술 콘텐츠를 데스크톱에서 곧바로 받으려면 Cisco 제품 설명서의 새로운 사항 RSS 피드를 구독하십시오. RSS 피드는 무료 서비스입니다.

I 부

Site-to-Site 및 클라이언트 VPN



1 장

IPsec 및 ISAKMP

터널링, IPsec 및 ISAKMP 정보

이 주제에서는 VPN(Virtual Private Networks: 가상 사설 네트워크)을 구축하는 데 사용되는 IPsec(Internet Protocol Security: 인터넷 프로토콜 보안) 및 ISAKMP(Internet Security Association and Key Management Protocol: 인터넷 보안 연계 및 키 관리 프로토콜) 표준에 대해 설명합니다.

터널링을 통해 인터넷과 같은 공용 TCP/IP 네트워크를 사용하고 원격 사용자와 사설 기업 네트워크 간의 안전한 연결을 생성할 수 있습니다. 각 보안 연결을 터널이라고 부릅니다.

ASA는 터널을 구축하고 관리하기 위해 ISAKMP 및 IPsec 터널링 표준을 사용합니다. ISAKMP 및 IPsec는 다음 사항을 수행합니다.

- 터널 매개변수 협상
- 터널 설정
- 사용자 및 데이터 인증
- 보안 키 관리
- 데이터 암호화 및 암호 해독
- 터널을 통한 데이터 전송 관리
- 터널 엔드포인트 또는 라우터로 데이터 전송 인바운드 및 아웃바운드 관리

ASA는 양방향 터널 엔드포인트로서의 기능을 합니다. 사설 네트워크에서 일반 패킷을 수신하여 캡슐화하고 터널을 생성하며, 캡슐 해제하여 최종 대상에 전송하는 다른 쪽 터널의 끝으로 보낼 수 있

습니다. 또한 공용 네트워크에서 캡슐화된 패킷을 수신하여 캡슐을 해제하여 사설 네트워크의 최종 대상에 보낼 수 있습니다.

IPsec 개요

ASA는 LAN-to-LAN VPN 연결을 위해 IPsec을 사용하고 client-to-LAN VPN 연결을 위해 IPsec을 사용하는 옵션을 제공합니다. IPsec 용어에서 피어는 원격 액세스 클라이언트 또는 다른 보안 게이트웨이를 말합니다. 두 연결 유형에서 ASA는 Cisco 피어만 지원합니다. VPN 업계 표준을 준수하므로 ASA가 다른 공급업체의 피어와 작동할 수는 있으나 이를 지원하지 않습니다.

터널을 구성하는 동안 2개의 피어가 인증, 암호화, 캡슐화 및 키 관리를 제어하는 보안 연계를 협상합니다. 이 협상은 2단계로 이루어집니다. 첫 번째 단계에서는 터널(IKE SA)을 구성하고 두 번째 단계에서는 터널(IPsec SA) 내에서 트래픽을 제어합니다.

LAN-to-LAN VPN은 다양한 위치에 있는 네트워크를 연결합니다. IPsec LAN-to-LAN 연결에서 ASA가 초기자 또는 응답자로 작동할 수 있습니다. IPsec client-to-LAN 연결에서는 ASA가 응답자로만 작동합니다. 초기자는 SA를 제안하는 반면 응답자는 구성된 SA 매개변수에 따라 카운터 제안을 수락, 거절 또는 생성합니다. 연결을 설정하려면 두 엔터티가 모두 SA에 동의해야 합니다.

IPsec 터널 이해

IPsec 터널은 피어 간에 ASA를 설정하는 SA 집합입니다. SA는 프로토콜과 알고리즘을 지정하여 민감한 데이터에 지정하고 피어가 사용하는 키 요소도 지정합니다. IPsec SA는 사용자 트래픽의 실제 전송을 제어합니다. SA는 단방향이지만 일반적으로 쌍(인바운드 및 아웃바운드)으로 설정됩니다.

피어가 각 SA에 사용할 설정을 협상합니다. 각 SA는 다음으로 구성됩니다.

- IKEv1 변형 집합 또는 IKEv2 제안서
- 암호화 맵
- ACL
- 터널 그룹
- 사전 조각화 정책

ISAKMP 및 IKE 개요

ISAKMP는 2개의 호스트가 IPsec SA(security association: 보안 연계)를 구축하는 방법에 대해 합의할 수 있는 협상 프로토콜입니다. 이는 SA 특성의 형식에 대한 합의의 일반적인 프레임워크를 제공합니다. 이 보안 연계에는 SA에 관하여 피어와 협상하고 SA를 변경하거나 삭제하는 것이 포함됩니다. ISAKMP는 1단계와 2단계의 두 단계로 협상을 분리합니다. 1단계에서는 최신 ISAKMP 협상 메시지를 보호하는 첫 번째 터널을 생성합니다. 2단계에서는 데이터를 보호하는 터널을 생성합니다.

IKE는 ISAKMP를 통해 IPsec용 SA를 사용할 수 있도록 설정합니다. IKE는 피어를 인증하는 데 사용되는 암호화 키를 생성합니다.

ASA는 레거시 Cisco VPN 클라이언트에서의 연결을 위해 IKEv1을 지원하고 AnyConnect VPN 클라이언트를 위해 IKEv2를 지원합니다.

ISAKMP 협상 기간을 설정하려면 다음을 포함하는 IKE 정책을 생성하십시오.

- IKEv1 피어에 필요한 인증 유형 즉, 인증서를 사용하는 RSA 서명 또는 사전 공유 키(PSK)
- 데이터를 보호하고 개인정보 보호를 보장하는 암호화 방식
- 발신자의 ID를 확인하고 메시지가 전송 중에 변경되지 않았는지 확인하는 HMAC(Hashed Message Authentication Codes: 해시된 메시지 인증 코드) 방식
- encryption-key-determination 알고리즘의 수준을 결정하는 Diffie-Hellman 그룹. ASA는 이 알고리즘을 사용하여 암호화 및 해시 키를 파생합니다.
- IKEv2의 경우 IKEv2 터널 암호화 등에 필요한 키 요소 및 해싱 작업을 파생하기 위한 알고리즘으로 별도의 PRF(Pseudo-Random Function: 의사 난수 함수)가 사용됩니다.
- ASA가 교체 전 암호 키를 사용하는 시간 제한

IKEv1 정책을 사용하면 각 매개변수에 1개의 값을 설정하게 됩니다. IKEv2의 경우 단일 정책에 여러 개의 암호화와 인증 유형 및 여러 개의 무결성 알고리즘을 구성할 수 있습니다. ASA는 설정을 가장 안전한 것부터 가장 안전하지 않은 것까지 나열하고 해당 순서를 사용하여 피어와 협상합니다. 이 순서를 사용하면 IKEv1과 마찬가지로 허용된 각 조합을 전송하는 대신 모든 허용된 변형을 전달하는 단일 제안서를 보낼 수 있습니다.

IKEv1 변형 집합 및 IKEv2 제안서 이해

IKEv1 변형 집합 또는 IKEv2 제안서는 ASA가 데이터를 보호하는 방법을 정의하는 보안 프로토콜과 알고리즘의 조합입니다. IPsec SA 협상 중에 피어는 두 피어에서 동일한 변형 집합 또는 제안서를 식별해야 합니다. 그러면 ASA가 일치하는 변형 집합 또는 제안서를 적용하여 해당 암호화 맵에 대한 ACL에서 데이터 흐름을 보호하는 SA를 생성합니다.

IKEv1 변형 집합을 사용하여 각 매개변수에 1개의 값을 설정합니다. IKEv2 제안서의 경우 단일 제안서에 여러 개의 암호화와 인증 유형 및 여러 개의 무결성 알고리즘을 구성할 수 있습니다. ASA는 설정을 가장 안전한 것부터 가장 안전하지 않은 것까지 나열하고 해당 순서를 사용하여 피어와 협상합니다. 이를 통해 IKEv1과 마찬가지로 허용된 각 조합을 개별적으로 전송하는 대신 모든 허용된 조합을 전달하는 단일 제안서를 보낼 수 있습니다.

SA를 생성하기 위해 사용되는 변형 집합 또는 제안서의 정의를 변경하려는 경우 ASA가 터널을 해제합니다. 자세한 내용은 보안 연계 지우기, 43 페이지를 참조하십시오.

참고 변형 집합 또는 제안서에서 유일한 요소를 지우거나 삭제하면 ASA가 해당 요소에 대한 암호화 맵 참조를 자동으로 제거합니다.

IPsec VPN에 대한 라이센싱

참고 No Payload Encryption 모델에서는 이 기능을 사용할 수 없습니다.

IKEv2를 사용하는 IPsec 원격 액세스 VPN에는 각각 사용 가능한 AnyConnect Plus 또는 Apex 라이센스가 필요합니다. AnyConnect 라이센스 구매 시 다음의 최대값을 참조하십시오. IKEv1을 사용하는 IPsec 원격 액세스 VPN과 IKEv1 또는 IKEv2를 사용하는 IPsec site-to-site VPN은 Base 라이센스와 함께 제공되는 기타 VPN 라이센스를 사용합니다. 모든 유형의 결합 VPN 세션의 최대 수는 이 표에 표시된 최대 세션 수를 초과할 수 없습니다.

모델	라이센스 요건
ASA 5506-X, 5506H-X, 5506W-X	• IKEv2를 사용하는 IPsec 원격 액세스 VPN: 세션 50개. • IKEv1을 사용하는 IPsec 원격 액세스 VPN 및 IKEv1 또는 IKEv2를 사용하는 IPsec Site-to-Site VPN: • Base 라이센스: 세션 10개. • Security Plus 라이센스: 세션 50개.
ASA 5508-X	세션 100개.
ASA 5512-X	세션 250개.
ASA 5515-X	세션 250개.
ASA 5516-X	세션 300개.
ASA 5525-X	세션 750개.
ASA 5545-X	세션 2500개.
ASA 5555-X	세션 5000개.
ASA 5585-X(SSP-10 포함)	세션 5000개.
ASA 5585-X(SSP-20, -40 및 -60 포함)	세션 10,000개.
ASASM	세션 10,000개.
ASAv5	세션 250개.
ASAv10	세션 250개.

모델	라이센스 요건
ASAv30	세션 750개.

IPsec VPN에 대한 지침

상황 모드 지침

단일 또는 다중 상황 모드에서 지원됩니다. 다중 상황 모드에서 원격 액세스 VPN을 사용하려면 AnyConnect Apex 라이선스가 필요합니다. ASA에서 AnyConnect Apex 라이선스를 인식하지 못하더라도, Apex 라이선스(예: 플랫폼 한도 내에서 라이선스가 허가된 AnyConnect Premium, AnyConnect for Mobile, AnyConnect for Cisco VPN Phone, 고급 엔드포인트 평가)의 라이선스 특성이 적용됩니다.

방화벽 모드 지침

라우팅된 방화벽 모드에서만 지원됩니다. 투명한 방화벽 모드를 지원하지 않습니다.

장애 조치 지침

IPsec VPN 세션이 활성/대기 장애 조치 구성에서만 복제됩니다.

ISAKMP 구성

IKEv1 및 IKEv2 정책 구성

IKEv1 및 IKEv2는 각각 최대 20개의 IKE 정책을 지원하고 서로 다른 설정 값을 사용합니다. 생성한 각 정책에 고유 우선순위를 지정하십시오. 우선순위 번호가 낮을수록 우선순위가 더 높습니다.

IKE 협상이 시작되면 협상을 시작하는 피어가 모든 정책을 원격 피어로 전송하고 원격 피어가 일치하는 항목 검색을 시도합니다. 원격 피어가 일치하는 항목을 찾을 때까지 각각의 구성된 정책에 대한 피어의 모든 정책을 우선순위 순서로(가장 높은 우선순위부터) 확인합니다.

두 피어의 정책이 같은 암호화, 해시, 인증 및 Diffie-Hellman 매개변수 값을 포함하는 경우 일치하는 항목이 존재합니다. 또한 IKEv1의 경우 원격 피어 정책이 초기자에서 보낸 정책보다 짧거나 같도록 수명을 지정해야 합니다. 수명이 같지 않은 경우 ASA가 더 짧은 수명을 사용합니다. IKEv2의 경우 수명은 협상되는 것이 아니라 각 피어 간에 로컬에서 관리되며, 각 피어에서 독립적으로 수명을 구성할 수 있습니다. 허용 가능한 일치 항목이 존재하지 않는 경우 IKE는 협상을 거부하고 SA가 설정되지 않습니다.

매개변수마다 특정 값을 선택하는 경우 보안 및 성능 간에 암시적인 절충이 이루어집니다. 기본값이 제공하는 보안 수준은 대부분 조직의 보안 요건에 적합합니다. 매개변수 값 중 1개만 지원하는 피어와 상호 운용하는 경우 선택 항목이 해당 값으로 제한됩니다.

각 ISAKMP 명령의 우선순위를 포함해야 합니다. 우선순위 번호는 정책을 고유한 방법으로 식별하고 IKE 협상에서 정책의 우선순위를 결정합니다.

프로시저

단계 **1** IKE 정책을 생성하려면 단일 또는 다중 상황 모드의 전역 구성 모드에서 **crypto** *ikev1* | *ikev2* policy 명령을 입력하십시오. IKE 정책 구성 모드 확인 상자가 표시됩니다.

예제:

```
hostname(config)# crypto ikev1 policy 1
```

참고 새로운 ASA 구성에는 기본 IKEv1 또는 IKEv2 정책이 없습니다.

단계 **2** 암호화 알고리즘을 지정합니다. 기본값은 삼중 DES입니다.

encryption [aes | aes-192 | aes-256 | des | 3des]

예제:

```
hostname(config-ikev1-policy)# encryption des
```

단계 **3** 해시 알고리즘을 지정합니다. 기본값은 SHA-1입니다.

hash [md5 | sha]

예제:

```
hostname(config-ikev1-policy)# hash md5
```

단계 **4** 인증 방법을 지정합니다. 기본값은 사전 공유 키입니다.

authentication[**pre-shared**]**rsa-sig**]

예제:

```
hostname(config-ikev1-policy)# authentication rsa-sig
```

단계 **5** Diffie-Hellman 그룹 식별자를 지정하십시오. 기본값은 그룹 2입니다.

group[**1** | **2** | **5**]

예제:

```
hostname(config-ikev1-policy)# group 5
```

단계 **6** SA 수명을 지정하십시오. 기본값은 86400초(24시간)입니다.

lifetime *seconds*

예제:

다음 예는 수명을 4시간(14400초)으로 설정합니다.

```
hostname(config-ikev1-policy)# lifetime 14400
```

단계 **7** IKE 정책 키워드 및 값, 7 페이지에서 제공되는 IKEv1 및 IKEv2 정책 키워드와 해당 값을 사용하여 추가 설정을 지정합니다. 제공된 Policy 매개변수의 값을 지정하지 않으면 기본값이 적용됩니다.

IKE 정책 키워드 및 값

	키워드	의미	설명
authentication	**rsa-sig**	RSA 서명 알고리즘에서 생성한 키를 사용하는 디지털 인증서	각 IPsec 피어의 ID를 설정하기 위해 ASA가 사용하는 인증 방법을 지정합니다.
	pre-share(기본값)	사전 공유 키	사전 공유 키는 증가하는 네트워크와 잘 비례하지 않지만 소규모 네트워크에서 설치하기 쉽습니다.
encryption	**des** **3des**(기본값)	56비트 DES-CBC 168비트 삼중 DES	두 IPsec 피어 간에 전송된 데이터를 보호하는 대칭 암호화 알고리즘을 지정합니다. 기본값은 168비트 삼중 DES입니다.
hash	**sha**(기본값)	SHA-1(HMAC 변형)	데이터 무결성을 보장하기 위해 사용된 해시 알고리즘을 지정합니다. 패킷이 표시된 시작 위치에서 제대로 시작하는지, 전송 중 변경되지 않았는지 확인합니다.
	md5	MD5(HMAC 변형)	기본값은 SHA-1입니다. MD5의 다이제스트가 더 작으며, 속도는 SHA-1보다 약간 더 빠른 것으로 간주됩니다. 그러나 MD5에 대한 공격(매우 어려움)이 발생하는 경우 IKE가 사용하는 HMAC 변형이 이 공격을 방지합니다.

	키워드	의미	설명
group	**1**	그룹 1(768비트)	서로 전달하지 않고 공유 비밀을 파생하기 위해 두 IPsec 피어가 사용하는 Diffie-Hellman 그룹의 식별자를 지정합니다. Diffie-Hellman 그룹 번호가 낮을수록 실행하는 데 필요한 CPU 시간이 줄어듭니다. Diffie-Hellman 그룹 번호가 높을수록 보안이 우수합니다. AES 지원은 VPN-3DES에 대해서만 라이센스가 허용된 보안 어플라이언스에서 사용할 수 있습니다. AES에서 요구하는 대형 키 크기를 지원하려면 ISAKMP 협상이 DH(Diffie-Hellman) 그룹 5를 사용해야 합니다.
	2(기본값)	그룹 2(1024비트)	
	5	그룹 5(1536비트)	
lifetime	정수 값 (86400 = 기본값)	120 - 2147483647초	SA 수명을 지정합니다. 기본값은 86,400초 또는 24시간입니다. 일반적으로 어느 정도까지는 수명이 짧을수록 더 안전한 ISAKMP 협상을 제공합니다. 그러나 수명이 짧을 경우 ASA가 이후 IPsec SA를 더 빨리 구성합니다.

	키워드	의미	설명
integrity	sha(기본값)	SHA-1(HMAC 변형)	데이터 무결성을 보장하기 위해 사용된 해시 알고리즘을 지정합니다. 패킷이 표시된 시작 위치에서 제대로 시작하는지, 전송 중 변경되지 않았는지 확인합니다.

	키워드	의미	설명
	md5	MD5(HMAC 변형)	기본값은 SHA-1입니다. MD5의 다이제스트가 더 작으며, 속도는 SHA-1보다 약간 더 빠른 것으로 간주됩니다. 그러나 MD5에 대한 공격(매우 어려움)이 발생하는 경우 HMAC 변형 IKE 사용자가 이 공격을 방지합니다.
	sha256	SHA 2, 256비트 다이제스트	256비트 다이제스트로 Secure Hash Algorithm SHA 2를 지정합니다.
	sha384	SHA 2, 384비트 다이제스트	384비트 다이제스트로 Secure Hash Algorithm SHA 2를 지정합니다.
	sha512	SHA 2, 512비트 다이제스트	512비트 다이제스트로 Secure Hash Algorithm SHA 2를 지정합니다.
	null		AES-GCM이 암호화 알고리즘으로 지정된 경우 관리자가 IKEv2 무결성 알고리즘으로 null을 선택할 수 있습니다.
encryption	des 3des(기본값)	56비트 DES-CBC 168비트 삼중 DES	두 IPsec 피어 간에 전송된 데이터를 보호하는 대칭 암호화 알고리즘을 지정합니다. 기본값은 168비트 삼중 DES입니다.
	aes aes-192 aes-256		고급 표준 암호화가 128비트, 192비트, 256비트의 키 길이를 지원합니다.
	aes-gcm aes-gcm-192 aes-gcm-256 null	IKEv2 암호화를 위해 사용하는 AES-GCM 알고리즘 옵션	고급 표준 암호화가 128비트, 192비트, 256비트의 키 길이를 지원합니다.
policy_index			IKEv2 정책 서브모드에 액세스합니다.

	키워드	의미	설명
prf	sha(기본값)	SHA-1(HMAC 변형)	키 요소를 생성하는 데 사용되는 알고리즘인 PRF(Pseudo Random Function: 의사 난수 함수)을 지정합니다.
	md5	MD5(HMAC 변형)	기본값은 SHA-1입니다. MD5의 다이제스트가 더 작으며, 속도는 SHA-1보다 약간 더 빠른 것으로 간주됩니다. 그러나 MD5에 대한 공격(매우 어려움)이 발생하는 경우 IKE가 사용하는 HMAC 변형이 이 공격을 방지합니다.
	sha256	SHA 2, 256비트 다이제스트	256비트 다이제스트로 Secure Hash Algorithm SHA 2를 지정합니다.
	sha384	SHA 2, 384비트 다이제스트	384비트 다이제스트로 Secure Hash Algorithm SHA 2를 지정합니다.
	sha512	SHA 2, 512비트 다이제스트	512비트 다이제스트로 Secure Hash Algorithm SHA 2를 지정합니다.
priority			추가 IPsec V3 기능을 지원하도록 정책 모드를 확장하고 Suite B의 AES-GCM 및 ECDH 설정 일부를 지원합니다.

	키워드	의미	설명
group	**1**	그룹 1(768비트)	서로 전달하지 않고 공유 비밀을 파생하기 위해 두 IPsec 피어가 사용하는 Diffie-Hellman 그룹의 식별자를 지정합니다. Diffie-Hellman 그룹 번호가 낮을수록 실행하는 데 필요한 CPU 시간이 줄어듭니다. Diffie-Hellman 그룹 번호가 높을수록 보안이 우수합니다. 비FIPS 모드에서는 AnyConnect 클라이언트가 그룹 1, 그룹 2 및 그룹 5를 지원하고 FIPS 모드에서는 그룹 2만 지원합니다. AES 지원은 VPN-3DES에 대해서만 라이센스가 허용된 보안 어플라이언스에서 사용할 수 있습니다. AES에서 요구하는 대형 키 크기를 지원하려면 ISAKMP 협상이 DH(Diffie-Hellman) 그룹 5를 사용해야 합니다.
	2(기본값)	그룹 2(1024비트)	
	5	그룹 5(1536비트)	
	14 19 20 21 24		
lifetime	정수 값 (86400 = 기본값)	120 - 2147483647초	SA 수명을 지정합니다. 기본값은 86,400초 또는 24시간입니다. 일반적으로 어느 정도까지는 수명이 짧을수록 더 안전한 ISAKMP 협상을 제공합니다. 그러나 수명이 짧을 경우 ASA가 이후 IPsec SA를 더 빨리 구성합니다.

외부 인터페이스에서 **IKE** 활성화

VPN 터널을 종료하는 인터페이스에서 IKE를 활성화해야 합니다. 일반적으로 이는 외부 또는 공유 인터페이스입니다. IKEv1 또는 IKEv2를 활성화하려면 단일 또는 다중 상황 모드의 전역 구성 모드에서 [**ikev1** | **ikev2**] **enable** *interface-name* 명령을 사용하십시오.

예를 들면 다음과 같습니다.

```
hostname(config)# crypto ikev1 enable outside
```

IKEv1 Aggressive(적극적인) 모드 비활성화

1단계 IKEv1 협상이 Main(기본) 모드 또는 Aggressive(적극적인) 모드를 사용할 수 있습니다. 두 모드는 같은 서비스를 제공하지만 적극적인 모드에서는 피어 간에 총 6개 메시지를 3번 교환하는 대신 총 3개 메시지를 2번만 교환합니다. 적극적인 모드가 조금 더 빠르지만 통신 당사자의 ID를 보호하지 않습니다. 따라서 피어는 안전한 SA를 설정하기 전에 식별 정보를 교환해야 합니다. 기본적으로 적극적인 모드가 활성화되어 있습니다.

참고 적극적인 모드를 비활성화하면 Cisco VPN 클라이언트가 ASA에 대한 터널을 설정하는 데 사전 공유 키 인증을 사용할 수 없습니다. 그러나 인증서 기반의 인증(즉, ASA 또는 RSA)을 사용하여 터널을 설정할 수 있습니다.

적극적인 모드를 비활성화하려면 단일 또는 다중 상황 모드에서 다음 명령을 입력하십시오.

```
hostname(config)# crypto ikev1 am-disable
```

적극적인 모드를 비활성화했다가 다시 활성화 상태로 되돌리려면 no 형식의 명령을 사용하십시오. 예를 들면 다음과 같습니다.

```
hostname(config)#  no crypto ikev1 am-disable
```

IKEv1 및 IKEv2 ISAKMP 피어의 ID 방식 구성

IKEv1 또는 IKEv2 ISAKMP I단계 협상 동안 피어는 서로 식별해야 합니다. 다음 옵션 중에서 식별 방식을 선택할 수 있습니다.

Address	ISAKMP ID 정보를 교환하는 호스트의 IP 주소를 사용합니다.
Automatic (기본값)	연결 유형별 ISAKMP 협상을 결정합니다. • 사전 공유 키의 IP 주소 • 인증서 인증을 위한 인증서 고유 이름
Hostname	ISAKMP ID 정보(기본값)를 교환하는 호스트의 정규화된 도메인 이름을 사용합니다. 이 이름은 호스트 이름 및 도메인 이름으로 구성됩니다.
Key ID *key_id_string*	사전 공유 키를 검색하기 위해 원격 피어가 사용하는 문자열을 지정합니다.

ASA는 I단계 ID를 사용하여 피어로 전송합니다. 이는 사전 공유 키를 사용하여 인증하는 기본 모드에서 LAN-to-LAN IKEv1 연결을 제외한 모든 VPN 시나리오에 적용됩니다.

피어 식별 방식을 변경하려면 단일 또는 다중 상황 모드에서 다음 명령을 입력하십시오.

crypto isakmp identity {*address* | *hostname* | **key-id** *id-string* | **auto**}

예를 들어 다음 명령은 호스트 이름에 대한 피어 식별 방식을 설정합니다.

```
hostname(config)# crypto isakmp identity hostname
```

INVALID_SELECTORS 알림

IPsec 시스템이 SA의 인바운드 패킷을 수신하고 패킷 헤더 필드가 SA의 선택사항과 일치하지 않는 경우, 패킷을 버려야 합니다. 이 이벤트에 대한 감사 로그 항목에는 패킷의 현재 날짜/시간, SPI, IPsec 프로토콜, 소스 및 대상, 사용 가능한 패킷의 다른 모든 벡터 값과 관련된 SA 항목의 선택기 값이 포함됩니다. 시스템에서 발신자(IPsec 피어)에게 수신된 패킷이 선택기 확인을 전달하는 데 실패했기 때문에 삭제되었음을 표시하는 INVALID_SELECTORS의 IKE 알림을 생성하고 전송합니다.

ASA는 아래에 표시된 기존 syslog를 사용하여 CTM에서 이 이벤트의 로그를 구현합니다.

```
%ASA-4-751027: IKEv2 Received INVALID_SELECTORS Notification from peer: <peer IP>. Peer
received a packet (SPI=<spi>) from <local_IP>. The decapsulated inner packet didn't match
 the negotiated policy in the SA. Packet destination <pkt_daddr>, port <pkt_dest_port>,
source <pkt_saddr>, port <pkt_src_port>, protocol <pkt_prot>
```

관리자는 이제 SA에서 해당 SA에 대한 트래픽 선택기와 일치하지 않는 인바운드 패킷을 수신하는 경우 피어에 대한 IKEv2 알림 전송을 활성화하거나 비활성화할 수 있습니다. 활성화할 경우, IKEv2 알림 메시지가 5초마다 SA당 1개의 알림 메시지로 속도가 제한됩니다. IKEv2 알림은 피어에 IKEv2 정보 교환으로 전송됩니다.

IKEv2 사전 공유 키 16진수로 구성

로컬 및 원격 사전 공유 키 명령에 *hex* 키워드를 추가하여 IKEv2 사전 공유 키를 16진수로 구성할 수 있습니다.

```
ikev2 local-authentication pre-shared-key [ 0 | 8 | hex ] <string>
ikev2 remote-authentication pre-shared-key [ 0 | 8 | hex ] <string>
```

IKE 알림 전송 활성화 또는 비활성화

관리자는 IKEv2 IPsec VPN에서 해당 연결에 대한 트래픽 선택기와 일치하지 않는 인바운드 패킷을 수신하는 경우 피어에 대한 IKE 알림 전송을 활성화하거나 비활성화할 수 있습니다. 이 알림의 전송은 기본적으로 비활성화되어 있습니다. ASDM 인증서에서 사용자 이름의 권한 부여가 다음 CLI를 사용하여 활성화 또는 비활성화되는 경우 IKE INVALID_SELECTORS 알림이 전송됩니다.

[**no**] **crypto ikev2 notify invalid-selectors**

인증서 인증을 수행할 경우, 인증서의 CN은 사용자 이름이며, 권한은 로컬 서버를 대상으로 부여됩니다. “Service-type” 특성을 검색하는 경우, 앞에서 설명한 대로 처리됩니다.

IKEv2 프래그멘테이션 옵션 구성

ASA에서 IKEv2 프래그멘테이션을 활성화하거나 비활성화할 수 있고, IKEv2 패킷을 프래그멘테이션할 때 사용되는 MTU(Maximum Transmission Unit)를 지정할 수 있으며, 관리자가 다음 명령을 사용하여 기본 프래그멘테이션 메서드를 구성할 수 있습니다.

[**no**] **crypto ikev2 fragmentation** [**mtu** <*mtu-size*>] | [**preferred-method** [**ietf** | **cisco**]]

기본적으로 IKEv2 프래그멘테이션의 모든 메서드가 활성화되면 MTU는 IPv4의 경우 576, IPv6의 경우 1280이고, 메서드는 IETF 표준 RFC-7383를 사용하는 것이 좋습니다.

다음 사항을 고려하여 [**mtu** <*mtu-size*>]를 지정합니다.

- 사용되는 MTU 값에는 IP(IPv4/IPv6) 헤더 + UDP 헤더 크기를 포함해야 합니다.
- 관리자가 지정하지 않은 경우 기본 MTU는 IPv4의 경우 576, IPv6의 경우 1280입니다.
- 지정한 경우에는 IPv4와 IPv6 모두에 대해 동일한 MTU가 사용됩니다.
- 유효한 범위는 68-1500입니다.

지원되는 다음 프래그멘테이션 메서드 중 하나를 IKEv2 [**preferred-method** [**ietf** | **cisco**]]에 대한 기본 프래그멘테이션 메서드로 구성할 수 있습니다.

- IETF RFC-7383 표준 기반 IKEv2 프래그멘테이션.
  - 협상 중에 두 피어 모두 지원 및 기본 설정을 지정하는 경우 이 메서드를 사용됩니다.
  - 이 메서드를 사용하면 각 IKEv2 Fragment(IKEv2 프래그먼트) 메시지에 대한 개별 보호를 제공하는 프래그멘테이션 후에 암호화가 수행됩니다.
- Cisco의 독점 프래그멘테이션입니다.
  - 이 메서드가 AnyConnect 클라이언트와 같은 피어가 제공하는 유일한 메서드거나 두 피어 모두 협상 중에 지원 및 기본 설정을 지정하는 경우 이 메서드가 사용됩니다.
  - 이 메서드를 사용하면 암호화 후에 프래그멘테이션이 수행됩니다. 모든 프래그먼트를 수신할 때까지 수신 피어가 암호를 해독하거나 메시지를 인증할 수 없습니다.
  - 이 방법은 Cisco 이외의 피어와 상호 운용될 수 없습니다.

show running-config crypto ikev2 명령은 현재 구성을 표시하고, **show crypto ikev2 sa detail**은 SA에 프래그멘테이션이 사용된 경우에 적용된 MTU를 표시합니다.

시작하기 전에

- 경로 MTU 검색은 지원되지 않으므로, MTU를 네트워크의 요구 사항에 맞게 수동으로 구성해야 합니다.
- 이 구성은 전역으로, 구성을 적용한 후에 설정되는 향후의 SA에 영향을 줍니다. 이전 SA에는 영향을 주지 않습니다. 프래그멘테이션이 비활성화되면 동일한 동작이 일어납니다.
- 최대 100개의 프래그먼트를 수신할 수 있습니다.

예

- IKEv2 프래그멘테이션을 비활성화하려는 경우:

```
no crypto ikev2 fragmentation
```

- 기본 작업을 복구하려는 경우:

```
crypto ikev2 fragmentation
```

또는

```
crypto ikev2 fragmentation mtu 576
preferred-method ietf
```

- MTU 값을 600으로 변경하려는 경우:

```
crypto ikev2 fragmentation mtu 600
```

- 기본 MTU 값을 복원하려는 경우:

```
 no crypto ikev2 fragmentation mtu 576
```

- 프래그멘테이션의 기본 메서드를 Cisco로 변경하려는 경우:

```
crypto ikev2 fragmentation preferred-method cisco
```

- 기본 프래그멘테이션 메서드를 IETF로 복원하려는 경우:

```
no crypto ikev2 fragmentation preferred-method cisco
```

또는

```
 crypto ikev2 fragmentation preferred-method ietf
```

권한 부여를 통한 **AAA** 인증

```
aaa authentication http console LOCAL
aaa authorization http console radius
```

AAA 인증은 사용자가 입력한 사용자 이름/비밀번호를 사용하여 로컬 서버를 대상으로 수행됩니다. *radius* 서버에 대한 추가 권한 부여는 동일한 사용자 이름을 사용하여 수행됩니다. *service-type* 속성이 검색되면 앞에서 설명한 대로 처리됩니다.

IPsec over NAT-T 활성화

NAT-T를 사용하면 IPsec 피어가 NAT 디바이스를 통한 연결을 설정할 수 있습니다. 이는 NAT 디바이스에 포트 정보를 제공하는 포트 4500을 사용하여 UDP 데이터그램 내의 IPsec 트래픽을 캡슐화하는 방법으로 수행됩니다. NAT-T는 모든 NAT 디바이스를 자동으로 감지하고 필요한 경우 IPsec 트래픽만 캡슐화합니다. 이 기능은 기본적으로 비활성화되어 있습니다.

참고 AnyConnect 클라이언트의 한계를 고려하여 IKEv2를 통해 AnyConnect 클라이언트에 대한 NAT-T가 성공적으로 연결할 수 있도록 해야 합니다. 이 요건은 클라이언트가 NAT-T 디바이스를 지원하지 않는 경우에도 적용됩니다.

ASA는 데이터를 교환 중인 클라이언트에 따라 표준 IPsec, TCP를 통한 IPsec, NAT-T 및 UDP를 통한 IPsec을 동시에 지원할 수 있습니다.

다음 세부 사항은 활성화된 각 옵션과의 연결을 보여줍니다.

옵션	활성화된 기능	클라이언트 위치	사용되는 기능
옵션 1	NAT-T 활성화	클라이언트가 NAT 뒤에 있는 경우	NAT-T가 사용됨
		NAT가 존재하지 않는 경우	네이티브 IPsec(ESP)이 사용됨
옵션 2	UDP를 통한 IPsec 활성화	클라이언트가 NAT 뒤에 있는 경우	UDP를 통한 IPsec이 사용됨
		NAT가 존재하지 않는 경우	UDP를 통한 IPsec이 사용됨
옵션 3	NAT-T 및 UDP를 통한 IPsec 활성화	클라이언트가 NAT 뒤에 있는 경우	NAT-T가 사용됨
		NAT가 존재하지 않는 경우	UDP를 통한 IPsec이 사용됨

참고 TCP를 통한 IPsec이 활성화되면 이 기능이 기타 모든 연결 방법보다 우선시됩니다.

NAT-T를 활성화하면 ASA에서 IPsec이 활성화된 모든 인터페이스의 포트 4500을 자동으로 엽니다.

ASA는 단일 NAT/PAT 디바이스 뒤에 있는 여러 IPsec 피어를 지원합니다. 이는 LAN-to-LAN 또는 원격 액세스 네트워크 중 하나에서만 작동합니다. 혼합 환경에서는 모든 피어가 같은 공용 IP 주소, NAT 디바이스 주소에서 오는 것으로 나타나므로 원격 액세스 터널이 협상에 실패합니다. 또한 원격 액세스 터널은 종종 LAN-to-LAN 터널 그룹(NAT 디바이스의 IP 주소)과 같은 이름을 사용하기 때문에 혼합 환경에서 실패합니다. 이렇게 이름이 일치하는 경우 NAT 디바이스 뒤 피어의 혼합 LAN-to-LAN 및 원격 액세스 네트워크에 있는 여러 피어에서 협상 실패의 원인이 될 수 있습니다.

NAT-T를 사용하려면 단일 또는 다중 상황 모드에서 다음 Site-to-Site 단계를 수행하십시오.

프로시저

단계 1 다음 명령을 입력하여 ASA에서 NAT-T를 통한 IPsec을 활성화하십시오.

crypto isakmp nat-traversal *natkeepalive*

natkeepalive 인수의 범위는 10-3600초입니다. 기본값은 20초입니다.

예제:

NAT-T를 활성화하고 킵얼라이브 값을 1시간으로 설정하려면 다음 명령을 입력하십시오.

```
hostname(config)# crypto isakmp nat-traversal 3600
```

단계 2 다음 명령을 입력하여 IPsec 단편화 정책에 대한 암호화 이전 옵션을 선택하십시오.

```
hostname(config)# crypto ipsec fragmentation before-encryption
```

이 옵션을 사용하면 트래픽이 IP 단편화를 지원하지 않는 NAT 디바이스를 통과할 수 있습니다. IP 단편화를 지원하는 NAT 디바이스의 작동을 방해하지 않습니다.

TCP를 통한 IKEv1을 사용하는 IPsec 활성화

TCP를 통한 IPsec은 TCP와 같은 패킷 내에서 IKEv1 및 IPsec 프로토콜을 캡슐화하여 NAT 및 PAT 디바이스와 방화벽을 통해 안전한 터널링을 활성화합니다. 이 기능은 기본적으로 비활성화되어 있습니다. TCP를 통한 IPsec/IKEv1은 Cisco VPN 클라이언트가 표준 ESP 또는 IKEv1이 작동할 수 없거나 기존 방화벽 규칙의 변경을 통해서만 작동할 수 있는 환경에서 작동할 수 있게 합니다.

참고 이 기능은 프록시 기반 방화벽에서 작동하지 않습니다.

IPsec over TCP는 원격 액세스 클라이언트에서 작동합니다. 연결하는 ASA 및 클라이언트에서 TCP를 통한 IPsec을 활성화합니다. ASA에서 전역적으로 활성화되며 모든 IKEv1 활성화 인터페이스에서 작동합니다. LAN-to-LAN 연결에서 작동하지 않습니다.

ASA는 데이터를 교환 중인 클라이언트에 따라 표준 IPsec, TCP를 통한 IPsec, NAT-Traversal 및 UDP를 통한 IPsec을 동시에 지원할 수 있습니다. TCP를 통한 IPsec이 활성화되면 이 기능이 기타 모든 연결 방법보다 우선시됩니다.

사용자가 지정하는 최대 10개의 포트에 대해 TCP를 통한 IPsec을 활성화할 수 있습니다. 포트 80(HTTP) 또는 포트 443(HTTPS)과 같이 잘 알려진 포트를 입력하면 해당 포트에 연계된 프로토콜이 공용 인터페이스에서 더 이상 작동하지 않는다는 경고를 시스템이 표시합니다. 결과적으로 공용 인터페이스를 통해 ASA를 관리하는 데 더 이상 브라우저를 사용할 수 없습니다. 이 문제를 해결하려면 HTTP/HTTPS 관리를 다른 포트로 재설정하십시오.

기본 포트는 10000입니다.

ASA뿐만 아니라 클라이언트에서도 TCP 포트를 구성해야 합니다. 클라이언트 구성은 ASA를 위해 설정한 포트를 최소 1개 이상 포함해야 합니다.

ASA에서 IKEv1에 대하여 TCP를 통한 IPsec을 전역으로 활성화하려면 단일 또는 다중 상황 모드에서 다음 명령을 수행하십시오.

crypto ikev1 ipsec-over-tcp [port *port 1...port0]*

이 예는 포트 45에서 TCP를 통한 IPsec을 활성화합니다.

```
hostname(config)# crypto ikev1 ipsec-over-tcp port 45
```

IKEv1에 대한 인증서 그룹 일치 구성

터널 그룹이 사용자 연결 조건 및 권한을 정의합니다. 인증서 그룹 일치를 통해 사용자 인증서의 주체 DN 또는 발급자 DN을 사용하여 터널 그룹에 사용자를 일치시킬 수 있습니다.

참고 인증서 그룹 일치는 IKEv1 및 IKEv2 LAN-to-LAN 연결에만 적용됩니다. IKEv2 원격 액세스 연결은 터널 그룹의 webvpn 특성 및 인증서 그룹 맵 등의 webvp 구성 모드에서 구성된 풀다운 그룹 선택을 지원합니다.

인증서의 해당 필드에 따라 사용자와 터널 그룹을 일치시키려면 먼저 일치 기준을 정의하는 규칙을 생성하고 각 규칙을 필요한 터널 그룹과 연계해야 합니다.

인증서 맵을 생성하려면 **use the crypto ca certificate map** 명령을 사용합니다. 터널 그룹을 정의하려면 tunnel-group 명령을 사용하십시오.

또한 규칙 또는 조직 단위(OU) 필드에서 그룹을 일치시키거나 모든 인증서 사용자에게 기본 그룹을 사용하도록 지정하는 인증서 그룹 일치 정책을 구성할 수도 있습니다. 이러한 방법 중 하나 또는 모두를 사용할 수 있습니다.

프로시저

단계 **1** 터널 그룹에 대한 인증서 기반 ISAKMP 세션 맵에 따라 정책과 규칙을 구성하고 인증서 맵 항목과 터널 그룹을 연계하려면 단일 또는 다중 상황 모드에서 tunnel-group-map 명령을 입력하십시오.

tunnel-group-map enable {*rules* | *ou* | *ike-id* | *peer ip*}

tunnel-group-map [*rule-index*] **enable** *policy*

policy	인증서에서 터널 그룹 이름 파생에 대한 정책을 지정합니다. Policy는 다음 중 하나가 될 수 있습니다. *ike-id* - 터널 그룹이 규칙 조회를 기반으로 결정되거나 OU에서 가져온 것이 아니라 인증서 기반 ISAKMP 세션이 1단계 ISAKMP ID의 콘텐츠에 따라 터널 그룹에 매핑되는 것을 나타냅니다. *ou* - 터널 그룹이 규칙 조회를 기반으로 결정되지 않고 주체 DN(고유 이름)에서 OU의 값을 사용하는 것을 나타냅니다. *peer-ip* - 터널 그룹이 규칙 조회를 기반으로 결정되거나 OU 또는 ike-id 방식에서 가져온 것이 아니라 피어 IP 주소를 사용하는 것을 나타냅니다. *rules* - 인증서 기반 ISAKMP 세션이 이 명령에 의해 구성된 인증서 맵 연계를 기반으로 터널 그룹에 매핑되는 것을 나타냅니다.
rule index	(선택 사항) **crypto ca certificate map** 명령을 통해 지정된 매개변수를 참조하십시오. 값은 1 - 65535입니다.

다음 사항에 유의하십시오.

- 각 호출이 고유하고 및 맵 색인을 두 번 이상 참조하지 않는 경우에만 해당 명령을 여러 번 호출할 수 있습니다.
- 규칙은 255자를 초과할 수 없습니다.
- 같은 그룹에 여러 규칙을 할당할 수 있습니다. 이렇게 하려면 먼저 규칙 우선순위와 그룹을 추가합니다. 그런 다음 각 그룹에 필요한 만큼 기준 명령문을 정의합니다. 같은 그룹에 여러 규칙이 할당된 경우 true를 테스트하는 첫 번째 규칙과 일치하게 됩니다.
- 하나의 규칙을 생성하면 사용자를 특정 터널 그룹에 할당하기 전에 모든 기준을 일치시켜야 할 수 있습니다. 논리적 AND 연산에서도 모든 기준이 일치해야 합니다. 또는 사용자를 특정 터널 그룹에 할당하기 전에 1개의 기준만 일치시키려는 경우 각 기준에 1개의 규칙을 생성하십시오. 논리적 OR 연산에서도 1개의 기준만 일치해야 합니다.

단계 **2** 구성에서 터널 그룹을 지정하지 않는 경우 기본 터널 그룹을 사용하도록 지정합니다.

구문은**tunnel-group-map** [*rule-index*] **default-group** *tunnel-group-name*이며 *rule-index*는 규칙의 우선순위입니다. 또한 터널 그룹 이름은 이미 존재하는 터널 그룹이어야 합니다.

예

다음 예는 1단계 ISAKMP ID의 콘텐츠 기반의 터널 그룹에 인증서 기반 ISAKMP 세션을 매핑합니다.

```
hostname(config)# tunnel-group-map enable ike-id
```

다음 예는 피어의 IP 주소 기반의 터널 그룹에 인증서 기반 ISAKMP 세션을 매핑합니다.

```
hostname(config)# tunnel-group-map enable peer-ip
```

다음 예는 주체 DN(고유 이름)에서 OU(조직 단위)를 기반으로 인증서 기반 ISAKMP 세션을 매핑합니다.

```
hostname(config)# tunnel-group-map enable ou
```

다음 예는 설정한 규칙을 기반으로 인증서 기반 ISAKMP 세션을 매핑합니다.

```
hostname(config)# tunnel-group-map enable rules
```

IPsec 구성

이 섹션에서는 VPN을 구현하기 위해 IPsec을 사용하는 경우 ASA를 구성하는 데 필요한 절차를 설명합니다.

암호화 맵 정의

암호화 맵은 IPsec SA에서 협상되는 IPsec 정책을 정의합니다. 암호화 맵은 다음을 포함합니다.

- IPsec 연결이 허용하고 보호하는 패킷을 식별하기 위한 ACL
- 피어 식별
- IPsec 트래픽의 로컬 주소(자세한 내용은 암호화 맵을 인터페이스에 적용, 30 페이지 참조)
- 피어 보안 설정의 일치를 시도하는 최대 11개의 IKEv1 변형 집합 또는 IKEv2 제안서

암호화 맵 집합은 같은 맵 이름을 가진 하나 이상의 암호화 맵으로 구성되어 있습니다. 첫 번째 암호화 맵을 생성할 때 암호화 맵 집합을 생성할 수 있습니다. 다음 Site-to-Site 작업이 단일 또는 다중 상황 모드의 암호화 맵을 생성 또는 추가합니다.

crypto map *map-name seq-num* **match address** *access-list-name*

access-list-name을 사용하여 최대 241자의 문자열 또는 정수로 ACL ID를 지정하십시오.

팁 구성에서 ACL ID를 쉽게 식별하려면 모두 대문자를 사용하십시오.

이 명령을 계속 입력하여 암호화 맵을 암호화 맵 집합에 추가할 수 있습니다. 다음 예에서 *mymap*은 암호화 맵을 추가하려는 암호화 맵 집합의 이름입니다.

crypto map mymap 10 match address 101

위 구문에 표시된 시퀀스 번호(*seq-num*)를 통해 같은 이름을 사용하는 암호화 맵을 서로 구별합니다. 또한 암호화 맵에 할당된 시퀀스 번호가 암호화 맵 집합 내에서 다른 암호화 맵 간의 우선순위를 결정합니다. 시퀀스 번호가 낮을수록 우선순위가 더 높습니다. 암호화 맵 집합을 인터페이스에 할당하면 ASA가 시퀀스 번호가 가장 낮은 암호화 맵부터 시작하여 세트 내 암호화 맵에 대해 인터페이스를 통과하는 모든 IP 트래픽을 평가합니다.

[no] crypto map *map_name map_index* **set pfs [group1 | group2 | group5 | group14 | group19 | group20 | group21 | group24]**

암호화 맵을 위해 완전 순방향 비밀성(PFS)에 사용되는 ECDH 그룹을 지정하십시오. IKEv1 정책을 사용할 경우 암호화 맵에 대해 group14 및 group24 옵션 구성을 방지합니다.

[no] crypto map *map_name seq-num* **set reverse-route** [**dynamic**]

이 암호화 맵 항목에 기반하여 모든 연결에 대해 역방향 라우팅 삽입(RRI)을 활성화합니다.Dynamic(동적)이 지정되지 않은 경우 RRI는 구성할 때 수행되며 정적이라고 간주되어 구성이 변경될 때까지 그대로 남아 있거나 제거됩니다. ASA에서는 라우팅 테이블에 고정 경로를 자동으로 추가하고, OSPF를 사용하여 사설 네트워크 또는 경계선 라우터에 이 경로를 알립니다.

Dynamic(동적)이 지정된 경우, 라우팅은 IPsec 보안 연계(SA)를 성공적으로 설정할 경우 생성되며 IPsec SA가 삭제된 후에 삭제됩니다.

참고 동적 RRI는 IKEv2 기반 정적 암호화 맵에만 적용됩니다.

[no] crypto map *name priority* **set validate-icmp-errors**

OR

[**no**]**crypto dynamic-map** *name priority* **set validate-icmp-errors**

암호화 또는 동적 암호화 맵에 대한 수신 ICMP 오류 메시지의 확인 여부를 지정합니다.

[no] crypto map <name> <priority> set df-bit [clear-df | copy-df | set-df}

OR

[no] crypto map dynamic-map <name> <priority> set df-bit [clear-df | copy-df | set-df]

암호화 또는 동적 암호화 맵에 대한 보안 연계 수준의 기존 DF(do not fragment) 정책을 구성하십시오.

- *clear-df* — DF 비트를 무시합니다.
- *copy-df* — DF 비트를 유지합니다.
- *set-df* — DF 비트를 설정하고 사용합니다.

[no] crypto map <name> <priority> set tfc-packets [burst <length | auto] [payload-size <bytes | auto> [timeout <seconds | auto>

OR

[no] crypto dynamic-map <name> <priority> set tfc-packets [burst <length | auto] [payload-size <bytes | auto> [timeout <seconds | auto>

관리자가 IPsec 보안 연계에서 임의의 길이 및 간격으로 더미 TFC(Traffic Flow Confidentiality: 트래픽 흐름 기밀성)를 활성화할 수 있습니다. TFC를 활성화하기 전에 IKEv2 IPsec 제안서가 있어야 합니다.

암호화 맵에 할당된 ACL은 다음 명령 구문에 표시된 것과 같이 같은 ACL 이름을 가진 모든 ACE로 구성됩니다.

access-list *access-list-name* **{deny | permit} ip** *source source-netmask destination destination-netmask*

첫 번째 ACE를 생성할 때 ACL을 생성합니다. 다음 명령 구문은 ACL을 생성하거나 추가합니다.

access-list *access-list-name* **{deny | permit} ip** *source source-netmask destination destination-netmask*

다음 예에서는 ASA가 암호화 맵에 할당된 IPsec 보호를 10.0.0.0 서브넷부터 10.1.1.0 서브넷에 이르는 모든 트래픽 흐름에 적용합니다.

access-list 101 permit ip 10.0.0.0 255.255.255.0 10.1.1.0 255.255.255.0

패킷과 일치하는 암호화 맵이 SA 협상에 사용되는 보안 설정을 결정합니다. 로컬 ASA가 협상을 시작하면 지정된 피어에게 전송할 제안을 생성하기 위해 정적 암호화 맵에서 지정된 정책을 사용합니다. 피어가 협상을 시작하면 ASA가 정책과 정적 암호화 맵을 일치시키려고 시도합니다. 실패할 경우 피어 제안의 수락 또는 거절을 결정하기 위해 암호화 맵 집합 내 모든 동적 암호화 맵을 일치시키려고 시도합니다.

SA를 성공적으로 설정한 두 피어의 경우 최소 1개 이상의 호환 가능한 암호화 맵이 있어야 합니다. 호환되려면 암호화 맵이 다음 기준을 충족해야 합니다.

- 암호화 맵이 호환 가능한 암호화 ACL(예: 미러 이미지 ACL)을 포함해야 합니다. 응답 피어가 동적 암호화 맵을 사용하는 경우에도 마찬가지로 ASA가 IPsec을 적용하기 위한 요건에 따라 호환 가능한 암호화 ACL을 포함해야 합니다.
- 응답 피어가 동적 암호화 맵을 사용하지 않는 한 각 암호화 맵은 다른 피어를 식별합니다.
- 암호화 맵에는 공통된 하나 이상의 변형 집합 또는 제안서가 있습니다.

단일 인터페이스에 하나의 암호화 맵 집합만 적용할 수 있습니다. 다음과 같은 조건이 있는 경우 ASA의 특정 인터페이스에 대해 두 개 이상의 암호화 맵을 생성하십시오.

- 특정 피어가 다른 데이터 흐름을 처리하도록 하려는 경우
- 다른 IPsec 보안을 다른 유형의 트래픽에 적용하려는 경우

예를 들어 암호화 맵을 생성하고 두 개의 서브넷 간 트래픽을 식별하기 위해 ACL을 할당하고 한 개의 IKEv1 변형 집합 또는 IKEv2 제안서를 할당하십시오. 다른 두 개의 서브넷 간 트래픽을 식별하기 위해 다른 ACL을 사용하여 또 다른 암호화 맵을 생성하고 다른 VPN 매개변수를 사용하여 변형 집합 또는 제안서를 적용하십시오.

인터페이스에 두 개 이상의 암호화 맵을 생성하는 경우 각 맵 항목의 시퀀스 번호(seq-num)를 지정하고 암호화 맵 집합 내에서 우선순위를 지정하십시오.

각 ACE에는 permit(허용) 또는 deny(거부) 명령문이 포함되어 있습니다. 다음 표에서는 암호화 맵에 적용된 ACL에서 permit 및 deny ACE의 특수한 의미를 설명합니다.

암호화 맵 평가 결과	응답
permit 명령문을 포함하는 ACE의 일치 기준	암호화 맵 집합에 남아 있는 ACE에 대한 패킷의 추가 평가를 중단하고 암호화 맵에 할당된 IKEv1 변형 집합 또는 IKEv2 제안서의 ACE에 대한 패킷 보안 설정을 평가합니다. 보안 설정을 변형 집합 또는 제안서의 ACE와 일치시킨 후 ASA에서 연계된 IPsec 설정을 적용합니다. 일반적으로 아웃바운드 트래픽의 경우 이는 패킷의 암호 해독, 인증 및 라우팅을 의미합니다.
deny 명령문을 포함하는 ACE의 일치 기준	평가 중인 암호화 맵에 남아 있는 ACE에 대한 패킷의 추가 평가를 중단하고 할당된 다음 시퀀스 번호에 따라 다음 암호화 맵의 ACE에 대한 평가를 다시 시작합니다.
암호화 맵 집합의 테스트된 모든 permit ACE 일치에 실패합니다.	암호화하지 않고 패킷을 라우팅합니다.

deny 명령문을 포함하는 ACE는 라우팅 프로토콜 트래픽과 같이 IPsec 보호가 필요하지 않은 아웃바운드 트래픽을 필터링합니다. 따라서 암호화 ACL의 permit 명령문에 대해 평가되지 않아야 하는 아웃바운드 트래픽을 필터링하려면 초기 deny 명령문을 삽입하십시오.

인바운드의 경우 암호화된 패킷인 보안 어플라이언스가 소스 주소 및 ESP SPI를 사용하여 암호 해독 매개변수를 결정합니다. 보안 어플라이언스가 패킷을 암호 해독한 후 해독한 패킷의 내부 헤더를 패킷 SA와 연계된 ACL의 permit ACE와 비교합니다. 내부 헤더가 프록시와 일치하지 않으면 보안 어플라이언스가 패킷을 삭제합니다. 내부 헤더가 프록시와 일치하는 경우 보안 어플라이언스가 패킷을 라우팅합니다.

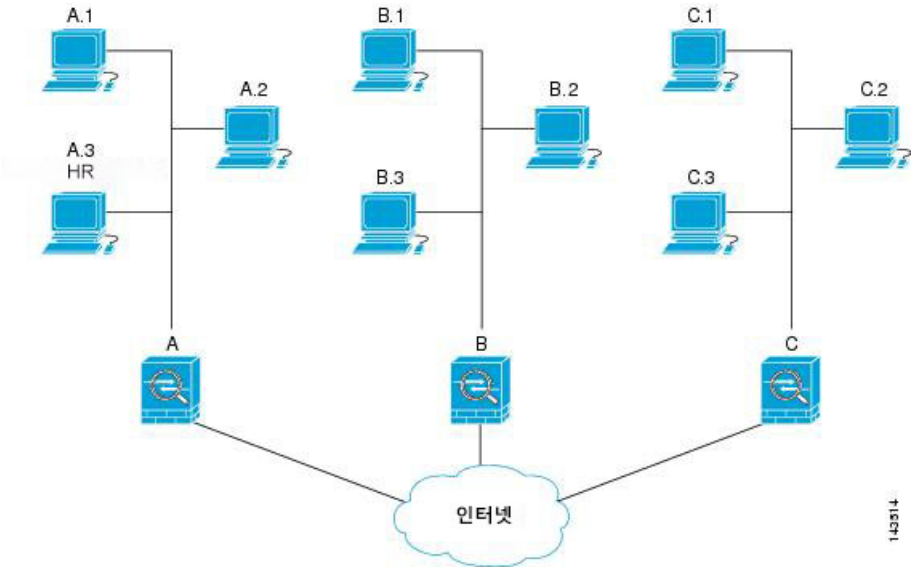
암호화되지 않은 인바운드 패킷의 내부 헤더를 비교할 때 거부 규칙이 2단계 SA의 설정을 막을 수 있으므로 보안 어플라이언스에서 모든 거부 규칙을 무시합니다.

참고 일반 텍스트와 같이 인바운드의 암호화되지 않은 트래픽을 라우팅하려면 permit ACE 전에 deny ACE를 삽입하십시오.

LAN-to-LAN 암호화 맵의 예

이 LAN-to-LAN 네트워크 예시에서 보안 어플라이언스 A, B 및 C를 구성하는 목적은 다른 호스트로 향하는 호스트 중 하나에서 발생한 모든 트래픽의 터널링을 허용하는 것입니다. 그러나 호스트 A.3의 트래픽은 인사 부서의 민감한 데이터를 포함하고 있으므로 다른 트래픽보다 강력한 암호화가 필

요하며 더 자주 키를 재설정해야 합니다. 따라서 호스트 A.3의 트래픽에 특별한 변형 집합을 할당하려고 할 수 있습니다.



이 그림 및 다음 설명에 사용된 간단한 주소 표기법은 추상적인 개념입니다. 실제 IP 주소를 사용하는 예는 설명을 따릅니다.

아웃바운드 트래픽을 위해 보안 어플라이언스 A를 구성하려면 다음 예와 같이 2개의 암호화 맵 즉, 호스트 A.3의 트래픽을 위한 1개의 암호화 맵 및 네트워크 A에 있는 다른 호스트의 트래픽을 위한 1개의 암호화 맵을 생성합니다.

```
Crypto Map Seq_No_1
    deny packets from A.3 to B
    deny packets from A.3 to C
    permit packets from A to B
    permit packets from A to C
Crypto Map Seq_No_2
    permit packets from A.3 to B
    permit packets from A.3 to C
```

ACL을 생성한 후 변형 집합을 각 암호화 맵에 할당하여 필요한 IPsec을 일치하는 각 패킷에 적용합니다.

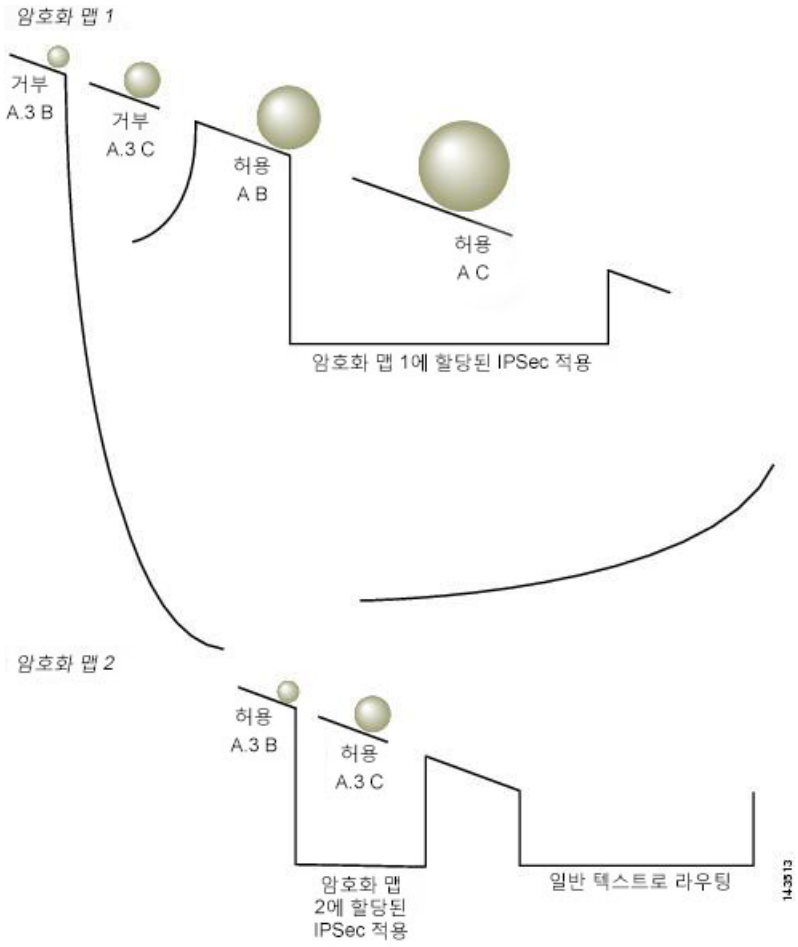
연속 ACL에는 ACL에 대한 평가를 우회하고 암호화 맵 집합에서 후속 ACL에 대한 평가를 다시 시작하기 위한 deny ACE의 삽입이 포함됩니다. 각 암호화 맵과 다른 IPsec 설정을 연계할 수 있으므로 deny ACE를 사용하여 해당 암호화 맵의 추가 평가에서 특정 트래픽을 제외하고 특정 트래픽을 다른 암호화 맵의 permit 명령문과 일치시켜 다른 보안을 제공하거나 요구할 수 있습니다. 암호화 ACL에 할당된 시퀀스 번호가 암호화 맵 집합 내 평가 시퀀스의 위치를 결정합니다.

다음 그림은 이 예에서 개념적 ACE로부터 생성된 연속 ACL을 보여줍니다. 각 기호의 의미는 다음과 같습니다.

	암호화 맵 집합 내 암호화 맵을 의미합니다.

	(직선에 간격이 있음) 패킷이 ACE와 일치할 때 암호화 맵을 종료합니다.
	한 ACE의 설명에 적합한 패킷을 의미합니다. 서로 다른 크기의 공은 그림에서 각 ACE와 일치하는 다른 패킷을 나타냅니다. 크기의 차이는 단지 각 패킷의 소스와 대상의 차이를 나타냅니다.
	암호화 맵 집합에서 다음 암호화 맵으로 리디렉션하는 것을 의미합니다.
	패킷이 ACE와 일치하거나 암호화 맵 집합의 모든 permit ACE와 일치하지 않는 경우의 응답을 의미합니다.

그림 ***1:*** 암호화 맵 집합의 연속 ***ACL***



보안 어플라언스 A가 permit ACE와 일치할 때까지 호스트 A.3에서 발생한 패킷을 평가하고 해당 암호화 맵에 연계된 IPsec 보안을 할당하려고 시도합니다. 패킷이 deny ACE와 일치할 때마다 ASA가 암

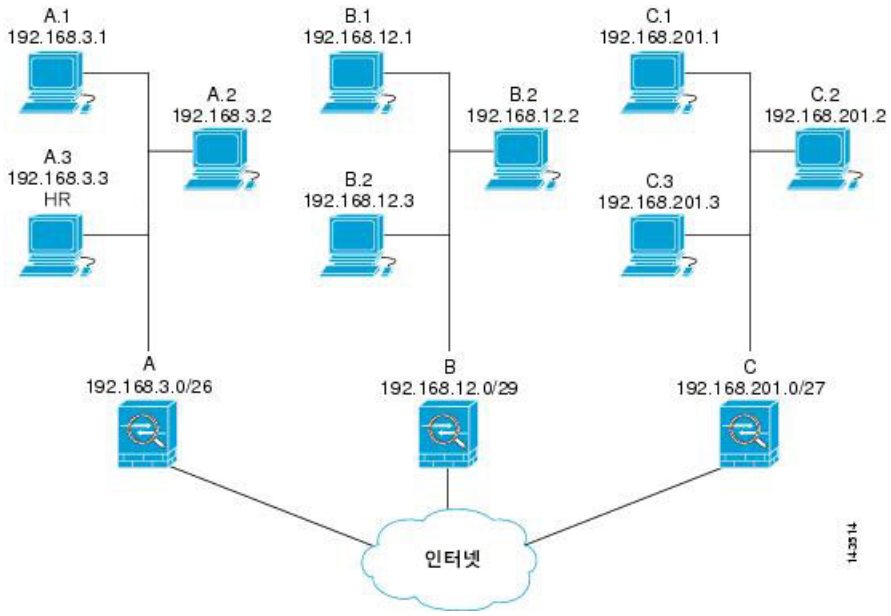
호화 맵에 남아 있는 ACE를 무시하고 할당된 시퀀스 번호에 따라 다음 암호화 맵에 대한 평가를 다시 시작합니다. 이 예와 같이 보안 어플라이언스 A가 호스트 A.3에서 패킷을 수신하는 경우 패킷을 첫 번째 암호화 맵의 deny ACE와 일치시키고 다음 암호화 맵에 대한 패킷의 평가를 다시 시작합니다. 패킷과 암호화 맵의 permit ACE를 일치시키는 경우 연계된 IPsec 보안(강력한 암호 및 빈번한 키 재설정)을 적용합니다.

예시 네트워크에서는 ASA 구성을 완료하기 위해 미러 암호화 맵을 ASA의 B와 C에 할당합니다. 그러나 인바운드의 암호화된 트래픽을 평가할 때 ASA가 deny ACE를 무시하므로 deny A.3 B 및 deny A.3 C ACE의 미러 등가를 생략하고 이에 따라 암호화 맵 2의 미러 등가를 생략할 수 있습니다. 따라서 ASA B와 C의 연속 ACL 구성이 필요하지 않습니다.

다음 표에서는 ASA의 세 가지 A, B, C 모두에 대해 구성되어 암호화 맵에 할당된 ACL을 보여줍니다.

보안 어플라이언스 **A**		보안 어플라이언스 **B**		보안 어플라이언스 **C**	
암호화 맵 시퀀스 번호	**ACE** 패턴	암호화 맵 시퀀스 번호	**ACE** 패턴	암호화 맵 시퀀스 번호	**ACE** 패턴
1	deny A.3 B	1	permit B A	1	permit C A
	deny A.3 C				
	permit A B				
	permit A C		permit B C		permit C B
2	permit A.3 B				
	permit A.3 C				

다음 그림은 이전에 표시된 개념적 주소를 실제 IP 주소로 매핑합니다.



다음 표에 표시된 실제 ACE는 해당 네트워크 내에서 평가 중인 모든 IPsec 패킷이 올바른 IPsec 설정을 수신하도록 보장합니다.

보안 어플라이언스	암호화 맵 시퀀스 번호	ACE 패턴	실제 ACE
A	1	deny A.3 B	deny 192.168.3.3 255.255.255.192 192.168.12.0 255.255.255.248
		deny A.3 C	deny 192.168.3.3 255.255.255.192 192.168.201.0 255.255.255.224
		permit A B	permit 192.168.3.0 255.255.255.192 192.168.12.0 255.255.255.248
		permit A C	permit 192.168.3.0 255.255.255.192 192.168.201.0 255.255.255.224
	2	permit A.3 B	permit 192.168.3.3 255.255.255.192 192.168.12.0 255.255.255.248
		permit A.3 C	permit 192.168.3.3 255.255.255.192 192.168.201.0 255.255.255.224
B	필요하지 않음	permit B A	permit 192.168.12.0 255.255.255.248 192.168.3.0 255.255.255.192
		permit B C	permit 192.168.12.0 255.255.255.248 192.168.201.0 255.255.255.224

보안 어플라이언스	암호화 맵 시퀀스 번호	ACE 패턴	실제 ACE
C	필요하지 않음	permit C A	permit 192.168.201.0 255.255.255.224 192.168.3.0 255.255.255.192
		permit C B	permit 192.168.201.0 255.255.255.224 192.168.12.0 255.255.255.248

예시 네트워크에 표시된 같은 논리를 적용하면 연속 ACL을 사용하여 ASA에서 보호하는 다른 호스트 또는 서브넷에 다른 보안 설정을 할당할 수 있습니다.

참고 기본적으로 ASA는 입력하는 것과 동일한 인터페이스로 향하는 IPsec 트래픽을 지원하지 않습니다. 이러한 트래픽 유형의 이름에는 U-turn, hub-and-spoke 및 hairpinning이 포함됩니다. 그러나 네트워크 간에 트래픽을 허용하는 ACE를 삽입하여 U-turn 트래픽을 지원하도록 IPsec을 구성할 수 있습니다. 예를 들어 보안 어플라이언스 B에서 U-turn 트래픽을 지원하려면 ACL 1에 개념적 "permit B B" ACE를 추가하십시오. 실제 ACE는 다음과 같습니다.**permit 192.168.12.0 255.255.255.248 192.168.12.0 255.255.255.248**

PKI(Public Key Infrastructure) 키 집합

관리자가 키 쌍을 생성하거나 제로화할때 Suite B ECDSA 알고리즘을 선택하려면 PKI(Public Key Infrastructure: 공개 키 인프라)를 설정해야 합니다.

시작하기 전에

인증 시 RSA 또는 ECDSA 신뢰 지점을 사용하기 위해 암호화 맵을 구성하는 경우 먼저 키 집합을 생성해야 합니다. 그런 다음 터널 그룹 구성에서 신뢰 지점 및 참조를 생성할 수 있습니다.

프로시저

단계 **1** 키 쌍을 생성할 때 Suite B ECDSA 알고리즘을 선택하십시오.

crypto key generate [rsa [general-keys | label <name> | modules [512 | 768 | 1024 | 2048 | 4096] | noconfirm | usage-keys] | ecdsa [label <name> | elliptic-curve [256 | 384 | 521] | noconfirm]]

단계 **2** 키 쌍을 제로화할 때 Suite B ECDSA 알고리즘을 선택하십시오.

crypto key zeroize [rsa | ecdsa] [default | label <name> | noconfirm]

암호화 맵을 인터페이스에 적용

IPsec 트래픽 흐름을 통해 암호화 맵 집합을 각 인터페이스에 할당해야 합니다. ASA는 모든 인터페이스에서 IPsec을 지원합니다. 암호화 맵 집합을 인터페이스에 할당하면 ASA에 암호화 맵 집합에 대한 모든 트래픽을 평가하고 연결 또는 SA 협상 시 지정된 정책을 사용하도록 지시합니다.

또한 암호화 맵을 인터페이스에 할당하면 SA 데이터베이스 및 보안 정책 데이터베이스와 같은 런타임 데이터 구조를 초기화합니다. 수정된 암호화 맵을 인터페이스에 재할당하면 암호화 맵 설정으로 런타임 데이터 구조를 재동기화합니다. 또한 새 시퀀스 번호를 사용하여 새 피어를 추가하고 암호화 맵을 재할당하면 기존의 연결을 해제하지 않습니다.

인터페이스 **ACL** 사용

기본적으로 ASA를 통해 IPsec 패킷이 인터페이스 ACL을 우회할 수 있습니다. 인터페이스 ACL을 IPsec 트래픽에 적용하려면 **sysopt connection permit-vpn** 명령의 **no** 형식을 사용하십시오.

발신 인터페이스에 바인딩된 암호화 맵 ACL은 VPN 터널을 통한 IPsec 패킷을 허용 또는 거부합니다. IPsec는 IPsec 터널에서 도착하는 패킷을 인증하고 암호를 해독하며 터널에 연계된 ACL에 대한 평가를 받게 합니다.

ACL이 보호할 IP 트래픽을 정의합니다. 예를 들어 2개의 서브넷 또는 2개의 호스트 간에 모든 IP 트래픽을 보호하도록 ACL을 생성할 수 있습니다. 이 ACL은 **access-group** 명령과 함께 사용된 ACL과 유사합니다. 그러나 **access-group** 명령을 사용하면 ACL이 인터페이스에서 전달 또는 차단될 트래픽을 결정합니다.

암호화 맵에 할당하기 전에 ACL은 IPsec에 한정되지 않습니다. 각 암호화 맵은 ACL 중 하나에서 허용과 일치할 경우, ACL을 참조하고 패킷에 적용할 IPsec 속성을 결정합니다.

IPsec 암호화 맵에 할당된 ACL에는 다음과 같은 네 가지 주요 기능이 있습니다.

- IPsec을 통해 보호할 아웃바운드 트래픽을 선택합니다(허용 = 보호).
- 설정된 SA 없이 이동하는 데이터에 대한 ISAKMP 협상을 트리거합니다.
- 프로세스 인바우드 트래픽이 IPsec을 통해 보호했어야 하는 트래픽을 제외하고 무시합니다.
- 피어의 IKE 협상을 처리할 때 IPsec SA에 대한 요청 수락 여부를 결정합니다. (협상은 **ipsec-isakmp crypto map** 항목에만 적용됩니다.) 피어는 협상 시 승인을 위해 **ipsec-isakmp crypto map** 명령 항목과 연계된 데이터 흐름을 허용해야 합니다.

참고 ACL에서 유일한 요소를 삭제하는 경우 ASA 또한 연계된 암호화 맵을 제거합니다.

현재 하나 이상의 암호화 맵에서 참조하는 ACL을 수정하려면 **crypto map interface** 명령을 사용하여 런타임 SA 데이터베이스를 다시 초기화하십시오. 자세한 내용은 **crypto map** 명령을 참조하십시오.

로컬 피어에서 정의한 정적 암호화 맵에 지정된 모든 암호화 ACL에 대해 원격 피어에서 "미러 이미지" 암호화 ACL을 지정하는 것이 좋습니다. 또한 암호화 맵이 공통의 변형을 지원하고 피어로서 다른 시스템을 참조해야 합니다. 이를 통해 두 피어에서 IPsec을 올바르게 처리할 수 있습니다.

참고 모든 정적 암호화 맵이 ACL 및 IPsec 피어를 정의해야 합니다. 하나가 누락된 경우 암호화 맵이 완료되지 않으며 ASA가 이전의 완료된 암호화 맵과 일치하지 않는 트래픽을 삭제할 수 있습니다. 모든 암호화 맵이 완료되었는지 확인하려면 show conf 명령을 사용하십시오. 완료되지 않은 암호화 맵을 수정하려면 암호화 맵을 제거하고 누락된 항목을 추가하여 다시 적용하십시오.

문제가 발생할 수 있으므로 암호화 ACL에서 소스 또는 수신 주소를 지정하는 **any** 키워드를 사용하지 않는 것이 좋습니다. 또한 다음과 같은 이유로 **permit any any** 명령문을 사용하지 않는 것을 권장합니다.

- 해당 암호화 맵에서 지정된 피어에 전송되는 모든 보호 트래픽을 포함하여 모든 아웃바운드 트래픽을 보호합니다.
- 모든 인바운드 트래픽에 대한 보호가 필요합니다.

이 시나리오에서는 ASA가 IPsec 보호가 부족한 모든 인바운드 패킷을 자동으로 삭제합니다.

보호할 패킷을 정의했는지 확인하십시오. **permit** 명령문에 **any** 키워드를 사용하는 경우 키워드 앞에 일련의 **deny** 명령문을 사용하여 보호하지 않으려는 **permit** 명령문 범위에 속할 수 있는 트래픽을 제외시키십시오.

참고 **no sysopt connection permit-vpn**이 구성되는 동안 deny ip any any access-list를 호출하는 외부 인터페이스의 액세스 그룹이 있음에도 불구하고 트래픽을 통한 암호 해독이 클라이언트에서 허용됩니다.

외부 인터페이스의 ACL(Access Control List: 액세스 제어 목록)과 함께 **no sysopt permit** 명령을 사용하여 사이트 대 사이트 또는 원격 액세스 VPN을 통해 보호된 네트워크에 대한 액세스를 제어하려는 경우 사용자는 실패합니다.

이러한 상황에서 내부 액세스 관리 기능이 활성화되어 있는 경우 ACL이 적용되지 않으며 사용자가 보안 어플라이언스에 SSH를 사용하여 계속 연결할 수 있습니다. 내부 네트워크의 호스트에 대한 트래픽이 ACL에 의해 올바르게 차단되지만 내부 인터페이스에 대한 트래픽을 통해 암호 해독되는 것을 차단할 수 없습니다.

ssh 및 **http** 명령은 ACL보다 우선순위가 높습니다. 즉 VPN 세션의 디바이스에 대한 SSH, 텔넷 또는 ICMP 트래픽을 거부하려면 IP 로컬 풀 거부를 추가해야 하는 **ssh**, **telnet** 및 **icmp** 명령을 사용하십시오.

트래픽의 인바운드 또는 아웃바운드 여부에 관계없이 ASA가 인터페이스에 할당된 ACL에 대한 트래픽을 평가합니다. 인터페이스에 IPsec을 할당하려면 다음 단계를 수행하십시오.

프로시저

단계 **1** IPsec에 사용될 ACL을 생성하십시오.

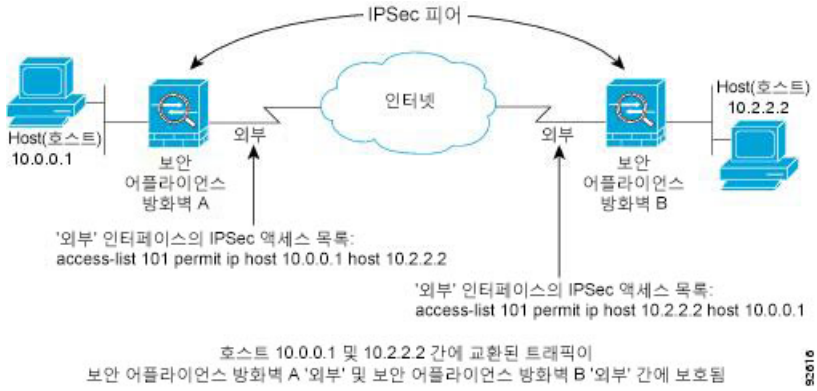
단계 **2** 같은 암호화 맵 이름을 사용하여 하나 이상의 암호화 맵에 목록을 매핑하십시오.

단계 **3** IPsec을 데이터 흐름에 적용하려면 IKEv1 변형 집합 또는 IKEv2 제안서를 암호화 맵에 매핑하십시오.

단계 **4** 인터페이스에 공유하는 암호화 맵 이름을 지정하여 암호화 맵 집합으로서 암호화 맵을 전체적으로 적용하십시오.

예

이 예에서는 데이터가 Host 10.2.2.2로 향하는 ASA A의 외부 인터페이스를 종료하므로 IPsec 보호가 Host 10.0.0.1과 Host 10.2.2.2 간의 트래픽에 적용됩니다.



ASA A는 다음과 같이 Host 10.0.0.1에서 Host 10.2.2.2로 트래픽을 평가합니다.

- 소스 = host 10.0.0.1
- 대상 = host 10.2.2.2

또한 ASA A는 다음과 같이 Host 10.2.2.2에서 Host 10.0.0.1로 트래픽을 평가합니다.

- 소스 = host 10.2.2.2
- 대상 = host 10.0.0.1

평가 중인 패킷과 일치하는 첫 번째 permit 명령문이 IPsec SA의 범위를 결정합니다.

IPsec SA 수명 변경

새 IPsec SA를 협상할 때 ASA가 사용하는 전체 수명 값을 변경할 수 있습니다. 이러한 전체 수명 값을 특정 암호화 맵을 위해 재정의할 수 있습니다.

IPsec SA는 파생 및 공유된 비밀 키를 사용합니다. 키가 SA의 핵심적인 부분으로 키의 시간 제한이 초과되면 키를 새로 고침해야 합니다. 각 SA에는 시간 제한과 트래픽 볼륨 수명의 두 가지 수명이 있습니다. SA는 각 수명과 협상이 새로운 SA에 대해 시작된 후 만료됩니다. 기본 수명은 28,800초(8시간) 및 4,608,000킬로바이트(1시간 동안 초당 10메가바이트)입니다.

전체 수명을 변경하는 경우 ASA가 터널을 삭제하고 그 후에 설정된 SA의 협상에서 새로운 값을 사용합니다.

암호화 맵에 수명 값을 구성하지 않았으며 ASA가 새로운 SA를 요청하는 경우 기존 SA에서 사용된 전체 수명 값을 피어로 전송된 요청에 삽입합니다. 피어가 협상 요청을 받으면 피어가 제안하는 수명 값 또는 로컬에서 구성한 수명 값 중 더 작은 값을 새 SA의 수명으로 사용합니다.

피어는 기존 SA가 만료될 경우 새 SA가 마련될 수 있도록 기존 SA의 수명 임계값을 초과하기 전에 새 SA를 협상합니다. 기존 SA의 수명이 약 5-15% 남아 있을 때 피어가 새 SA를 협상합니다.

VPN 라우팅 변경

기본적으로 패킷별 인접성 조회는 외부 ESP 패킷에 대해서만 수행되며 IPsec 터널을 통해 전송된 패킷에 대해서는 조회가 수행되지 않습니다.

일부 네트워크 토폴로지에서 라우팅 업데이트가 내부 패킷의 경로를 변경했지만 로컬 IPsec 터널이 계속해서 작동 중인 경우, 터널을 통과하는 패킷은 올바르게 라우팅되지 않으며 목적지에 연결하는 데 실패합니다.

이를 방지하려면 IPsec 내부 패킷에 대한 패킷별 라우팅 조회를 활성화하십시오.

시작하기 전에

이러한 조회에서 성능 저하를 방지하기 위해 이 기능은 기본적으로 비활성화됩니다. 필요한 경우에만 활성화하십시오.

프로시저

IPsec 내부 패킷에 대한 패킷별 라우팅 조회를 활성화합니다.

[**no**] [**crypto**] **ipsec inner-routing-lookup**

예

```
ciscoasa(config)# crypto ipsec inner-routing-lookup
ciscoasa(config)# show run crypto ipsec
 crypto ipsec ikev2 ipsec-proposal GCM
 protocol esp encryption aes-gcm
 protocol esp integrity null
 crypto ipsec inner-routing-lookup
```

정적 암호화 맵 생성

정적 암호화 맵을 사용하여 기본 IPsec 구성을 생성하려면 다음 단계를 수행하십시오.

프로시저

단계 **1** 보호할 트래픽을 정의하기 위해 ACL을 생성하려면 다음 명령을 입력하십시오.

access-list *access-list-name* **{deny | permit} ip** *source source-netmask destination destination-netmask*

*access-list-name*은 최대 241자의 문자열 또는 정수로 ACL ID를 지정합니다. *destination-netmask* 및 *source-netmask*는 IPv4 네트워크 주소와 서브넷 마스크를 지정합니다. 이 예에서 **permit** 키워드는 암호화를 통해 보호될 지정된 조건에 일치하는 모든 트래픽을 발생시킵니다.

예제**:**

```
hostname(config)# access-list 101 permit ip 10.0.0.0 255.255.255.0 10.1.1.0 255.255.255.0
```

단계 **2** 트래픽을 보호하는 방법을 정의하는 IKEv1 변형 집합을 구성하려면 다음 명령을 입력하십시오.

crypto ipsec ikev1 transform-set *transform-set-name encryption* [*authentication*]

*Encryption*은 IPsec 데이터 흐름을 보호하는 암호화 방식의 종류를 지정합니다.

- esp-aes — 128비트 키의 AES를 사용합니다.
- esp-aes-192 — 192비트 키의 AES를 사용합니다.
- esp-aes-256 — 256비트 키의 AES를 사용합니다.
- esp-des — 56비트 DES-CBC를 사용합니다.
- esp-3des — 삼중 DES 알고리즘을 사용합니다.
- esp-null — 암호화하지 않습니다.

*Authentication*은 IPsec 데이터 흐름을 보호하는 암호화 방식의 종류를 지정합니다.

- esp-md5-hmac — MD5/HMAC-128을 해시 알고리즘으로 사용합니다.
- esp-sha-hmac — SHA/HMAC-160을 해시 알고리즘으로 사용합니다.
- esp-none — HMAC 인증을 사용하지 않습니다.

예제**:**

이 예에서 myset1, myset2 및 aes_set는 변형 집합의 이름입니다.

```
hostname(config)# crypto ipsec ikev1 transform-set myset1 esp-des esp-sha-hmac
hostname(config)# crypto ipsec ikev1 transform-set myset2 esp-3des esp-sha-hmac
hostname(config)# crypto ipsec ikev1 transform-set aes_set esp-md5-hmac esp-aes-256
```

단계 **3** 트래픽을 보호하는 방법도 정의하는 IKEv2 제안을 구성하려면 다음 명령을 입력하십시오.

crypto ipsec ikev2 ipsec-proposal [*proposal tag*]

*proposal tag*는 1-64자의 문자열로 이루어진 IKEv2 IPsec 제안서의 이름입니다.

proposal을 생성하고, proposal을 위해 여러 암호화 및 무결성 유형을 지정할 수 있는 ipsec proposal 구성 모드로 들어갑니다.

예제:

```
hostname(config)# crypto ipsec ikev2 ipsec-proposal secure
```

이 예에서 secure는 제안서의 이름입니다. 프로토콜과 암호화 유형을 입력하십시오.

```
hostname(config-ipsec-proposal)# protocol esp encryption 3des aes des
```

예제:

이 명령은 사용할 AES-GCM 또는 AES-GMAC 알고리즘의 종류를 선택합니다.

[no] protocol esp encryption [3des | aes | aes-192 | aes-256 | aes-gcm | aes-gcm-192 | aes-gcm-256 | aes-gmac | aes-gmac-192 | aes-gmac-256 | des | null]

SHA-2 또는 null을 선택한 경우 IPsec 무결성 알고리즘으로 사용할 알고리즘을 선택해야 합니다. AES-GCM/GMAC가 암호화 알고리즘으로 구성된 경우 다음과 같이 null 무결성 알고리즘을 선택해야 합니다.

[no] protocol esp integrity [md5 | sha-1 | sha-256 | sha-384 | sha-512 | null]

참고 AES-GCM/GMAC가 암호화 알고리즘으로 구성된 경우 null 무결성 알고리즘을 선택해야 합니다. SHA-256은 IKEv2 터널을 설정하기 위해 무결성 및 PRF에 사용될 수 있으며 ESP 무결성 보호에도 사용될 수 있습니다.

단계 **4** (선택 사항) 관리자는 PMTU(Path Maximum Transfer Unit: 경로 최대 전송 단위) 에이징을 활성화하고 PMTU 값이 원래 값으로 재설정되는 간격을 설정할 수 있습니다.

[no] crypto ipsec security-association pmtu-aging *reset-interval*

단계 **5** 암호화 맵을 생성하려면 단일 또는 다중 상황 모드를 사용하여 다음 Site-to-Site 단계를 수행하십시오.

a) 암호화 맵에 ACL을 할당하십시오.

crypto map *map-name seq-num* **match address** *access-list-name*

암호화 맵 집합은 각각 다른 시퀀스 번호(*seq-num)*를 사용하지만 같은 *map name*을 사용하는 암호화 맵 항목의 모음입니다. *access-list-name*을 사용하여 최대 241자의 문자열 또는 정수로 ACL ID를 지정하십시오. 다음 예에서 mymap은 암호화 맵 집합의 이름입니다. 맵 집합 시퀀스 번호는 10이고 1개의 암호화 맵 집합 내에서 여러 항목의 순위를 지정하는 데 사용됩니다. 시퀀스 번호가 낮을수록 우선순위가 더 높습니다.

예제:

이 예에서는 101이라는 이름의 ACL이 mymap 암호화 맵으로 할당됩니다.

```
crypto map mymap 10 match address 101
```

b) IPSec 보호 트래픽이 전달될 수 있는 피어를 지정하십시오.

crypto map *map-name seq-num* **set peer** *ip-address*

예제:

```
crypto map mymap 10 set peer 192.168.1.100
```

ASA가 IP 주소 192.168.1.100으로 할당된 피어를 사용하는 SA를 구성합니다. 이 명령을 반복하여 여러 피어를 지정하십시오.

c) 이 암호화 맵에 허용되는 IKEv1 변형 집합 또는 IKEv2 제안서를 지정하십시오. 여러 변형 집합 또는 제안서를 우선순위에 따라(가장 높은 우선순위부터) 나열하십시오. 다음 두 명령 중 하나를 사용하여 암호화 맵에서 최대 11개의 변형 집합 또는 제안서를 지정할 수 있습니다.

crypto map *map-name seq-num* **set ikev1 transform-set** *transform-set-name1 [transform-set-name2, …transform-set-name11*]

OR

crypto map *map-name seq-num* **set ikev2 ipsec-proposal** *proposal-name1* [*proposal-name2, … proposal-name11*]

Proposal-name1 및 *proposal-name11*이 하나 이상의 IKEv2용 IPsec 제안서의 이름을 지정합니다. 각 암호화 맵 항목은 최대 11개의 제안서를 지원합니다.

예제:

IKEv1에 관한 이 예에서 트래픽이 ACL 101과 일치하는 경우 SA에서 피어의 변형 집합과 일치하는 변형 집합에 따라 myset1(첫 번째 우선순위) 또는 myset2(두 번째 우선순위) 중 하나를 사용할 수 있습니다.

```
crypto map mymap 10 set ikev1 transform-set myset1 myset2
```

d) (선택 사항) IKEv2의 경우 터널에 ESP 암호화 및 인증을 적용하려면 **mode**를 지정합니다. 이는 원래 IP 패킷의 어느 부분에 ESP가 적용되어 있는지 결정합니다.

crypto map *map-name seq-num* **set ikev2 mode** [**transport | tunnel | transport-require**]

- **Tunnel(**터널**)** 모드 - (기본값) 캡슐화 모드가 터널 모드가 됩니다. Tunnel(터널) 모드는 전체 원래 IP 패킷(IP 헤드 및 데이터)에 ESP 암호화 및 인증을 적용하여 최종 소스 및 대상 주소를 숨깁니다. 원래 IP 데이터그램 전체가 암호화되어 있으며 새 IP 패킷에서 페이로드가 됩니다.

  이 모드에서는 라우터와 같은 네트워크 디바이스가 IPsec 프록시 역할을 합니다. 즉, 라우터는 호스트를 대신하여 암호화를 수행합니다. 소스 라우터는 패킷을 암호화하고 IPsec 터널을 따라 패킷을 전달합니다. 대상 라우터는 원래 IP 데이터그램을 암호 해독하고 대상 시스템으로 전달합니다.

  터널 모드의 주요 장점은 IPsec이 보장하는 이점을 위해 최종 시스템을 수정할 필요가 없다는 점입니다. 터널 모드는 또한 트래픽 분석으로부터 보호 기능을 제공하므로 터널 모드를 통해 공격자는 터널 엔드포인트만 판단할 수 있으며 터널링된 패킷이 터널 엔드포인트와 동일하더라도 해당 소스 및 대상은 판단할 수 없습니다.

- **Transport(**전송**)** 모드 - 피어가 지원하지 않는 경우 캡슐화 모드는 터널 모드에 대한 폴백 옵션을 사용하는 전송 모드가 됩니다. Transport(전송) 모드에서는 IP 페이로드만 암호화되며 원래 IP 헤더는 그대로 유지됩니다.

이 모드는 적은 바이트만 각각의 패킷에 추가하고 공용 네트워크에서 디바이스가 패킷의 최종 소스 및 대상을 확인할 수 있다는 이점이 있습니다. 전송 모드를 사용하면 IP 헤더의 정보에 기반하여 중간 네트워크에서 특수 처리(예: QoS)를 활성화할 수 있습니다. 그러나 패킷 검사를 제한하는 Layer 4 헤더가 암호화됩니다.

- 전송 필요 - 캡슐화 모드가 전송 모드만 되며, 터널 모드의 폴백이 허용되지 않습니다.

여기서는 **tunnel** 캡슐화 모드가 기본값입니다. **transport** 캡슐화 모드는 피어가 지원하지 않는 경우 터널 모드로 폴백하는 옵션을 사용하는 전송 모드가 되고, **transport-require** 캡슐화 모드는 전송 모드만 적용합니다.

참고 원격 액세스 VPN에는 전송 모드가 권장되지 않습니다.

캡슐화 모드의 협상의 예는 다음과 같습니다.

- 이니시에이터가 전송 모드를 제안하고 응답자가 터널 모드를 사용하여 응답하는 경우 이니시에이터가 터널 모드로 폴백됩니다.
- 이니시에이터가 터널 모드를 제안하고 응답자가 전송 모드를 사용하여 응답하는 경우 응답자가 터널 모드로 폴백됩니다.
- 이니시에이터가 터널 모드를 제안하고 응답자가 전송-필수 모드에 있는 경우 선택한 제안이 응답자에 의해 전송되지 않습니다.
- 마찬가지로 이니시에이터가 전송-필수 모드에 있고 응답자가 터널 모드에 있는 경우 선택한 제안이 응답자에 의해 전송되지 않습니다.

e) (선택 사항) 전체 수명을 재정의하려는 경우 암호화 맵의 SA 수명을 지정하십시오.

crypto map *map-name seq-num* **set security-association lifetime** { **seconds** *number* | **kilobytes** {*number* | **unlimited**}}

*Map-name*은 암호화 맵 집합의 이름을 지정합니다. *Seq-num*은 암호화 맵 항목에 할당하는 번호를 지정합니다. 전송되는 데이터 또는 시간에 따라 두 수명 주기를 모두 설정할 수 있습니다. 그러나, 전송되는 데이터 수명 주기는 사이트 대 사이트 VPN에만 적용되며 원격 액세스 VPN에는 적용되지 않습니다.

예제**:**

이 예에서는 암호화 맵 mymap 10의 시간 제한 수명을 2,700초(45분)로 단축합니다. 트래픽 볼륨 수명은 변경되지 않습니다.

```
crypto map mymap 10 set security-association lifetime seconds 2700
```

f) (선택 사항) 이 암호화 맵을 위한 새 SA를 요청하거나 피어로부터 수신한 요청에서 완전 순방향 비밀성(PFS)이 필요한 경우 IPsec이 PFS를 요청하도록 지정하십시오.

crypto map *map_name seq-num* **set pfs** [**group1** | **group2** | **group5**]

예제**:**

이 예에서는 암호화 맵 mymap 10에 대해 새 SA를 협상할 때 PFS가 필요합니다. ASA는 새 SA에서 1024비트 Diffie-Hellman 프라임 모듈러스 그룹을 사용합니다.

```
crypto map mymap 10 set pfs group2
```

g) (선택 사항) 이 암호화 맵 항목에 기반하여 모든 연결에 대해 역방향 라우팅 삽입(RRI)을 활성화합니다.

crypto map *map_name seq-num* **set reverse-route** [**dynamic**]

Dynamic(동적)이 지정되지 않은 경우 RRI는 구성할 때 수행되며 정적이라고 간주되어 구성이 변경될 때까지 그대로 남아 있거나 제거됩니다. ASA에서는 라우팅 테이블에 고정 경로를 자동으로 추가하고, OSPF를 사용하여 사설 네트워크 또는 경계선 라우터에 이 경로를 알립니다.

Dynamic(동적)이 지정된 경우, 라우팅은 IPsec 보안 연계(SA)를 성공적으로 설정할 경우 생성되며 IPsec SA가 삭제된 후에 삭제됩니다.

참고 동적 RRI는 IKEv2 기반 정적 암호화 맵에만 적용됩니다.

예제:

```
crypto map mymap 10 set reverse-route dynamic
```

단계 **6** IPsec 트래픽을 평가하기 위해 암호화 맵 집합을 인터페이스에 적용하십시오.

crypto map *map-name* **interface** *interface-name*

*Map-name*은 암호화 맵 집합의 이름을 지정합니다. *Interface-name*은 ISAKMP IKEv1 협상을 활성화 또는 비활성화하는 인터페이스의 이름을 지정합니다.

예제:

이 예에서는 ASA가 암호화 맵 mymap에 대해 외부 인터페이스를 통과하는 트래픽을 평가하여 보호 여부를 결정합니다.

```
crypto map mymap interface outside
```

동적 암호화 맵 생성

동적 암호화 맵은 모든 매개변수가 구성되지 않은 암호화 맵입니다. 정책 템플릿과 같은 기능을 하는데, 추후 IPsec 협상의 결과에 따라 누락된 매개변수를 동적으로 습득하면서 피어 요구사항과 매칭합니다. ASA는 IP 주소를 정적 암호화 맵에서 아직 식별할 수 없는 경우 동적 암호화 맵을 사용하여 피어가 터널을 협상하게 합니다. 이는 다음 피어 유형을 사용하는 경우 발생합니다.

- 동적으로 할당되는 공용 IP 주소를 사용하는 피어.

  LAN-LAN 및 원격 액세스 피어 모두 DHCP를 사용하여 공용 IP 주소를 얻을 수 있습니다. ASA는 터널을 초기화하는 데만 이 주소를 사용합니다.

- 동적으로 할당되는 사설 IP 주소를 사용하는 피어.

원격 액세스 터널을 요청하는 피어는 대개 헤드엔드를 통해 사설 IP 주소가 할당되어 있습니다. 일반적으로 LAN-LAN 터널은 미리 결정된 사설 네트워크 세트가 있으며, 이는 고정 맵을 구성하고 궁극적으로는 IPsec SA를 설정하는 데 사용됩니다.

고정 암호화 맵을 구성하는 관리자는 (DHCP 또는 기타 방법을 통해) 동적으로 할당되는 IP 주소를 모를 수 있습니다. 또한 할당 방식에 관계없이 다른 클라이언트의 사설 IP 주소도 모를 것입니다. VPN 클라이언트는 고정 IP 주소를 거의 사용하지 않습니다. IPsec 협상이 이루어지려면 동적 암호화 맵이 필요합니다. 예를 들어, 헤드엔드에서 IKE 협상 중에 Cisco VPN 클라이언트에 IP 주소를 할당합니다. 클라이언트는 IPec SA를 협상하는 데 이를 사용합니다.

참고 동적 암호화 맵은 **transform-set** 매개변수만 필요합니다.

동적 암호화 맵은 편리하게 IPsec을 구성하도록 할 수 있으므로 피어가 항상 사전 결정되지 않는 네트워크에서 사용하는 것이 좋습니다. 모바일 사용자와 같은 Cisco VPN 클라이언트 및 동적으로 할당된 IP 주소를 가져오는 라우터에 동적 암호화 맵을 사용하십시오.

팁 동적 암호화 맵에서 **permit** 항목에 **any** 키워드를 사용하는 경우 주의하십시오. **permit** 항목 등으로 처리된 트래픽에 멀티캐스트 또는 브로드캐스트 트래픽이 포함될 수 있는 경우 적절한 주소 범위에 대한 **deny** 항목을 ACL에 삽입하십시오. 네트워크 및 서브넷 브로드캐스트 트래픽 및 IPsec이 보호해서는 안 되는 기타 트래픽에 대해 **deny** 항목을 삽입해야 합니다.

동적 암호화 맵은 연결을 시작하는 원격 피어를 통해 SA와 협상하는 경우에만 작동합니다. ASA는 원격 피어에 대한 연결 시작에 동적 암호화 맵을 사용할 수 없습니다. 동적 암호화 맵을 사용하면 아웃바운드 트래픽이 ACL의 permit 항목과 일치하고 해당 SA가 아직 존재하지 않는 경우, ASA가 트래픽을 삭제합니다.

암호화 맵 집합이 동적 암호화 맵을 포함할 수도 있습니다. 동적 암호화 맵 세트는 암호화 맵 세트에서 우선 순위가 가장 낮은 암호화 맵이어야 합니다. 그러면 ASA에서 다른 암호화 맵을 먼저 평가합니다. 다른 (정적) 맵 항목이 서로 일치하지 않을 때만 동적 암호화 맵을 검사합니다.

정적 암호화 맵 집합과 유사하게 동적 암호화 맵 집합은 같은 dynamic-map-name을 사용하는 모든 동적 암호화 맵으로 구성됩니다. dynamic-seq-num은 집합에서 동적 암호화 맵을 구별합니다. 동적 암호화 맵을 구성하는 경우 암호화 ACL에 대한 IPsec 피어의 데이터 흐름을 식별할 수 있도록 permit ACL을 삽입하십시오. 그렇지 않으면 ASA가 피어가 제안하는 모든 데이터 흐름 ID를 허용할 수 있습니다.

주의 동적 암호화 맵 집합으로 구성된 ASA 인터페이스로 터널링되는 트래픽에 대해 모듈 기본 경로를 할당하지 마십시오. 터널링해야 하는 트래픽을 식별하려면 동적 암호화 맵에 ACL을 추가하십시오. 원격 액세스 터널과 연계된 ACL을 구성하는 경우 적절한 주소 풀을 식별하도록 주의하십시오. 터널을 설정한 후에만 경로를 설치하도록 역방향 경로 삽입을 사용하십시오.

단일 또는 다중 상황 모드를 사용하여 암호화 동적 맵 항목을 생성하십시오. 하나의 암호화 맵 세트에서 고정 맵 엔트리와 동적 맵 엔트리를 조합할 수 있습니다.

프로시저

단계 **1** (선택 사항) 동적 암호화 맵에 ACL을 할당하십시오.

crypto dynamic-map *dynamic-map-name dynamic-seq-num* **match address** *access-list-name*

이를 통해 보호해야 할 트래픽과 보호하지 않아야 하는 트래픽을 결정합니다. *Dynamic-map-name*은 기존 동적 암호화 맵을 참조하는 암호화 맵 항목의 이름을 지정합니다. *Dynamic-seq-num*은 동적 암호화 맵 항목에 해당하는 시퀀스 번호를 지정합니다.

예제**:**

이 예에서는 ACL 101이 동적 암호화 맵 dyn1에 할당됩니다. 맵 시퀀스 번호는 10입니다.

```
crypto dynamic-map dyn1 10 match address 101
```

단계 **2** 이 동적 암호화 맵에 허용되는 IKEv1 변형 집합 또는 IKEv2 제안서를 지정하십시오. IKEv1 변형 집합 또는 IKEv2 제안서에 대한 명령을 사용하여 여러 변형 집합 또는 제안서를 우선순위에 따라(가장 높은 우선순위부터) 나열하십시오.

crypto dynamic-map *dynamic-map-name dynamic-seq-num* **set ikev1 transform-set** *transform-set-name1*, [*transform-set-name2*, …*transform-set-name9*]

crypto dynamic-map *dynamic-map-name dynamic-seq-num* **set ikev2 ipsec-proposal** *proposal-name1* [*proposal-name2, … proposal-name11*]

*Dynamic-map-name*은 기존 동적 암호화 맵을 참조하는 암호화 맵 항목의 이름을 지정합니다. *Dynamic-seq-num*은 동적 암호화 맵 항목에 해당하는 시퀀스 번호를 지정합니다. *transform-set-name*은 생성 또는 수정된 변형 집합의 이름입니다. *proposal-name*은 하나 이상의 IKEv2용 IPsec 제안서의 이름을 지정합니다.

예제**:**

IKEv1에 관한 이 예에서 트래픽이 ACL 101과 일치하는 경우 SA에서 피어의 변형 집합과 일치하는 변형 집합에 따라 myset1(첫 번째 우선순위) 또는 myset2(두 번째 우선순위) 중 하나를 사용할 수 있습니다.

```
crypto dynamic-map dyn 10 set ikev1 transform-set myset1 myset2
```

단계 **3** (선택 사항) 전체 수명 값을 재정의하려는 경우 암호화 동적 맵 항목의 SA 수명을 지정하십시오.

crypto dynamic-map *dynamic-map-name dynamic-seq-num* **set security-association lifetime** { **seconds** *number* | **kilobytes** {*number* | **unlimited**}}

*Dynamic-map-name*은 기존 동적 암호화 맵을 참조하는 암호화 맵 항목의 이름을 지정합니다. *Dynamic-seq-num*은 동적 암호화 맵 항목에 해당하는 시퀀스 번호를 지정합니다. 전송되는 데이터 또는 시간에 따라 두 수명 주기를 모두 설정할 수 있습니다. 그러나, 전송되는 데이터 수명 주기는 사이트 대 사이트 VPN에만 적용되며 원격 액세스 VPN에는 적용되지 않습니다.

예제**:**

이 예에서는 동적 암호화 맵 dyn1 10의 시간 제한 수명을 2,700초(45분)로 단축합니다. 트래픽 볼륨 수명은 여기서 변경되지 않습니다.

```
crypto dynamic-map dyn1 10 set security-association lifetime seconds 2700
```

단계 **4** (선택 사항) 이 동적 암호화 맵을 위한 새 SA를 요청하거나 피어로부터 수신한 요청에서 PFS가 필요한 경우 IPsec이 PFS를 요청하도록 지정하십시오.

crypto dynamic-map *dynamic-map-name dynamic-seq-num* **set pfs** [**group1** | **group2** | **group5** | **group7**]

*Dynamic-map-name*은 기존 동적 암호화 맵을 참조하는 암호화 맵 항목의 이름을 지정합니다. *Dynamic-seq-num*은 동적 암호화 맵 항목에 해당하는 시퀀스 번호를 지정합니다.

예제:

```
crypto dynamic-map dyn1 10 set pfs group5
```

단계 **5** 정적 암호화 맵 집합에 동적 암호화 맵 집합을 추가하십시오.

동적 맵을 참조하는 암호화 맵을 암호화 맵 집합에서 가장 우선순위가 낮은 항목(가장 높은 시퀀스 번호)이 되도록 설정하십시오.

crypto map *map-name seq-num* **ipsec-isakmp dynamic** *dynamic-map-name*

*Map-name*은 암호화 맵 집합의 이름을 지정합니다. *Dynamic-map-name*은 기존 동적 암호화 맵을 참조하는 암호화 맵 항목의 이름을 지정합니다.

예제:

```
crypto map  mymap 200 ipsec-isakmp dynamic dyn1
```

Site-to-Site 이중화 제공

암호화 맵을 사용하여 이중화를 제공하도록 여러 IKEv1 피어를 정의할 수 있습니다. 이 구성은 Site-to-Site VPN에 유용합니다. 이 기능은 IKEv2에서 지원되지 않습니다.

하나의 피어가 실패하는 경우 ASA가 암호화 맵과 연계된 다음 피어에 터널을 설정합니다. 성공적으로 협상한 피어에 데이터를 전송하고 해당 피어가 활성 피어가 됩니다. 활성 피어는 협상이 실패할 때까지 ASA가 후속 협상에 대해 계속해서 가장 먼저 시도하는 피어입니다. 협상에 실패하는 경우에는 ASA가 다음 피어로 넘어갑니다. ASA는 암호화 맵과 연계된 모든 피어가 실패한 경우 첫 번째 피어로 다시 순환합니다.

IPsec VPN 관리

IPsec 구성 보기

이러한 표에는 IPsec 구성 정보에 대한 정보를 보기 위해 단일 또는 다중 상황 모드에서 입력할 수 있는 명령이 나열되어 있습니다.

표 *1: IPsec* 구성 정보를 보기 위한 명령

show running-configuration crypto	IPsec, 암호 맵, 동적 암호 맵, ISAKMP 등 전체 암호(crypto) 구성을 표시합니다.
show running-config crypto ipsec	전체 IPsec 구성을 표시합니다.
show running-config crypto isakmp	전체 ISAKMP 구성을 표시합니다.
show running-config crypto map	전체 암호화 맵 구성을 표시합니다.
show running-config crypto dynamic-map	동적 암호화 맵 구성을 표시합니다.
show all crypto map	기본값을 사용하는 구성 매개변수를 포함하여 모든 구성 매개변수를 표시합니다.
show crypto ikev2 sa detail	암호화 통계에서의 Suite B 알고리즘 지원을 표시합니다.
show crypto ipsec sa	단일 또는 다중 상황 모드의 Suite B 알고리즘 지원 및 ESPv3 IPsec 출력을 표시합니다.
show ipsec stats	단일 또는 다중 상황 모드의 IPsec 하위 시스템에 대한 정보를 표시합니다. ESPv3 통계가 TFC 패킷과 유효 및 무효 수신 ICMP 오류에 표시됩니다.

재부팅 전에 활성 세션이 종료하도록 대기

모든 액티브 세션이 자발적으로 종료한 경우에만 ASA를 재부팅하도록 예약할 수 있습니다. 이 기능은 기본적으로 비활성화되어 있습니다.

ASA를 재부팅하려면 **reload** 명령을 사용하십시오. **reload-wait** 명령을 설정한 경우 **reload quick** 명령을 사용하여 **reload-wait** 설정을 재정의할 수 있습니다. **reload** 및 **reload-wait** 명령은 특권 EXEC 모드에서 사용할 수 있으며 두 명령 모두 **isakmp** 접두사를 포함하지 않습니다.

프로시저

ASA를 재부팅하기 전에 모든 활성 세션이 자발적으로 종료할 때까지 대기하도록 하려면 단일 또는 다중 상황 모드에서 다음 사이트 대 사이트 작업을 수행하십시오.

crypto isakmp reload-wait

예제:

```
hostname(config)# crypto isakmp reload-wait
```

연결 해제 전 피어에 알림

원격 액세스 또는 LAN-to-LAN 세션이 ASA 종료 또는 재부팅, 세션 유휴 시간 제한, 최대 연결 시간 초과 또는 관리자 중단 등의 몇 가지 이유로 중지될 수 있습니다.

ASA에서는 연결이 해제될 예정인 세션의 적격 피어(LAN-to-LAN 구성 또는 VPN 클라이언트에서)를 알려줍니다. 알림을 받은 피어나 클라이언트는 원인을 디코딩하여 이벤트 로그 또는 팝업 창에 표시합니다. 이 기능은 기본적으로 비활성화되어 있습니다.

적격 클라이언트 및 피어에는 다음이 포함되어 있습니다.

- 알림이 활성화된 보안 어플라이언스
- 소프트웨어 4.0 이상 버전(구성 필요 없음)을 실행 중인 Cisco VPN 클라이언트

IPsec 피어에 대한 연결 해제 알림을 활성화하려면 단일 또는 다중 상황 모드에서 **crypto isakmp disconnect-notify** 명령을 입력하십시오.

보안 연계 지우기

특정 구성 변경 사항은 차후 SA의 협상 시에만 적용됩니다. 새 설정을 즉시 적용하려는 경우 기존 SA를 지우고 변경된 구성을 사용하여 다시 설정하십시오. ASA가 IPsec 트래픽을 적극적으로 처리하는 경우 구성 변경이 적용되는 SA 데이터베이스 부분만 지우십시오. 대규모 변경 사항을 위해 전체 SA 데이터베이스를 지우거나 ASA가 소량의 IPsec 트래픽을 처리하고 있는 경우에는 보류하십시오.

다음 표에서는 단일 또는 다중 상황 모드에서 IPsec SA를 지우고 다시 초기화하기 위해 입력할 수 있는 명령이 나열되어 있습니다.

표 ***2: IPsec SA***를 지우고 다시 초기화하는 명령

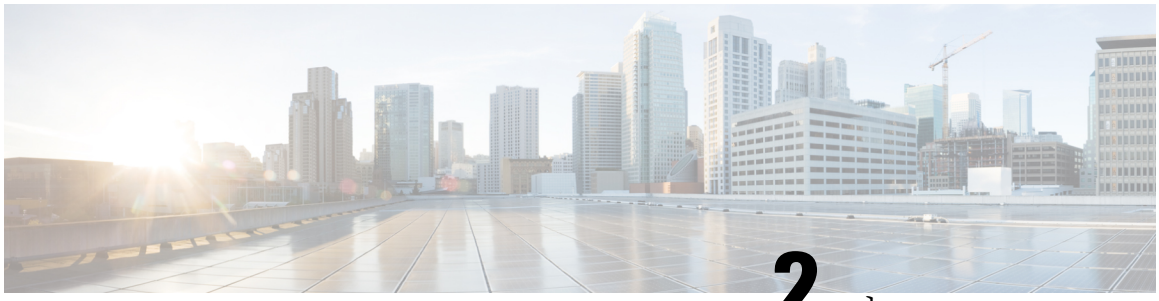
clear configure crypto	IPsec, 암호화 맵, 동적 암호화 맵 및 ISAKMP를 포함한 전체 암호화 구성을 제거합니다.
clear configure crypto ca trustpoint	모든 신뢰 지점을 제거합니다.
clear configure crypto dynamic-map	모든 동적 암호화 맵을 제거합니다. 특정 동적 암호화 맵을 제거할 수 있는 키워드가 포함되어 있습니다.
clear configure crypto map	모든 암호화 맵을 제거합니다. 특정 암호화 맵을 제거할 수 있는 키워드가 포함되어 있습니다.
clear configure crypto isakmp	전체 ISAKMP 구성을 제거합니다.
clear configure crypto isakmp policy	모든 ISAKMP 정책 또는 특정 정책을 제거합니다.
clear crypto isakmp sa	전체 ISAKMP SA 데이터베이스를 제거합니다.

암호화 맵 구성 지우기

clear configure crypto 명령에는 IPsec, 암호화 맵, 동적 암호화 맵, CA 트러스트 포인트, 모든 인증서, 인증서 맵 구성 및 ISAKMP를 포함하여 암호화 구성의 요소를 제거할 수 있는 인수가 포함되어 있습니다.

인수 없이 **clear configure crypto** 명령을 입력하는 경우 모든 인증서를 포함하여 전체 암호화 구성을 제거합니다.

자세한 내용은 *Cisco ASA Series* 명령 참조에서 **clear configure crypto** 명령을 참조하십시오.



2 장

L2TP over IPsec

이 장에서는 ASA에서 L2TP over IPsec/IKEv1을 구성하는 방법에 대해 설명합니다.

L2TP over IPsec/IKEv1 VPN 정보

L2TP(Layer 2 Tunneling Protocol: 계층 2 터널링 프로토콜)는 원격 클라이언트가 공용 IP 네트워크를 사용하여 사설 기업 네트워크 서버와 안전하게 통신하도록 해주는 VPN 터널링 프로토콜입니다. L2TP는 데이터를 터널링하기 위해 UDP(포트 1701)를 통한 PPP를 사용합니다.

L2TP 프로토콜은 클라이언트/서버 모델을 기반으로 합니다. 기능은 LNS(L2TP Network Server) 및 LAC(L2TP Access Concentrator)로 구분됩니다. LNS는 일반적으로 라우터와 같은 네트워크 게이트웨이에서 실행되지만 LAC는 Microsoft Windows, Apple iPhone 또는 Android와 같이 번들로 제공되는 L2TP 클라이언트가 있는 엔드포인트 디바이스 또는 다이얼업 NAS(Network Access Server: 네트워크 액세스 서버)가 될 수 있습니다.

원격 액세스 시나리오에서 IPsec/IKEv1을 통해 L2TP를 구성하는 주요 이점은 원격 사용자가 게이트웨이 또는 전용선 없이 공용 IP 네트워크를 통해 VPN에 액세스할 수 있어 POTS를 통해 가상의 위치에서 원격 액세스가 활성화된다는 점입니다. 또 다른 이점은 Cisco VPN 클라이언트 소프트웨어와 같은 클라이언트 소프트웨어가 추가로 필요하지 않다는 점입니다.

참고 L2TP over IPsec은 IKEv1만 지원합니다. IKEv2는 지원되지 않습니다.

IPsec/IKEv1을 통한 L2TP 구성은 사전 공유 키 또는 RSA 서명 방법을 사용하는 인증서 및 동적(정적의 반대) 암호화 맵의 사용을 지원합니다. 작업에 대한 이 요약에서는 IKEv1 완료를 비롯해 사전 공유 키 또는 RSA 서명 구성을 가정합니다. 사전 공유 키, RSA 및 동적 암호화 맵 구성을 위한 단계에 대해서는 일반 작업 구성 가이드에서 41장 “디지털 인증서”를 참조하십시오.

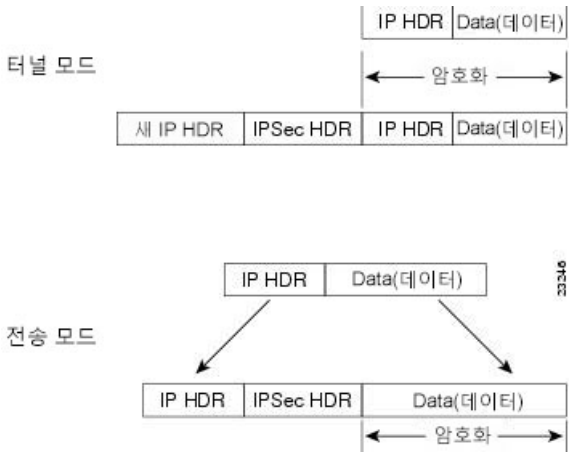
참고 ASA에서 IPsec을 통한 L2TP는 LNS가 Windows, MAC OS X, Android 및 Cisco IOS와 같은 운영 체제에서 통합된 네이티브 VPN 클라이언트와 상호 작용하도록 해줍니다. IPsec을 사용하는 L2TP만 지원되며 네이티브 L2TP 자체는 ASA에서 지원되지 않습니다. Windows 클라이언트에서 지원되는 최소 IPsec 보안 연계 수명은 300초입니다. ASA의 수명이 300초 미만으로 설정된 경우 Windows 클라이언트는 이를 무시하고 300초로 수명을 교체합니다.

IPsec 전송 및 터널 모드

기본적으로 ASA는 IPsec 터널 모드를 지원하며 원래 IP 데이터그램 전체가 암호화되어 있으며 새 IP 패킷에서 페이로드가 됩니다. 이 모드에서는 라우터와 같은 네트워크 디바이스가 IPsec 프록시 역할을 합니다. 즉, 라우터는 호스트를 대신하여 암호화를 수행합니다. 소스 라우터는 패킷을 암호화하고 IPsec 터널을 따라 패킷을 전달합니다. 대상 라우터는 원래 IP 데이터그램을 암호 해독하고 대상 시스템으로 전달합니다. 터널 모드의 주요 장점은 IPsec이 보장하는 이점을 위해 최종 시스템을 수정할 필요가 없다는 점입니다. 터널 모드는 또한 트래픽 분석으로부터 보호 기능을 제공하므로 터널 모드를 통해 공격자는 터널 엔드포인트만 판단할 수 있으며 터널링된 패킷이 터널 엔드포인트와 동일하더라도 해당 소스 및 대상은 판단할 수 없습니다.

그러나 Windows L2TP/IPsec 클라이언트는 IPsec 전송 모드를 사용합니다. 즉, IP 페이로드만 암호화되며 원래 IP 헤더는 그대로 유지됩니다. 이 모드는 적은 바이트만 각각의 패킷에 추가하고 공용 네트워크에서 디바이스가 패킷의 최종 소스 및 대상을 확인할 수 있다는 이점이 있습니다. 다음 그림은 IPsec의 터널 모드와 전송 모드 간의 차이점을 보여줍니다.

그림 *2:* 터널 모드와 전송 모드의 ***IPsec***



Windows L2TP 및 IPsec 클라이언트를 ASA에 연결하려면 **crypto ipsec transform-set trans_name mode transport** 명령을 사용하여 변형 집합에 대해 IPsec 전송 모드를 구성해야 합니다. 이 명령은 구성 절차에서 사용됩니다..

이 전송 기능을 사용하여 IP 헤더의 정보에 기반하여 중간 네트워크에서 특수 처리(예: QoS)를 활성화할 수 있습니다. 그러나 패킷 검사를 제한하는 계층 4 헤더가 암호화되었습니다. IP 헤더가 암호화

되지 않은 텍스트로 전송되는 경우 전송 모드를 통해 공격자가 일부 트래픽 분석을 수행할 수 있습니다.

L2TP over IPsec의 라이센싱 요건

참고 No Payload Encryption 모델에서는 이 기능을 사용할 수 없습니다.

IKEv2를 사용하는 IPsec 원격 액세스 VPN에는 각각 사용 가능한 AnyConnect Plus 또는 Apex 라이센스가 필요합니다. AnyConnect 라이센스 구매 시 다음의 최대값을 참조하십시오. IKEv1을 사용하는 IPsec 원격 액세스 VPN과 IKEv1 또는 IKEv2를 사용하는 IPsec site-to-site VPN은 Base 라이센스와 함께 제공되는 기타 VPN 라이센스를 사용합니다. 모든 유형의 결합 VPN 세션의 최대 수는 이 표에 표시된 최대 세션 수를 초과할 수 없습니다.

모델	라이센스 요건
ASA 5506-X, 5506H-X, 5506W-X	• IKEv2를 사용하는 IPsec 원격 액세스 VPN: 세션 50개. • IKEv1을 사용하는 IPsec 원격 액세스 VPN 및 IKEv1 또는 IKEv2를 사용하는 IPsec Site-to-Site VPN: • Base 라이센스: 세션 10개. • Security Plus 라이센스: 세션 50개.
ASA 5508-X	세션 100개.
ASA 5512-X	세션 250개.
ASA 5515-X	세션 250개.
ASA 5516-X	세션 300개.
ASA 5525-X	세션 750개.
ASA 5545-X	세션 2500개.
ASA 5555-X	세션 5000개.
ASA 5585-X(SSP-10 포함)	세션 5000개.
ASA 5585-X(SSP-20, -40 및 -60 포함)	세션 10,000개.
ASASM	세션 10,000개.
ASAv5	세션 250개.

모델	라이센스 요건
ASAv10	세션 250개.
ASAv30	세션 750개.

L2TP over IPsec 구성의 사전 요구 사항

L2TP over IPsec 구성에는 다음과 같은 사전 요구 사항이 있습니다.

- 그룹 정책 - 기본 그룹 정책(DfltGrpPolicy) 또는 L2TP/IPsec 연결을 위한 사용자 정의 그룹 정책을 구성할 수 있습니다. 두 경우 모두 그룹 정책을 L2TP/IPsec 터널링 프로토콜을 사용하도록 구성해야 합니다. L2TP/IPsec 터널링 프로토콜이 사용자 정의 그룹 정책에 대해 구성되지 않은 경우, L2TP/IPsec 터널링 프로토콜에 대해 DfltGrpPolicy를 구성하고 사용자 정의 그룹 정책이 이 특성을 상속하는 것을 허용하십시오.
- 연결 프로파일 - “사전 공유 키” 인증을 수행 중인 경우 기본 연결 프로파일(터널 그룹) DefaultRAGroup을 구성해야 합니다. 인증서 기반 인증을 수행 중인 경우 인증서 식별자를 기준으로 선택할 수 있는 사용자 정의 연결 프로파일을 사용할 수 있습니다.
- IP 연결을 피어 간에 설정해야 합니다. 연결을 테스트하기 위해 엔드포인트에서 ASA의 IP 주소를 ping하려고 시도하고 ASA에서 엔드포인트의 IP 주소를 ping하려고 시도하십시오.
- UDP 포트 1701이 연결 경로를 따라 차단된 곳이 없는지 확인하십시오.
- Windows 7 엔드포인트 디바이스가 SHA 서명 유형을 지정하는 인증서를 사용하여 인증하는 경우, 서명 유형은 ASA의 서명 유형인 SHA1 또는 SHA2 중 하나와 일치해야 합니다.

지침 및 제한 사항

이 섹션에는 이 기능을 위한 지침 및 제한 사항이 포함되어 있습니다.

상황 모드 지침

단일 및 다중 상황 모드에서 지원합니다. 다중 상황 모드에서 원격 액세스 VPN을 사용하려면 AnyConnect Apex 라이선스가 필요합니다. ASA에서 AnyConnect Apex 라이선스를 인식하지 못하더라도, Apex 라이선스(예: 플랫폼 한도 내에서 라이선스가 허가된 AnyConnect Premium, AnyConnect for Mobile, AnyConnect for Cisco VPN Phone, 고급 엔드포인트 평가)의 라이선스 특성이 적용됩니다.

방화벽 모드 지침

라우팅된 방화벽 모드에서만 지원됩니다. 투명 모드는 지원되지 않습니다.

장애 조치 지침

L2TP over IPsec 세션은 상태 저장 장애 조치에서 지원되지 않습니다.

IPv6 지침

L2TP over IPsec에 대한 네이티브 IPv6 터널 설정이 지원되지 않습니다.

인증 지침

ASA는 로컬 데이터베이스에서 PPP 인증 PAP 및 Microsoft CHAP 버전 1, 2만 지원합니다. EAP 및 CHAP는 프록시 인증 서버에서 수행됩니다. 따라서 원격 사용자가 **authentication eap-proxy** 또는 **authentication chap** 명령을 사용하여 구성된 터널 그룹에 속하며 ASA가 로컬 데이터베이스를 사용하도록 구성된 경우, 이 사용자는 연결할 수 없습니다.

지원되는 PPP 인증 유형

ASA에서 L2TP over IPsec 연결은 아래에 표시된 PPP 인증 유형만 지원합니다.

표 *3: AAA* 서버 지원 및 *PPP* 인증 유형

AAA 서버 유형	지원되는 PPP 인증 유형
LOCAL	PAP, MSCHAPv1, MSCHAPv2
RADIUS	PAP, CHAP, MSCHAPv1, MSCHAPv2, EAP-Proxy
TACACS+	PAP, CHAP, MSCHAPv1
LDAP	PAP
NT	PAP
Kerberos	PAP
SDI	SDI

표 *4: PPP* 인증 유형 특징

키워드	인증 유형	특징
chap	CHAP	서버 챌린지에 대한 응답으로 클라이언트에서 일반 텍스트 사용자 이름과 함께 암호화된 [챌린지와 비밀번호]를 반환합니다. 이 프로토콜은 PAP보다 안전하지만 데이터를 암호화하지 않습니다.
eap-proxy	EAP	보안 어플라이언스에서 외부 RADIUS 인증 서버에 대한 PPP 인증 프로세스의 프록시를 허용하는 EAP를 활성화합니다.

키워드	인증 유형	특징
ms-chap-v1 **ms-chap-v2**	Microsoft CHAP, 버전 1 Microsoft CHAP, 버전 2	CHAP와 유사하지만 일반 텍스트 비밀번호를 사용하는 CHAP와 달리 서버에서 암호화된 비밀번호만 저장하고 비교한다는 점에서 보다 안전합니다. 이 프로토콜에서도 MPPE를 통해 데이터 암호화용 키를 생성합니다.
pap	PAP	인증하는 동안 일반 텍스트 사용자 이름 및 비밀번호를 전달하므로 안전하지 않습니다.

CLI를 통한 L2TP over IPsec 구성

기본 VPN 클라이언트가 L2TP over IPsec 프로토콜을 사용하여 ASA에 VPN 연결이 가능하도록 IKEv1(ISAKMP) 정책 설정을 구성해야 합니다.

- IKEv1 1단계 — SHA1 해시 방법을 사용하는 3DES 암호화
- IPsec 2단계 — MD5 또는 SHA 해시 방법을 사용하는 3DES 또는 AES 암호화
- PPP 인증 — PAP, MS-CHAPv1 또는 MSCHAPv2(권장사항)
- 사전 공유 키(iPhone에만 해당)

프로시저

단계 **1** 특정한 ESP 암호화 유형 및 인증 유형이 있는 변형 집합을 생성합니다.

crypto ipsec ike_version transform-set *transform_name ESP_Encryption_Type ESP_Authentication_Type*

예제:

```
crypto ipsec ikev1 transform-set my-transform-set-ikev1 esp-des esp-sha-hmac
```

단계 **2** 터널 모드 대신 전송 모드를 사용하도록 IPsec에 지시합니다.

crypto ipsec ike_version transform-set*trans_name***mode transport**

예제:

```
crypto ipsec ikev1 transform-set my-transform-set-ikev1 mode transport
```

단계 **3** L2TP/IPsec을 vpn 터널링 프로토콜로 지정합니다.

vpn-tunnel-protocol *tunneling_protocol*

예제:

```
hostname(config)# group-policy DfltGrpPolicy attributes
hostname(config-group-policy)# vpn-tunnel-protocol l2tp-ipsec
```

단계 **4** (선택 사항) 그룹 정책을 위해 DNS 서버 IP 주소를 클라이언트에 전송하도록 Adaptive Security Appliance에 지시합니다.

dns value [**none** | *IP_Primary* | *IP_Secondary*]

예제:

```
hostname(config)# group-policy DfltGrpPolicy attributes
hostname(config-group-policy)# dns value 209.165.201.1 209.165.201.2
```

단계 **5** (선택 사항) 그룹 정책을 위해 WINS 서버 IP 주소를 클라이언트에 전송하도록 Adaptive Security Appliance에 지시합니다.

wins-server value [**none** | *IP_primary* [*IP_secondary*]]

예제:

```
hostname(config)# group-policy DfltGrpPolicy attributes
hostname (config-group-policy)# wins-server value 209.165.201.3 209.165.201.4
```

단계 **6** (선택 사항) IP 주소 풀을 생성합니다.

ip local pool *pool_name starting_address-ending_address* **mask** *subnet_mask*

예제:

```
hostname(config)# ip local pool sales_addresses 10.4.5.10-10.4.5.20 mask 255.255.255.0
```

단계 **7** (선택 사항) IP 주소 풀을 연결 프로파일(터널 그룹)에 연결합니다.

address-pool *pool_name*

예제:

```
hostname(config)# tunnel-group DefaultRAGroup general-attributes
hostname(config-tunnel-general)# address-pool sales_addresses
```

단계 **8** 연결 프로파일(터널 그룹)을 생성합니다.

tunnel-group *name* **type remote-access**

예제:

```
hostname(config)# tunnel-group sales-tunnel type remote-access
```

단계 **9** 그룹 정책 이름을 연결 프로파일(터널 그룹)에 연결합니다.

default-group-policy name

예제:

```
hostname(config)# tunnel-group DefaultRAGroup general-attributes
hostname(config-tunnel-general)# default-group-policy DfltGrpPolicy
```

단계 **10** 연결 프로파일(터널 그룹)에 대해 L2TP over IPsec 연결을 시도하는 사용자를 인증하도록 방법을 지정합니다. ASA를 사용하여 로컬 인증을 수행하지 않은 상태에서 로컬 인증으로 대체하려는 경우 LOCAL을 명령의 마지막에 추가합니다.

authentication-server-group *server_group* [**local**]

예제:

```
hostname(config)# tunnel-group DefaultRAGroup general-attributes
hostname(config-tunnel-general)# authentication-server-group sales_server LOCAL
```

단계 **11** 연결 프로파일(터널 그룹)에 대해 L2TP over IPsec 연결을 시도하는 사용자를 인증하도록 방법을 지정합니다. ASA를 사용하여 로컬 인증을 수행하지 않은 상태에서 로컬 인증으로 대체하려는 경우 LOCAL을 명령의 마지막에 추가합니다.

authentication *auth_type*

예제:

```
hostname(config)# tunnel-group name ppp-attributes
hostname(config-ppp)# authentication ms-chap-v1
```

단계 **12** 연결 프로파일(터널 그룹)에 대해 사전 공유 키를 설정합니다.

tunnel-group 터널 그룹 이름 **ipsec-attributes**

예제:

```
hostname(config)# tunnel-group DefaultRAGroup ipsec-attributes
hostname(config-tunnel-ipsec)# ikev1 pre-shared-key cisco123
```

단계 **13** (선택 사항) 연결 프로파일(터널 그룹)에 대한 L2TP 세션용 AAA 계정 관리 시작 및 중지 레코드를 생성합니다.

accounting-server-group *aaa_server_group*

예제:

```
hostname(config)# tunnel-group sales_tunnel general-attributes
hostname(config-tunnel-general)# accounting-server-group sales_aaa_server
```

단계 **14** Hello 메시지 간의 시간 간격(초)을 구성합니다. 범위는 10초부터 300초까지입니다. 기본 간격은 60초입니다.

l2tp tunnel hello *seconds*

예제:

```
hostname(config)# l2tp tunnel hello 100
```

단계 **15** (선택 사항) ESP 패킷이 하나 이상의 NAT 디바이스를 통과할 수 있도록 NAT 통과를 활성화합니다.

NAT 디바이스를 지원하는 여러 L2TP 클라이언트가 Adaptive Security Appliance에 대해 L2TP over IPsec 연결을 시도할 것으로 예상하는 경우, NAT 통과를 활성화해야 합니다.

crypto isakmp nat-traversal *seconds*

NAT 통과를 전역으로 활성화하려면 ISAKMP가 전역 구성 모드에서 활성화(**crypto isakmp enable** 명령을 통해 활성화 가능)되었는지 확인한 다음 **crypto isakmp nat-traversal** 명령을 사용합니다.

예제:

```
hostname(config)# crypto ikev1 enable
hostname(config)# crypto isakmp nat-traversal 1500
```

단계 **16** (선택 사항) 터널 그룹 전환을 구성합니다. 터널 그룹 전환은 프록시 인증 서버를 사용하여 인증할 때 VPN 연결을 설정하기 위한 더 좋은 기회를 사용자에게 제공하기 위한 것입니다. 터널 그룹은 연결 프로파일과 동일합니다.

strip-group

strip-realm

예제:

```
hostname(config)# tunnel-group DefaultRAGroup general-attributes
hostname(config-tunnel-general)# strip-group
hostname(config-tunnel-general)# strip-realm
```

단계 **17** (선택 사항) 사용자 이름이 **jdoe**이고 비밀번호가 **j!doe1**인 사용자를 생성합니다. mschap 옵션은 사용자가 비밀번호를 입력하면 MD4를 사용하여 비밀번호가 유니코드로 변환되어 해시되도록 지정합니다.

다음 단계는 로컬 사용자 데이터베이스를 사용 중인 경우에만 필요합니다.

username이름 **password** 암호 **mschap**

예제:

```
asa2(config)# username jdoe password j!doe1 mschap
```

단계 **18** 1단계에 대한 IKE 정책을 생성하고 번호를 할당합니다.

crypto ikev1 policy *priority*

group *Diffie-Hellman Group*

사용자가 구성할 수 있는 IKE 정책의 여러 가지 다양한 매개변수가 있습니다. 또한 정책에 대해 Diffie-Hellman 그룹을 지정할 수 있습니다. ASA에서 isakamp 정책을 사용하여 IKE 협상을 완료합니다.

예제:

```
hostname(config)# crypto ikev1 policy 5
hostname(config-ikev1-policy)# group 5
```

Windows 7 제안서에 응답하기 위한 IKE 정책 생성

Windows 7 L2TP/IPsec 클라이언트는 ASA와 VPN 연결을 설정하기 위해 여러 IKE 정책 제안서를 전송합니다. Windows 7 VPN 네이티브 클라이언트에서의 연결을 용이하게 하려면 다음 IKE 정책 중 하나를 정의합니다.

ASA에 대한 L2TP over IPsec을 구성하는 절차를 따릅니다. Windows 7 네이티브 VPN 클라이언트에 대해 IKE 정책을 구성하려면 이 작업에 있는 추가 단계를 추가합니다.

프로시저

단계 **1** 기존 IKE 정책의 특성과 번호를 표시합니다.

예제:

```
hostname(config)# show run crypto ikev1
```

단계 **2** IKE 정책을 구성합니다. 번호 인수는 구성 중인 IKE 정책의 번호를 지정합니다. 이 번호는 **show run crypto ikev1** 명령의 출력에 표시되어 있습니다.

crypto ikev1 policy *number*

단계 **3** ASA에서 사전 공유 키를 사용하기 위해 각 IPsec 피어의 ID를 설정하는 데 사용하는 인증 방법을 설정합니다.

예제:

```
hostname(config-ikev1-policy)# authentication pre-share
```

단계 **4** 두 IPsec 피어 간에 전송되는 데이터를 보호하는 대칭 암호화 방법을 선택합니다. Windows 7의 경우 128비트 AES 또는 **aes-256**에 대해 **3des** 또는 **aes**를 선택합니다.

encryption {**3des**| **aes**| **aes-256**}

단계 **5** 데이터 무결성을 보장하는 해시 알고리즘을 선택합니다. Windows 7의 경우 SHA-1 알고리즘을 위해 **sha**를 지정합니다.

예제:

```
hostname(config-ikev1-policy)# hash sha
```

단계 **6** Diffie-Hellman 그룹 식별자를 선택합니다. aes, aes-256 또는 3des 암호화 유형에 대해 5를 지정할 수 있습니다. 3des 암호화 유형에 대해서만 2를 지정할 수 있습니다.

예제:

```
hostname(config-ikev1-policy)# group 5
```

단계 **7** SA 수명(초 단위)을 지정합니다. Windows 7의 경우 24시간을 나타내도록 86400초를 지정합니다.

예제:

```
hostname(config-ikev1-policy)# lifetime 86400
```

L2TP over IPsec 구성 예

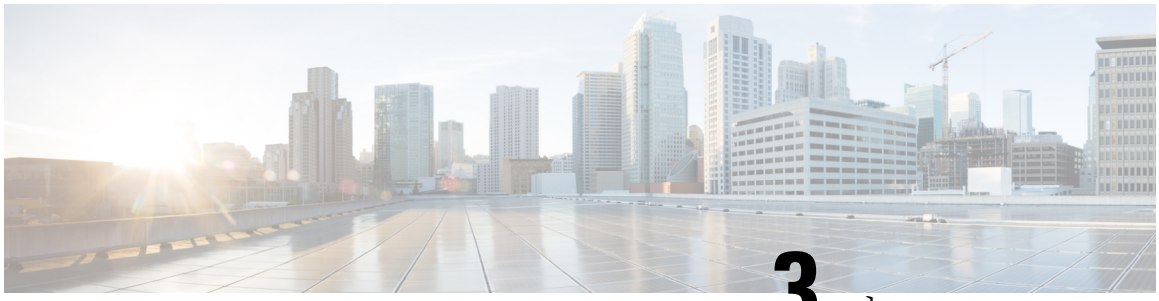
다음 예는 모든 운영 체제의 네이티브 VPN 클라이언트와 ASA의 호환성을 보장하는 구성 파일 명령을 보여줍니다.

```
ip local pool sales_addresses 209.165.202.129-209.165.202.158
group-policy sales_policy internal
group-policy sales_policy attributes
 wins-server value 209.165.201.3 209.165.201.4
 dns-server value 209.165.201.1 209.165.201.2
 vpn-tunnel-protocol l2tp-ipsec
tunnel-group DefaultRAGroup general-attributes
 default-group-policy sales_policy
 address-pool sales_addresses
tunnel-group DefaultRAGroup ipsec-attributes
 pre-shared-key *
tunnel-group DefaultRAGroup ppp-attributes
 no authentication pap
```

```
 authentication chap
 authentication ms-chap-v1
 authentication ms-chap-v2
crypto ipsec ikev1 transform-set trans esp-des esp-sha-hmac
crypto ipsec ikev1 transform-set trans mode transport
crypto dynamic-map dyno 10 set ikev1 transform-set trans
crypto map vpn 20 ipsec-isakmp dynamic dyno
crypto map vpn interface outside
crypto ikev1 enable outside
crypto ikev1 policy 10
 authentication pre-share
 encryption 3des
 hash sha
 group 2
 lifetime 86400
```

L2TP over IPsec에 대한 기능 기록

기능 이름	릴리스	기능 정보
L2TP over IPsec	7.2(1)	L2TP over IPsec은 단일 플랫폼에서 IPsec VPN 및 방화벽 서비스와 함께 L2TP VPN 솔루션을 배포 및 관리하는 기능을 제공합니다. 원격 액세스 시나리오에서 L2TP over IPsec을 구성하는 주요 이점은 원격 사용자가 게이트웨이 또는 전용선 없이 공용 IP 네트워크를 통해 VPN에 액세스할 수 있어 POTS를 통해 가상의 위치에서 원격 액세스가 활성화된다는 점입니다. 또 다른 이점은 VPN 액세스를 위한 유일한 클라이언트 요건이 Microsoft DUN(Dial-Up Networking: 다이얼업 네트워킹)이 가능한 Windows 사용이라는 점입니다. Cisco VPN 클라이언트 소프트웨어와 같은 클라이언트 소프트웨어가 추가로 필요하지 않습니다. 다음 명령은 새로 도입되었거나 수정되었습니다. authentication eap-proxy, authentication ms-chap-v1, authentication ms-chap-v2, authentication pap, l2tp tunnel hello, vpn-tunnel-protocol l2tp-ipsec.



3 장

고가용성 옵션

고가용성 옵션

분산 VPN 클러스터링, 로드 밸런싱과 장애 조치 둘 다 고가용성 기능이지만 서로 다르게 작동하고 요건도 다릅니다. 경우에 따라 구축의 여러 기능을 사용할 수 있습니다. 다음 섹션에서는 이러한 기능에 대해 설명합니다. 분산 VPN 및 장애 조치에 대한 자세한 내용 해당 릴리스의 ASA 일반적인 작업 CLI 구성 가이드를 참조하십시오. 여기에 로드 밸런싱 세부 정보가 포함되어 있습니다.

FXOS 섀시에서의 VPN 및 클러스터링

ASA FXOS 클러스터는 중앙 집중식 또는 분산 S2S VPN에 함께 사용할 수 없는 다음 두 가지 모드 중 하나를 지원합니다.

- 중앙 집중식 VPN 모드. 기본 모드. 중앙 집중식 모드에서 VPN 연결은 클러스터의 마스터로만 설정됩니다.

  VPN 기능은 마스터 유닛에만 제한되며 클러스터 고가용성 기능을 사용하지 않습니다. 마스터 유닛에 오류가 발생할 경우, 모든 기존 VPN 연결이 손실되며 VPN에 연결된 사용자에게는 서비스 중단 메시지가 표시됩니다. 새 마스터가 선택되면 VPN 연결을 다시 설정해야 합니다.

  VPN 터널을 스팬 인터페이스 주소에 연결할 경우 연결이 마스터 유닛에 자동으로 전달됩니다. VPN 관련 키 및 인증서는 모든 유닛에 복제됩니다.

- 분산 VPN 모드. 이 모드에서 S2S IPsec IKEv2 VPN 연결은 확장성을 제공하는 ASA 클러스터의 멤버 전체에서 분산됩니다. 클러스터 멤버 전체에서 VPN 연결을 분산시키면 클러스터의 용량 및 처리량 모두를 완전히 활용하며 특히 중앙 집중식 VPN 기능 이상으로 VPN 지원을 크게 확장합니다.

참고 중앙 집중식 VPN 클러스터링 모드는 S2S IKEv1 및 S2S IKEv2를 지원합니다.

분산 VPN 클러스터링 모드는 S2S IKEv2만 지원합니다.

분산 VPN 클러스터링 모드는 Firepower 9300에서만 지원됩니다.

원격 액세스 VPN은 중앙 집중식 또는 분산 VPN 클러스터링 모드에서 지원되지 않습니다.

부하 균형

부하 균형은 가상 클러스터의 디바이스 간에 원격 액세스 VPN 트래픽을 균등하게 분산시키는 메커니즘입니다. 처리량이나 기타 요인을 고려하지 않고 트래픽의 단순한 분산을 기반으로 합니다. 부하 균형 클러스터는 둘 이상의 디바이스로 구성되며, 그 중 하나는 가상 마스터이고 나머지는 백업입니다. 이러한 디바이스는 정확히 동일한 유형이거나 동일한 소프트웨어 버전 또는 구성일 필요가 없습니다.

가상 클러스터의 모든 활성 디바이스는 세션 부하를 수반합니다. 부하 균형은 클러스터에서 부하가 가장 적은 디바이스로 트래픽을 디렉션하여 모든 디바이스 간에 부하를 분산시킵니다. 따라서 시스템 리소스가 효율적으로 사용되며, 성능 및 고가용성이 증가합니다.

페일오버

장애 조치 구성에는 전용 장애 조치 링크 및 선택적 상태 저장 장애 조치 링크를 통해 서로 연결된 두 개의 동일한 ASA가 필요합니다. 액티브 인터페이스 및 유닛의 상태를 모니터링하여 특정 장애 조치 조건이 충족되는 시점을 확인합니다. 이러한 조건이 충족되면 장애 조치가 발생합니다. 장애 조치에서는 VPN 구성과 방화벽 구성을 둘 다 지원합니다.

ASA에서는 두 가지 장애 조치 구성, 즉 활성/활성 장애 조치와 활성/대기 장애 조치를 지원합니다.

활성/활성 장애 조치의 경우 두 장치 모두 네트워크 트래픽을 전달할 수 있습니다. 하지만 부하 균형에서는 같은 효과가 있는 것처럼 보일 수 있지만 실제로 두 디바이스 모두 네트워크 트래픽을 전달할 수 있는 것은 아닙니다. 장애 조치가 발생하면 남은 활성 장치가 구성된 매개변수를 기반으로 결합된 트래픽을 전달하는 역할을 합니다. 따라서 액티브/액티브 장애 조치를 구성할 때는 두 유닛의 결합된 트래픽이 각 유닛의 용량 내에 있는지 확인해야 합니다.

액티브/스탠바이 장애 조치에서는 하나의 유닛만 트래픽을 전달하며 다른 유닛은 트래픽을 전달하지 않고 스탠바이 상태로 대기합니다. 액티브/스탠바이 장애 조치에서는 두 번째 ASA가 장애가 발생한 유닛의 역할을 수행할 수 있습니다. 액티브 유닛에서 장애가 발생한 경우 이 유닛은 스탠바이 상태로 변경되며, 스탠바이 유닛이 액티브 상태로 변경됩니다. 활성 상태로 변경된 장치는 장애가 발생한 장치의 IP 주소(또는 투명 방화벽을 위해 관리 IP 주소) 및 MAC 주소를 인수하여 트래픽 전달을 시작합니다. 스탠바이 상태가 된 유닛은 액티브 유닛의 스탠바이 IP 주소를 인수합니다. 액티브 유닛에서 장애가 발생한 경우 스탠바이 유닛은 클라이언트 VPN 터널의 중단 없이 액티브 유닛의 역할을 수행합니다.

부하 균형

로드 밸런싱 정보

동일한 네트워크에 연결된 둘 이상의 ASA를 사용하여 원격 세션을 처리하는 원격-클라이언트 구성의 경우 이러한 디바이스에서 해당 세션 로드를 공유하도록 구성할 수 있습니다. 이 기능을 로드 밸런싱이라고 합니다. 로드 밸런싱은 로드가 가장 적은 디바이스로 세션 트래픽을 전달하여 모든 디바이스 간에 로드를 분산시킵니다. 따라서 시스템 리소스가 효율적으로 사용되며, 성능 및 가용성이 증가합니다.

로드 밸런싱을 구현하려면 동일한 비공개 LAN-to-LAN 네트워크에 있는 둘 이상의 디바이스를 가상 클러스터로 논리적으로 그룹화합니다.

가상 클러스터의 모든 디바이스는 세션 로드를 수반합니다. 가상 클러스터에 있는 하나의 디바이스인 가상 클러스터 마스터는 수신 연결 요청을 백업 디바이스라는 나머지 디바이스로 디렉션합니다. 가상 클러스터 마스터는 클러스터의 모든 디바이스를 모니터링하고 각각의 사용량을 추적하며 그에 따라 세션 로드를 분산시킵니다. 가상 클러스터 마스터 역할은 물리적 디바이스와 연관이 없으며, 디바이스 간에 전환될 수 있습니다. 예를 들어 현재 가상 클러스터 마스터에서 장애가 발생한 경우 클러스터의 백업 디바이스 중 하나가 해당 역할을 맡아 즉시 새로운 가상 클러스터 마스터가 됩니다.

가상 클러스터는 단일 가상 클러스터 *IP* 주소로 외부 클라이언트에 표시됩니다. 이 IP 주소는 특정 물리적 디바이스에 연결되지 않으며, 현재 가상 클러스터 마스터에 속하므로 가상 주소입니다. 연결을 설정하려는 VPN 클라이언트는 먼저 이 가상 클러스터 IP 주소에 연결합니다. 그러면 가상 클러스터 마스터가 클러스터에서 사용 가능한 호스트 중 로드가 가장 적은 호스트의 공개 IP 주소를 클라이언트로 다시 전송합니다. 두 번째 트랜잭션(사용자에게 투명함)에서 클라이언트는 해당 호스트에 직접 연결합니다. 가상 클러스터 마스터는 이러한 방식으로 리소스 간에 트래픽을 균등하고 효율적으로 디렉션합니다.

클러스터의 시스템에서 장애가 발생한 경우 종료된 세션이 가상 클러스터 IP 주소에 즉시 다시 연결될 수 있습니다. 그러면 가상 클러스터 마스터가 이러한 연결을 클러스터의 다른 액티브 디바이스로 디렉션합니다. 가상 클러스터 마스터 자체에서 장애가 발생한 경우에는 클러스터의 백업 디바이스가 즉시 자동으로 새로운 가상 세션 마스터의 역할을 합니다. 클러스터의 여러 디바이스에서 장애가 발생한 경우에도 클러스터에 실행되고 사용 가능한 디바이스가 남아 있는 한 사용자는 클러스터에 계속 연결할 수 있습니다.

VPN 부하 균형 알고리즘

마스터 디바이스는 IP 주소가 오름차순으로 정렬된 백업 클러스터 요소의 목록을 유지 관리합니다. 각 백업 클러스터 요소의 부하는 정수 백분율(활성 세션의 수)로 계산됩니다. AnyConnect 비활성화 세션은 부하 균형에 대한 SSL VPN 부하에 포함되지 않습니다. 마스터 디바이스는 나머지보다 1% 더 높을 때까지 가장 부하가 낮은 디바이스로 IPsec 및 SSL VPN 터널을 리디렉션합니다. 모든 백업 클러스터 요소가 마스터보다 1% 높은 경우 마스터 디바이스가 자체적으로 리디렉션합니다.

예를 들어 마스터 1개와 백업 클러스터 요소 2개가 있는 경우 다음 주기가 적용됩니다.

참고 모든 노드가 0%로 시작하고 모든 백분율이 반올림됩니다.

1. 모든 요소에 마스터보다 1% 더 높은 로드가 있는 경우 마스터 디바이스가 연결을 수행합니다.
2. 마스터 디바이스가 연결을 수행하지 않은 경우 부하 백분율이 가장 작은 백업 디바이스가 세션을 수행합니다.
3. 모든 요소에 같은 백분율 부하가 있는 경우 세션 수가 가장 작은 백업 디바이스가 해당 세션을 가져옵니다.
4. 모든 요소에 같은 백분율 부하가 있고 세션 수가 같은 경우 IP 주소가 가장 작은 디바이스가 해당 세션을 가져옵니다.

VPN 부하 균형 클러스터 구성

로드 밸런싱 클러스터는 다음 제한 사항에 따라 동일한 릴리스 또는 혼합된 릴리스의 ASA로 구성될 수 있습니다.

- 동일한 릴리스의 ASA로 구성된 로드 밸런싱 클러스터는 IPsec, AnyConnect 및 클라이언트리스 SSL VPN 클라이언트와 클라이언트리스 세션이 혼합된 세션에 대해 로드 밸런싱을 실행할 수 있습니다.
- 혼합된 릴리스의 ASA 또는 동일한 릴리스의 ASA가 포함된 로드 밸런싱 클러스터는 IPsec 세션만 지원할 수 있습니다. 그러나 이러한 구성에서는 ASA가 전체 IPsec 용량에 도달하지 않을 수도 있습니다.

7.1(1) 릴리스부터 클러스터의 각 디바이스에 수반되는 로드를 결정할 때 IPsec 세션과 SSL VPN 세션을 동일하게 계산하거나 가중치를 부여합니다. 이는 ASA 릴리스 7.0(x) 소프트웨어에 대한 로드 밸런싱 계산과 다르다는 것을 의미합니다. 즉, 이 플랫폼에서는 일부 하드웨어 플랫폼에서 SSL VPN 세션 로드를 IPsec 세션 로드와 다르게 계산하는 가중치 알고리즘을 사용합니다.

클러스터의 가상 마스터는 클러스터의 요소에 세션 요청을 할당합니다. ASA에서는 모든 세션, SSL VPN 또는 IPsec을 동일하게 간주하여 그에 따라 세션 요청을 할당합니다. 구성 및 라이센스에서 허용하는 최대 범위 내에서 허용할 IPsec 및 SSL VPN 세션 수를 구성할 수 있습니다.

Cisco에서는 하나의 로드 밸런싱 클러스터에서 최대 10개의 노드를 테스트했습니다. 더 큰 클러스터도 작동할 수 있지만 공식적으로는 이러한 토폴로지를 지원하지 않습니다.

일반적인 혼합 클러스터 시나리오의 예

혼합 구성을 사용하는 경우, 즉 로드 밸런싱 클러스터에 ASA 소프트웨어 릴리스의 혼합을 실행 중인 디바이스가 포함된 경우, 초기 클러스터 마스터에 장애가 발생하여 다른 디바이스가 마스터 역할을 하면 가중치 알고리즘의 차이로 인해 문제가 발생합니다.

다음 시나리오는 ASA 릴리스 7.1(1) 및 ASA 릴리즈 7.0(x) 소프트웨어가 실행 중인 ASA가 혼합으로 구성된 클러스터에서 VPN 로드 밸런싱의 사용을 보여줍니다.

시나리오 **1: SSL VPN** 연결을 하지 않는 혼합 클러스터

이 시나리오에서 클러스터는 ASA의 혼합으로 구성됩니다. ASA 클러스터 피어의 일부는 ASA 릴리스 7.0(x)을 실행하고 일부는 Release 7.1(1)을 실행합니다. 7.1(1) 이전 피어에는 SSL VPN 연결이 없으며 7.1(1) 클러스터 피어에는 두 개의 SSL VPN 세션을 허용하지만 SSL VPN 연결이 없는 기본 SSL VPN 라이선스만 있습니다. 이러한 경우 모든 연결이 IPsec이며 부하 균형이 올바르게 작동합니다.

시나리오 **2: SSL VPN** 연결을 처리하는 혼합 클러스터

예를 들어 ASA Release 7.1(1) 소프트웨어를 실행 중인 ASA가 초기 클러스터 마스터이고 해당 디바이스에 장애가 발생한다고 가정해 보십시오. 클러스터의 다른 디바이스가 자동으로 마스터의 역할을 수행하고 클러스터 내에서 프로세서 부하를 결정하기 위해 자체 부하 균형 알고리즘을 적용합니다. ASA Release 7.1(1) 소프트웨어에서 실행 중인 클러스터 마스터는 해당 소프트웨어가 제공하는 부분 이외에는 어떤 방식으로도 세션 로드에 가중치를 부여할 수 없습니다. 따라서 IPsec 및 SSL VPN 세션 부하의 혼합을 이전 버전을 실행 중인 ASA 디바이스에 적절히 할당할 수 없습니다. 다음 시나리오는 이러한 딜레마를 보여줍니다.

이 시나리오는 클러스터가 ASA의 혼합으로 구성되었다는 점에서 이전 시나리오와 유사합니다. ASA 클러스터 피어의 일부는 ASA 릴리스 7.0(x)을 실행하고 일부는 Release 7.1(1)을 실행합니다. 그러나 이 경우 클러스터는 SSL VPN 연결뿐만 아니라 IPsec 연결을 처리합니다.

ASA 릴리스 7.1(1) 이전 버전의 소프트웨어를 실행 중인 디바이스가 클러스터 마스터인 경우 이 마스터는 릴리스 7.1(1) 이전의 프로토콜과 로직을 적용합니다. 즉, 세션이 세션 제한을 초과한 부하 균형 피어에게 디렉션될 수 있습니다. 이 경우 사용자는 액세스가 거부됩니다.

클러스터 마스터가 ASA 릴리스 7.0(x) 소프트웨어를 실행 중인 디바이스인 경우 기존 세션 가중치 알고리즘이 클러스터의 7.1(1) 이전 피어에만 적용됩니다. 이 경우에 액세스가 거부되지 않습니다. 7.1(1) 이전 피어는 세션 가중치 알고리즘을 사용하기 때문에 좀 더 가볍게 로드됩니다.

그러나 7.1(1) 피어가 항상 클러스터 마스터가 된다고 보장할 수 없기 때문에 문제가 발생합니다. 클러스터 마스터에 장애가 발생하는 경우 다른 피어가 마스터의 역할을 수행합니다. 새 마스터는 자격을 갖춘 피어 중 하나일 수 있습니다. 결과를 예측할 수 없으므로 해당 유형의 클러스터는 구성하지 않는 것이 좋습니다.

부하 균형에 대한 자주 묻는 질문(FAQ)

멀티 컨텍스트 모드

Q. 다중 상황 모드에서 로드 밸런싱이 지원됩니까?

A. 다중 상황 모드에서는 로드 밸런싱과 상태 저장 장애 조치 모두 지원됩니다.

IP 주소 풀 소모

Q. ASA에서는 VPN 로드 밸런싱 방법의 일환으로 IP 주소 풀 소모를 고려합니까?

A. 아니요. 원격 액세스 VPN 세션이 소모된 IP 주소 풀이 있는 디바이스로 디렉션되는 경우 세션이 설정되지 않습니다. 부하 균형 알고리즘은 부하를 기반으로 하며 각 백업 클러스터 요소가 제공하는 정수 백분율(활성 세션 및 최대 세션의 수)로 계산됩니다.

고유한 **IP** 주소 풀

Q. VPN 로드 밸런싱을 구현하려면 다른 ASA의 AnyConnect 클라이언트 또는 IPsec 클라이언트에 대한 IP 주소 풀이 고유해야 합니까?

A. 예. IP 주소 풀은 디바이스별로 고유해야 합니다.

같은 디바이스에서 부하 균형 및 장애 조치 사용

Q. 하나의 디바이스에서 부하 균형과 장애 조치를 모두 사용할 수 있습니까?

A. 예. 이 구성에서는 클라이언트가 클러스터의 IP 주소에 연결되고 클러스터에서 부하가 가장 적은 ASA로 리디렉션됩니다. 해당 디바이스에서 장애가 발생하면 대기 장치가 즉시 해당 역할을 맡아 VPN 터널에 아무런 영향을 미치지 않습니다.

여러 인터페이스의 부하 균형

Q. 여러 인터페이스에서 SSL VPN을 활성화한 경우 모든 인터페이스에서 부하 균형을 구현할 수 있습니까?

A. 1개의 인터페이스만 공유 인터페이스로 클러스터에 참여하도록 정의할 수 있습니다. 이는 CPU 부하의 균형을 유지하기 위한 것입니다. 여러 인터페이스가 같은 CPU에서 통합되므로 여러 인터페이스에서 부하 균형의 개념은 의미가 없습니다.

부하 균형 클러스터에 대한 최대 동시 세션 수

Q. 각각 100개의 사용자 SSL VPN 라이센스를 사용하는 2개의 ASA 5525-X을 배포한다는 점을 고려하십시오. 부하 균형 클러스터에서 최대 전체 사용자 수는 200개의 동시 세션을 허용합니까

아니면 100개만 허용합니까? 100개의 사용자 라이센스를 사용하는 제3의 디바이스를 추가하는 경우 300개의 동시 세션을 지원할 수 있습니까?

A. VPN 부하 균형을 사용하면 모든 디바이스가 활성화되므로 사용자가 클러스터에서 지원할 수 있는 최대 세션 수는 클러스터의 각 디바이스에 대한 세션 수의 총합과 같습니다. 이 경우에서는 300개의 세션을 지원합니다.

로드 밸런싱에 대한 라이센싱

VPN 로드 밸런싱을 사용하려면 Security Plus 라이센스가 있는 ASA 모델 5512-X 또는 ASA 모델 5515-X 이상이 있어야 합니다. VPN 로드 밸런싱에도 활성 3DES/AES 라이센스가 필요합니다. 보안 어플라이언스는 로드 밸런싱을 활성화하기 전에 이러한 암호화 라이센스가 있는지 확인합니다. 활성 3DES 또는 AES 라이센스가 탐지되지 않는 경우 보안 어플라이언스가 로드 밸런싱의 활성화를 방지하며 라이센스에서 허용할 때까지 로드 밸런싱을 통한 3DES의 내부 구성을 방지합니다.

VPN 로드 밸런싱에 대한 지침 및 제한 사항

또한 로드 밸런싱을 위한 사전 요구 사항, 65 페이지의 내용을 참조하십시오.

적격 플랫폼

로드 밸런싱 클러스터에는 Security Plus 라이선스가 포함된 ASA 모델 ASA 5512-X 및 모델 5515-X 이상이 포함될 수 있습니다. 혼합된 구성을 사용할 수 있는 경우 일반적으로 클러스터의 종류가 같으면 관리가 더 간단합니다.

적격 클라이언트

로드 밸런싱은 다음 클라이언트에서 시작되는 원격 세션에만 적용됩니다.

- Cisco AnyConnect Secure Mobility Client(릴리스 3.0 이상)
- Cisco ASA 5505 Security Appliance(Easy VPN 클라이언트 역할을 하는 경우)
- IKE 리디렉션을 지원하는 Cisco IOS EZVPN 클라이언트 디바이스(IOS 831/871)
- 클라이언트리스 SSL VPN(클라이언트가 아님)

클라이언트 고려 사항

로드 밸런싱은 IPsec 클라이언트와 SSL VPN 클라이언트 및 클라이언트리스 세션에서 작동합니다. LAN-to-LAN을 비롯한 다른 모든 VPN 연결 유형(L2TP, PPTP, L2TP/IPsec)은 로드 밸런싱이 활성화된 ASA에 연결할 수 있지만 로드 밸런싱에 참여할 수는 없습니다.

로드 밸런싱을 위해 여러 개의 ASA 노드가 클러스터링된 경우, AnyConnect 클라이언트 연결에 대해 그룹 URL을 사용하는 것이 바람직한 경우, 개별 ASA 노드는 다음을 수행해야 합니다.

- 각 로드 밸런싱 가상 클러스터 주소(IPv4 및 IPv6)에 대한 그룹 URL을 사용하여 각 원격 액세스 연결 프로파일을 구성합니다.

- 이 노드의 VPN 로드 밸런싱 공용 주소에 대해 그룹 URL을 구성합니다.

상황 모드

다중 상황 모드에서는 VPN 로드 밸런싱이 지원되지 않습니다.

인증서 확인

AnyConnect에서의 로드 밸런싱을 위해 인증서 확인을 수행할 때 연결이 IP 주소를 통해 리디렉션되는 경우 클라이언트는 이 IP 주소를 통해 모든 이름 확인을 수행합니다. 리디렉션 IP 주소가 인증서 공통 이름 또는 주체 대체 이름에 나열되어 있는지 확인합니다. IP 주소가 이러한 필드에 없으면 인증서가 신뢰할 수 없는 것으로 간주됩니다.

주체 대체 이름이 인증서에 포함된 경우에는 RFC 2818에 정의된 지침에 따라 이름 확인에 주체 대체 이름만 사용하며, 공통 이름은 무시합니다. 인증서를 제시하는 서버의 IP 주소가 인증서의 주체 대체 이름에 정의되어 있는지 확인합니다.

독립형 ASA의 경우 IP 주소는 해당 ASA의 IP입니다. 클러스터링 상황에서는 인증서 구성에 따라 달라집니다. 클러스터에서 하나의 인증서를 사용하는 경우에는 해당 클러스터의 IP이며, 각 ASA의 IP와 FQDN이 있는 주체 대체 이름 확장이 인증서에 포함되어 있을 수 있습니다. 클러스터에서 여러 인증서를 사용하는 경우에는 ASA의 IP 주소여야 합니다.

지리적 로드 밸런싱

DNS 확인이 정기적으로 변경되는 로드 밸런싱 환경에서는 TTL(Time to Live) 값을 설정하는 방법을 신중하게 고려해야 합니다. AnyConnect에서 DNS 로드 밸런싱 구성이 제대로 작동하려면 ASA를 선택한 시점부터 터널이 완전히 설정될 때까지 ASA 이름-주소 매핑이 동일하게 유지되어야 합니다. 자격 증명을 입력하기 전에 너무 많은 시간이 경과한 경우에는 조회가 다시 시작되고 다른 IP 주소가 확인된 주소가 될 수도 있습니다. 자격 증명을 입력하기 전에 DNS 매핑이 다른 ASA로 변경되면 VPN 터널이 실패합니다.

VPN에 대한 지리적 로드 밸런싱에서는 Cisco GSS(Global Site Selector)를 사용하는 경우가 많습니다. GSS는 로드 밸런싱에 DNS를 사용하며, DNS 확인에 대한 TTL(Time to Live) 값이 기본적으로 20초로 설정됩니다. GSS에서 TTL 값을 늘리면 연결에 실패할 가능성을 크게 낮출 수 있습니다. 훨씬 더 높은 값으로 늘리면 인증 단계에서 사용자가 자격 증명을 입력하고 터널을 설정할 수 있는 충분한 시간이 허용됩니다.

자격 증명 입력 시간을 늘리기 위해 Connect on Start Up(시작 시 연결)을 비활성화할 수도 있습니다.

부하 균형 구성

동일한 네트워크에 연결된 둘 이상의 ASA를 사용하여 원격 세션을 처리하는 원격-클라이언트 구성의 경우 이러한 디바이스에서 해당 세션 로드를 공유하도록 구성할 수 있습니다. 로드 밸런싱이라고 하는 이 기능은 로드가 가장 적은 디바이스로 세션 트래픽을 전달하여 모든 디바이스 간에 로드를 분산시킵니다. 로드 밸런싱은 시스템 리소스의 효율적 사용을 지원하며, 성능 및 고가용성을 증가시킵니다.

로드 밸런싱을 사용하려면 클러스터의 각 디바이스에서 다음을 수행합니다.

- 공통 VPN 로드 밸런싱 클러스터 속성을 설정하여 로드 밸런싱 클러스터를 구성합니다. 이 클러스터에는 가상 클러스터 IP 주소, UDP 포트(필요한 경우) 및 클러스터의 IPsec 공유 암호가 포함됩니다. 클러스터의 모든 참여자는 클러스터 내에서 디바이스 우선순위를 제외하고 클러스터 구성이 같아야 합니다.
- 디바이스에서 로드 밸런싱을 활성화하고 디바이스별 속성(공용 주소 및 사설 주소)을 정의하여 참여하는 디바이스를 구성합니다. 이러한 값은 디바이스마다 다릅니다.

로드 밸런싱을 위한 사전 요구 사항

또한 VPN 로드 밸런싱에 대한 지침 및 제한 사항, 63 페이지의 내용을 참조하십시오.

- 부하 균형은 기본적으로 비활성화되어 있습니다. 명시적으로 부하 균형을 활성화해야 합니다.
- 먼저 공용(외부) 및 사설(내부) 인터페이스를 구성해야 합니다. 이 섹션의 후속 참조는 내부 및 외부의 이름을 사용합니다.

  해당 인터페이스에 다른 이름을 구성하기 위해 **interface** 및 **nameif** 명령을 사용할 수 있습니다.
- 가상 클러스터 IP 주소가 참조하는 인터페이스를 미리 구성해 두어야 합니다. 공통 가상 클러스터 IP 주소, UDP 포트(필요한 경우) 및 클러스터의 IPsec 공유 암호를 설정합니다.
- 클러스터에 참여하는 모든 디바이스는 클러스터 특정 값(IP 주소, 암호화 설정, 암호 키 및 포트)이 같아야 합니다.
- 암호화를 사용하는 경우 로드 밸런싱 내부 인터페이스를 구성해야 합니다. 이 인터페이스가 로드 밸런싱 내부 인터페이스에서 활성화되지 않은 경우에는 클러스터 암호화를 구성하려고 할 때 오류 메시지가 나타납니다.
- 활성/활성 상태 저장 장애 조치 또는 VPN 부하 균형을 사용하는 경우 로컬 CA 기능이 지원되지 않습니다. 로컬 CA는 다른 CA에 종속될 수 없고 루트 CA의 역할만 수행할 수 있습니다.

부하 균형을 위한 공용 및 사설 인터페이스 구성

부하 균형 클러스터 디바이스를 위한 공용(외부) 및 사설(내부) 인터페이스를 구성하려면 다음 단계를 수행하십시오.

프로시저

단계 **1** vpn-load-balancing 구성 모드에서 **lbpublic** 키워드와 함께 **interface** 명령을 입력하여 ASA에서 공용 인터페이스를 구성하십시오. 이 명령은 해당 디바이스의 부하 균형에 대한 공용 인터페이스의 이름 또는 IP 주소를 지정합니다.

예제:

```
hostname(config)# vpn load-balancing
hostname(config-load-balancing)# interface lbpublic outside
hostname(config-load-balancing)#
```

단계 **2** vpn-load-balancing 구성 모드에서 **lbprivate** 키워드와 함께 **interface** 명령을 입력하여 ASA에서 사설 인터페이스를 구성하십시오. 이 명령은 해당 디바이스의 부하 균형에 대한 사설 인터페이스의 이름 또는 IP 주소를 지정합니다.

예제**:**

```
hostname(config-load-balancing)# interface lbprivate inside
hostname(config-load-balancing)#
```

단계 **3** 클러스터 내에서 해당 디바이스에 할당할 우선순위를 설정하십시오. 범위는 1에서 10까지입니다. 우선순위는 시작 시 또는 기존 마스터에서 장애가 발생한 경우 해당 디바이스가 가상 클러스터 마스터가 될 가능성을 나타냅니다. 우선순위가 높을수록(예: 10) 해당 디바이스가 가상 클러스터 마스터가 될 가능성이 더 높습니다.

예제**:**

예를 들어 클러스터 내에서 해당 디바이스에 우선순위 6을 할당하려면 다음 명령을 입력하십시오.

```
hostname(config-load-balancing)# priority 6
hostname(config-load-balancing)#
```

단계 **4** 이 디바이스에 대한 네트워크 주소 변환을 적용하려면, 디바이스의 NAT 할당 주소와 함께 **nat** 명령을 입력하십시오. IPv4 및 IPv6 주소를 정의하거나 디바이스의 호스트 이름을 지정할 수 있습니다.

예제**:**

예를 들어 해당 디바이스에 192.168.30.3 및 2001:DB8::1의 NAT 주소를 할당하려면 다음 명령을 입력하십시오.

```
hostname(config-load-balancing)# nat 192.168.30.3 2001:DB8::1
hostname(config-load-balancing)#
```

부하 균형 클러스터 특성 구성

클러스터의 각 디바이스에 대한 부하 균형 클러스터 특성을 구성하려면 다음 단계를 수행하십시오.

프로시저

단계 **1** 전역 구성 모드에서 **vpn load-balancing** 명령을 입력하여 VPN 로드 밸런싱을 설정하십시오.

예제**:**

```
hostname(config)# vpn load-balancing
hostname(config-load-balancing)#
```

이렇게 하면 나머지 부하 균형 특성을 구성할 수 있는 vpn-load-balancing 구성 모드를 시작할 수 있습니다.

단계 **2** 해당 디바이스가 속해 있는 클러스터의 IP 주소 또는 정규화된 도메인 이름을 구성하십시오. 이 명령은 단일 IP 주소 또는 전체 가상 클러스터를 나타내는 FQDN을 지정합니다. 가상 클러스터의 모든 ASA에서 공유하는 공용 서브넷 주소 범위 내에 있는 IP 주소를 선택합니다. IPv4 또는 IPv6 주소를 지정할 수 있습니다.

예제**:**

예를 들어 클러스터 IP 주소를 IPv6 주소 2001:DB8::1로 설정하려면 다음 명령을 입력하십시오.

```
hostname(config-load-balancing)# cluster ip address 2001:DB8::1
hostname(config-load-balancing)#
```

단계 **3** 클러스터 포트를 구성하십시오. 이 명령은 해당 디바이스가 참여하는 가상 클러스터의 UDP 포트를 지정합니다. 기본값은 9023입니다. 다른 애플리케이션에서 이 포트를 사용하는 경우 로드 밸런싱에 사용할 UDP 대상 포트 번호를 입력합니다.

예제**:**

예를 들어 클러스터 포트에 4444를 설정하려면 다음과 같은 명령을 입력하십시오.

```
hostname(config-load-balancing)# cluster port 4444
hostname(config-load-balancing)#
```

단계 **4** (선택 사항) 클러스터의 IPsec 암호화를 활성화하십시오.

기본 설정은 암호화하지 않는 것입니다. 이 명령을 사용하여 IPsec 암호화를 활성화하거나 비활성화합니다. 이 확인 속성을 구성하는 경우 먼저 공유 암호를 지정하고 확인해야 합니다. 가상 클러스터의 ASA는 IPsec을 사용하는 LAN-to-LAN 터널을 통해 통신합니다. 디바이스 간에 전달되는 모든 부하 균형 정보를 암호화하려면 이 특성을 활성화하십시오.

참고 암호화를 사용하는 경우 부하 균형 내부 인터페이스를 미리 구성해야 합니다. 해당 인터페이스가 부하 균형 내부 인터페이스에서 활성화되지 않은 경우에는 클러스터 암호화를 구성하려고 할 때 오류 메시지가 나타납니다.

클러스터 암호화를 구성했을 때 부하 균형 내부 인터페이스를 활성화했으나 가상 클러스터의 디바이스 참여를 구성하기 전에 비활성화한 경우 **participate** 명령을 입력하거나 ASDM에서 **Participate in Load Balancing Cluster** 확인란을 선택하면 오류 메시지가 나타나고 클러스터에 대한 암호화가 활성화되지 않습니다.

클러스터 암호화를 사용하려면 지정된 내부 인터페이스와 함께 **crypto ikev1 enable** 명령을 사용하십시오.

예제**:**

```
hostname(config-load-balancing)# cluster encryption
hostname(config-load-balancing)#
```

단계 **5** 또한 클러스터 암호화를 활성화한 경우 **cluster key** 명령을 입력하여 IPsec 공유 암호를 지정해야 합니다. 다음 명령은 IPsec 암호화를 활성화했을 때 IPsec 피어 간에 공유 암호를 지정합니다. 이 상자에 입력하는 값은 연속된 별표(*) 문자로 표시됩니다.

예제:

예를 들어 공유 암호를 123456789로 설정하려면 다음 명령을 입력하십시오.

```
hostname(config-load-balancing)# cluster key 123456789
hostname(config-load-balancing)#
```

단계 **6** 참여 명령을 입력하여 클러스터에 있는 해당 디바이스의 참여를 활성화하십시오.

예제:

```
hostname(config-load-balancing)# participate
hostname(config-load-balancing)#
```

다음에 수행할 작업

로드 밸런싱을 위해 여러 개의 ASA 노드가 클러스터링된 경우, AnyConnect 클라이언트 연결에 대해 그룹 URL을 사용하는 것이 바람직한 경우, 개별 ASA 노드에서 다음 작업을 수행해야 합니다.

- 각 로드 밸런싱 가상 클러스터 주소(IPv4 및 IPv6)에 대한 그룹 URL을 사용하여 각 원격 액세스 연결 프로필을 구성합니다.
- 이 노드의 VPN 로드 밸런싱 공용 주소에 대해 그룹 URL을 구성합니다.

이러한 그룹 URL을 구성하려면 **tunnel-group**, **general-attributes**, **group-url** 명령을 사용합니다.

정규화된 도메인 이름을 사용하여 리디렉션 활성화

기본적으로 ASA는 로드 밸런싱 리디렉션에서 IP 주소만 클라이언트로 전송합니다. DNS 이름을 기반으로 하는 인증서를 사용 중인 경우 백업 디바이스로 리디렉션할 때는 인증서가 유효하지 않습니다.

VPN 클러스터 마스터로서 이 ASA는 VPN 클라이언트 연결을 클러스터 디바이스(클러스터의 다른 ASA)로 리디렉션할 때 역방향 DNS 조회를 사용하여 외부 IP 주소 대신 해당 클러스터 디바이스의 FQDN(Fully Qualified Domain Name: 정규화된 도메인 이름)을 전송할 수 있습니다.

vpn 로드 밸런싱 모드에서 정규화된 도메인 이름을 사용하여 리디렉션을 활성화 또는 비활성화하려면 전역 구성 모드에서 **redirect-fqdn enable** 명령을 사용합니다. 이 동작은 기본적으로 비활성화되어 있습니다.

시작하기 전에

클러스터 내 로드 밸런싱 디바이스의 모든 외부 및 내부 네트워크 인터페이스는 동일한 IP 네트워크에 있어야 합니다.

프로시저

단계 **1** **redirect-fqdn enable** 명령을 사용하여 로드 밸런싱을 위한 FQDN의 사용을 활성화하십시오.

[**no**] **redirect-fqdn** {**enable** | **disable**}

예제**:**

```
hostname(config)# vpn load-balancing
hostname(config-load-balancing)# redirect-fqdn enable
hostname(config-load-balancing)#
```

단계 **2** 해당 항목이 없는 경우 각 ASA 외부 인터페이스의 항목을 DNS 서버에 추가하십시오. 각 ASA 외부 IP 주소에는 조회를 위한 관련 DNS 항목이 있어야 합니다. 또한 역방향 조회에 대해 이러한 DNS 항목을 활성화해야 합니다.

단계 **3** **dns domain-lookup inside** 명령 또는 DNS 서버로 라우팅하는 인터페이스를 사용하여 ASA의 DNS 조회를 활성화하십시오.

단계 **4** **dns name-server 10.2.3.4**(DNS 서버의 IP 주소)와 같이 ASA의 DNS 서버 IP 주소를 정의하십시오.

VPN 로드 밸런싱에 대한 구성 예

기본 VPN 로드 밸런싱 CLI 구성

다음은 정규화된 도메인 이름에 대한 리디렉션을 활성화하고 클러스터의 공용 인터페이스를 **test**로 지정하고 클러스터의 사설 인터페이스를 **foo**로 지정하는 인터페이스 명령을 포함한 VPN 부하 균형 명령 시퀀스의 예입니다.

```
hostname(config)# interface GigabitEthernet 0/1
hostname(config-if)# ip address 209.165.202.159 255.255.255.0
hostname(config)# nameif test
hostname(config)# interface GigabitEthernet 0/2
hostname(config-if)# ip address 209.165.201.30 255.255.255.0
hostname(config)# nameif foo
hostname(config)# vpn load-balancing
hostname(config-load-balancing)# nat 192.168.10.10
hostname(config-load-balancing)# priority 9
hostname(config-load-balancing)# interface lbpublic test
hostname(config-load-balancing)# interface lbprivate foo
hostname(config-load-balancing)# cluster ip address 209.165.202.224
hostname(config-load-balancing)# cluster key 123456789
hostname(config-load-balancing)# cluster encryption
hostname(config-load-balancing)# cluster port 9023
hostname(config-load-balancing)# redirect-fqdn enable
hostname(config-load-balancing)# participate
```

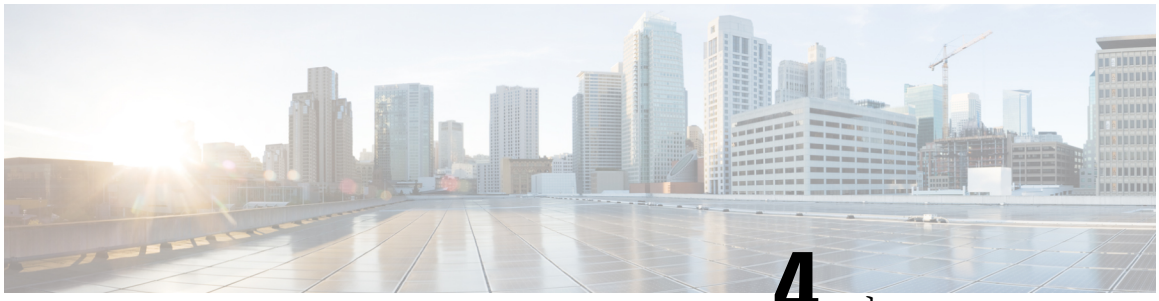
부하 균형 보기

부하 균형 클러스터 마스터는 클러스터의 각 ASA로부터 활성 AnyConnect 및 클라이언트리스 세션의 수 및 구성된 제한 또는 라이센스 제한에 따라 허용된 최대 세션의 수가 포함된 메시지를 주기적으로 수신합니다. 클러스터의 ASA가 100%의 최대 용량을 표시하는 경우 클러스터 마스터는 여기에 추가 연결을 리디렉션할 수 없습니다. ASA가 최대 용량으로 표시되더라도 일부 사용자는 라이센스를 낭비하는 비활성 또는 재개 대기 상태일 수 있습니다. 한 가지 해결 방법으로 각 ASA는 전체 세션

수 대신 비활성 상태인 세션을 제외한 전체 세션 수를 제공합니다. 명령 참조서에서 **-sessiondb summary** 명령을 참조하십시오. 즉, 비활성 세션이 클러스터 마스터에 보고되지 않습니다. ASA가 일부 비활성 세션으로 가득 찬 경우에도 필요한 경우 클러스터 마스터는 여전히 연결을 리디렉션합니다. ASA가 새 연결을 수신하는 경우 새 연결이 해당 라이센스를 사용할 수 있도록 가장 오래 비활성화된 세션이 로그 오프됩니다.

다음 예는 100개의 SSL 세션(활성 세션만 해당) 및 2%의 SSL 부하를 보여줍니다. 이 개수에는 비활성 세션이 포함되지 않습니다. 즉, 비활성 세션은 부하 균형을 위한 부하에 포함되지 않습니다.

```
hostname# show vpn load-balancing
 Status :    enabled
 Role :    Master
 Failover :    Active
 Encryption :    enabled
 Cluster IP :    192.168.1.100
 Peers :    1

 Load %
Sessions
 Public IP     Role   Pri Model    IPsec SSL IPsec SSL
 192.168.1.9   Master 7   ASA-5540 4     2   216   100
 192.168.1.19  Backup 9   ASA-5520 0     0   0     0
```



4 장

일반적인 VPN 매개변수

가상 사설 네트워킹의 ASA 구현에는 범주에 명확하게 적용되지 않는 유용한 기능이 포함되어 있습니다. 이 장에서는 이러한 기능 중 일부에 대해 설명합니다.

지침 및 제한 사항

이 섹션에는 이 기능을 위한 지침 및 제한 사항이 포함되어 있습니다.

상황 모드 지침

단일 및 다중 상황 모드에서 지원합니다. 해당 릴리스의 ASA 일반적인 작업 CLI 구성 가이드에서 다중 상황 모드에서 지원되지 않는 목록에 대한 다중 상황 모드를 위한 지침과, 릴리스 전체에 추가된 내용에 대한 분석을 제공하는 새로운 기능을 참조하십시오.

방화벽 모드 지침

라우팅된 방화벽 모드에서만 지원됩니다. 투명 모드는 지원되지 않습니다.

ACL을 우회하는 IPsec 구성

소스 및 대상 인터페이스에 대한 ACL을 확인하지 않고 IPsec 터널에서부터 오는 모든 패킷을 허용하려면 전역 구성 모드에서 **sysopt connection permit-vpn** 명령을 입력하십시오.

ASA를 지원하는 별도의 VPN Concentrator를 사용하고 ASA 성능을 최대화하려는 경우 IPsec 트래픽에 대한 인터페이스 ACL을 우회하고자 할 수 있습니다. 일반적으로 **access-list** 명령을 사용하여 IPsec 패킷을 허용하는 ACL을 생성하여 소스 인터페이스에 적용합니다. ACL을 사용하면 ASA를 통해 허용하려는 정확한 트래픽을 지정할 수 있습니다.

다음 예에서는 ACL을 확인하지 않고 ASA를 통해 IPsec 트래픽을 활성화합니다.

```
hostname(config)# sysopt connection permit-vpn
```

참고 **no sysopt connection permit-vpn**이 구성되는 경우 **deny ip any any** ACL을 호출하는 외부 인터페이스의 액세스 그룹이 있더라도 클라이언트에서 암호 해독된 통과 트래픽을 허용합니다.

외부 인터페이스의 ACL(Access Control List: 액세스 제어 목록)과 함께 **no sysopt permit-vpn** 명령을 사용하여 사이트 대 사이트 또는 원격 액세스 VPN을 통해 보호된 네트워크에 대한 액세스를 제어하려는 경우 실패합니다.

sysopt connection permit-vpn 해당 관련 트래픽에 대한 암호화 맵이 활성화된 인터페이스의 ACL(수신 및 발신 모두)과 함께 다른 모든 인터페이스의 이그레스(egress)(발신) ACL을 우회하지만 인그레스(ingress)(수신) ACL은 우회하지 않습니다.

이러한 상황에서 내부 관리 액세스가 활성화되어 있는 경우 ACL이 적용되지 않으며 사용자가 SSH를 사용하여 ASA에 계속 연결할 수 있습니다. 내부 네트워크의 호스트에 대한 트래픽은 ACL에 의해 올바르게 차단되지만 내부 인터페이스에 대한 암호 해독된 통과 트래픽은 차단되지 않습니다.

ssh 및 **http** 명령은 ACL보다 우선순위가 높습니다. VPN 세션에서 상자에 대한 SSH, 텔넷 또는 ICMP 트래픽을 거부하려면 **ssh**, **telnet** 및 **icmp** 명령을 사용하십시오.

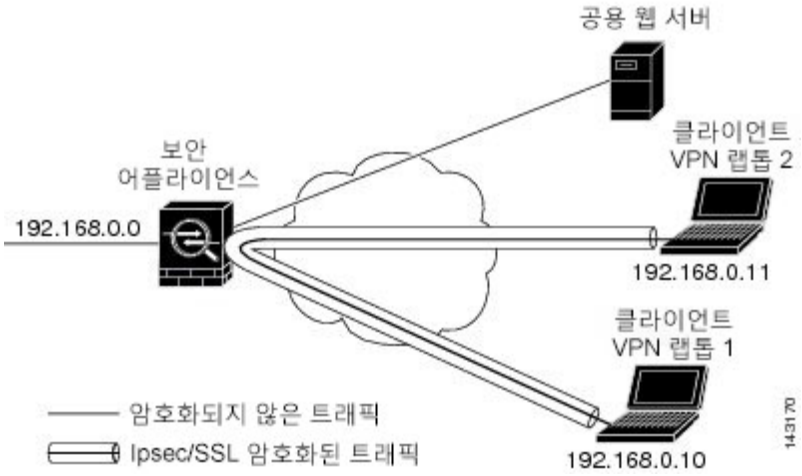
Intra-Interface 트래픽 허용(헤어피닝)

ASA는 VPN 클라이언트에서 IPsec 보호 트래픽을 같은 인터페이스 내부 및 외부에서 허용하여 다른 VPN 사용자에게 전송할 수 있는 기능을 포함합니다. 이 기능은 "헤어피닝(Hairpinning)"이라고도 하며 VPN 허브(ASA)를 통해 연결하는 VPN 스포크(클라이언트)로 간주될 수 있습니다.

헤어피닝은 또한 암호화되지 않은 트래픽과 같이 동일한 인터페이스를 통해 수신 VPN 트래픽을 리디렉션하여 내보낼 수 있습니다. 이 기능은 스플릿 터널링이 없으나 VPN에 액세스하고 웹을 찾아야 하는 VPN 클라이언트 등에 유용할 수 있습니다.

아래 그림에서는 보안 IPsec 트래픽을 VPN Client 2에 전송하는 동시에 암호화되지 않은 트래픽을 공용 웹 서버에 전송하는 VPN Client 1을 보여줍니다.

그림 3: 헤어피닝의 *Intra-Interface* 기능을 사용하는 *VPN* 클라이언트



이 기능을 구성하려면 intra-interface 인수와 함께 전역 구성 모드에서 **same-security-traffic** 명령을 사용하십시오.

명령 구문은 same-security-traffic permit {*inter-interface* | *intra-interface*}입니다.

다음 예는 intra-interface 트래픽을 활성화하는 방법을 보여줍니다.

```
hostname(config)# same-security-traffic permit intra-interface
hostname(config)#
```

참고 같은 보안 수준의 인터페이스 간 통신을 허용하기 위해 **same-security-traffic** 명령을 **inter-interface** 인수와 함께 사용하십시오. 이 기능은 IPsec 연결에만 국한되지 않습니다. 자세한 내용은 본 설명서의 "인터페이스 매개변수 구성"장을 참조하십시오.

헤어피닝을 사용하려면 Intra-Interface 트래픽에 대한 NAT 고려 사항에서 설명한 바와 같이 적절한 NAT 규칙을 ASA 인터페이스에 적용해야 합니다.

Intra-Interface 트래픽에 대한 NAT 고려 사항

ASA의 경우 암호화되지 않은 트래픽을 인터페이스를 통해 되돌려 보내려면 로컬 IP 주소 풀에서 공용 IP 주소를 이미 사용하지 않는 한 공개적으로 라우팅할 수 있는 주소가 사설 IP 주소를 바꿀 수 있도록 인터페이스에 대한 NAT를 활성화해야 합니다. 다음 예는 인터페이스 PAT 규칙을 클라이언트 IP 풀에서 제공된 트래픽에 적용합니다.

```
hostname(config)# ip local pool clientpool 192.168.0.10-192.168.0.100
hostname(config)# object network vpn_nat
hostname(config-network-object)# subnet 192.168.0.0 255.255.255.0
hostname(config-network-object)# nat (outside,outside) interface
```

그러나 ASA가 암호화된 VPN 트래픽을 같은 인터페이스로 되돌려 보내는 경우 NAT는 선택 사항입니다. VPN-to-VPN 헤어피닝은 NAT와 함께 또는 NAT 없이 작동합니다. NAT를 모든 나가는 트래픽에 적용하려면 위에서 사용한 명령만 구현하십시오. NAT에서 VPN-to-VPN 트래픽을 제외하려면 다음과 같이 VPN-to-VPN 트래픽에 대한 NAT 제외를 구현하는 명령을 위의 예에 추가하십시오.

```
hostname(config)# nat (outside,outside) source static vpn_nat vpn_nat destination static
vpn_nat vpn_nat
```

NAT 규칙에 대한 자세한 내용은 본 설명서의" NAT 적용" 장을 참조하십시오.

최대 활성 IPsec 또는 SSL VPN 세션 설정

VPN 세션을 ASA가 허용하는 것보다 더 낮은 값으로 제한하려면 다음과 같이 전역 구성 모드에서 **vpn-sessiondb** 명령을 입력하십시오.

vpn-sessiondb {**max-anyconnect-premium-or-essentials-limit** <number> | **max-other-vpn-limit** <number>}

max-anyconnect-premium-or-essentials-limit 키워드는 AnyConnect 세션의 최대 수를 지정하며 그 범위는 1부터 라이선스에서 허용하는 최대 세션 수까지입니다.

참고 올바른 라이선싱, 기간, 계층 및 사용자 수는 더 이상 이 명령으로 결정되지 않습니다. 다음의 AnyConnect 주문 가이드를 참조하십시오. http://www.cisco.com/c/dam/en/us/products/collateral/security/anyconnect-og.pdf

max-other-vpn-limit 키워드는 AnyConnect 클라이언트 세션 이외의 VPN 세션의 최대 수를 지정하며 그 범위는 1부터 라이선스에서 허용하는 최대 세션 수까지 입니다. 여기에는 Cisco VPN 클라이언트(IPsec IKEv1) 및 Lan-to-Lan VPN 세션이 포함됩니다.

이러한 제한은 VPN 부하 균형의 계산된 부하 백분율에 적용됩니다.

다음 예는 최대 Anyconnect VPN 세션 제한을 450으로 설정하는 방법을 보여줍니다.

```
hostname(config)# vpn-sessiondb max-anyconnect-premium-or-essentials-limit 450
hostname(config)#
```

허용 가능한 IPsec 클라이언트 수정 수준을 보장하는 클라이언트 업데이트 사용

참고 이 섹션의 정보는 IPsec 연결에만 적용됩니다.

클라이언트 업데이트 기능을 사용하면 중앙 위치에 있는 관리자가 VPN 클라이언트 사용자에게 VPN 클라이언트 소프트웨어의 업데이트 시기를 자동으로 알려줍니다.

원격 사용자가 기한이 지난 VPN 하드웨어 또는 소프트웨어 클라이언트 버전을 사용 중일 수 있습니다. 언제든지 **client-update** 명령을 사용하여 클라이언트 수정 버전으로 업데이트할 수 있습니다. 해당 명령을 통해 업데이트를 적용할 클라이언트의 유형 및 수정 번호를 지정하며 업데이트를 가져올 URL 또는 IP 주소를 제공할 수 있습니다. Windows 클라이언트의 경우 필요에 따라 VPN 클라이언트 버전을 업데이트해야 하는 사용자에게 알림을 제공합니다. Windows 클라이언트의 경우 사용자에게 해당 업데이트를 수행하는 메커니즘을 제공할 수 있습니다. 해당 명령은 IPsec remote-access tunnel-group 유형에만 적용됩니다.

클라이언트 업데이트를 수행하려면 일반 구성 모드나 터널 그룹 ipsec 속성 구성 모드에서 **client-update** 명령을 입력하십시오. 클라이언트가 이미 수정 번호 목록에 있는 소프트웨어 버전을 실행하고 있는 경우 해당 소프트웨어를 업데이트할 필요가 없습니다. 클라이언트가 목록에 있는 소프트웨어 버전을 실행하고 있지 않은 경우 해당 소프트웨어를 업데이트하십시오. 다음 절차는 클라이언트 업데이트를 수행하는 방법에 대해 설명합니다.

프로시저

단계 **1** 전역 구성 모드에서 다음 명령을 입력하여 클라이언트 업데이트를 활성화하십시오.

```
hostname(config)# client-update enable
hostname(config)#
```

단계 **2** 전역 구성 모드에서 특정 유형의 모든 클라이언트에 적용하려는 클라이언트 업데이트의 매개변수를 지정하십시오. 즉 클라이언트의 유형, 업데이트된 이미지를 가져올 URL 또는 IP 주소 및 해당 클라이언트에 허용 가능한 하나 이상의 수정 번호를 지정하십시오. 최대 4개의 수정 번호를 쉼표로 구분하여 지정할 수 있습니다.

사용자의 클라이언트 수정 번호가 지정된 수정 번호 중 하나와 일치하는 경우 클라이언트를 업데이트하지 않아도 됩니다. 이 명령은 전체 ASA에서 지정된 유형의 모든 클라이언트에 대한 클라이언트 업데이트 값을 지정합니다.

다음 구문을 사용하십시오.

```
hostname(config)# client-update type type url url-string rev-nums rev-numbers
hostname(config)#
```

사용 가능한 클라이언트 유형은 **win9X**(Windows 95, Windows 98 및 Windows ME 플랫폼 포함), **winnt**(Windows NT 4.0, Windows 2000 및 Windows XP 플랫폼 포함), **windows**(모든 Windows 기반 플랫폼 포함)입니다.

클라이언트가 이미 수정 번호 목록에 있는 소프트웨어 버전을 실행하고 있는 경우 해당 소프트웨어를 업데이트할 필요가 없습니다. 클라이언트가 목록에 있는 소프트웨어 버전을 실행하고 있지 않은 경우 해당 소프트웨어를 업데이트하십시오. 이 클라이언트 업데이트 항목 중 최대 3개를 지정할 수 있습니다. 키워드 **windows**는 모든 허용 가능한 Windows 플랫폼을 지원합니다. **windows**를 지정한 경우 개별 Windows 클라이언트 유형을 지정하지 마십시오.

참고 모든 Windows 클라이언트의 경우 URL의 접두사로 http:// 또는 https:// 프로토콜을 사용해야 합니다.

다음 예에서는 원격 액세스 터널 그룹에 대한 클라이언트 업데이트 매개변수를 구성합니다. 수정 번호를 4.6.1로, 업데이트 검색용 URL을 https://support/updates로 지정합니다.

```
hostname(config)# client-update type windows url https://support/updates/ rev-nums 4.6.1
hostname(config)#
```

또는 특정 유형의 모든 클라이언트가 아닌 개별 터널 그룹에 대한 클라이언트 업데이트를 구성할 수 있습니다. (3단계를 참조)

참고 **https://support/updates/vpnclient.exe**와 같이 URL의 끝에 애플리케이션의 이름을 포함하여 브라우저가 자동으로 애플리케이션을 시작하도록 할 수 있습니다.

단계 **3** 특정 ipsec-ra 터널 그룹에 대한 client-update 매개변수 집합을 정의하십시오.

tunnel-group ipsec-attributes 모드에서 터널 그룹 이름과 유형, 업데이트된 이미지를 가져올 URL 또는 IP 주소 및 수정 번호를 지정하십시오. 사용자의 클라이언트 수정 번호가 지정된 수정 번호 중 하나와 일치하는 경우 클라이언트를 업데이트하지 않아도 됩니다. 예를 들어 Windows 클라이언트의 경우 다음 명령을 입력하십시오.

```
hostname(config)# tunnel-group remotegrp type ipsec-ra
hostname(config)# tunnel-group remotegrp ipsec-attributes
hostname(config-tunnel-ipsec)# client-update type windows url https://support/updates/
rev-nums 4.6.1
hostname(config-tunnel-ipsec)#
```

단계 **4** (선택 사항) 기한이 지난 Windows 클라이언트를 사용하는 활성 사용자에게 클라이언트 업데이트가 필요하다는 알림을 보냅니다. 이러한 사용자에게 브라우저를 열고 URL에서 지정한 사이트에서 업데이트된 소프트웨어를 다운로드할 수 있는 팝업 창이 표시됩니다. 해당 메시지에서 사용자는 URL만 구성할 수 있습니다. (2단계 또는 3단계 참조) 활성 상태가 아닌 사용자는 다음에 로그온할 때 알림 메시지를 받습니다. 모든 터널 그룹의 모든 활성 클라이언트 또는 특정 터널 그룹의 클라이언트로 알림을 보낼 수 있습니다. 예를 들어 모든 터널 그룹의 모든 활성 클라이언트에게 알림을 보내려면 특권 EXEC 모드에서 다음 명령을 입력하십시오.

```
hostname# client-update all
hostname#
```

사용자의 클라이언트 수정 번호가 지정된 수정 번호 중 하나와 일치하는 경우 클라이언트를 업데이트할 필요가 없으며 사용자에게 알림 메시지가 전달되지 않습니다.

다음에 수행할 작업

참고 client-update 유형을 모든 Windows 기반 플랫폼을 지정하는 **windows**로 지정하고 같은 엔터티에 대해 **win9x** 또는 **winnt**의 client-update 유형을 나중에 입력하려는 경우 **no** 형식의 명령을 사용하여 windows 클라이언트 유형을 먼저 제거한 다음 새 client-update 명령을 사용하여 새 클라이언트 유형을 지정하십시오.

NAT 할당 IP를 공용 IP 연결에 구현

드문 경우이지만 할당된 로컬 IP 주소 대신 내부 네트워크에 있는 VPN 피어의 실제 IP 주소를 사용하고자 할 수 있습니다. 일반적으로 VPN을 사용하면 내부 네트워크에 액세스할 수 있는 로컬 IP 주소가 피어에 할당됩니다. 그러나 내부 서버 및 네트워크 보안이 피어의 실제 IP 주소를 기반으로 하는 경우와 같이 로컬 IP 주소를 피어의 실제 공용 주소로 다시 변환하고자 할 수 있습니다.

Cisco ASA 55xx에서는 내부 또는 보호된 네트워크의 VPN 클라이언트의 할당된 IP 주소를 공용(소스) IP 주소로 변환할 수 있는 방법을 도입했습니다. 이 기능은 내부 네트워크 및 네트워크 보안 정책의 대상 서버 또는 서비스에 내부 기업 네트워크에 할당된 IP 대신 VPN 클라이언트의 공용 또는 소스 IP와 통신이 필요한 경우의 시나리오를 지원합니다.

터널 그룹당 1개의 인터페이스에서 해당 기능을 활성화할 수 있습니다. VPN 세션이 설정되거나 연결이 해제되면 개체 NAT 규칙이 동적으로 추가 및 삭제됩니다.

라우팅 문제로 인해 필요한 경우에만 이 기능을 사용하는 것이 좋습니다.

- 레거시(IKEv1) 및 AnyConnect 클라이언트만 지원합니다.
- NAT 정책 및 VPN 정책을 적용하려면 공용 IP 주소에 반환 트래픽을 ASA로 다시 라우팅해야 합니다.
- 할당된 IPv4 및 공용 주소만 지원합니다.
- NAT/PAT 디바이스 뒤에 있는 여러 개의 피어를 지원하지 않습니다.
- 라우팅 문제로 인해 부하 균형을 지원하지 않습니다.
- 로밍을 지원하지 않습니다.

프로시저

단계 **1** 전역 구성 모드에서 **tunnel general**을 입력하십시오.

단계 **2** 주소 변환을 활성화하려면 다음 구문을 사용하십시오.

```
hostname(config-tunnel-general)# nat-assigned-to-public-ip interface
```

이 명령은 할당된 IP 주소의 NAT 정책을 소스의 공용 IP 주소에 동적으로 설치합니다. *interface*는 NAT를 적용할 위치를 결정합니다.

단계 **3** 주소 변환을 비활성화하려면 다음 구문을 사용하십시오.

```
hostname(config-tunnel-general)# no nat-assigned-to-public-ip
```

VPN NAT 정책 표시

주소 변환은 기본 객체 NAT 메커니즘을 사용하므로 VPN NAT 정책이 수동으로 구성된 객체 NAT 정책과 같이 표시됩니다. 다음 예에서는 할당된 IP로 95.1.226.4를 사용하고 피어의 공용 IP로 75.1.224.21을 사용합니다.

```
hostname# show nat
Auto NAT Policies (Section 2)
1 (outside) to (inside) source static _vpn_nat_95.1.226.4 75.1.224.21
    translate_hits = 315, untranslate_hits = 315

prompt# show nat detail

Auto NAT Policies (Section 2)
1 (outside) to (inside) source static _vpn_nat_95.1.226.4 75.1.224.21
    translate_hits = 315, untranslate_hits = 315
    Source - Origin: 95.1.226.4/32, Translated: 75.1.224.21/32
```

*Outside*는 AnyConnect 클라이언트가 연결할 인터페이스이고 *inside*는 새로운 터널 인터페이스 그룹에 한정된 인터페이스입니다.

참고 VPN NAT 정책은 동적이고 구성에 추가되지 않으므로 VPN NAT 객체 및 NAT 정책은 show run 객체 및 show run nat 보고서에 나타나지 않습니다.

VPN 세션 제한 구성

플랫폼과 ASA 라이선스가 지원하는 만큼 IPsec 및 SSL VPN 세션을 실행할 수 있습니다. ASA의 최대 세션 수를 포함한 라이선싱 정보를 보려면 전역 구성 모드에서 **show version** 명령을 입력하고 라이선싱 섹션을 찾아보십시오. 다음 예는 명령 및 이 명령의 출력에서 나타나는 라이선싱 정보를 보여줍니다. 다른 출력은 명확히 알 수 있도록 삭제했습니다.

```
hostname(config)# show version
...
Licensed features for this platform:
Maximum Physical Interfaces       : Unlimited      perpetual
Maximum VLANs                     : 500            perpetual
Inside Hosts                      : Unlimited      perpetual
Failover                          : Active/Active  perpetual
```

```
Encryption-DES                    : Enabled        perpetual
Encryption-3DES-AES               : Enabled        perpetual
Security Contexts                 : 100            perpetual
Carrier                           : Enabled        perpetual
AnyConnect Premium Peers          : 5000           perpetual
AnyConnect Essentials             : 5000           perpetual
Other VPN Peers                   : 5000           perpetual
Total VPN Peers                   : 5000           perpetual
AnyConnect for Mobile             : Enabled        perpetual
AnyConnect for Cisco VPN Phone    : Enabled        perpetual
Advanced Endpoint Assessment      : Enabled        perpetual
Shared License                    : Disabled       perpetual
Total TLS Proxy Sessions          : 3000           perpetual
Botnet Traffic Filter             : Disabled       perpetual
IPS Module                        : Disabled       perpetual
Cluster                           : Enabled        perpetual
Cluster Members                   : 2              perpetual

This platform has an ASA5555 VPN Premium license.
```

라이선스 리소스 할당 표시

리소스 할당을 표시하려면 다음 명령을 사용합니다.

```
asa2(config)# sh resource allocation
Resource       Total    % of Avail
Conns[rate]    100(U)      0.00%
Inspects[rate] unlimited
Syslogs[rate]  unlimited
Conns          unlimited
Hosts          unlimited
IPsec          unlimited
Mac-addresses  unlimited
ASDM           10          5.00%
SSH            10          10.00%
Telnet         10          10.0%
Xlates         unlimited
AnyConnect     1000        10%
AnyConnectBurst 200        2%
OtherVPN       2000        20%
OtherVPNBurst  1000        10%
```

라이선스 리소스 사용량 표시

리소스 사용량을 표시하려면 다음 명령을 사용합니다.

참고 **sh resource usage system controller all 0** 명령을 사용하여 플랫폼 제한으로 제한을 설정하여 시스템 레벨 사용량을 표시할 수도 있습니다.

```
ASA(config-ca-trustpoint)# sh resource usage
Resource        Current  Peak  Limit  Denied  Context
Conns           1        16    280000 0       System
Hosts           2        10    N/A    0       System
AnyConnect      2        25    1000   0       cust1
AnyConnectBurst 0        0     200    0       cust1
OtherVPN        1        1     2000   0       cust2
OtherVPNBurst   0        0     1000   0       cust2
```

VPN 세션 제한

AnyConnect VPN 세션(IPsec/IKEv2 또는 SSL)을 ASA에서 허용하는 것보다 낮은 값으로 제한하려면 전역 구성 모드에서 **vpn-sessiondb** max-anyconnect-premium-or-essentials-limit 명령을 사용하십시오. 세션 제한을 해제하려면 다음 명령의 **no** 버전을 사용하십시오.

ASA 라이선스가 SSL VPN 세션 500개를 허용할 때 AnyConnect VPN 세션의 수를 250개로 제한하려면 다음 명령을 입력하십시오.

```
hostname(config)# vpn-sessiondb max-anyconnect-premium-or-essentials-limit 250
hostname(config)#
```

세션 제한을 해제하려면 다음 명령의 **no** 버전을 사용하십시오.

```
hostname(config)# no vpn-sessiondb max-anyconnect-premium-or-essentials-limit 250
hostname(config)#
```

협상 시 ID 인증서 사용

AnyConnect 클라이언트와 IKEv2 터널을 협상할 때 ASA는 ID 인증서를 사용해야 합니다. IKEv2 원격 액세스 신뢰 지점을 구성하려면 다음 명령을 사용하십시오.

```
crypto ikev2 remote-access trustpoint <name> [line<number>]
```

이 명령을 사용하면 AnyConnect 클라이언트가 엔드 유저의 그룹 선택을 지원할 수 있습니다. RSA 2개, ECDSA 2개 또는 각 1개씩에서 2개의 신뢰 지점을 동시에 구성할 수 있습니다. ASA는 구성된 신뢰 지점 목록을 검사하고 클라이언트가 지원하는 첫 번째 신뢰 지점을 선택합니다. ECDSA를 선호할 경우 이 신뢰 지점을 RSA 신뢰 지점보다 먼저 구성해야 합니다.

회선 번호 옵션은 원하는 회선 번호에서 신뢰 지점이 삽입되는 위치를 지정합니다. 일반적으로 이 옵션은 다른 회선을 제거하거나 다시 연결하지 않고 최상위 신뢰 지점을 삽입하는 데 사용됩니다. 회선을 지정하지 않은 경우 ASA가 목록의 끝에 신뢰 지점을 추가합니다.

이미 존재하는 신뢰 지점을 추가하려는 경우 오류 메시지가 표시됩니다. 제거할 신뢰 지점 이름을 지정하지 않고 *no crypto ikev2 remote-access trustpoint* 명령을 사용할 경우 모든 신뢰 지점 구성이 제거됩니다.

암호화 코어 풀 구성

SMP(Symmetric Multi-Processing: 대칭적 다중 처리) 플랫폼에서 암호화 코어의 할당을 변경하여 AnyConnect TLS/DTLS 트래픽의 처리량을 늘릴 수 있습니다. 변경을 통해 SSL VPN 데이터 경로를 가속화하고 AnyConnect, 스마트 터널 및 포트 전달에서 눈에 띄는 성능 향상을 제공할 수 있습니다. 다음 단계에서는 단일 또는 다중 상황 모드에서 암호화 코어의 풀 구성을 설명합니다.

다음 플랫폼에서 암호화 코어 균형 다시 맞추기 작업을 할 수 있습니다.

- 5585-X
- 5545-X
- 5555-X
- ASASM

프로시저

암호화 가속화 프로세서를 할당하는 방법을 지정합니다.

crypto engine accelerator-bias

- **balanced** — 암호화 하드웨어 리소스(Admin/SSL 및 IPsec 코어)를 동등하게 배포합니다.
- **ipsec** — IPsec을 지원하도록 암호화 하드웨어 리소스를 할당합니다(SRTP 암호화된 음성 트래픽 포함).
- **ssl** — Admin/SSL을 지원하도록 암호화 하드웨어 리소스를 할당합니다.

예제:

```
hostname(config)# crypto engine ?

configure mode commands/options:
accelerator-bias
Specify how to allocate crypto accelerator processors

hostname(config)# crypto engine accelerator-bias ?
configure mode commands/options
balanced - Equally distribute crypto hardware resources
ipsec - Allocate crypto hardware resources to favor IPsec/Encrypted Voice (SRTP)
ssl - Allocate crypto hardware resources to favor SSL

hostname(config)# crypto engine accelerator-bias ssl
```

활성 VPN 세션 보기

다음 주제에서는 VPN 세션 정보를 보는 방법을 설명합니다.

IP 주소 유형별 활성 AnyConnect 세션 보기

명령행 인터페이스를 사용하여 활성 AnyConnect 세션을 보려면 특권 EXEC 모드에서 **show vpn-sessiondb anyconnect filter p-ipversion** 또는 **show vpn-sessiondb anyconnect filter a-ipversion** 명령을 입력하십시오.

- 엔드포인트의 공용 IPv4 또는 IPv6 주소에 따라 필터링한 활성 AnyConnect 세션을 표시합니다. 공용 주소는 기업에서 엔드포인트로 할당한 주소입니다.

  ```
  show vpn-sessiondb anyconnect filter p-ipversion {v4 | v6}
  ```

- 엔드포인트의 할당된 IPv4 또는 IPv6 주소에 따라 필터링한 활성 AnyConnect 세션을 표시합니다. 할당된 주소는 ASA에 의해 AnyConnect Secure Mobility Client로 할당된 주소입니다.

  ```
  show vpn-sessiondb anyconnect filter a-ipversion {v4 | v6}
  ```

show vpn-sessiondb anyconnect filter p-ipversion [v4 | v6] 명령의 출력 예

```
hostname(config)# show vpn-sessiondb anyconnect filter p-ipversion v4

Session Type: AnyConnect

Username     : user1                  Index        : 40
Assigned IP  : 192.168.17.10          Public IP    : 198.51.100.1
Protocol     : AnyConnect-Parent SSL-Tunnel
License      : AnyConnect Premium
Encryption   : AnyConnect-Parent: (1)none  SSL-Tunnel: (1)RC4
Hashing      : AnyConnect-Parent: (1)none  SSL-Tunnel: (1)SHA1
Bytes Tx     : 10570                  Bytes Rx     : 8085
Group Policy : GroupPolicy_SSLACCLIENT
Tunnel Group : SSLACCLIENT
Login Time   : 15:17:12 UTC Mon Oct 22 2012
Duration     : 0h:00m:09s
Inactivity   : 0h:00m:00s
NAC Result   : Unknown
VLAN Mapping : N/A                    VLAN         : none
```

show vpn-sessiondb anyconnect filter a-ipversion [v4 | v6] 명령의 출력

```
hostname(config)# show vpn-sessiondb anyconnect filter a-ipversion v6

Session Type: AnyConnect

Username     : user1                  Index        : 45
Assigned IP  : 192.168.17.10
Public IP    : 2001:DB8:8:1:90eb:3fe5:9eea:fb29
```

```
Assigned IPv6: 2001:DB8:9:1::24
Protocol     : AnyConnect-Parent SSL-Tunnel
License      : AnyConnect Premium
Encryption   : AnyConnect-Parent: (1)none  SSL-Tunnel: (1)RC4
Hashing      : AnyConnect-Parent: (1)none  SSL-Tunnel: (1)SHA1
Bytes Tx     : 10662                 Bytes Rx     : 17248
Group Policy : GroupPolicy_SSL_IPv6  Tunnel Group : SSL_IPv6
Login Time   : 17:42:42 UTC Mon Oct 22 2012
Duration     : 0h:00m:33s
Inactivity   : 0h:00m:00s
NAC Result   : Unknown
VLAN Mapping : N/A                   VLAN         : none
```

IP 주소 유형별 활성 클라이언트리스 SSL VPN 세션 보기

명령행 인터페이스를 사용하여 활성 클라이언트리스 SSL VPN 세션을 보려면 특권 EXEC 모드에서 **show vpn-sessiondb webvpn filter ipversion** 명령을 입력하십시오.

공용 주소는 기업에서 엔드포인트로 할당한 주소입니다.

show vpn-sessiondb webvpn filter ipversion {v4 | v6}

예

```
hostname# sh vpn-sessiondb webvpn filter ipversion v4

Session Type: WebVPN

Username     : user1                 Index        : 63
Public IP    : 171.16.17.6
Protocol     : Clientless
License      : AnyConnect Premium
Encryption   : Clientless: (1)RC4    Hashing      : Clientless: (1)SHA1
Bytes Tx     : 62454                 Bytes Rx     : 13082
Group Policy : SSLv6                 Tunnel Group : SSL_IPv6
Login Time   : 18:07:48 UTC Mon Oct 22 2012
Duration     : 0h:00m:16s
Inactivity   : 0h:00m:00s
NAC Result   : Unknown
VLAN Mapping : N/A                   VLAN         : none
```

IP 주소 유형별 활성 LAN-to-LAN VPN 세션 보기

명령행 인터페이스를 사용하여 활성 클라이언트리스 SSL VPN 세션을 보려면 특권 EXEC 모드에서 **show vpn-sessiondb l2l filter ipversion** 명령을 입력하십시오.

이 명령은 연결의 공용 IPv4 또는 IPv6 주소에 따라 필터링한 활성 LAN-to-LAN VPN 세션을 보여줍니다.

공용 주소는 기업에서 엔드포인트로 할당한 주소입니다.

show vpn-sessiondb l2l filter ipversion {v4 | v6}

ISE 정책 시행 정보

Cisco ISE(Identity Services Engine)는 보안 정책 관리 및 제어 플랫폼입니다. 유선, 무선 및 VPN 연결의 액세스 제어와 보안 컴플라이언스를 자동화하고 간소화해줍니다. Cisco ISE는 주로 Cisco TrustSec과 연계하여 보안 액세스 및 게스트 액세스를 제공하고 BYOD(Bring Your Own Device) 이니셔티브를 지원하고 사용량 정책을 적용하는 데 쓰입니다.

ISE CoA(Change of Authorization: 권한 부여 변경) 기능은 설정 후 AAA(인증, 권한 부여 및 계정 관리) 세션의 특성을 변경하는 메커니즘을 제공합니다. 정책이 AAA의 사용자 또는 사용자 그룹을 변경하는 경우 CoA 패킷이 ISE에서 ASA로 직접 연결되어 인증을 다시 시작하고 새 정책을 적용할 수 있습니다. IPEP(Inline Posture Enforcement Point: 인라인 상태 시행 지점)에는 ASA로 설정된 각 VPN 세션에 대한 ACL(Access Control List: 액세스 제어 목록)이 필요하지 않습니다.

ISE 정책 시행은 다음과 같은 VPN 클라이언트에서 지원됩니다.

- IPSec
- AnyConnect
- L2TP/IPSec

참고 dACL(Dynamic ACL) 및 SGT(Security Group Tag)와 같은 일부 정책 요소는 지원되지만, VLAN 할당 및 IP 주소 할당과 같은 정책 요소는 지원되지 않습니다.

시스템 흐름은 다음과 같습니다.

1. 엔드 유저가 VPN 연결을 요청합니다.
2. ASA가 ISE에 대한 사용자를 인증하고 네트워크에 제한된 액세스를 제공하는 사용자 ACL을 수신합니다.
3. 세션을 등록할 수 있도록 계정 관리 시작 메시지가 ISE로 전송됩니다.
4. NAC 에이전트 및 ISE 간에 직접 상태 평가가 이루어집니다. 이 프로세스는 ASA에 투명성을 제공합니다.
5. ISE는 CoA "정책 푸시"를 통해 ASA에 정책 업데이트를 전송합니다. 이는 강화된 네트워크 액세스 권한을 제공하는 새 사용자 ACL을 식별합니다.

참고 연결 수명 동안 후속 CoA 업데이트를 통해 ASA에 투명성을 제공하는 추가 정책 평가가 발생할 수 있습니다.

ISE 정책 시행을 위해 RADIUS 서버 그룹 구성

ISE 정책 평가 및 적용을 활성화하려면 ISE 서버에 대한 RADIUS AAA 서버 그룹을 구성하고 그룹에 서버를 추가합니다. VPN에 대한 터널 그룹을 구성할 때 그룹에서 AAA 서비스에 대한 이 서버 그룹을 지정합니다.

프로시저

단계 **1** RADIUS AAA 서버 그룹을 생성합니다.

aaa-server *group_name* **protocol radius**

```
hostname(config)# aaa-server servergroup1 protocol radius
hostname(config-aaa-server-group)#
```

단계 **2** AAA 서버 그룹에 대한 RADIUS 동적 권한 부여(CoA) 서비스를 활성화합니다.

dynamic-authorization[**port** *number*]

포트를 지정하는 것은 선택 사항입니다. 기본값은 1700이고, 범위는 1024~65535입니다.

VPN 터널에서 서버 그룹을 사용하면 RADIUS 서버 그룹이 CoA 알림에 등록되고 ASA는 ISE에서 보내는 CoA 정책 업데이트를 포트에서 수신합니다.

```
hostname(config-aaa-server-group)# dynamic-authorization
```

단계 **3** 인증에 ISE를 사용하지 않으려면 RADIUS 서버 그룹에 대해 권한 부여 전용 모드를 활성화합니다.

authorize-only

이것은 이 서버 그룹이 권한 부여에 사용될 때 RADIUS Access Request 메시지가 AAA 서버에 대해 정의된 구성된 비밀번호 방식이 아니라 "Authorize Only" 요청으로 작성됨을 의미합니다. RADIUS 서버에 대한 **radius-common-pw** 명령을 사용하여 공통 비밀번호를 구성하지 않으면 무시됩니다.

예를 들어, 인증에 이 서버 그룹보다 인증서를 사용하려면 권한 부여 전용 모드를 사용합니다. VPN 터널에서 권한 부여 및 어카운팅에 대한 이 서버 그룹을 계속 사용합니다.

```
hostname(config-aaa-server-group)# authorize-only
```

단계 **4** RADIUS interim-accounting-update 메시지를 정기적으로 생성하도록 활성화합니다.

interim-accounting-update [**periodic** [*hours*]]

ISE는 ASA와 같은 NAS 디바이스에서 수신하는 어카운팅 레코드를 기반으로 하는 활성 세션의 디렉터리를 유지합니다. 그러나 ISE가 5일 동안 세션이 여전히 활성 상태(어카운팅 메시지 또는 포스처 트랜잭션)임을 나타내는 메시지를 수신하지 않은 경우 데이터베이스에서 세션 레코드를 제거합니다. 장기 VPN 연결이 제거되지 않도록 하려면 모든 활성 세션에 대해 정기적으로 ISE에 interim-accounting-update 메시지를 전송하도록 그룹을 구성합니다.

- **periodic** [*hours*]는 문제의 서버 그룹으로 계정 관리 기록을 전송하도록 구성된 모든 VPN 세션에 대한 계정 관리 기록의 주기적 생성 및 전송을 활성화합니다. 선택적으로 이러한 업데이트를 전송할 간격을 시간 단위로 포함할 수 있습니다. 기본값은 24시간, 범위는 1~120입니다.
- (매개변수가 없습니다.) **periodic** 키워드 없이 이 명령을 사용하는 경우 VPN 터널 연결이 클라이언트리스 VPN 세션에 추가될 경우에만 ASA에서 interim-accounting-update 메시지를 전송합니다. 이 경우 어카운팅 업데이트가 생성되어 RADIUS 서버에 새로 할당된 IP 주소를 알려줍니다.

```
hostname(config-aaa-server-group)# interim-accounting-update periodic 12
```

단계 **5** (선택 사항). RADIUS 패킷에서 Cisco AV 쌍으로 수신된 ACL과 다운로드 가능한 ACL을 병합합니다.

merge-dacl {**before-avpair** | **after-avpair**}

이 옵션은 VPN 연결에만 적용됩니다. VPN 사용자의 경우 ACL은 Cisco AV 쌍 ACL, 다운로드 가능한 ACL 및 ASA에서 구성된 ACL의 형식이 될 수 있습니다. 이 옵션은 다운로드 가능한 ACL과 AV 쌍 ACL의 병합 여부를 결정하며 ASA에 구성된 ACL에는 적용되지 않습니다.

기본 설정은 다운로드 가능한 ACL을 Cisco AV 쌍 ACL과 병합하지 않도록 지정하는 **no merge dacl** 입니다. AV 쌍과 다운로드 가능한 ACL이 모두 수신되는 경우 AV 쌍이 우선 사용됩니다.

before-avpair 옵션은 다운로드 가능한 ACL 항목이 Cisco AV 쌍 항목 앞에 배치되도록 지정합니다.

after-avpair 옵션은 다운로드 가능한 ACL 항목이 Cisco AV 쌍 항목 뒤에 배치되도록 지정합니다.

```
hostname(config)# aaa-server servergroup1 protocol radius
hostname(config-aaa-server-group)# merge-dacl before-avpair
```

단계 **6** (선택 사항). 다음 서버를 시도하기 전에 그룹의 RADIUS 서버로 보낼 수 있는 최대 요청 횟수를 지정합니다.

max-failed-attempts *number*

범위는 1~5입니다. 기본값은 3입니다.

로컬 데이터베이스를 사용하여 장애 조치 방법을 구성한 경우(관리 액세스에만 해당) 그룹의 모든 서버가 응답하지 않으면 그룹이 응답하지 않는 것으로 간주되고 장애 조치 방법이 시도됩니다. 서버 그룹은 10분(기본값) 동안 무응답으로 표시됩니다. 그러면 이 기간에 다른 AAA 요청에서 서버 그룹 접속을 시도하지 않으며 즉시 대비책이 사용됩니다. 무응답 기간을 기본값이 아닌 값으로 변경하려면 다음 단계의 **reactivation-mode** 명령을 참조하십시오.

대비책이 없는 경우 ASA는 그룹의 서버를 계속 재시도합니다.

```
hostname(config-aaa-server-group)# max-failed-attempts 2
```

단계 **7** (선택 사항). 그룹에서 실패한 서버가 다시 활성화되는 방법(재활성화 정책)을 지정합니다.

reactivation-mode {**depletion** [**deadtime** *minutes*] | **timed**}

여기서 각 항목은 다음을 나타냅니다.

- **depletion** [**deadtime** *minutes*]는 그룹의 모든 서버가 비활성되어야만 실패한 서버를 재활성화합니다. 이것이 기본 재활성화 모드입니다. 그룹의 마지막 서버를 비활성화한 시점부터 나중에 모든 서버를 다시 활성화한 시점까지 경과한 시간을 0~1440분 범위에서 지정할 수 있습니다. 기본은 10분입니다.
- **timed** 가동 중단되고 30초가 지나면 실패한 서버를 재활성화합니다.

```
hostname(config-aaa-server-group)# reactivation-mode deadtime 20
```

단계 **8** (선택 사항). 그룹의 모든 서버에 어카운팅 메시지를 전송합니다.

accounting-mode simultaneous

활성 서버로만 메시지를 전송하는 기본 설정을 복원하려면 **accounting-mode single** 명령을 입력합니다.

```
hostname(config-aaa-server-group)# accounting-mode simultaneous
```

단계 **9** ISE RADIUS 서버를 그룹에 추가합니다.

aaa-server*group_name* [(*interface_name*)] **host** {*server_ip* | *name*} [*key*]

여기서 각 항목은 다음을 나타냅니다.

- *group_name*은 RADIUS 서버 그룹의 이름입니다.
- (*interface_name*)은 서버에 도달하기 위해 통과할 인터페이스의 이름입니다. 기본값은 (내부)입니다. 괄호가 필요합니다.
- **host** {*server_ip* | *name*}은 ISE RADIUS 서버의 IP 주소 또는 호스트 이름입니다.
- *key*는 연결을 암호화할 선택적 키입니다. aaa-server-host 모드를 입력하면 보다 쉽게 **key** 명령에 이 키를 입력할 수 있습니다. 키를 구성하지 않으면 연결이 암호화되지 않습니다. 이 키는 대/소문자를 구분하는 최대 127자의 영숫자 문자열로 RADIUS 서버의 키와 같은 값입니다.

그룹에 둘 이상의 서버를 추가할 수 있습니다.

```
hostname(config)# aaa-server servergroup1 (inside) host 10.1.1.3
hostname(config-aaa-server-host)# key sharedsecret
hostname(config-aaa-server-host)# exit
```

ISE 정책 시행을 위한 구성 예

비밀번호와 **ISE** 동적 인증에 대한 **VPN** 터널 구성

다음 예는 동적 권한 부여(CoA) 업데이트 및 시간별 주기적 계정 관리를 위해 ISE 서버 그룹을 구성하는 방법을 보여 줍니다. ISE와 비밀번호 인증을 구성하는 터널 그룹 구성이 포함됩니다.

```
ciscoasa(config)# aaa-server ise protocol radius
ciscoasa(config-aaa-server-group)# interim-accounting-update periodic 1
ciscoasa(config-aaa-server-group)# dynamic-authorization
ciscoasa(config-aaa-server-group)# exit
ciscoasa(config)# aaa-server ise (inside) host 10.1.1.3
ciscoasa(config-aaa-server-host)# key sharedsecret
ciscoasa(config-aaa-server-host)# exit
ciscoasa(config)# tunnel-group aaa-coa general-attributes
ciscoasa(config-tunnel-general)# address-pool vpn
ciscoasa(config-tunnel-general)# authentication-server-group ise
ciscoasa(config-tunnel-general)# accounting-server-group ise
ciscoasa(config-tunnel-general)# exit
```

ISE 권한 부여 전용에 대한 VPN 터널 구성

다음 예는 ISE를 사용하여 로컬 인증서 검증 및 권한 부여를 위한 터널 그룹을 구성하는 방법을 보여 줍니다. 서버 그룹이 인증에 사용되지 않으므로 서버 그룹 구성에서 권한 부여 전용 명령을 포함합니다.

```
ciscoasa(config)# aaa-server ise protocol radius
ciscoasa(config-aaa-server-group)# authorize-only
ciscoasa(config-aaa-server-group)# interim-accounting-update periodic 1
ciscoasa(config-aaa-server-group)# dynamic-authorization
ciscoasa(config-aaa-server-group)# exit
ciscoasa(config)# aaa-server ise (inside) host 10.1.1.3
ciscoasa(config-aaa-server-host)# key sharedsecret
ciscoasa(config-aaa-server-host)# exit
ciscoasa(config)# tunnel-group aaa-coa general-attributes
ciscoasa(config-tunnel-general)# address-pool vpn
ciscoasa(config-tunnel-general)# authentication certificate
ciscoasa(config-tunnel-general)# authorization-server-group ise
ciscoasa(config-tunnel-general)# accounting-server-group ise
ciscoasa(config-tunnel-general)# exit
```

정책 시행 트러블슈팅

다음의 명령은 디버깅을 위해 사용할 수 있습니다.

CoA 활동을 추적하려면 다음 명령을 사용하십시오.

```
debug radius dynamic-authorization
```

리디렉션 URL 기능을 추적하려면 다음 명령을 사용하십시오.

```
debug aaa url-redirect
```

URL 리디렉션 기능에 해당하는 NP 분류 규칙을 보려면 다음 명령을 사용하십시오.

```
show asp table classify domain url-redirect
```

고급 SSL 설정 구성

ASA는 ASDM, 클라이언트리스 SSL VPN, VPN 및 브라우저 기반 세션을 위해 보안 메시지 전송을 지원하는 SSL(Secure Socket Laye) 프로토콜과 TLS(Transport Layer Security)를 사용합니다. 또한 ASA는 SSL 기반 VPN 및 관리 연결을 위해 SSLv3, TLSv1, TLv1.1 및 TLSv1.2 프로토콜을 지원합니다.

TLSv1.2는 다음과 같은 암호화에 대한 지원을 추가합니다.

- ECDHE-ECDSA-AES256-GCM-SHA384
- ECDHE-RSA-AES256-GCM-SHA384
- DHE-RSA-AES256-GCM-SHA384
- AES256-GCM-SHA384
- ECDHE-ECDSA-AES256-SHA384
- ECDHE-RSA-AES256-SHA384
- ECDHE-ECDSA-AES128-GCM-SHA256
- ECDHE-RSA-AES128-GCM-SHA256
- DHE-RSA-AES128-GCM-SHA256
- RSA-AES128-GCM-SHA256
- ECDHE-ECDSA-AES128-SHA256
- ECDHE-RSA-AES128-SHA256

참고 9.4(1) 릴리스의 경우 모든 SSLv3 키워드가 ASA 구성에서 제거되고, SSLv3 지원이 ASA에서 제거되었습니다. SSLv3을 활성화한 경우 SSLv3 옵션이 포함된 명령에서 부팅 시간 오류가 표시됩니다. 그런 다음 ASA가 기본값인 TLSv1을 사용하도록 되돌아갑니다.

Citrix Mobile Receiver가 TLS 1.1/1.2 프로토콜을 지원하지 않을 수 있습니다. 호환성에 대한 자세한 내용은 https://www.citrix.com/content/dam/citrix/en_us/documents/products-solutions/citrix-receiver-feature-matrix.pdf 를 참조하십시오.

ASA가 SSL/TLS 연결을 협상할 최소 프로토콜 버전을 지정하려면 다음 단계를 수행합니다.

프로시저

단계 **1** ASA가 SSL/TLS 연결을 협상할 최소 프로토콜 버전을 설정합니다.

```
ssl server-version [tlsv1 | tlsv1.1 | tlsv1.2]
```

```
hostname(config)# ssl server-version tlsv1
```

tlsv1 키워드는 ASA가 SSLv2 클라이언트 Hello를 허용하고 TLSv1 이상과 협상하도록 지정합니다. **tlsv1.1** 키워드는 ASA가 SSLv2 클라이언트 Hello를 허용하고 TLSv1.1 이상과 협상하도록 지정합니다. **tlsv1.2** 키워드는 ASA가 SSLv2 클라이언트 Hello를 허용하고 TLSv1.2 이상과 협상하도록 지정합니다.

단계 **2** ASA가 클라이언트로 작동할 때 사용하는 SSL/TLS 프로토콜 버전을 지정합니다.

```
ssl client-version [tlsv1 | tlsv1.1 | tlsv1.2]
```

```
hostname(config)# ssl client-version tlsv1
```

tlsv1 키워드는 ASA가 TLSv1 클라이언트 Hello를 전송하고 TLSv1 이상과 협상하도록 지정합니다. **tlsv1.1** 키워드는 ASA가 TLSv1.1 클라이언트 Hello를 전송하고 TLSv1.1 이상과 협상하도록 지정합니다. **tlsv1.2** 키워드는 ASA가 TLSv1.2 클라이언트 Hello를 전송하고 TLSv1.2 이상과 협상하도록 지정합니다.

단계 **3** SSL, DTLS 및 TLS 프로토콜에 대한 암호화 알고리즘을 지정합니다.

```
ssl cipher version [level | custom "string"]
```

```
hostname(config)# ssl cipher tlsv1.1 fips
hostname(config)#ssl cipher tlsv1 custom "RC4-SHA:ALL"
```

version 인수는 SSL, DTLS 또는 TLS 프로토콜 버전을 지정합니다. 지원되는 버전은 다음과 같습니다.

- **default** - 아웃바운드 연결을 위한 암호 집합입니다.
- **dtlsv1** - DTLSv1 인바운드 연결을 위한 암호입니다.
- **tlsv1** - TLSv1 인바운드 연결을 위한 암호입니다.
- **tlsv1.1** - TLSv1.1 인바운드 연결을 위한 암호입니다.
- **tlsv1.2** - TLSv1.2 인바운드 연결을 위한 암호입니다.

level 인수는 암호의 강도를 지정하고 구성된 최소 암호 수준을 나타냅니다. 증가하는 강도 순서의 유효한 값은 다음과 같습니다.

- **all** - NULL-SHA를 비롯한 모든 암호를 포함합니다.
- **low** - NULL-SHA를 제외한 모든 암호를 포함합니다.
- **medium**(모든 프로토콜 버전의 기본값) - NULL-SHA, DES-CBC-SHA 및 RC4-MD5를 제외한 모든 암호를 포함합니다.
- **fips** - 모든 FIPS 호환 암호(NULL-SHA, DES-CBC-SHA, RC4-MD5, RC4-SHA 및 DES-CBC3-SHA 제외)를 포함합니다.
- **high**(TLSv1.2에만 적용됨) - SHA-2 암호를 사용하는 AES-256만 포함합니다.

custom "*string*" 키워드 인수 쌍을 사용하면 OpenSSL 암호 정의 문자열을 사용하는 암호 그룹을 전체적으로 제어할 수 있습니다. 자세한 내용은 https://www.openssl.org/docs/apps/ciphers.html을 참조하십시오.

권장 설정은 **medium**입니다. **high**를 사용하면 연결이 제한될 수 있습니다. **custom**을 사용하면 소수의 암호만 구성된 경우 기능이 제한될 수 있습니다. 기본 사용자 지정 값을 제한하면 클러스터링을 포함하여 아웃바운드 연결이 제한됩니다.

ASA에서는 지원되는 암호에 대한 우선 순위를 다음과 같이 지정합니다. 자세한 내용은 명령 참조를 참조하십시오.

이 명령은 버전 9.3(2)부터 더 이상 사용되지 않는 **ssl encryption** 명령을 대체합니다.

단계 **4** 단일 인터페이스에서 여러 신뢰 지점을 허용합니다.

```
ssl trust-point name [interface [vpnlb-ip]| domain domain-name]
```

```
hostname(config)# ssl trust-point www-cert domain www.example.com
```

name 인수는 신뢰 지점의 이름을 지정합니다. *interface* 인수는 신뢰 지점이 구성된 인터페이스의 이름을 지정합니다. **vpnlb-ip** 키워드는 인터페이스에만 적용되며 이 인터페이스에서 VPN 부하 균형 클러스터 IP 주소와 신뢰 지점을 연결합니다. **domain** *domain-name* 키워드 인수 쌍은 인터페이스에 액세스하는 데 사용되는 특정 도메인 이름과 연결된 신뢰 지점을 지정합니다.

인터페이스당 최대 16개의 신뢰 지점을 구성할 수 있습니다.

인터페이스 또는 도메인을 지정하지 않는 경우, 이 명령은 구성된 신뢰 지점이 없는 모든 인터페이스에 대한 대체 신뢰 지점을 생성합니다.

ssl trustpoint ? 명령을 입력하면 사용 가능한 구성된 신뢰 지점이 나타납니다. **ssl trust-point** *name* **?** 명령(예: **ssl trust-point mysslcert ?**)을 입력한 경우 트러스트 포인트-SSL 인증서 연계에 사용 가능한 구성된 인터페이스가 표시됩니다.

이 명령을 사용할 때 다음 지침을 따르십시오.

- trustpoint 값은 **crypto ca trustpoint** *name* 명령에 구성된 CA 트러스트 포인트의 이름이어야 합니다.
- interface는 이전에 구성된 인터페이스의 nameif 이름이어야 합니다.
- 트러스트 포인트를 제거하면 해당 트러스트 포인트를 참조하는 모든 **ssl trust-point** 항목도 제거됩니다.
- 인터페이스당 하나의 **ssl trust-point** 항목과 인터페이스 없음을 지정하는 항목을 유지할 수 있습니다.
- 여러 항목에 동일한 신뢰 지점을 다시 사용할 수 있습니다.
- **domain** 키워드로 구성된 신뢰 지점은 연결 방법에 따라 여러 인터페이스에 적용될 수 있습니다.
- *domain-name* 값당 하나의 **ssl trust-point**만 유지할 수 있습니다.
- 이 명령을 입력한 후 다음 오류가 표시되는 경우

```
error:0B080074:x509 certificate routines:X509_check_private_key:key values
mismatch@x509_cmp.c:339
```

사용자가 이전에 구성된 인증서를 대체할 새 인증서를 구성했음을 의미합니다. 추가 작업은 필요하지 않습니다.

- 인증서가 다음 순서대로 선택됩니다.
  - 연결이 **domain** 키워드 값과 일치하지 않는 경우 해당 인증서가 먼저 선택됩니다. (**ssl trust-point** *name* **domain** *domain-name* 명령)
  - 부하 균형 주소로 연결이 설정된 경우 vpnlb-ip 인증서가 선택됩니다. (**ssl trust-point** *name* **interface vpnlb-ip** 명령)
  - 인터페이스에 대해 구성된 인증서 (**ssl trust-point** *name* **interface** 명령)
  - 인터페이스와 연결되지 않은 기본 인증서 (**ssl trust-point** *name* 명령)
  - ASA의 자체 서명 및 자체 생성된 인증서

단계 **5** TLS에서 사용되는 DHE-RSA 암호와 함께 사용할 DH 그룹을 지정합니다.

ssl dh-group [**group1** | **group2** | **group5** | **group14** | **group24**]

```
hostname(config)# ssl dh-group group5
```

group1 키워드는 DH 그룹 1(768비트 모듈러스)을 구성합니다. **group2** 키워드는 DH 그룹 2(1024비트 모듈러스)를 구성합니다. **group5** 키워드는 DH 그룹 5(1536비트 모듈러스)를 구성합니다. **group14** 키워드는 DH 그룹 14(2048비트 모듈러스, 224비트 소수 위수 하위 그룹)를 구성합니다. **group24** 키워드는 DH 그룹 24(2048비트 모듈러스, 256비트 소수 위수 하위 그룹)를 구성합니다.

그룹 1 및 2는 Java 7 이하 버전과 호환됩니다. 그룹 5, 14 및 24는 Java 7과 호환되지 않습니다. 모든 그룹은 Java 8과 호환됩니다. 그룹 14 및 24는 FIPS와 호환됩니다. 기본값은 **ssl dh-group group2**입니다.

단계 **6** TLS에서 사용되는 ECDHE-ECDSA 암호와 함께 사용할 그룹을 지정합니다.

ssl ecdh-group [**group19** | **group20** | **group21**]

```
hostname(config)# ssl ecdh-group group20
```

group19 키워드는 그룹 19(256비트 EC)를 구성합니다. **group20** 키워드는 그룹 20(384비트 EC)을 구성합니다. **group21** 키워드는 그룹 21(521비트 EC)을 구성합니다.

기본값은 **ssl ecdh-group group19**입니다.

참고 ECDSA 및 DHE 암호가 우선 순위가 가장 높습니다.

지속적인 IPsec 터널링 흐름

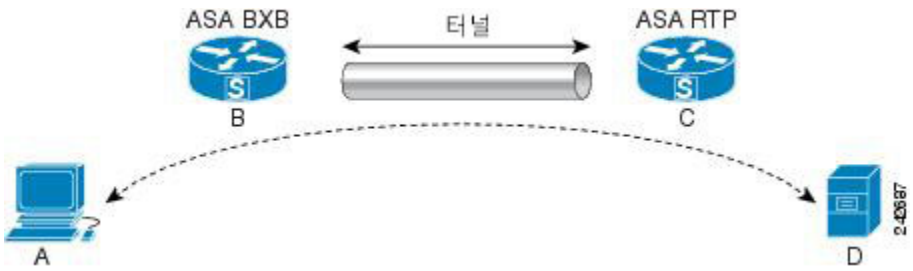
릴리스 8.0.4 이전의 ASA 소프트웨어 버전을 실행 중인 네트워크에서 터널이 삭제되면 IPSec 터널을 통과하는 기존 IPsec LAN-to-LAN 또는 원격 액세스 TCP 트래픽 흐름이 삭제됩니다. 흐름은 필요에 따라 터널이 복구되면 하고 다시 생성됩니다. 이 정책은 리소스 관리 및 보안 측면에서 잘 작동합니다. 그러나 이러한 동작은 특히 PIX에서 ASA 전용 환경으로 마이그레이션하거나 쉽게 다시 시작하지 않는 레거시 TCP 애플리케이션 또는 터널을 자주 삭제하는 게이트웨이를 포함한 네트워크에서는 사용자에게 문제를 유발할 수 있습니다(자세한 내용은 CSCsj40681 및 CSCsi47630 참조).

지속적인 IPsec 터널 흐름 기능이 이 문제를 해결합니다. 이 기능을 활성화하면 ASA가 상태 저장(TCP) 터널링 흐름을 보존하고 재개합니다. 터널이 삭제되면 다른 모든 흐름이 삭제되므로 새 터널이 생성되면 이를 재설정해야 합니다.

참고 이 기능은 네트워크 확장 모드에서 실행하는 IPsec LAN-to-LAN 터널 및 IPsec 원격 액세스 터널을 지원하지만 IPsec 또는 AnyConnect/SSL VPN 원격 액세스 터널은 지원하지 않습니다.

다음 예에서는 지속적인 IPsec 터널 흐름 기능이 작동하는 방법을 보여줍니다.

그림 *4:* 네트워크 시나리오



이 예에서는 BXB 및 RTP 네트워크가 보안 어플라이언스의 쌍으로 보안 LAN-to-LAN 터널을 통해 연결되어 있습니다. BXB 네트워크에 있는 PC가 보안 터널을 통해 RTP 네트워크에 있는 서버로부터 FTP 전송을 실행하고 있습니다. 이 시나리오에서는 PC가 서버에 로그인하고 전송을 시작한 후 어떠한 원인으로 인해 터널이 삭제된다고 가정합니다. 데이터 흐름이 계속 시도되고 있으므로 터널이 재설정되더라도 FTP 전송이 완료되지 않습니다. 사용자가 전송을 종료하고 서버에 다시 로그인하여 전송을 시작해야 합니다. 그러나 지속적인 IPsec 터널 흐름이 활성화된 경우 보안 어플라이언스가 해당 흐름에 대한 기록(상태 정보)을 유지하므로 시간 제한 간격 내에서 터널이 다시 생성되면 새로운 터널을 통해 데이터 흐름이 성공적으로 계속 진행됩니다.

시나리오

다음 섹션에서는 지속적인 IPsec 터널링 흐름 기능을 비활성화한 경우와 이후에 활성화한 경우, 삭제 및 복구된 터널의 데이터 흐름 상황을 설명합니다. 이 두 경우에서 네트워크에 대한 설명은 이전 그림을 참조하십시오. 이 그림에서,

- 흐름 B-C는 터널을 정의하고 암호화된 ESP 데이터를 전송합니다.

- 흐름 A-D는 FTP 전송을 위한 TCP 연결이며 흐름 B-C에서 정의한 터널을 통과합니다. 이러한 흐름에는 TCP/FTP 흐름을 검사하기 위해 방화벽에서 사용하는 상태 정보가 포함되어 있습니다. 상태 정보는 꼭 필요한 정보로 전송이 진행될 때 방화벽에 의해 꾸준히 업데이트됩니다.

참고 간단한 설명을 위해 각 방향의 역방향 흐름은 생략되었습니다.

지속적인 **IPsec** 터널링 흐름 비활성화

LAN-to-LAN 터널이 삭제되면 흐름 A-D와 흐름 B-C 및 여기에 속하는 모든 상태 정보가 삭제됩니다. 이후에 터널이 재설정되고 흐름 B-C가 다시 생성되어 터널링된 데이터 전송을 재개할 수 있습니다. 그러나 TCP/FTP 흐름 A-D에서 문제가 발생합니다. 지금까지 FTP 전송의 흐름을 설명하는 상태 정보가 삭제되었으므로 상태 저장 방화벽이 진행 중인 FTP 데이터를 차단하고 흐름 A-D 생성을 거부합니다. 기존까지 해당 흐름의 기록이 손실되었으므로 방화벽이 FTP 전송을 이탈한 TCP 패킷으로 간주하여 삭제합니다. 이는 기본 동작입니다.

지속적인 **IPsec** 터널링 흐름 활성화

지속적인 IPsec 터널링 흐름 기능을 활성화한 경우 ASA가 흐름 A-D의 상태 정보로 여전히 액세스할 수 있으므로 시간 제한 창에서 터널이 다시 생성되면 데이터 흐름이 성공적으로 계속 진행됩니다.

이 기능을 활성화하면 ASA가 흐름을 독립적으로 처리합니다. 이는 흐름 B-C를 통해 정의된 터널이 삭제될 때 흐름 A-D가 삭제되지 않는 것을 의미합니다. ASA가 상태 저장(TCP) 터널링 흐름을 보존하고 재개합니다. 다른 모든 흐름이 삭제되므로 새 터널에서 이를 재설정해야 합니다. 터널이 다운될 때 ASA가 흐름 A-D에 도착하는 모든 패킷을 삭제하므로 터널링된 흐름의 보안 정책을 약화시키지 않습니다.

터널링 TCP 흐름은 삭제되지 않으므로 정리를 위해 TCP 시간 제한을 사용합니다. 그러나 특정 터널링 흐름의 시간 제한을 비활성화한 경우 해당 흐름은 수동으로 또는 피어의 TCP RST와 같이 다른 수단을 통해 삭제될 때까지 시스템에 남아 있습니다.

CLI를 사용하여 지속적인 IPsec 터널링 흐름 구성

구성 예시

지속적인 IPsec 터널링 흐름 문제 해결

show asp table 및 **show conn** 명령은 모두 지속적인 IPsec 터널링 흐름을 사용하여 문제를 해결하는 데 유용할 수 있습니다.

지속적인 IPsec 터널링 흐름 기능이 활성화되어 있습니까?

특정 터널에서 이 기능을 활성화했는지 확인하려면 **show asp table** 명령을 사용하여 터널에 연계된 VPN 상황을 살펴보십시오. show asp table vpn-context 명령이 다음 예에 표시된 대로(굵게 처리됨) 터널 삭제 이후 상태 저장 흐름을 유지 관리하는 각 상황에 대해 “+PRESERVE” 플래그를 표시합니다.

```
hostname(config)# show asp table vpn-context
VPN CTX=0x0005FF54, Ptr=0x6DE62DA0, DECR+ESP+PRESERVE, UP, pk=0000000000, rk=0000000000,
gc=0
VPN CTX=0x0005B234, Ptr=0x6DE635E0, ENCR+ESP+PRESERVE, UP, pk=0000000000, rk=0000000000,
gc=0

------------------------------------------------------------------------------

hostname(config)# show asp table vpn-context detail

VPN CTX  = 0x0005FF54

Peer IP  = ASA_Private
Pointer  = 0x6DE62DA0
State    = UP
Flags    = DECR+ESP+PRESERVE
SA       = 0x001659BF
SPI      = 0xB326496C
Group    = 0
Pkts     = 0
Bad Pkts = 0
Bad SPI  = 0
Spoof    = 0
Bad Crypto = 0
Rekey Pkt  = 0
Rekey Call = 0

VPN CTX  = 0x0005B234

Peer IP  = ASA_Private
Pointer  = 0x6DE635E0
State    = UP
Flags    = ENCR+ESP+PRESERVE
SA       = 0x0017988D
SPI      = 0x9AA50F43
Group    = 0
Pkts     = 0
Bad Pkts = 0
Bad SPI  = 0
Spoof    = 0
Bad Crypto = 0
Rekey Pkt  = 0
Rekey Call = 0
hostname(config)#
Configuration and Restrictions
This configuration option is subject to the same CLI configuration restrictions as other
sysopt VPN CLI.
```

분리된 흐름 찾기

LAN-to-LAN/네트워크 확장 모드 터널이 삭제되고 시간 제한 전에 복구되지 않는 경우 여러 분리된 터널 흐름이 있을 수 있습니다. 이러한 플로우는 터널 중단으로 인해 끊어지지는 않지만 이러한 통과하려고 시도하는 모든 데이터는 드롭됩니다. 이 흐름을 보려면 다음 예에서와 같이 **show conn** 명령을 사용하십시오. 해당 예에서는 이 명령이 강조를 위해 굵게 처리되어 있으며 사용자 입력이 나와 있습니다.

```
asa2(config)# show conn detail
9 in use, 14 most used
Flags: A - awaiting inside ACK to SYN, a - awaiting outside ACK to SYN,
       B - initial SYN from outside, C - CTIQBE media, D - DNS, d - dump,
```

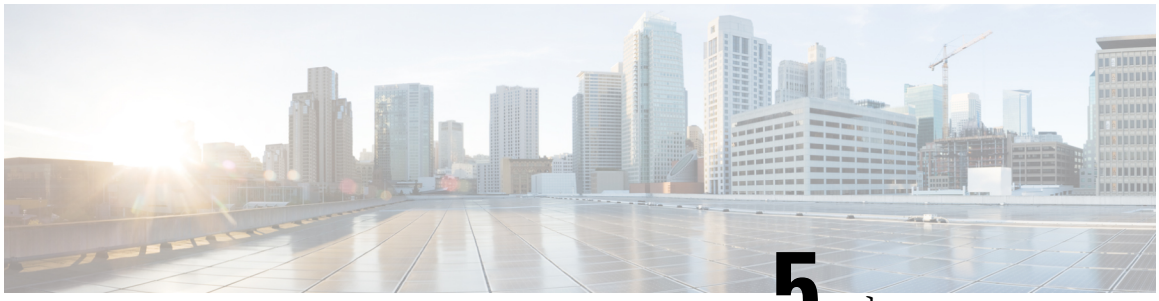
```
E - outside back connection, F - outside FIN, f - inside FIN,
G - group, g - MGCP, H - H.323, h - H.225.0, I - inbound data,
i - incomplete, J - GTP, j - GTP data, K - GTP t3-response
k - Skinny media, M - SMTP data, m - SIP media, n - GUP
O - outbound data, P - inside back connection, p - Phone-proxy TFTP connection,
q - SQL*Net data, R - outside acknowledged FIN,
R - UDP SUNRPC, r - inside acknowledged FIN, S - awaiting inside SYN,
s - awaiting outside SYN, T - SIP, t - SIP transient, U - up,
V - VPN orphan, W - WAAS,
X - inspected by service module
```

다음 예에서는 **V** 플래그로 표시된 대로 분리된 흐름이 존재할 때 **show conn** 명령의 샘플 출력을 보여 줍니다.

```
hostname# show conn
16 in use, 19 most used
TCP out 192.168.110.251:7393 in 192.168.150.252:21 idle 0:00:00 bytes 1048 flags UOVB
TCP out 192.168.110.251:21137 in 192.168.150.252:21 idle bytes 1048 flags UIOB
```

보고서를 분리 흐름이 있는 연결로 제한하려면 다음 예와 같이 **vpn_orphan** 옵션을 **show conn state** 명령에 추가합니다.

```
hostname# show conn state vpn_orphan
14 in use, 19 most used
TCP out 192.168.110.251:7393 in 192.168.150.252:5013 idle 0:00:00 bytes 2841019 flags UOVB
```



5 장

연결 프로파일, 그룹 정책 및 사용자

이 장에서는 VPN 연결 프로파일(이전의 "터널 그룹"), 그룹 정책 및 사용자를 구성하는 방법에 대해 설명합니다. 이 장은 다음 섹션으로 구성됩니다.

연결 프로파일, 그룹 정책 및 사용자 개요

그룹 및 사용자는 VPN(Virtual Private Network: 가상 프라이빗 네트워크) 보안 관리 및 ASA 구성의 코어 개념입니다. 이 두 가지는 VPN에 대한 사용자 액세스 및 VPN 사용을 결정하는 특성을 지정합니다. 그룹은 단일 엔터티로 처리된 사용자의 컬렉션입니다. 사용자는 그룹 정책에서 특성을 가져옵니다. 연결 프로파일은 특정 연결에 대한 그룹 정책을 식별합니다. 사용자에게 특정한 그룹 정책을 할당하지 않은 경우 연결에 대한 기본 그룹 정책이 적용됩니다.

요약하자면, 먼저 연결 프로파일을 구성하여 연결 값을 설정합니다. 그런 다음 그룹 정책을 구성합니다. 그룹 정책은 전체적으로 사용자에게 값을 설정합니다. 그룹의 값을 상속하고 개별 사용자별로 특정한 값을 구성할 수 있는 사용자를 구성합니다. 이 장에서는 이러한 엔터티를 구성하는 방법 및 이유에 대해 설명합니다.

참고 **tunnel-group** 명령을 사용하여 연결 프로파일을 구성하십시오. 이 장에서는 "연결 프로파일" 및 "터널 그룹"이라는 용어를 교대로 자주 사용합니다.

연결 프로파일 및 그룹 정책은 시스템 관리를 단순화합니다. 구성 작업을 간소화하기 위해 ASA는 기본 LAN-to-LAN 연결 프로파일(DefaultL2Lgroup), IKEv2 VPN에 대한 기본 원격 액세스 연결 프로파일(DefaultRAgroup), 클라이언트리스 SSL 및 AnyConnect SSL 연결에 대한 기본 연결 프로파일(DefaultWEBVPNgroup) 및 기본 그룹 정책(DfltGrpPolicy)을 제공합니다. 기본 연결 프로파일과 그룹 정책은 여러 사용자에게 공통으로 해당될 수 있는 설정을 제공합니다. 사용자를 추가할 때 사용자가

그룹 정책에서 매개변수를 "상속"받도록 지정할 수 있습니다. 따라서 여러 명의 사용자용으로 VPN 액세스를 신속하게 구성할 수 있습니다.

모든 VPN 사용자에게 동일한 권한을 부여하기로 결정한 경우 특정 연결 프로파일 또는 그룹 정책을 구성할 필요가 없지만 VPN이 드물게 이 방식으로 작동하는 경우가 있습니다. 예를 들어 금융 그룹에서 사설 네트워크의 특정 부분에 액세스하고 고객 지원 그룹에서 다른 부분에 액세스하며 MIS 그룹에서 기타 부분에 액세스하도록 허용할 수 있습니다. 또한, MIS 내에 있는 특정 사용자가 다른 MIS 사용자는 액세스할 수 없는 시스템에 액세스하도록 허용할 수도 있습니다. 연결 프로파일 및 그룹 정책은 이 작업을 안전하게 수행할 수 있도록 유연성을 제공합니다.

참고 ASA에는 또한 네트워크 목록의 상위 집합인 개체 그룹의 개념이 포함되어 있습니다. 개체 그룹을 사용하여 포트와 네트워크에 대한 VPN 액세스를 정의할 수 있습니다. 개체 그룹은 그룹 정책 및 연결 프로파일보다는 ACL과 관련이 있습니다. 개체 그룹 사용에 대한 자세한 내용은 일반 작업 구성 가이드의 20장에서 "개체"를 참조하십시오.

보안 어플라이언스는 다양한 소스의 특성 값을 적용할 수 있습니다. 다음 계층 구조에 따라 특성 값이 적용됩니다.

1. DAP(Dynamic Access Policy: 동적 액세스 정책) 레코드
2. 사용자 이름
3. 그룹 정책
4. 연결 프로파일에 대한 그룹 정책
5. 기본 그룹 정책

따라서 특성에 대한 DAP 값은 사용자, 그룹 정책 또는 연결 프로파일에 대해 구성된 DAP 값보다 우선순위가 높습니다.

DAP 레코드에 대한 속성을 활성화하거나 비활성화하면 ASA는 해당 값을 강제적으로 적용합니다. 예를 들어 dap webvpn 구성 모드에서 HTTP 프록시를 비활성화하는 경우 ASA는 값을 더 이상 검색하지 않습니다. http-proxy 명령에 no 값을 대신 사용하는 경우, 이 특성은 DAP 레코드에 표시되지 않으므로 보안 어플라이언스가 사용자 이름 및 그룹 정책(필요 시)의 AAA 특성 아래로 이동하여 적용할 값을 찾습니다. ASA 클라이언트리스 SSL VPN 구성에서는 **http-proxy**와 **https-proxy** 명령을 각각 하나씩만 지원합니다. ASDM을 사용하여 DAP를 구성할 것을 권장합니다.

연결 프로파일

연결 프로파일은 터널 연결 정책을 결정하는 레코드 집합으로 구성됩니다. 이 레코드는 터널 사용자가 인증한 서버 및 연결 정보가 전송된 계정 관리 서버(있는 경우)를 식별합니다. 또한 연결에 대한 기본 그룹 정책을 식별하고 프로토콜별 연결 매개변수를 포함합니다. 연결 프로파일은 터널 자체 생성과 관련된 적은 수의 특성을 포함합니다. 연결 프로파일은 사용자 중심의 특성을 정의하는 그룹 정책에 대한 포인터를 포함합니다.

ASA는 LAN-to-LAN 연결용 DefaultL2Lgroup, IPSEC 원격 액세스 연결용 DefaultRAgroup, SSL VPN(브라우저 기반 및 Anyconnect Client 기반) 연결을 위한 DefaultWEBVPNGroup의 기본 연결 프로파일을 제공합니다. 이 기본 연결 프로파일을 수정할 수 있지만 삭제할 수는 없습니다. 또한 환경에 고유한 하나 이상의 연결 프로파일을 생성할 수 있습니다. 연결 프로파일은 ASA에 대해 로컬로 구성되며 외부 서버에서 구성할 수 없습니다.

일반적인 연결 프로파일 연결 매개변수

일반적인 매개변수는 모든 VPN 연결에 공통적입니다. 일반적인 매개변수에는 다음이 포함됩니다.

- 연결 프로파일 이름 — 연결 프로파일을 추가하거나 수정할 경우 연결 프로파일 이름을 지정합니다. 다음 고려사항이 적용됩니다.
  - 인증을 위해 사전 공유 키를 사용하는 클라이언트의 경우 연결 프로파일 이름이 클라이언트에서 ASA에 전달하는 그룹 이름과 동일합니다.
  - 인증을 위해 인증서를 사용하는 클라이언트는 이 이름을 인증서의 일부로 전달하고 ASA는 인증서에서 이름을 추출합니다.
- 연결 유형 - 연결 유형에는 IKEv1 원격 액세스, IPsec LAN-to-LAN 및 AnyConnect(SSL/IKEv2)가 포함됩니다. 연결 프로파일의 연결 유형은 한 가지만 가능합니다.
- 인증, 권한 부여, 계정 관리 서버 - 이 매개변수는 ASA가 다음 목적으로 사용하는 서버 그룹 또는 목록을 식별합니다.
  - 사용자 인증
  - 액세스 권한이 부여된 서비스 사용자에 대한 정보 얻기
  - 계정 레코드 저장

서버 그룹은 하나 이상의 서버로 구성될 수 있습니다.

- 연결을 위한 기본 그룹 정책 — 그룹 정책은 사용자 중심 특성의 집합입니다. 기본 그룹 정책은 터널 사용자를 인증하거나 권한 부여할 때 ASA가 기본값으로 사용하는 속성을 포함하는 그룹 정책입니다.
- 클라이언트 주소 할당 방법 - 이 방법에는 ASA가 클라이언트에 할당한 하나 이상의 DHCP 서버 또는 주소 풀의 값이 포함되어 있습니다.
- 비밀번호 관리 — 이 매개변수를 사용하면 현재 비밀번호가 지정된 날짜 수 이내에(기본값은 14일) 만료될 예정임을 사용자에게 경고하고 비밀번호를 변경할 수 있는 기회를 사용자에게 제공할 수 있습니다.
- 그룹 제거 및 영역 제거 - 이 매개변수는 ASA가 수신한 사용자 이름을 처리하는 방식을 지시합니다. 이 매개변수는 user@realm 형식으로 수신한 사용자 이름에만 적용됩니다.

  영역은 @구분 기호(user@abc)가 있는 사용자 이름에 추가된 관리 도메인입니다. 영역을 제거하는 경우 ASA는 사용자 이름 및 그룹(있는 경우)을 인증에 사용합니다. 그룹을 제거하는 경우 ASA는 사용자 이름 및 영역(있는 경우)을 인증에 사용합니다.

인증 중에 사용자 이름에서 영역 한정자를 제거하려면 strip-realm 명령을 입력하고 그룹 한정자를 제거하려면 strip-group 명령을 입력합니다. 두 가지 한정자를 모두 제거하는 경우, 인증은 사용자 이름만 기반으로 합니다. 기타의 경우, 인증은 전체 *username@realm* 또는 사용자 이름 <delimiter> 그룹 문자열을 기반으로 합니다. 서버에서 구분 기호를 분석할 수 없는 경우 strip-realm을 지정하십시오.

또한 L2TP/IPsec 클라이언트의 경우에만 strip-group 명령을 지정한 경우 ASA는 VPN 클라이언트가 제공한 사용자 이름에서 그룹 이름을 가져와 사용자 연결을 위해 연결 프로파일(터널 그룹)을 선택합니다.

- 권한 부여 필요함 — 이 매개변수를 사용하면 사용자 연결 전에 권한 부여를 요구하거나 이 요구를 취소할 수 있습니다.
- 권한 부여 DN 특성 — 이 매개변수는 권한 부여를 수행할 때 어떤 고유 이름 특성을 사용할지 지정합니다.

IPsec 터널 그룹 연결 매개변수

IPsec 매개변수는 다음과 같습니다.

- 클라이언트 인증 방법: 사전 공유 키, 인증서 또는 두 가지 모두
  - 사전 공유 키를 기반으로 하는 IKE 연결은 영숫자 키 자체(최대 128자 길이)이며 연결 정책과 연계되어 있습니다.
  - Peer-ID 검증 요건 — 이 매개변수는 피어 인증서를 사용하는 피어 ID의 검증 필요 여부를 지정합니다.
  - 인증 방법으로 인증서 또는 두 가지 모두를 지정한 경우, 엔드 유저는 인증을 위해 유효한 인증서를 제공해야 합니다.
- 확장된 하이브리드 인증 방법: XAUTH 및 하이브리드 XAUTH.

  ASA 인증에 디지털 인증서를 사용하고 RADIUS TACACS+ 또는 SecurID 등의 원격 VPN 사용자 인증에 다른 레거시 방법을 사용해야 하는 경우, **isakmp ikev1-user-authentication** 명령을 사용하여 하이브리드 XAUTH 인증을 구현합니다.
- ISAKMP(IKE) 킵얼라이브 설정. 이 기능을 통해 ASA는 원격 피어의 지속적인 상태를 모니터링하고 해당 피어에 자신의 상태를 보고할 수 있습니다. 피어가 응답하지 않는 경우 ASA는 연결을 제거합니다. IKE 킵얼라이브를 활성화하면 IKE 피어의 연결이 끊어질 때 연결이 중단되는 것을 방지합니다.

  다양한 형식의 IKE 킵얼라이브가 있습니다. 이 기능이 작동하려면 ASA 및 원격 피어 모두 일반적인 형식을 지원해야 합니다. 이 기능은 다음 피어에서 작동합니다.
  - Cisco AnyConnect VPN 클라이언트
  - Cisco IOS Software
  - Cisco Secure PIX Firewall

Cisco 이외의 VPN 클라이언트는 IKE 킵얼라이브를 지원하지 않습니다.

혼합 피어 그룹을 구성 중이며 이 피어 중 일부에서 IKE 킵얼라이브를 지원하고 나머지에서 지원하지 않는 경우, 전체 그룹에 대해 IKE 킵얼라이브를 활성화하십시오. 이 기능은 IKE 킵얼라이브를 지원하지 않는 피어에는 영향을 주지 않습니다.

IKE 킵얼라이브를 비활성화하면 응답하지 않는 피어와의 연결이 시간 제한 때까지 활성 상태로 남아 있으므로 유휴 시간 제한을 짧게 유지하는 것을 권장합니다. 유휴 시간 제한을 변경하려면 그룹 정책 구성, 143 페이지의 내용을 참조하십시오.

참고 연결 비용을 줄이려면 이 그룹에 ISDN 회선을 통해 연결 중인 클라이언트가 포함된 경우 IKE 킵얼라이브를 비활성화하십시오. ISDN 연결은 유휴 시 일반적으로 연결이 끊어지지만 IKE 킵얼라이브 메커니즘은 연결이 유휴 상태가 되어 끊어지는 것을 방지합니다.

IKE 킵얼라이브를 비활성화한 경우, IKE 또는 IPsec 키가 만료되는 경우에만 클라이언트의 연결이 끊어집니다. 실패한 트래픽은 IKE 킵얼라이브가 활성화된 경우와 마찬가지로 피어 시간 제한 프로파일 값이 있는 터널의 연결을 끊지 않습니다.

IKE 기본 모드를 사용하는 LAN-to-LAN 구성을 사용하는 경우, 두 개의 피어에 동일한 IKE 킵얼라이브가 구성되어 있는지 확인하십시오. 두 개의 피어 모두 IKE 킵얼라이브가 활성화되어 있거나 두 가지 모두 비활성화되어 있어야 합니다.

- 디지털 인증서를 사용하여 인증을 구성하는 경우 전체 인증서 체인(피어 ID 인증서 및 모든 발급 중인 인증서를 전송함) 또는 방금 발급한 인증서(루트 인증서 및 하위 CA 인증서 포함)의 전송 여부를 지정할 수 있습니다.
- 만료된 버전의 Windows 클라이언트 소프트웨어를 사용 중인 사용자에게 클라이언트를 업데이트해야 한다고 알려주고 이 사용자가 업데이트된 클라이언트 버전을 확보할 수 있도록 메커니즘을 제공할 수 있습니다. 모든 연결 프로파일 또는 특정 연결 프로파일 중 하나에 대해 클라이언트 업데이트를 구성하고 변경할 수 있습니다.
- 디지털 인증서를 사용하여 인증을 구성하는 경우 IKE 피어에 전송할 인증서를 식별하는 신뢰 지점의 이름을 지정할 수 있습니다.

SSL VPN 세션에 대한 연결 프로파일 연결 매개변수

아래 표는 SSL VPN(AnyConnect 클라이언트 및 클라이언트리스) 연결에 특정한 연결 프로파일 특성의 목록을 제공합니다. 이 특성 외에 모든 VPN 연결에 공통적인 일반 연결 프로파일 특성을 구성하십시오. 구성 연결 프로파일에 대한 단계적인 내용은 클라이언트리스 SSL VPN 세션에 대한 연결 프로파일 구성, 119 페이지를 참조하십시오.

참고 이전 릴리스에서 "연결 프로파일"은 "터널 그룹"이라고 했습니다. tunnel-group 명령을 사용하여 연결 프로파일을 구성하십시오. 이 장에서는 이 용어를 교대로 자주 사용합니다.

표 ***5: SSL VPN***에 대한 연결 프로파일 특성

	기능
authentication	인증 방법, AAA 또는 인증서를 설정합니다.
customization	적용하기 위해 이전에 정의한 사용자 지정 이름을 식별합니다. 사용자 지정은 사용자가 로그인 시 확인하는 창의 모양을 결정합니다. 클라이언트리스 SSL VPN 구성의 일부로 사용자 지정 매개변수를 구성하십시오.
nbns-server	CIFS 이름 확인에 사용할 NetBIOS 이름 서비스 서버(nbns-server)의 이름을 식별합니다.
group-alias	서버에서 연결 프로파일을 나타낼 수 있는 하나 이상의 대체 이름을 지정합니다. 로그인 시 사용자는 드롭다운 메뉴에서 그룹 이름을 선택합니다.
group-url	하나 이상의 그룹 URL을 식별합니다. 이 특성을 구성하는 경우, 지정된 URL에 로그인하는 사용자는 로그인 시 그룹을 선택할 필요가 없습니다. AnyConnect 클라이언트 연결에 그룹 URL을 사용하는 로드 밸런싱 배포를 수행하려면 클러스터의 각 ASA 노드에서 가상 클러스터 주소에 대한 그룹 URL뿐 아니라 노드의 로드 밸런싱 공용 주소에 대한 그룹 URL을 구성해야 합니다.
dns-group	연결 프로파일에 사용하기 위해 DNS 서버 이름, 도메인 이름, 이름 서버, 재시도 횟수 및 DNS 서버의 시간 제한 값을 지정하는 DNS 서버 그룹을 식별합니다.
hic-fail-group-policy	Cisco Secure Desktop Manager를 사용하여 그룹 기반 정책 특성을 "실패 그룹 정책 사용" 또는 "기준이 일치하는 경우 성공 그룹 정책 사용"으로 설정하는 경우, VPN 기능 정책을 지정합니다.
override-svc-download	원격 사용자를 대상으로 AnyConnect VPN 클라이언트를 다운로드하도록 구성된 그룹 정책 또는 사용자 이름 특성의 다운로드를 재정의합니다.

	기능
radius-reject-message	인증이 거부될 경우 로그인 화면에서 RADIUS 거부 메시지 표시를 활성화합니다.

연결 프로파일 구성

이 섹션에서는 단일 상황 모드 또는 다중 상황 두 가지에서 연결 프로파일의 콘텐츠 및 구성에 대해 설명합니다.

참고 다중 상황 모드는 IKEv2 및 IKEv1 사이트 간에만 적용되며 AnyConnect, 클라이언트리스 SSL VPN, 레거시 Cisco VPN 클라이언트, Apple 네이티브 VPN 클라이언트, Microsoft 네이티브 VPN 클라이언트 또는 IKEv1 IPsec용 cTCP에는 적용되지 않습니다.

기본 연결 프로파일을 수정할 수 있으며 3가지 터널 그룹 유형 중 하나로 새로운 연결 프로파일을 구성할 수 있습니다. 연결 프로파일에서 특성을 명시적으로 구성하지 않은 경우, 해당 특성은 기본 연결 프로파일에서 값을 가져옵니다. 기본 연결 프로파일 유형은 원격 액세스입니다. 후속 매개변수는 터널 유형의 선택사항에 따라 달라집니다. 기본 연결 프로파일을 포함하여 모든 연결 프로파일의 현재 구성된 기본 구성을 확인하려면 **show running-config all tunnel-group** 명령을 입력합니다.

최대 연결 프로파일 수

ASA가 지원할 수 있는 연결 프로파일(터널 그룹)의 최대 수는 플랫폼 + 5개에 대한 최대 동시 VPN 세션 수의 함수입니다. 이 제한을 초과하는 추가 터널 그룹을 추가하려고 시도하면 다음 메시지가 나타납니다. “오류: 30개의 구성된 터널 그룹 제한에 도달했습니다."

기본 **IPsec** 원격 액세스 연결 프로파일 구성

기본 원격 액세스 연결 프로파일의 콘텐츠는 다음과 같습니다.

```
tunnel-group DefaultRAGroup type remote-access
tunnel-group DefaultRAGroup general-attributes
 no address-pool
 no ipv6-address-pool
 authentication-server-group LOCAL
 accounting-server-group RADIUS
 default-group-policy DfltGrpPolicy
 no dhcp-server
 no strip-realm
 no password-management
 no override-account-disable
 no strip-group
 no authorization-required
 authorization-dn-attributes CN OU
tunnel-group DefaultRAGroup webvpn-attributes
 hic-fail-group-policy DfltGrpPolicy
```

```
 customization DfltCustomization
 authentication aaa
 no override-svc-download
 no radius-reject-message
 dns-group DefaultDNS
tunnel-group DefaultRAGroup ipsec-attributes
 no pre-shared-key
 peer-id-validate req
 no chain
 no trust-point
 isakmp keepalive threshold 1500 retry 2
 no radius-sdi-xauth
 isakmp ikev1-user-authentication xauth
tunnel-group DefaultRAGroup ppp-attributes
 no authentication pap
 authentication chap
 authentication ms-chap-v1
 no authentication ms-chap-v2
 no authentication eap-proxy


tunnel-group DefaultRAGroup type remote-access
tunnel-group DefaultRAGroup general-attributes
 no address-pool
 no ipv6-address-pool
 authentication-server-group LOCAL
 accounting-server-group RADIUS
 default-group-policy DfltGrpPolicy
 no dhcp-server
 no strip-realm
 no password-management
 no strip-group
 no authorization-required
 authorization-dn-attributes CN OU
tunnel-group DefaultRAGroup webvpn-attributes
 hic-fail-group-policy DfltGrpPolicy
 customization DfltCustomization
 authentication aaa
 no override-svc-download
 no radius-reject-message
 dns-group DefaultDNS
tunnel-group DefaultRAGroup ipsec-attributes
 no pre-shared-key
 peer-id-validate req
 no chain
 no trust-point
 isakmp keepalive threshold 1500 retry 2
 no radius-sdi-xauth
 isakmp ikev1-user-authentication xauth
tunnel-group DefaultRAGroup ppp-attributes
 no authentication pap
 authentication chap
 authentication ms-chap-v1
 no authentication ms-chap-v2
 no authentication eap-proxy
```

IPsec 터널 그룹 일반 특성

일반 특성은 두 개 이상의 터널 그룹 유형에서 공통적입니다. IPsec 원격 액세스 및 클라이언트리스 SSL VPN 터널은 동일한 일반 특성 대부분을 공유합니다. IPsec LAN-to-LAN 터널은 하위 집합을 사

용합니다. 모든 명령 전체에 대한 설명은 *Cisco ASA Series* 명령 참조를 참조하십시오. 이 섹션에서는 순서대로 원격 액세스 및 LAN-to-LAN 연결 프로파일을 구성하는 방법에 대해 설명합니다.

원격 액세스 연결 프로파일 구성

다음의 원격 클라이언트와 중앙 사이트 ASA 간에 연결을 설정할 경우 원격 액세스 연결 프로파일을 사용하십시오.

- AnyConnect Secure Mobility Client(SSL 또는 IPsec/IKEv2와 연결)
- 클라이언트리스 SSL VPN(SSL과의 브라우저 기반 연결)
- Cisco ASA 5500 Easy VPN 하드웨어 클라이언트(IPsec/IKEv1과 연결)

또한 이름이 DfltGrpPolicy인 기본 그룹 정책을 제공합니다.

원격 액세스 연결 프로파일을 구성하려면 먼저 터널 그룹 일반 특성을 구성한 다음 원격 액세스 특성을 구성하십시오. 다음 섹션을 참조하십시오.

- 원격 액세스 연결 프로파일에 대한 이름 및 유형 지정, 105 페이지.
- 원격 액세스 연결 프로파일 일반 특성 구성, 105 페이지.
- 이중 인증 구성, 110 페이지
- 원격 액세스 연결 프로파일 IPsec IKEv1 특성 구성, 112 페이지.
- IPsec 원격 액세스 연결 프로파일 PPP 특성 구성, 114 페이지

원격 액세스 연결 프로파일에 대한 이름 및 유형 지정

프로시저

	명령 또는 동작	목적
단계 **1**	**tunnel-group** 명령을 입력하여 연결 프로파일을 생성하고, 그 이름과 유형을 지정합니다. 예제: 예를 들어 이름이 TunnelGroup1인 원격 액세스 연결 프로파일을 생성하려면 다음 명령을 입력합니다. `hostname(config)# tunnel-group TunnelGroup1 type remote-access` `hostname(config)#`	원격 액세스 터널의 유형은 **remote-access**입니다. **tunnel-group** *tunnel_group_name* **type remote-access**

원격 액세스 연결 프로파일 일반 특성 구성

연결 프로파일 일반 특성을 구성하거나 변경하려면 다음 단계대로 매개변수를 지정하십시오.

프로시저

단계 1 일반 속성을 구성하려면 단일 또는 다중 상황 모드 중 하나에서 **tunnel-group general-attributes** 작업을 입력하여 터널 그룹 일반 속성 구성 모드를 시작합니다. 확인 상자가 변경되어 모드의 변경사항을 나타냅니다.

```
hostname(config)# tunnel-group tunnel_group_name general-attributes
hostname(config-tunnel-general)#
```

단계 2 사용할 인증 서버 그룹이 있는 경우 이름을 지정합니다. 지정된 서버 그룹이 실패하는 경우 인증을 위해 로컬 데이터베이스를 사용하려면 다음과 같이 키워드 **LOCAL**을 추가합니다.

```
hostname(config-tunnel-general)# authentication-server-group [(interface_name)] groupname
[LOCAL]
hostname(config-tunnel-general)#
```

인증 서버 그룹의 이름은 최대 16자까지 입력할 수 있습니다.

그룹 이름 다음에 인터페이스 이름을 포함시켜 선택에 따라 인터페이스 특정 인증을 구성할 수 있습니다. 터널이 종료되는 위치를 지정하는 인터페이스 이름은 괄호로 묶어야 합니다. 다음 명령은 인증을 위해 이름이 servergroup1인 서버를 사용하는 인터페이스 이름이 지정된 테스트에 대해 인터페이스 특정 인증을 구성합니다.

```
hostname(config-tunnel-general)# authentication-server-group (test) servergroup1
hostname(config-tunnel-general)#
```

단계 3 사용할 권한 부여 서버 그룹이 있는 경우 이름을 지정합니다. 이 값을 구성하는 경우 사용자가 다음과 같이 연결하려는 권한 부여 데이터베이스에 있어야 합니다.

```
hostname(config-tunnel-general)# authorization-server-group groupname
hostname(config-tunnel-general)#
```

권한 부여 서버 그룹의 이름은 최대 16자까지 입력할 수 있습니다. 예를 들어 다음 명령은 권한 부여 서버 그룹인 FinGroup을 사용하도록 지정합니다.

```
hostname(config-tunnel-general)# authorization-server-groupFinGroup
hostname(config-tunnel-general)#
```

단계 4 사용할 계정 관리 서버 그룹이 있는 경우 이름을 다음과 같이 지정합니다.

```
hostname(config-tunnel-general)# accounting-server-group groupname
hostname(config-tunnel-general)#
```

계정 관리 서버 그룹의 이름은 최대 16자까지 입력할 수 있습니다. 예를 들어 다음 명령은 이름이 comptroller인 계정 관리 서버 그룹을 사용하도록 지정합니다.

```
hostname(config-tunnel-general)# accounting-server-group comptroller
hostname(config-tunnel-general)#
```

단계 **5** 기본 그룹 정책의 이름을 다음과 같이 지정합니다.

```
hostname(config-tunnel-general)# default-group-policy policyname
hostname(config-tunnel-general)#
```

그룹 정책의 이름은 최대 64자까지 입력할 수 있습니다. 다음은 DfltGrpPolicy를 기본 그룹 정책의 이름으로 설정한 예입니다.

```
hostname(config-tunnel-general)# default-group-policy DfltGrpPolicy
hostname(config-tunnel-general)#
```

단계 **6** DHCP 서버(최대 10개의 서버)의 이름 또는 IP 주소 및 DHCP 주소 풀(최대 6개의 풀)의 이름을 지정합니다. 기본값은 DHCP 서버 없음(no dhcp-server) 및 주소 풀 없음(no address-pool)입니다. dhcp-server 명령을 사용하면 ASA가 VPN 클라이언트에 대한 IP 주소를 가져오려고 시도할 때 지정된 DHCP 서버에 추가 옵션을 전송하도록 구성할 수 있습니다. 자세한 내용은 Cisco ASA Series 명령 참조 설명서의 dhcp-server 명령을 참조하십시오.

```
hostname(config-tunnel-general)# dhcp-server server1 [...server10]
hostname(config-tunnel-general)# address-pool [(interface name)] address_pool1
[...address_pool6]
hostname(config-tunnel-general)#
```

참고 인터페이스 이름을 지정하는 경우 괄호로 묶어야 합니다.

전역 구성 모드에서 **ip local pool** 명령을 사용하여 주소 풀을 구성합니다.

단계 **7** Network Admission Control을 사용하는 경우 Network Admission Control 보안 상태 검증에 사용할 인증 서버 그룹을 식별하기 위해 NAC 인증 서버 그룹의 이름을 지정합니다. NAC를 지원하려면 Access Control Server를 하나 이상 구성합니다. ACS 그룹의 이름을 지정하려면 **aaa-server** 명령을 사용합니다. 그런 다음 서버 그룹에 대한 동일한 이름을 사용하여 **nac-authentication-server-group** 명령을 사용합니다.

다음 예는 acs-group1을 NAC 상태 검증에 사용할 인증 서버 그룹으로 식별합니다.

```
hostname(config-group-policy)# nac-authentication-server-group acs-group1
hostname(config-group-policy)
```

다음은 기본 원격 액세스 그룹에서 인증 서버 그룹을 상속받는 예입니다.

```
hostname(config-group-policy)# no nac-authentication-server-group
hostname(config-group-policy)
```

참고 NAC에는 원격 호스트에 있는 Cisco Trust Agent가 필요합니다.

단계 **8** AAA 서버로 전달하기 전에 사용자 이름에서 그룹 또는 영역의 제거 여부를 지정합니다. 기본값은 다음과 같이 그룹 이름 또는 영역 중 하나를 제거하지 않는 것입니다.

```
hostname(config-tunnel-general)# strip-group
hostname(config-tunnel-general)# strip-realm
hostname(config-tunnel-general)#
```

영역은 관리 도메인입니다. 영역을 제거하는 경우 ASA는 사용자 이름 및 그룹(있는 경우)을 인증에 사용합니다. 그룹을 제거하는 경우 ASA는 사용자 이름 및 영역(있는 경우)을 인증에 사용합니다. 인증 중에 사용자 이름에서 영역 한정자를 제거하려면 **strip-realm** 명령을 입력하고 그룹 한정자를 제거하려면 strip-group 명령을 사용합니다. 두 가지 한정자를 모두 제거하는 경우, 인증은 사용자 이름만 기반으로 합니다. 기타의 경우, 인증은 전체 *username@realm* 또는 사용자 이름<delimiter> 그룹 문자열을 기반으로 합니다. 서버에서 구분 기호를 분석할 수 없는 경우 **strip-realm**을 지정하십시오.

단계 **9** 서버가 RADIUS, NT를 사용하는 RADIUS 또는 LDAP 서버인 경우, 선택에 따라 비밀번호 관리를 활성화할 수 있습니다.

참고 인증을 위해 LDAP 디렉토리 서버를 사용 중인 경우, 비밀번호 관리가 Sun Microsystems JAVA System Directory Server(이전 이름은 Sun ONE Directory Server) 및 Microsoft Active Directory에서 지원됩니다.

Sun - Sun 디렉터리 서버에 액세스하려면 ASA에 구성된 DN이 이 서버의 기본 비밀번호 정책에 액세스할 수 있어야 합니다. 디렉토리 관리자 또는 디렉토리 관리자 권한이 있는 사용자를 DN으로 사용할 것을 권장합니다. 또는 기본 비밀번호 정책에 ACI를 배치할 수 있습니다.

Microsoft - Microsoft Active Directory에서 비밀번호 관리를 활성화하려면 LDAP over SSL을 구성해야 합니다.

이 기능은 기본적으로 비활성화되어 있으며 현재 비밀번호가 만료되는 시기를 사용자에게 경고합니다. 기본값은 만료 14일 전부터 사용자에게 경고를 시작하는 것입니다.

```
hostname(config-tunnel-general)# password-management
hostname(config-tunnel-general)#
```

LDAP 서버인 경우 보류 중인 만료에 대해 사용자에게 경고를 시작하기 위해 다음과 같이 만료 전 날짜 수(0부터 180까지)를 지정할 수 있습니다.

```
hostname(config-tunnel-general)# password-management [password-expire in days n]
hostname(config-tunnel-general)#
```

참고 터널 그룹 일반 속성 구성 모드에 입력한 **password-management** 명령은 터널 그룹 ipsec 속성 모드에서 이전에 입력한 더 이상 사용되지 않는 **radius-with-expiry** 명령을 대체합니다.

password-management 명령을 구성하는 경우, ASA는 로그인 시 원격 사용자에게 사용자의 현재 비밀번호가 만료 예정이거나 이미 만료되었음을 알립니다. 그런 다음 ASA에서는 사용자에게 비밀번호를 변경할 기회를 제공합니다. 현재 비밀번호가 아직 만료되지 않은 경우, 사용자는 이 비밀번호를

사용하여 계속 로그인할 수 있습니다. RADIUS 또는 LDAP 인증이 구성되어 있지 않으면 ASA는 이 명령을 무시합니다.

이 명령은 비밀번호 만료 이전 날짜 수는 변경하지 않으며 대신 ASA에서 비밀번호가 만료될 예정임을 사용자에게 경고하기 시작하는 만료일 이전 날짜 수는 변경할 수 있습니다.

이 **password-expire-in-days** 키워드를 지정하는 경우, 날짜 수도 지정하십시오.

이 명령에서 날짜 수를 0으로 설정하면 이 명령이 비활성화됩니다. ASA는 보류 중인 만료에 대해 사용자에게 알리지 않지만 사용자는 비밀번호가 만료된 이후에 비밀번호를 변경할 수 있습니다.

자세한 내용은 비밀번호 관리를 위한 Microsoft Active Directory 설정 구성, 136 페이지를 참조하십시오.

MS-CHAPv2를 지원하는 모든 RADIUS 연결 또는 LDAP를 통해 인증하는 경우, ASA 7.1 이상 버전은 일반적으로 AnyConnect VPN 클라이언트, Cisco IPsec VPN 클라이언트 및 SSL VPN 전체 터널링 클라이언트 및 클라이언트리스 연결을 위해 비밀번호 관리를 지원합니다. 비밀번호 관리는 Kerberos/AD(Windows 비밀번호) 또는 NT 4.0 도메인을 위한 이 연결 유형에 대해 지원되지 않습니다.

MS-CHAP를 지원하는 일부 RADIUS 서버는 현재 MS-CHAPv2를 지원하지 않습니다. **password-management** 명령에는 MS-CHAPv2가 필요하므로 공급업체에 확인하십시오.

참고 RADIUS 서버(예: Cisco ACS)는 인증 요청을 다른 인증 서버로 프록시할 수 있습니다. 그러나 ASA 관점에서 보면 RADIUS 서버와만 통신하는 것입니다.

LDAP의 경우 시중에 출시된 여러 LDAP 서버 전용의 비밀번호 변경 방법이 있습니다. 현재 ASA에서는 Microsoft Active Directory 및 Sun LDAP 서버에만 사용할 수 있는 독점적 비밀번호 관리 로직을 구축하고 있습니다. 기본 LDAP에는 SSL 연결이 필요합니다. LDAP에 대한 비밀번호 관리를 시도하기 전에 LDAP over SSL을 활성화해야 합니다. 기본적으로 LDAP는 포트 636을 사용합니다.

단계 **10**

단계 **11** 인증서에서 권한 부여 쿼리의 이름을 파생시키는 데 사용할 특성을 지정합니다. 이 특성은 다음과 같이 권한 부여를 위해 사용자 이름으로 주체 DN 필드의 어느 부분을 사용할지 지정합니다.

```
hostname(config-tunnel-general)# authorization-dn-attributes {primary-attribute
[secondary-attribute] | use-entire-name}
```

예를 들어 다음 명령은 권한 부여를 위해 사용자 이름으로 CN 특성을 사용하도록 지정합니다.

```
hostname(config-tunnel-general)# authorization-dn-attributes CN
hostname(config-tunnel-general)#
```

authorization-dn-attributes는 **C**(국가), **CN**(공통 이름), **DNQ**(DN 한정자), **EA**(이메일 주소), **GENQ**(세대 한정자), **GN**(이름), **I**(이니셜), **L**(위치), **N**(이름), **O**(조직), **OU**(조직 단위), **SER**(일련 번호), **SN**(성), **SP**(주/도), **T**(직함), **UID**(사용자 ID) 및 **UPN**(사용자 계정 이름)입니다.

단계 **12** 사용자가 연결할 수 있도록 허용하기 전에 권한 부여가 성공해야 하는지를 지정합니다. 기본값은 권한 부여 필요하지 않음입니다.

```
hostname(config-tunnel-general)# authorization-required
hostname(config-tunnel-general)#
```

이중 인증 구성

이중 인증은 로그인 화면에서 사용자에게 추가 인증 자격 증명(예: 두 번째 사용자 이름과 비밀번호)을 입력하도록 요구하는 선택적 기능입니다. 이중 인증을 구성하려면 다음과 같이 명령을 지정하십시오.

프로시저

단계 **1** 2차 인증 서버 그룹을 지정합니다. 이 명령은 AAA 서버 그룹을 2차 AAA 서버로 사용하도록 지정합니다.

참고 이 명령은 AnyConnect 클라이언트 VPN 연결에만 적용됩니다.

2차 서버 그룹은 SDI 서버 그룹을 지정할 수 없습니다. 기본적으로 2차 인증이 필요하지 않습니다.

```
hostname(config-tunnel-general)# secondary-authentication-server-group [interface_name]
{none | LOCAL | groupname [LOCAL]} [use-primary-name]
```

키워드를 사용하지 않는 경우 2차 인증이 필요하지 않습니다. *groupname* 값은 AAA 서버 그룹 이름을 지정합니다. LOCAL은 내부 서버 데이터베이스 사용을 지정하며 groupname(그룹 이름) 값과 함께 사용될 경우 대체를 지정합니다.

예를 들어 1차 인증 서버 그룹을 sdi_group으로 설정하고 2차 인증 서버 그룹을 ldap_server로 설정하려면 다음 명령을 입력합니다.

```
hostname(config-tunnel-general)# authentication-server-group
hostname(config-tunnel-general)# secondary-authentication-server-group
```

참고 **use-primary-name** 키워드를 사용하는 경우 로그인 대화 상자가 하나의 사용자 이름만 요청합니다. 또한 사용자 이름을 디지털 인증서에서 추출한 경우 1차 사용자 이름만 인증에 사용됩니다.

단계 **2** 인증서에서 2차 사용자 이름을 가져오는 경우 다음과 같이 **secondary-username-from-certificate**을 입력합니다.

```
hostname(config-tunnel-general)# secondary-username-from-certificate C | CN | ... | use-script
```

보조 사용자 이름으로 사용하기 위해 인증서에서 추출하는 DN 필드의 값은 기본 **username-from-certificate** 명령에 사용하는 값과 동일합니다. 또는 ASDM에서 생성한 스크립트 파일을 사용하도록 ASA에 지시하는 use-script 키워드를 지정할 수 있습니다.

예를 들어 공통 이름을 1차 사용자 이름 필드로 지정하고 조직 단위를 2차 사용자 이름 필드로 지정하려면 다음 명령을 입력합니다.

```
hostname(config-tunnel-general)# tunnel-group test1 general-attributes
hostname(config-tunnel-general)# username-from-certificate cn
hostname(config-tunnel-general)# secondary-username-from-certificate ou
```

단계 **3** 터널 그룹 webvpn 속성 모드에서 **secondary-pre-fill-username** 명령을 사용하여 인증에 사용하기 위해 클라이언트 인증서로부터의 보조 사용자 이름 추출을 활성화합니다. 이 키워드를 사용하여 이 명령을 클라이언트리스 연결 또는 SSL VPN(AnyConnect) 클라이언트 연결에 적용할지 및 엔드 유저에서 추출한 사용자 이름을 숨길지를 지정합니다. 이 기능은 기본적으로 비활성화되어 있습니다. 클라이언트리스 및 SSL 클라이언트 옵션은 동시에 사용할 수 있지만, 개별 명령에서 구성해야 합니다.

```
hostname(config-tunnel-general)# secondary-pre-fill-username-from-certificate
{clientless | client} [hide]
```

예를 들어 연결을 위한 1차 및 2차 인증에 pre-fill-username을 사용하도록 지정하려면 다음 명령을 입력합니다.

```
hostname(config-tunnel-general)# tunnel-group test1 general-attributes
hostname(config-tunnel-general)# pre-fill-username client
hostname(config-tunnel-general)# secondary-pre-fill-username client
```

단계 **4** 연결에 적용할 권한 부여 특성을 가져오기 위해 어떤 인증 서버를 사용할지 지정합니다. 1차 인증 서버는 기본 선택사항입니다. 다음 명령은 이중 인증에 대해서만 유효합니다.

```
hostname(config-tunnel-general)# authentication-attr-from-server {primary | secondary}
```

예를 들어 2차 인증 서버를 사용하도록 지정하려면 다음 명령을 입력합니다.

```
hostname(config-tunnel-general)# tunnel-group test1 general-attributes
hostname(config-tunnel-general)# authentication-attr-from-server secondary
```

단계 **5** 1차 또는 2차 중에서 어떤 인증 사용자 이름을 세션과 연계할지 지정합니다. 기본값은 1차 인증입니다. 이중 인증이 활성화된 경우, 2개의 고유 사용자 이름을 세션에 대해 인증할 수 있습니다. 관리자는 세션 사용자 이름으로 인증된 사용자 이름 중 하나를 지정해야 합니다. 세션 사용자 이름은 계정 관리, 세션 데이터베이스, syslog 및 디버그 출력을 위해 제공되는 사용자 이름입니다.

```
hostname(config-tunnel-general)# authenticated-session-username {primary | secondary}
```

예를 들어 세션과 연계된 인증 사용자 이름을 2차 인증 서버에서 가져오도록 지정하려면 다음 명령을 입력합니다.

```
hostname(config-tunnel-general)# tunnel-group test1 general-attributes
hostname(config-tunnel-general)# authenticated-session-username secondary
```

원격 액세스 연결 프로파일 IPsec IKEv1 특성 구성

원격 액세스 연결 프로파일용으로 IPsec IKEv1 특성을 구성하려면 다음 단계를 따르십시오. 다음 설명에서는 원격 액세스 연결 프로파일을 이미 생성한 것으로 가정합니다. 원격 액세스 연결 프로파일에는 LAN-to-LAN 연결 프로파일 보다 더 많은 특성이 있습니다.

프로시저

단계 **1** 원격 액세스 터널 그룹의 IPsec 특성을 지정하려면 단일 또는 다중 상황 모드에서 다음 명령을 입력하여 터널 그룹 ipsec 특성 모드를 시작합니다. 확인 상자가 변경되어 모드의 변경사항을 나타냅니다.

```
hostname(config)# tunnel-group tunnel-group-name ipsec-attributes
hostname(config-tunnel-ipsec)#
```

이 명령은 터널 그룹 ipsec 특성 구성 모드를 시작하며 이 구성 모드에서 단일 또는 다중 상황 모드로 원격 액세스 터널 그룹 IPsec 특성을 구성합니다.

예를 들어 다음 명령은 뒤에 오는 터널 그룹 ipsec 특성 모드 명령이 TG1 이름의 연결 프로파일과 관련이 있음을 지정합니다. 현재 터널 그룹 ipsec 특성 모드에 있음을 나타내도록 다음과 같이 확인 상자가 변경되었음을 유의하십시오.

```
hostname(config)# tunnel-group TG1 type remote-access
hostname(config)# tunnel-group TG1 ipsec-attributes
hostname(config-tunnel-ipsec)#
```

단계 **2** 사전 공유 키를 기반으로 하는 IKEv1 연결을 지원하도록 사전 공유 키를 지정합니다. 예를 들어 다음 명령은 IPsec IKEv1 원격 액세스 연결 프로파일에 대한 IKEv1 연결을 지원하도록 사전 공유 키인 xyzx를 지정합니다.

```
hostname(config-tunnel-ipsec)# ikev1 pre-shared-key xyzx
hostname(config-tunnel-ipsec)#
```

단계 **3** 다음과 같이 피어 인증서를 사용하여 피어 ID를 확인할지 지정합니다.

```
hostname(config-tunnel-ipsec)# peer-id-validate option
hostname(config-tunnel-ipsec)#
```

가능한 *option* 값은 **req**(필수), **cert (**인증서에서 지원하는 경우) 및 **nocheck (**선택하지 않음)입니다. 기본값은 **req**입니다.

예를 들어 다음 명령은 피어 ID 검증이 필수임을 지정합니다.

```
hostname(config-tunnel-ipsec)# peer-id-validate req
hostname(config-tunnel-ipsec)#
```

단계 **4** 인증서 체인의 전송을 활성화할지 지정합니다. 다음 명령은 전송 시 루트 인증서 및 하위 CA 인증서를 포함합니다.

```
hostname(config-tunnel-ipsec)# chain
hostname(config-tunnel-ipsec)#
```

이 특성은 모든 IPsec 터널 그룹 유형에 적용됩니다.

단계 **5** 다음과 같이 IKE 피어에 전송할 인증서를 식별하는 신뢰 지점의 이름을 지정합니다.

```
hostname(config-tunnel-ipsec)# ikev1 trust-point trust-point-name
hostname(config-tunnel-ipsec)#
```

다음 명령은 IKE 피어에 전송할 인증서의 이름으로 mytrustpoint를 지정합니다.

```
hostname(config-ipsec)# ikev1 trust-point mytrustpoint
```

단계 **6** 다음과 같이 허용되는 ISAKMP 킵얼라이브 임계값과 재시도 횟수를 지정합니다.

```
hostname(config-tunnel-ipsec)# isakmp keepalive threshold <number> retry <number>
hostname(config-tunnel-ipsec)#
```

threshold 매개변수는 피어가 킵얼라이브 모니터링을 시작하기 전에 유휴하도록 허용되는 초 단위의 수(10초부터 3600초)를 지정합니다. **retry** 매개변수는 킵얼라이브 응답이 수신되지 않은 이후 재시도 사이의 간격(2초부터 10초)입니다. IKE 킵얼라이브는 기본적으로 활성화되어 있습니다. ISAKMP 킵얼라이브를 비활성화하려면 **isakmp keepalive disable**을 입력합니다.

예를 들어 다음 명령은 IKE 킵얼라이브 임계값을 15초로 설정하고 재시도 간격을 10초로 설정합니다.

```
hostname(config-tunnel-ipsec)# isakmp keepalive threshold 15 retry 10
hostname(config-tunnel-ipsec)#
```

threshold 매개변수에 대한 기본값은 원격 액세스의 경우 300이고 LAN-to-LAN의 경우 10이며 재시도 매개변수에 대한 기본값은 2입니다.

중앙 사이트(보안 게이트웨이)에서 ISAKMP 모니터링을 시작하지 않도록 지정하려면 다음 명령을 입력합니다.

```
hostname(config-tunnel-ipsec)# isakmp keepalive threshold infinite
hostname(config-tunnel-ipsec)#
```

단계 **7** ISAKMP 하이브리드 인증 방법인 XAUTH 또는 하이브리드 XAUTH를 지정합니다.

ASA 인증에 디지털 인증서를 사용하고 RADIUS TACACS+ 또는 SecurID 등의 원격 VPN 사용자 인증에 다른 레거시 방법을 사용해야 하는 경우, **isakmp ikev1-user-authentication** 명령을 사용하여 하이브리드 XAUTH 인증을 구현합니다. 하이브리드 XAUTH는 IKE의 1단계를 다음의 2가지 단계로 분류하며 하이브리드 인증이라고도 합니다.

a) ASA는 표준 공개 키 기술을 사용하여 원격 VPN 사용자를 인증합니다. 그러면 단방향으로 인증되는 IKE 보안 연결이 설정됩니다.

b) 그런 다음 XAUTH exchange에서 원격 VPN 사용자를 인증합니다. 이 확장된 인증은 지원되는 레거시 인증 방법 중 하나를 사용할 수 있습니다.

참고 인증 유형을 하이브리드로 설정하려면 먼저 인증 서버를 구성하고 사전 공유 키를 생성하며 신뢰 지점을 구성해야 합니다.

선택적인 인터페이스 매개변수가 있는 **isakmp ikev1-user-authentication** 명령을 사용하여 특정 인터페이스를 지정할 수 있습니다. 인터페이스 매개변수를 생략한 경우, 이 명령은 모든 인터페이스에 적용되고 인터페이스별 명령이 지정되지 않은 경우 백업 역할을 합니다. 연결 프로파일에 대해 두 개의 **isakmp ikev1-user-authentication** 명령이 지정된 경우, 한 명령은 **interface** 매개변수를 사용하고 나머지 명령은 사용하지 않을 때는 인터페이스를 지정하는 매개변수가 특정 인터페이스용으로 우선시 됩니다.

예를 들어 다음 명령은 내부 인터페이스에서 example-group이라는 연결 프로파일에 대해 하이브리드 XAUTH를 활성화합니다.

```
hostname(config)# tunnel-group example-group type remote-access
hostname(config)# tunnel-group example-group ipsec-attributes
hostname(config-tunnel-ipsec)# isakmp ikev1-user-authentication (inside) hybrid
hostname(config-tunnel-ipsec)#
```

IPsec 원격 액세스 연결 프로파일 PPP 특성 구성

원격 액세스 연결 프로파일용으로 Point-to-Point 프로토콜 특성을 구성하려면 다음 단계를 따르십시오. PPP 특성은 IPsec 원격 액세스 연결 프로파일에만 적용됩니다. 다음 설명에서는 IPsec 원격 액세스 연결 프로파일을 이미 생성한 것으로 가정합니다.

프로시저

단계 **1** 터널 그룹 ppp 특성 구성 모드를 시작하며 다음 명령을 입력하여 이 구성 모드에서 원격 액세스 터널 그룹 PPP 특성을 구성합니다. 확인 상자가 변경되어 모드의 변경사항을 나타냅니다.

```
hostname(config)# tunnel-group tunnel-group-name type remote-access
hostname(config)# tunnel-group tunnel-group-name ppp-attributes
hostname(config-tunnel-ppp)#
```

예를 들어 다음 명령은 뒤에 오는 터널 그룹 ppp 특성 모드 명령이 TG1 이름의 연결 프로파일과 관련이 있음을 지정합니다. 현재 터널 그룹 ppp 특성 모드에 있음을 나타내도록 다음과 같이 확인 상자가 변경되었음을 유의하십시오.

```
hostname(config)# tunnel-group TG1 type remote-access
hostname(config)# tunnel-group TG1 ppp-attributes
hostname(config-tunnel-ppp)#
```

단계 **2** PPP 연결을 위해 특정 프로토콜을 사용하여 인증을 활성화할지 지정합니다. 프로토콜 값으로 다음 중 하나가 사용될 수 있습니다.

- pap — PPP 연결을 위해 비밀번호 인증 프로토콜의 사용을 활성화합니다.
- chap — PPP 연결을 위해 챌린지 핸드셰이크 인증 프로토콜의 사용을 활성화합니다.
- ms-chap-v1 또는 ms-chap-v2 — PPP 연결을 위해 Microsoft 챌린지 핸드셰이크 인증 프로토콜, 버전 1 또는 버전 2의 사용을 활성화합니다.
- eap — PPP 연결을 위해 확장 가능 인증 프로토콜의 사용을 활성화합니다.

CHAP 및 MSCHAPv1은 기본적으로 활성화되어 있습니다.

이 명령의 구문은 다음과 같습니다.

```
hostname(config-tunnel-ppp)# authentication protocol
hostname(config-tunnel-ppp)#
```

특정한 프로토콜에 대한 인증을 비활성화하려면 다음과 같이 **no** 형식의 명령을 사용합니다.

```
hostname(config-tunnel-ppp)# no authentication protocol
hostname(config-tunnel-ppp)#
```

예를 들어 다음 명령은 PPP 연결을 위해 PAP 프로토콜 사용을 활성화합니다.

```
hostname(config-tunnel-ppp)# authentication pap
hostname(config-tunnel-ppp)#
```

다음 명령은 PPP 연결을 위해 MS-CHAP, 버전 2 프로토콜 사용을 활성화합니다.

```
hostname(config-tunnel-ppp)# authentication ms-chap-v2
hostname(config-tunnel-ppp)#
```

다음 명령은 PPP 연결을 위해 EAP-PROXY 프로토콜 사용을 활성화합니다.

```
hostname(config-tunnel-ppp)# authentication pap
hostname(config-tunnel-ppp)#
```

다음 명령은 PPP 연결을 위해 MS-CHAP, 버전 1 프로토콜 사용을 비활성화합니다.

```
hostname(config-tunnel-ppp)# no authentication ms-chap-v1
hostname(config-tunnel-ppp)#
```

LAN-to-LAN 연결 프로파일 구성

IPsec LAN-to-LAN VPN 연결 프로파일은 LAN-to-LAN IPsec 클라이언트 연결에만 적용됩니다. 구성한 매개변수 중 다수가 IPsec 원격 액세스 연결 프로파일과 동일하지만 LAN-to-LAN 터널에는 동일한 매개변수가 더 적습니다. 다음 섹션에서는 LAN-to-LAN 연결 프로파일을 구성하는 방법을 보여줍니다.

기본 LAN-to-LAN 연결 프로파일 구성

기본 LAN-to-LAN 연결 프로파일의 콘텐츠는 다음과 같습니다.

```
tunnel-group DefaultL2LGroup type ipsec-l2l
tunnel-group DefaultL2LGroup general-attributes
 default-group-policy DfltGrpPolicy
tunnel-group DefaultL2LGroup ipsec-attributes
 no ikev1 pre-shared-key
 peer-id-validate req
 no chain
 no ikev1 trust-point
 isakmp keepalive threshold 10 retry 2
```

LAN-to-LAN 연결 프로파일에는 원격 액세스 연결 프로파일보다 적은 수의 매개변수가 있으며 대부분 두 그룹에 동일합니다. 연결을 보다 쉽게 구성할 수 있도록 아래에서 개별적으로 설명했습니다. 사용자가 명시적으로 구성하지 않은 모든 매개변수는 기본 연결 프로파일에서 값을 상속받습니다.

LAN-to-LAN 연결 프로파일에 대한 이름 및 유형 지정

연결 프로파일에 대해 이름 및 유형을 지정하려면 다음과 같이 **tunnel-group** 명령을 입력합니다.

```
hostname(config)# tunnel-group tunnel_group_name type tunnel_type
```

LAN-to-LAN 터널의 경우, 유형은 **ipsec-l2l**입니다. 예를 들어 이름이 docs인 LAN-to-LAN 연결 프로파일을 생성하려면 다음 명령을 입력합니다.

```
hostname(config)# tunnel-group docs type ipsec-l2l
hostname(config)#
```

LAN-to-LAN 연결 프로파일 일반 특성 구성

연결 프로파일 일반 특성을 구성하려면 다음 단계를 따르십시오.

프로시저

단계 **1** 단일 또는 다중 상황 모드에서 일반 특성 키워드를 지정하여 터널 그룹 일반 특성 모드를 시작합니다.

tunnel-group *tunnel-group-name* **general-attributes**

예제**:**

이름이 docs인 연결 프로파일의 경우 다음 명령을 입력합니다.

```
hostname(config)# tunnel-group docs general-attributes
hostname(config-tunnel-general)#
```

현재 config-general 모드에 있음을 나타내도록 확인 상자가 변경되며 이 모드에서 터널 그룹 일반 특성을 구성합니다.

단계 **2** 기본 그룹 정책의 이름을 다음과 같이 지정합니다.

default-group-policy *policyname*

예제**:**

다음 명령은 기본 그룹 정책 이름을 MyPolicy로 지정합니다.

```
hostname(config-tunnel-general)# default-group-policy MyPolicy
hostname(config-tunnel-general)#
```

LAN-to-LAN IPsec IKEv1 특성 구성

IPsec IKEv1 특성을 구성하려면 다음 단계를 수행하십시오.

프로시저

단계 **1** 터널 그룹 IPsec IKEv1 특성을 구성하려면 단일 또는 다중 상황 모드에서 IPSec 특성 키워드와 함께 터널 그룹 명령을 입력하여 터널 그룹 ipsec 특성 구성 모드를 시작합니다.

```
hostname(config)# tunnel-group tunnel-group-name ipsec-attributes
hostname(config-tunnel-ipsec)#
```

예를 들어 다음 명령은 이름이 TG1인 연결 프로파일에 대해 매개변수를 구성할 수 있도록 config-ipsec 모드를 시작합니다.

```
hostname(config)# tunnel-group TG1 ipsec-attributes
hostname(config-tunnel-ipsec)#
```

현재 터널 그룹 ipsec 특성 구성 모드에 있음을 나타내도록 확인 상자가 변경됩니다.

단계 **2** 사전 공유 키를 기반으로 하는 IKEv1 연결을 지원하도록 사전 공유 키를 지정합니다.

```
hostname(config-tunnel-ipsec)# ikev1 pre-shared-key key
hostname(config-tunnel-ipsec)#
```

예를 들어 다음 명령은 LAN-to-LAN 연결 프로파일에 대한 IKEv1 연결을 지원하도록 사전 공유 키인 XYZX를 지정합니다.

```
hostname(config-tunnel-ipsec)# ikev1 pre-shared-key xyzx
hostname(config-tunnel-general)#
```

단계 **3** 다음과 같이 피어 인증서를 사용하여 피어 ID를 확인할지 지정합니다.

```
hostname(config-tunnel-ipsec)# peer-id-validate option
hostname(config-tunnel-ipsec)#
```

가능한 옵션은 **req**(필수), **cert (**인증서에서 지원하는 경우) 및 **nocheck (**선택하지 않음)입니다. 기본값은 **req**입니다. 예를 들어 다음 명령은 peer-id-validate 옵션을 **nocheck**로 설정합니다.

```
hostname(config-tunnel-ipsec)# peer-id-validate nocheck
hostname(config-tunnel-ipsec)#
```

단계 **4** 인증서 체인의 전송을 활성화할지 지정합니다. 이 작업은 전송 시 루트 인증서 및 하위 CA 인증서를 포함합니다.

```
hostname(config-tunnel-ipsec)# chain
hostname(config-tunnel-ipsec)#
```

모든 터널 그룹 유형에 이 특성을 적용할 수 있습니다.

단계 **5** 다음과 같이 IKE 피어에 전송할 인증서를 식별하는 신뢰 지점의 이름을 지정합니다.

```
hostname(config-tunnel-ipsec)# trust-point trust-point-name
hostname(config-tunnel-ipsec)#
```

예를 들어 다음 명령은 신뢰 지점 이름을 mytrustpoint로 설정합니다.

```
hostname(config-tunnel-ipsec)# trust-point mytrustpoint
hostname(config-tunnel-ipsec)#
```

모든 터널 그룹 유형에 이 특성을 적용할 수 있습니다.

단계 **6** 허용되는 ISAKMP(IKE) 킵얼라이브 임계값과 재시도 횟수를 지정합니다. **threshold** 매개변수는 피어가 킵얼라이브 모니터링을 시작하기 전에 유휴하도록 허용되는 초 단위의 수(10초부터 3600초)를 지정합니다. **retry** 매개변수는 킵얼라이브 응답이 수신되지 않은 이후 재시도 사이의 간격(2초부터 10초)입니다. IKE 킵얼라이브는 기본적으로 활성화되어 있습니다. IKE 킵얼라이브를 비활성화하려면 다음과 같이 **no** 형식의 **isakmp** 명령을 입력합니다.

```
hostname(config)# isakmp keepalive threshold <number> retry <number>
hostname(config-tunnel-ipsec)#
```

예를 들어 다음 명령은 ISAKMP 킵얼라이브 임계값을 15초로 설정하고 재시도 간격을 10초로 설정합니다.

```
hostname(config-tunnel-ipsec)# isakmp keepalive threshold 15 retry 10
hostname(config-tunnel-ipsec)#
```

LAN-to-LAN에 대한 **threshold** 매개변수의 기본값은 10이며 재시도 매개변수에 대한 기본값은 2입니다.

중앙 사이트(보안 게이트웨이)에서 ISAKMP 모니터링을 시작하지 않도록 지정하려면 다음 명령을 입력합니다.

```
hostname(config-tunnel-ipsec)# isakmp keepalive threshold infinite
hostname(config-tunnel-ipsec)#
```

단계 **7** ISAKMP 하이브리드 인증 방법인 XAUTH 또는 하이브리드 XAUTH를 지정합니다.

ASA 인증에 디지털 인증서를 사용하고 RADIUS TACACS+ 또는 SecurID 등의 원격 VPN 사용자 인증에 다른 레거시 방법을 사용해야 하는 경우, **isakmp ikev1-user-authentication** 명령을 사용하여 하이브리드 XAUTH 인증을 구현합니다. 하이브리드 XAUTH는 IKE의 1단계를 다음의 2가지 단계로 분류하며 하이브리드 인증이라고도 합니다.

a) ASA는 표준 공개 키 기술을 사용하여 원격 VPN 사용자를 인증합니다. 그러면 단방향으로 인증되는 IKE 보안 연결이 설정됩니다.
b) 그런 다음 XAUTH exchange에서 원격 VPN 사용자를 인증합니다. 이 확장된 인증은 지원되는 레거시 인증 방법 중 하나를 사용할 수 있습니다.

참고 인증 유형을 하이브리드로 설정하려면 먼저 인증 서버를 구성하고 사전 공유 키를 생성하며 신뢰 지점을 구성해야 합니다.

예를 들어 다음 명령은 example-group이라는 연결 프로파일에 대해 하이브리드 XAUTH를 활성화합니다.

```
hostname(config)# tunnel-group example-group type remote-access
hostname(config)# tunnel-group example-group ipsec-attributes
hostname(config-tunnel-ipsec)# isakmp ikev1-user-authentication hybrid
hostname(config-tunnel-ipsec)#
```

클라이언트리스 SSL VPN 세션에 대한 연결 프로파일 구성

클라이언트리스 SSL VPN 연결 프로파일에 대한 터널 그룹 일반 속성은 터널 그룹 유형이 webvpn이며 **strip-group** 및 **strip-realm** 명령이 적용되지 않는다는 점을 제외하고 IPsec 원격 액세스 연결 프로

파일에 대한 터널 그룹 일반 속성과 동일합니다. 클라이언트리스 SSL VPN의 특정 특성을 개별적으로 정의합니다. 다음 섹션에서는 클라이언트리스 SSL VPN 연결 프로파일을 구성하는 방법에 대해 설명합니다.

- 클라이언트리스 SSL VPN 세션에 대한 일반 터널 그룹 특성 구성, 120 페이지
- 클라이언트리스 SSL VPN 세션에 대한 터널 그룹 특성 구성, 123 페이지

클라이언트리스 SSL VPN 세션에 대한 일반 터널 그룹 특성 구성

연결 프로파일 일반 특성을 구성하거나 변경하려면 다음 단계대로 매개변수를 지정하십시오.

프로시저

단계 1 일반 속성을 구성하려면 **tunnel-group general-attributes** 명령을 입력하여 단일 또는 다중 상황 모드 중 하나에서 터널 그룹 일반 속성 구성 모드를 시작합니다. 확인 상자가 다음과 같이 변경됩니다.

```
hostname(config)# tunnel-group tunnel_group_name general-attributes
hostname(config-tunnel-general)#
```

이전 섹션에서 생성한 TunnelGroup3에 대해 일반 특성을 구성하려면 다음 명령을 입력합니다.

```
hostname(config)# tunnel-group TunnelGroup3 general-attributes
hostname(config-tunnel-general)#
```

단계 2 사용할 인증 서버 그룹이 있는 경우 이름을 지정합니다. 지정된 서버 그룹이 실패하는 경우 인증을 위해 로컬 데이터베이스를 사용하려면 다음과 같이 키워드 LOCAL을 추가합니다.

```
hostname(config-tunnel-general)# authentication-server-group groupname [LOCAL]
hostname(config-tunnel-general)#
```

예를 들어 이름이 test인 인증 서버 그룹을 구성하고 인증 서버 그룹 실패 시 LOCAL 서버에 대체를 제공하려는 경우, 다음 명령을 입력합니다.

```
hostname(config-tunnel-general)# authentication-server-group test LOCAL
hostname(config-tunnel-general)#
```

인증 서버 그룹 이름은 이전에 구성한 인증 서버 또는 서버 그룹을 식별합니다. **aaa-server** 명령을 사용하여 인증 서버를 구성합니다. 그룹 태그의 최대 길이는 16자입니다.

또한 그룹 이름 앞에 인터페이스 이름을 괄호에 포함시켜 인터페이스 특정 인증을 구성할 수 있습니다. 다음 인터페이스는 기본적으로 사용할 수 있습니다.

- inside(내부) — 인터페이스 GigabitEthernet0/1의 이름
- outside(외부) — 인터페이스 GigabitEthernet0/0의 이름

참고 ASA의 외부 인터페이스 주소(IPv4/IPv6 모두 해당)는 사설 측 어드레스 스페이스와 중복될 수 없습니다.

구성한 다른 인터페이스(**interface** 명령 사용)도 사용할 수 있습니다. 다음 명령은 인증을 위해 servergroup1 서버를 사용하는 outside라는 이름의 인터페이스에 대해 인터페이스 특정 인증을 구성합니다.

```
hostname(config-tunnel-general)# authentication-server-group (outside) servergroup1
hostname(config-tunnel-general)#
```

단계 **3** 선택에 따라 사용할 권한 부여 서버 그룹이 있는 경우 이름을 지정합니다. 권한 부여를 사용하지 않는 경우에는 6단계로 이동합니다. 이 값을 구성하는 경우 사용자가 다음과 같이 연결하려는 권한 부여 데이터베이스에 있어야 합니다.

```
hostname(config-tunnel-general)# authorization-server-group groupname
hostname(config-tunnel-general)#
```

aaa-server 명령을 사용하여 권한 부여 서버를 구성합니다. 그룹 태그의 최대 길이는 16자입니다.

예를 들어 다음 명령은 권한 부여 서버 그룹인 FinGroup을 사용하도록 지정합니다.

```
hostname(config-tunnel-general)# authorization-server-group FinGroup
hostname(config-tunnel-general)#
```

단계 **4** 사용자가 연결할 수 있도록 허용하기 전에 권한 부여가 성공해야 하는지를 지정합니다. 기본값은 권한 부여 필요하지 않음입니다.

```
hostname(config-tunnel-general)# authorization-required
hostname(config-tunnel-general)#
```

단계 **5** 인증서에서 권한 부여 쿼리의 이름을 파생시키는 데 사용할 특성을 지정합니다. 이 특성은 다음과 같이 권한 부여를 위해 사용자 이름으로 주체 DN 필드의 어느 부분을 사용할지 지정합니다.

```
hostname(config-tunnel-general)# authorization-dn-attributes {primary-attribute
[secondary-attribute] | use-entire-name}
```

예를 들어 다음 명령은 권한 부여를 위해 사용자 이름으로 CN 특성을 사용하도록 지정합니다.

```
hostname(config-tunnel-general)# authorization-dn-attributes CN
hostname(config-tunnel-general)#
```

authorization-dn-attributes는 **C**(국가), **CN**(공통 이름), **DNQ**(DN 한정자), **EA**(이메일 주소), **GENQ**(세대 한정자), **GN**(이름), **I**(이니셜), **L**(위치), **N**(이름), **O**(조직), **OU**(조직 단위), **SER**(일련 번호), **SN**(성), **SP**(주/도), **T**(직함), **UID**(사용자 ID) 및 **UPN**(사용자 계정 이름)입니다.

단계 **6** 선택에 따라 사용할 계정 관리 서버 그룹이 있는 경우 이름을 지정합니다. 계정 관리를 사용하지 않는 경우에는 7단계로 이동합니다. **aaa-server** 명령을 사용하여 계정 관리 서버를 구성합니다. 그룹 태그의 최대 길이는 16자입니다.

```
hostname(config-tunnel-general)# accounting-server-group groupname
hostname(config-tunnel-general)#
```

예를 들어 다음 명령은 계정 관리 서버 그룹인 comptroller를 사용하도록 지정합니다.

```
hostname(config-tunnel-general)# accounting-server-group comptroller
hostname(config-tunnel-general)#
```

단계 **7** 선택에 따라 기본 그룹 정책의 이름을 다음과 같이 지정합니다. 기본값은 DfltGrpPolicy입니다.

```
hostname(config-tunnel-general)# default-group-policy policyname
hostname(config-tunnel-general)#
```

다음은 MyDfltGrpPolicy를 기본 그룹 정책의 이름으로 설정한 예입니다.

```
hostname(config-tunnel-general)# default-group-policy MyDfltGrpPolicy
hostname(config-tunnel-general)#
```

단계 **8** 선택에 따라 DHCP 서버(최대 10개의 서버)의 이름 또는 IP 주소 및 DHCP 주소 풀(최대 6개의 풀)의 이름을 지정합니다. 공백을 사용하여 목록 항목을 구분합니다. 기본값은 DHCP 서버 없음(no dhcp-server) 및 주소 풀 없음(no address-pool)입니다.

```
hostname(config-tunnel-general)# dhcp-server server1 [...server10]
hostname(config-tunnel-general)# address-pool [(interface name)] address_pool1
[...address_pool6]
hostname(config-tunnel-general)#
```

참고 인터페이스 이름은 괄호로 묶어야 합니다.

전역 구성 모드에서 **ip local pool** 명령을 사용하여 주소 풀을 구성합니다. 주소 풀 구성에 대한 자세한 내용은 VPN용 IP 주소, 199 페이지를 참조하십시오.

단계 **9** 서버가 RADIUS, NT를 사용하는 RADIUS 또는 LDAP 서버인 경우, 선택에 따라 비밀번호 관리를 활성화할 수 있습니다.

참고 인증을 위해 LDAP 디렉토리 서버를 사용 중인 경우, 비밀번호 관리가 Sun Microsystems JAVA System Directory Server(이전 이름은 Sun ONE Directory Server) 및 Microsoft Active Directory에서 지원됩니다.

- Sun - Sun 디렉토리 서버에 액세스하려면 ASA에 구성된 DN이 이 서버의 기본 비밀번호 정책에 액세스할 수 있어야 합니다. 디렉토리 관리자 또는 디렉토리 관리자 권한이 있는 사용자를 DN으로 사용할 것을 권장합니다. 또는 기본 비밀번호 정책에 ACI를 배치할 수 있습니다.
- Microsoft - Microsoft Active Directory에서 비밀번호 관리를 활성화하려면 LDAP over SSL을 구성해야 합니다.

이 기능은 기본적으로 활성화되어 있으며 현재 비밀번호가 만료되는 시기를 사용자에게 경고합니다. 기본값은 만료 14일 전부터 사용자에게 경고를 시작하는 것입니다.

```
hostname(config-tunnel-general)# password-management
hostname(config-tunnel-general)#
```

LDAP 서버인 경우 보류 중인 만료에 대해 사용자에게 경고를 시작하기 위해 다음과 같이 만료 전 날짜 수(0부터 180까지)를 지정할 수 있습니다.

```
hostname(config-tunnel-general)# password-management [password-expire in days n]
hostname(config-tunnel-general)#
```

참고 터널 그룹 일반 특성 구성 모드에 입력한 **password-management** 명령은 터널 그룹 ipsec 특성 모드에서 이전에 입력한 더 이상 사용되지 않는 **radius-with-expiry** 명령을 대체합니다.

이 명령을 구성하는 경우, ASA는 로그인 시 원격 사용자에게 사용자의 현재 비밀번호가 만료 예정이거나 이미 만료되었음을 알립니다. 그런 다음 ASA에서는 사용자에게 비밀번호를 변경할 기회를 제공합니다. 현재 비밀번호가 아직 만료되지 않은 경우, 사용자는 이 비밀번호를 사용하여 계속 로그인할 수 있습니다. RADIUS 또는 LDAP 인증이 구성되어 있지 않으면 ASA는 이 명령을 무시합니다.

이 명령은 비밀번호 만료 이전 날짜 수는 변경하지 않으며 대신 ASA에서 비밀번호가 만료될 예정임을 사용자에게 경고하기 시작하는 만료일 이전 날짜 수는 변경할 수 있습니다.

이 **password-expire-in-days** 키워드를 지정하는 경우, 날짜 수도 지정하십시오.

자세한 내용은 비밀번호 관리를 위한 Microsoft Active Directory 설정 구성, 136 페이지를 참조하십시오.

클라이언트리스 SSL VPN 세션에 대한 터널 그룹 특성 구성

클라이언트리스 SSL VPN 연결 프로파일에 특정한 매개변수를 구성하려면 다음 섹션의 단계를 수행하십시오. 클라이언트리스 SSL VPN은 이전에는 WebVPN이라고 했으며 터널 그룹 webvpn 특성 모드에서 이 특성을 구성하십시오.

프로시저

단계 **1** 클라이언트리스 SSL VPN 터널 그룹의 특성을 지정하려면 다음 명령을 입력하여 터널 그룹 webvpn 특성 모드를 시작합니다. 확인 상자가 변경되어 모드의 변경사항을 나타냅니다.

```
hostname(config)# tunnel-group tunnel-group-name webvpn-attributes
hostname(config-tunnel-ipsec)#
```

예를 들어 클라이언트리스 SSL VPN 터널 그룹 이름인 sales에 대해 webvpn 특성을 지정하려면 다음 명령을 입력합니다.

```
hostname(config)# tunnel-group sales webvpn-attributes
```

```
hostname(config-tunnel-webvpn)#
```

단계 **2** 사용할 인증 방법을 AAA, 디지털 인증서 또는 모두로 지정하려면 **authentication** 명령을 입력합니다. 임의 순서로 aaa나 인증서 또는 모두로 지정할 수 있습니다.

```
hostname(config-tunnel-webvpn)# authentication authentication_method
hostname(config-tunnel-webvpn)#
```

예를 들어 다음 명령은 AAA 및 인증서 인증을 모두 허용합니다.

```
hostname(config-tunnel-webvpn)# authentication aaa certificate
hostname(config-tunnel-webvpn)#
```

단계 **3** ASA는 IP 주소에 NetBIOS 이름을 매핑하기 위해 NetBIOS 이름 서버를 쿼리합니다. 클라이언트리스 SSL VPN에는 원격 시스템에 있는 파일에 액세스하거나 이 파일을 공유하기 위해 NetBIOS가 필요합니다. 클라이언트리스 SSL VPN은 NetBIOS 및 CIFS 프로토콜을 사용하여 원격 시스템에 있는 파일에 액세스하거나 이 파일을 공유합니다. 해당 컴퓨터 이름을 사용하여 Windows 컴퓨터에 파일 공유 연결을 시도할 경우 지정하는 파일 서버가 네트워크에서 리소스를 식별하는 특정 NetBIOS 이름과 일치합니다.

NBNS 기능이 작동하려면 최소한 하나 이상의 NetBIOS 서버(호스트)를 구성해야 합니다. 이중화를 위해 최대 3개까지 NBNS 서버를 구성할 수 있습니다. ASA는 NetBIOS/CIFS 이름 확인을 위해 목록에서 첫 번째 서버를 사용합니다. 쿼리가 실패할 경우 다음 서버를 사용합니다.

CIFS 이름 확인에 사용할 NBNS(NetBIOS Name Service: NetBIOS 이름 서비스) 서버의 이름을 지정하려면 **nbns-server** 명령을 사용합니다. 최대 3개까지 서버 항목을 입력할 수 있습니다. 구성한 첫 번째 서버는 1차 서버이고 나머지 하나는 이중화를 위한 백업 서버입니다. 마스터 브라우저(WINS 서버가 아닌 서버)인지 여부, 시간 제한 간격 및 재시도 횟수를 지정할 수 있습니다. WINS 서버 또는 마스터 브라우저는 일반적으로 ASA와 동일한 네트워크에 있거나 해당 네트워크에서 연결할 수 있습니다. 다음과 같이 재시도 횟수보다 먼저 시간 제한 간격을 지정해야 합니다.

```
hostname(config-tunnel-webvpn)# nbns-server {host-name | IP_address} [master] [seconds]
[retry number]
hostname(config-tunnel-webvpn)#
```

예를 들어 1차 서버로 이름이 nbnsprimary인 서버를 구성하고 2차 서버로 192.168.2.2 서버를 구성하며 각각 3번의 재시도와 5초의 시간 제한 간격을 허용하도록 다음 명령을 입력합니다.

```
hostname(config)# name 192.168.2.1 nbnsprimary
hostname(config-tunnel-webvpn)# nbns-server nbnsprimary master timeout 5 retry 3
hostname(config-tunnel-webvpn)# nbns-server 192.168.2.2 timeout 5 retry 3
hostname(config-tunnel-webvpn)#
```

시간 제한 간격은 1초에서 30초까지 가능하며(기본값은 2초) 재시도 횟수는 0번부터 10번까지 가능합니다(기본값은 2번).

터널 그룹 webvpn 속성 구성 모드의 **nbns-server** 명령은 webvpn 구성 모드에서 더 이상 사용되지 않는 **nbns-server** 명령을 대체합니다.

단계 **4** 그룹에 대해 대체 이름을 지정하려면 **group-alias** 명령을 사용합니다. 그룹 별칭을 지정하면 사용자가 터널 그룹을 나타낼 수 있는 하나 이상의 대체 이름이 생성됩니다. 여기에서 지정하는 그룹 별칭은 사용자의 로그인 페이지에 있는 드롭다운 목록에 나타납니다. 각 그룹에는 여러 개의 별칭이 있거나 별칭이 없을 수 있으며 각각은 개별 명령에 지정되어 있습니다. 이 기능은 동일한 그룹이 "Devtest" 및 "QA"와 같은 여러 가지 공통 이름을 사용하여 구분 가능한 경우 유용합니다.

각 그룹에 대한 별칭의 경우, **group-alias** 명령을 입력합니다. 각 별칭은 기본적으로 활성화되어 있습니다. 다음과 같이 선택에 따라 각 별칭을 명시적으로 활성화하거나 비활성화할 수 있습니다.

```
hostname(config-tunnel-webvpn)# group-alias alias [enable | disable]
hostname(config-tunnel-webvpn)#
```

예를 들어 이름이 QA인 터널 그룹에 대해 별칭 QA 및 Devtest를 활성화하려면 다음 명령을 입력합니다.

```
hostname(config-tunnel-webvpn)# group-alias QA enable
hostname(config-tunnel-webvpn)# group-alias Devtest enable
hostname(config-tunnel-webvpn)#
```

참고 webvpn 터널 그룹 목록은 표시될 드롭다운 그룹 목록에 대해 활성화되어 있어야 합니다.

단계 **5** 그룹에 대해 수신 URL 또는 IP 주소를 지정합니다.

group-url *url*[**enable** | **disable**]

그룹에 대해 여러 URL 또는 주소(또는 없음)를 구성할 수 있습니다. 각 그룹 URL 또는 주소의 경우 **group-url** 명령을 입력합니다. *url*은 이 터널 그룹의 URL 또는 IP 주소를 지정합니다. http 또는 https 프로토콜 중 하나를 포함하는 전체 URL 또는 주소를 지정해야 합니다. 각 URL 또는 주소는 개별적으로 활성화(기본값) 또는 비활성화할 수 있습니다.

그룹 URL 또는 IP 주소를 지정하면 사용자가 로그인 시 그룹을 선택할 필요가 없습니다. 사용자 로그인 시 ASA는 터널 그룹 정책 테이블에서 사용자의 수신 URL 또는 주소를 검색합니다. 이 URL 또는 주소를 찾았고 연결 프로파일에서 group-url이 활성화된 경우, ASA는 자동으로 연계된 연결 프로파일을 선택하고 사용자에게 로그인 창에서 사용자 이름 및 비밀번호 필드만 표시합니다. 이렇게 하면 사용자 인터페이스가 간소화되고 그룹 목록을 사용자에게 노출시키지 않는 이점이 있습니다. 사용자에게 표시되는 로그인 창에서 연결 프로파일에 대해 구성된 사용자 지정을 사용합니다.

URL 또는 주소가 비활성화되고 그룹 별칭이 구성된 경우, 그룹의 드롭다운 목록이 표시되며 사용자는 선택을 해야 합니다.

동일한 URL 또는 주소를 여러 그룹과 연계할 수 없습니다. ASA는 연결 프로파일에 대해 URL 또는 주소를 수락하기 전에 URL 또는 주소의 고유성을 확인합니다.

예제**:**

이름이 RadiusServer인 터널 그룹에 대해 그룹 URL인 http://www.example.com 및 http://192.168.10.10을 활성화하려면 다음 명령을 입력합니다.

```
hostname(config)# tunnel-group RadiusServer type webvpn
hostname(config)# tunnel-group RadiusServer general-attributes
hostname(config-tunnel-general)# authentication server-group RADIUS
hostname(config-tunnel-general)# accounting-server-group RADIUS
```

```
hostname(config-tunnel-general)# tunnel-group RadiusServer webvpn-attributes
hostname(config-tunnel-webvpn)# group-alias "Cisco Remote Access" enable
hostname(config-tunnel-webvpn)# group-url http://www.example.com enable
hostname(config-tunnel-webvpn)# group-url http://192.168.10.10 enable
hostname(config-tunnel-webvpn)#
```

보다 광범위하게 예를 확인하려면 클라이언트리스 SSL VPN 세션의 사용자에 대한 로그인 창 사용자 지정, 128 페이지의 내용을 참조하십시오.

AnyConnect 클라이언트 연결에 그룹 URL을 사용하는 로드 밸런싱 배포를 수행하려면 클러스터의 각 ASA 노드에서 가상 클러스터 주소에 대한 그룹 URL뿐 아니라 노드의 로드 밸런싱 공용 주소에 대한 그룹 URL을 구성해야 합니다.

예제:

클러스터에서 주소가 다음과 같은 두 ASA 노드로 로드 밸런싱 구축을 수행할 수 있도록 적절히 group-url을 구성합니다.

- 로드 밸런싱을 위한 가상 IP = https://vip-vpn.example.com/groupname
- ASA1 = https://asa1.example.com/groupname
- ASA2 = https://asa2.example.com/groupname

ASA1의 터널 그룹 구성에 다음 group-url이 구성되어 있어야 합니다.

```
hostname(config)# tunnel-group LB1 type webvpn
hostname(config)# tunnel-group LB1 general-attributes
hostname(config-tunnel-general)# group-url  https://vip-vpn.example.com/groupname
hostname(config-tunnel-general)# group-url  https://asa1.example.com/groupname
```

ASA2의 터널 그룹 구성에 다음 group-url이 구성되어 있어야 합니다.

```
hostname(config)# tunnel-group LB2 type webvpn
hostname(config)# tunnel-group LB2 general-attributes
hostname(config-tunnel-general)# group-url  https://vip-vpn.example.com/groupname
hostname(config-tunnel-general)# group-url  https://asa2.example.com/groupname
```

단계 **6** (선택 사항). 특정 사용자가 그룹 URL 중 하나를 입력한 경우 연결 프로파일 기준으로 Cisco Secure Desktop의 Hostscan 애플리케이션 실행에서 특정 사용자를 면제시키려면 다음 명령을 입력합니다.

```
hostname(config-tunnel-webvpn)# without-csd [anyconnect]
hostname(config-tunnel-webvpn)#
```

이 명령을 입력하면 해당 세션에 대한 엔드포인트 상태 감지를 방지하므로 DAP(Dynamic Access Policy: 동적 액세스 정책) 구성을 조정해야 할 수도 있습니다.

면제를 AnyConnect 연결로만 제한하려면 **anyconnect** 키워드를 포함합니다. 키워드를 포함하지 않은 경우 면제가 클라이언트리스, Layer 3 및 AnyConnect 연결에 적용됩니다.

단계 **7** 클라이언트리스 SSL VPN 세션에 대한 연결 프로파일에 사용하기 위해 DNS 서버 그룹을 지정하려면 dns-group 명령을 사용합니다. 지정한 그룹은 전역 구성 모드(dns server-group 및 name-server 명령 사용)에서 이미 구성한 그룹이어야 합니다.

기본적으로 연결 프로파일은 DNS 서버 그룹인 DefaultDNS를 사용합니다. 그러나 이 그룹은 보안 어플라이언스가 DNS 요청을 확인하기 전에 구성되어야 합니다.

다음은 이름이 corp_dns인 새로운 DNS 서버 그룹을 구성하고 연결 프로파일인 telecommuters에 대해 서버 그룹을 지정하는 예입니다.

```
hostname(config)# dns server-group corp_dns
hostname(config-dns-server-group)# domain-name cisco.com
hostname(config-dns-server-group)# name-server 209.165.200.224

hostname(config)# tunnel-group telecommuters webvpn-attributes
hostname(config-tunnel-webvpn)# dns-group corp_dns
hostname(config-tunnel-webvpn)#
```

단계 **8** (선택 사항) 인증 및 권한 부여에 사용할 클라이언트 인증서에서 사용자 이름을 추출하는 기능을 활성화하려면 터널 그룹 webvpn 속성 모드에서 **pre-fill-username** 명령을 사용합니다.

```
hostname(config)# pre-fill-username {client | clientless}
```

pre-fill-username 명령은 사용자 이름/비밀번호 인증 및 권한 부여를 위한 사용자 이름으로 **username-from-certificate** 명령(터널 그룹 일반 속성 모드에서)에 지정된 인증서 필드에서 추출한 사용자 이름을 사용하도록 활성화합니다. 인증서 기능에서 이 사전 채우기 사용자 이름을 사용하려면 두 가지 명령을 모두 구성해야 합니다.

참고 8.0.4 버전에서 사용자 이름은 사전 채우기가 되지 않으며 대신 사용자 이름 필드에서 전송되는 모든 데이터가 무시됩니다.

전역 구성 모드에서 입력한 다음 예는 이름이 remotegrp인 IPsec 원격 액세스 터널 그룹을 생성하고 인증서에서 사용자 이름 가져오기를 활성화하며 SSL VPN 클라이언트에 대한 인증 또는 권한 부여 쿼리의 이름을 디지털 인증서에서 파생시키도록 지정합니다.

```
hostname(config)# tunnel-group remotegrp type ipsec_ra
hostname(config)# tunnel-group remotegrp general-attributes
hostname(config-tunnel-general)# username-from-certificate CN OU
hostname(config)# tunnel-group remotegrp webvpn-attributes
hostname(config-tunnel-webvpn)# pre-fill-username client
hostname(config-tunnel-webvpn)#
```

단계 **9** 인증 및 권한 부여에 사용할 클라이언트 인증서에서 보조 사용자 이름을 추출하는 기능을 활성화하려면 터널 그룹 webvpn 속성 모드에서 **secondary-pre-fill-username** 명령을 사용합니다.

```
hostname(config)# secondary-pre-fill-username {client | clientless}
```

단계 **10** (선택 사항) AnyConnect 또는 SSL VPN 클라이언트 다운로드를 위해 그룹 정책 또는 사용자 이름 속성 구성을 재정의할지 지정하려면 **override-svc-download** 명령을 사용합니다. 이 기능은 기본적으로 비활성화되어 있습니다.

보안 어플라이언스는 클라이언트리스 및/또는 SSL VPN이 **vpn-tunnel-protocol** 명령을 사용하여 그룹 정책 또는 사용자 이름 속성에서 활성화되었는지에 따라 원격 사용자에 대한 클라이언트리스 또는 AnyConnect 클라이언트 연결을 허용합니다. **anyconnect ask** 명령은 사용자에게 클라이언트를 다운로드할지 또는 WebVPN 홈 페이지로 돌아갈지를 묻는 확인 상자 메시지를 표시하여 클라이언트 사용자 경험을 추가로 수정합니다.

그러나 클라이언트리스 SSL VPN 홈 페이지가 표시되기 전에 다운로드 확인 상자가 만료할 때까지 기다리지 않도록 특정 터널 그룹 아래에서 클라이언트리스 사용자 로그인을 원할 수도 있습니다. **override-svc-download** 명령을 사용하면 연결 프로파일 수준에서 이러한 사용자의 지연을 방지할 수 있습니다. 이 명령을 입력하면 연결 프로파일을 통해 로깅하는 사용자에게 **vpn-tunnel-protocol** 또는 **anyconnect ask** 명령 설정에 관계 없이 클라이언트리스 SSL VPN 홈 페이지가 즉시 표시됩니다.

다음 예에서 연결 프로파일 engineering에 대해 터널 그룹 webvpn 특성 구성 모드를 시작하고 클라이언트 다운로드 확인 상자를 위해 그룹 정책 및 사용자 이름 특성 설정을 재정의하도록 연결 프로파일을 활성화합니다.

```
hostname(config)# tunnel-group engineering webvpn-attributes
hostname(config-tunnel-webvpn)# override-svc-download
```

단계 **11** (선택 사항) 인증이 거부될 경우 로그인 화면에서 RADIUS 거부 메시지 표시를 활성화하려면 **radius-eject-message** 명령을 사용합니다.

다음은 이름이 engineering인 연결 프로파일에 대해 RADIUS 거부 메시지 표시를 활성화한 예입니다.

```
hostname(config)# tunnel-group engineering webvpn-attributes
hostname(config-tunnel-webvpn)# radius-reject-message
```

클라이언트리스 SSL VPN 세션의 사용자에 대한 로그인 창 사용자 지정

사용자 지정은 사용자가 로그인 시 확인하는 창의 모양을 결정합니다. 클라이언트리스 SSL VPN 구성의 일부로 사용자 지정 매개변수를 구성하십시오. 이미 정의된 웹 페이지 사용자 지정을 사용자가 로그인 시 표시되는 웹 페이지의 디자인을 변경하는 데 적용하려면 다음과 같이 그룹 정책 webvpn 구성 모드에서 사용자 지정 명령을 입력합니다.

```
hostname(config-group-webvpn)# customization customization_name
hostname(config-group-webvpn)#
```

예를 들어 이름이 blueborder인 사용자 지정을 사용하려면 다음 명령을 입력합니다.

```
hostname(config-group-webvpn)# customization blueborder
hostname(config-group-webvpn)#
```

webvpn 모드에서 **customization** 명령을 입력하여 맞춤화를 구성합니다.

다음 예는 비밀번호 확인 상자를 정의하는 이름이 123인 사용자 지정을 먼저 설정하는 명령 시퀀스를 보여줍니다. 그런 다음 이 예에서 그룹 정책 이름인 testpolicy를 정의하고 **customization** 명령을 사용하여 클라이언트리스 SSL VPN 세션에 대해 이름이 123인 맞춤화를 사용하도록 지정합니다.

```
hostname(config)# webvpn
hostname(config-webvpn)# customization 123
hostname(config-webvpn-custom)# password-prompt Enter password
hostname(config-webvpn)# exit
hostname(config)# group-policy testpolicy nopassword
hostname(config)# group-policy testpolicy attributes
hostname(config-group-policy)# webvpn
hostname(config-group-webvpn)# customization value 123
hostname(config-group-webvpn)#
```

사용자 지정 프로파일과 연결 프로파일 조합을 사용하여 여러 그룹별로 다른 로그인 창을 설정할 수 있습니다. 예를 들어 다음 예에서처럼 salesgui라는 이름의 사용자 지정 프로파일을 생성했다고 가정할 경우, 이 사용자 지정 프로파일을 사용하는 sales라는 이름의 클라이언트리스 SSL VPN 세션용으로 연결 프로파일을 생성할 수 있습니다.

프로시저

단계 **1** webvpn 모드에서 클라이언트리스 SSL VPN 액세스를 위해 사용자 지정을 정의하고(이 경우 salesgui라는 이름) 기본 로고를 mycompanylogo.gif로 변경합니다. 이전에 ASA의 플래시 메모리에 mycompanylogo.gif를 로드하고 구성을 저장했어야 합니다. 자세한 내용은 클라이언트리스 SSL VPN 개요, 305 페이지를 참조하십시오.

```
hostname# webvpn
hostname (config-webvpn)# customization value salesgui
hostname(config-webvpn-custom)# logo file disk0:\mycompanylogo.gif
hostname(config-webvpn-custom)#
```

단계 **2** 전역 구성 모드에서 다음과 같이 사용자 이름을 설정하고 방금 정의한 클라이언트리스 SSL VPN에 대한 사용자 지정과 연계합니다.

```
hostname# username seller attributes
hostname(config-username)# webvpn
hostname(config-username-webvpn)# customization value salesgui
hostname(config-username-webvpn)# exit
hostname(config-username)# exit
hostname#
```

단계 **3** 전역 구성 모드에서 다음과 같이 이름이 sales인 클라이언트리스 SSL VPN 세션에 대해 터널 그룹을 생성합니다.

```
hostname# tunnel-group sales type webvpn
hostname(config-tunnel-webvpn)#
```

단계 4 다음과 같이 이 연결 프로파일에 대해 salesgui 사용자 지정을 사용할지 지정합니다.

```
hostname# tunnel-group sales webvpn-attributes
hostname(config-tunnel-webvpn)# customization salesgui
```

단계 5 사용자가 ASA에 로그인하기 위해 브라우저에 입력하는 주소로 그룹 URL을 설정합니다. 예를 들어 ASA에 IP 주소 192.168.3.3이 있는 경우 그룹 URL을 https://192.168.3.3으로 설정합니다.

```
hostname(config-tunnel-webvpn)# group-url https://192.168.3.3.
hostname(config-tunnel-webvpn)#
```

성공적으로 로그인하기 위해 포트 번호가 필요한 경우 콜론 다음에 포트 번호를 포함시킵니다. ASA는 이 URL을 sales 연결 프로파일에 매핑하고 salesgui 맞춤화 프로파일을 https://192.168.3.3에 로깅 시 사용자에게 표시되는 로그인 화면에 적용합니다.

표준 기반 IKEv2 클라이언트에 대한 터널 그룹 정보

터널 그룹은 터널 연결 정책이 포함된 레코드 집합입니다. 터널 그룹이 AAA 서버를 식별하도록 구성하고 연결 매개변수를 지정하며 기본 그룹 정책을 정의합니다. ASA는 터널 그룹을 내부에서 저장합니다.

IPsec 원격 액세스를 위한 기본 터널 그룹은 DefaultRAGroup입니다. 기본 터널 그룹은 수정할 수 있지만 삭제할 수는 없습니다.

IKEv2를 사용하면 별도의 로컬 및 원격 인증 CLI를 사용하여 비대칭 인증 방법을 구성(즉, 발신자용으로 사전 공유 키 인증을 구성하지만 응답자용으로는 인증서 인증 또는 EAP 인증을 구성)할 수 있습니다. 따라서 IKEv2에서 비대칭 인증이 있는 경우, 한쪽에서는 하나의 자격 증명으로 인증하고 다른 쪽에서는 다른 자격 증명을 사용합니다(사전 공유 키, 인증서 또는 EAP 중 하나).

인증서 인증이 인증서 DN 매칭과 함께 사용되지 않는 경우 해당 클라이언트 연결이 특정 터널 그룹에 매핑될 수 없기 때문에 DefaultRAGroup을 EAP 인증용으로 구성해야 합니다.

표준 기반 IKEv2 특성 지원

ASA는 다음 IKEv2 속성을 지원합니다.

- INTERNAL_IP4_ADDRESS/INTERNAL_IP6_ADDRESS — IPv4 또는 IPv6 주소

참고 이중 스택(IPv4 및 IPv6 주소 모두 지정)은 IKEv2를 지원하지 않습니다. IPv4 및 IPv6 주소가 모두 필요하고 두 주소 모두 할당될 수 있지만, IPv4 주소만 할당됩니다.

- INTERNAL_IP4_NETMASK — IPv4 주소 네트워크 마스크
- INTERNAL_IP4_DNS/INTERNAL_IP6_DNS — 1차/2차 DNS 주소

- INTERNAL_IP4_NBNS — 1차/2차 WINS 주소
- INTERNAL_IP4_SUBNET/INTERNAL_IP6_SUBNET — 스플릿 터널링 목록
- APPLICATION_VERSION — 무시됨. 보안상의 이유로 ASA에 대한 버전 정보가 전달되는 것을 방지하기 위해 응답을 전송하지 않습니다. 그러나, 클라이언트 구성 페이로드 요청에는 이 특성이 포함될 수 있으며 해당 문자열이 ASA에서 **vpn-sessiondb** 명령 출력과 syslog에 나타납니다.

DAP 지원

연결 유형별로 DAP 정책 구성을 허용하려면 새로운 클라이언트 유형, IPsec-IKEv2-Generic-RA를 이 연결 유형에 대해 특정한 정책을 적용하는 데 사용할 수 있습니다.

원격 액세스 클라이언트에 대한 터널 그룹 선택

다음 표에서는 원격 액세스 클라이언트 및 사용 가능한 터널 그룹 옵션 목록을 제공합니다.

원격 액세스 클라이언트	터널 그룹 목록	그룹 URL	인증서 DN 일치	기본 그룹 (DefaultRAGroup)	기타
AnyConnect VPN 클라이언트	예	예	예	예	해당 없음
Windows L2TP/IPsec (기본 모드 IKEv1)	아니요	아니요	• 예(로컬 컴퓨터 인증서 사용 시) • 아니요(PSK 사용 시)	예	해당 없음
표준 기반 IKEv2	아니요	아니요	• 예(로컬 컴퓨터 인증서 사용 시) • 아니요(EAP 인증 사용 시)	예 참고 DefaultRAGroup 터널 그룹을 사용하십시오.	해당 없음

표준 기반 IKEv2 클라이언트에 대한 인증 지원

다음 표에서는 표준 기반 IKEv2 클라이언트 및 지원되는 인증 방법 목록을 제공합니다.

참고 인증 방법 제한은 ASA가 아니라 클라이언트에서의 지원이 부족한 경우에 기반합니다. 모든 EAP 방법 인증은 클라이언트와 EAP 서버 사이에서 ASA에 의해 프록시됩니다. EAP 방법 지원은 EAP 방법에 대한 클라이언트 및 EAP 서버 지원에 기반합니다.

클라이언트유형/인증 방법	EAP-TLS	EAP-MSCHAPv2	EAP-MD5	인증서 전용	PSK
Linux의 StrongSwan	해당 없음	• ISE — 예 • ACS — 예 • FreeRadius — 예 • FreeRadius를 통한 AD — 예	• ISE — 예 • ACS — 예 • FreeRadius — 예 • FreeRadius를 통한 AD — 예	예	예
Android의 StrongSwan	해당 없음	• ISE — 예 • ACS — 예 • FreeRadius — 예 • FreeRadius를 통한 AD — 예	아니요	Yes(예)	해당사항 없음
Windows 7/8/8.1	• ISE — 예 • ACS — 예 • FreeRadius — 예 • FreeRadius를 통한 AD — 예	• ISE — 예 • ACS — 예 • FreeRadius — 예 • FreeRadius를 통한 AD — 예	해당 없음	예	해당 없음
Windows 전화기	• ISE — 예 • ACS — 예 • FreeRadius — 예 • FreeRadius를 통한 AD — 예	• ISE — 예 • ACS — 예 • FreeRadius — 예 • FreeRadius를 통한 AD — 예	해당 없음	해당 없음	해당 없음

클라이언트 유형/인증 방법	EAP-TLS	EAP-MSCHAPv2	EAP-MD5	인증서 전용	PSK
Samsung Knox	해당 없음	• ISE — 예 • ACS — 예 • FreeRadius — 예 • FreeRadius를 통한 AD — 예	• ISE — 예 • ACS — 예 • FreeRadius — 예 • FreeRadius를 통한 AD — 예	예	해당 없음
iOS 8	• ISE — 예 • ACS — 예 • FreeRadius — 예 • FreeRadius를 통한 AD — 예	• ISE — 예 • ACS — 예 • FreeRadius — 예 • FreeRadius를 통한 AD — 예	해당 없음	예	Yes(예)
Android 기본 클라이언트	해당 없음	• ISE — 예 • ACS — 예 • FreeRadius — 예 • FreeRadius를 통한 AD — 예	해당 없음	예	예

다중 인증서 인증 추가

여러 인증서 인증을 위해 프로토콜 교환을 정의하고 두 가지 세션 유형에 활용하기 위해 Aggregate Authentication 프로토콜이 확장되었습니다. 클라이언트가 SSL 연결을 만들고 어그리게이트 인증을 시작하면 다른 SSL 연결이 만들어지고 ASA에 클라이언트가 인증서 인증을 요구하고 클라이언트 인증서를 요청하는 메시지가 표시됩니다.

ASA가 원격 액세스 유형 터널 그룹의 AnyConnect 연결에 대한 필수 인증을 구성합니다. 인증서 규칙 매핑, group-url 등과 같은 기존 방법으로 터널 그룹 매핑을 수행하지만 클라이언트와 필수 인증 방법이 협상됩니다.

예

tunnel-group <name> webvpn-attributes

authentication {{aaa {certificate | multiple-certificate})| saml}

인증 옵션으로는 AAA만, 인증서만, 다중 인증서만, AAA 및 인증서, AAA 및 다중 인증서, SAML이 있습니다.

```
ASA(config)# tunnel-group AnyConnect webvpn-attributes
ASA(config-tunnel-webvpn)# authentication?
tunnel-group-webvpn mode commands/options:
aaa         Use username and password for authentication
certificate Use certificate for authentication
multiple-certificate Use multiple certificates for authentication
saml   Use SAML for authentication
ASA(config-tunnel-webvpn)# authentication multiple-certificate?

tunnel-group-webvpn mode commands/options:
aaa  Use username and password for authentication
<cr>

ASA(config-tunnel-webvpn)# authentication aaa?

tunnel-group-webvpn mode commands/options:
certificate Use certificate for authentication
multiple-certificate Use multiple certificates for authentication
<cr>
```

EAP ID 검색을 위한 쿼리 ID 옵션 구성

Microsoft Windows 7 IKEv2 클라이언트는 Cisco ASA 서버가 터널 그룹 조회를 위해 IP 주소를 효율적으로 사용하지 못하게 하는 IKE(Internet Key Exchange: 인터넷 키 교환국) ID로 IP 주소를 전송합니다. ASA는 ASA가 클라이언트에서 유효한 EAP ID를 검색하는 것을 허용하도록 EAP 인증을 위한 **query-identity** 옵션을 사용하여 구성되어야 합니다.

인증서 기반 인증의 경우 ASA 서버 및 Microsoft Windows 7 클라이언트 인증서에 다음과 같이 EKU(Extended Key Usage: 확장 키 사용) 필드가 있어야 합니다.

- 클라이언트 인증서의 경우, EKU 필드 = 클라이언트 인증 인증서.
- 서버 인증서의 경우, EKU 필드 = 서버 인증 인증서.

Microsoft Certificate Server 또는 기타 CA 서버에서 인증서를 가져올 수 있습니다.

EAP 인증의 경우, Microsoft Windows 7 IKEv2 클라이언트는 다른 모든 EAP 요청 전에 EAP ID 요청을 예상합니다. EAP ID 요청을 클라이언트에 전송하려면 IKEv2 ASA 서버의 터널 그룹 프로파일에 **query-identity** 키워드를 구성해야 합니다.

참고 DHCP 가로채기는 Windows에서 스플릿 터널링이 가능하도록 IKEv2에 지원됩니다. 이 기능은 IPv4 스플릿 터널링 특성에서만 작동합니다.

프로시저

단계 **1** IPsec 원격 액세스에 연결 유형을 설정하려면 **tunnel-group** 명령을 입력합니다. 구문은 **tunnel-group** *name***type** *type*입니다. 이때 name은 터널 그룹에 할당한 이름이며 type은 터널 유형입니다.

다음 예에서 IKEv2 사전 공유 키는 44kkaol59636jnfx로 구성됩니다.

```
hostname(config-tunnel-ipsec)# ikev2 local-authentication pre-shared-key 44kkaol59636jnfx
```

참고 인증을 완료하려면 **ikev2 remote-authentication pre-shared-key** 명령 또는 **ikev2 remote-authentication certificate** 명령을 구성해야 합니다.

단계 **2** 표준 기반, 서드파티 IKEv2 원격 액세스 클라이언트를 통한 사용자 인증을 지원하는 방법으로 EAP(Extensible Authentication Protocol: 확장 가능 인증 프로토콜)를 지정하려면 **ikev2 remote-authentication eap** [**query-identity**] 명령을 사용합니다.

참고 원격 인증을 위해 EAP를 활성화하기 전에 인증서를 사용하여 로컬 인증을 구성하고 **ikev2 local-authentication** {**certificate** *trustpoint*} 명령을 사용하여 유효한 신뢰 지점을 구성해야 합니다. 그렇지 않으면, EAP 인증 요청이 거부됩니다.

클라이언트가 구성된 모든 옵션을 사용할 수 있도록 하는 여러 옵션을 구성할 수 있지만 원격 인증의 경우에는 구성된 모든 옵션에 대해 여러 옵션을 구성할 수 없습니다.

IKEv2 연결의 경우 터널 그룹 매핑은 원격 인증(PSK, 인증서, EAP) 및 로컬 인증(PSK와 인증서)에 대해 허용할 인증 방법, 그리고 로컬 인증에 사용할 신뢰 지점에 대해 알고 있어야 합니다. 현재는 피어 또는 피어 인증서 필드 값(인증서 맵 사용)에서 가져올 수 있는 IKE ID를 사용하여 매핑이 수행됩니다. 두 옵션이 모두 실패하면 들어오는 연결이 기본 원격 액세스 터널 그룹인 DefaultRAGroup으로 매핑됩니다. 인증서 맵은 인증서를 통해 원격 피어를 인증하는 경우에만 적용 가능한 옵션입니다. 이 맵은 서로 다른 터널 그룹에 대한 매핑을 허용합니다. 인증서 인증의 경우에만 규칙 또는 기본 설정을 사용하여 터널 그룹 조회가 수행됩니다. EAP 및 PSK 인증의 경우 클라이언트에 대해 IKE ID를 사용하거나(터널 그룹 이름을 맞춰봄) 기본 설정을 사용하여 터널 그룹 조회가 수행됩니다.

EAP 인증의 경우 클라이언트에서 IKE ID 및 사용자 이름을 개별적으로 구성할 수 있지 않는 한 DefaultRAGroup 터널 그룹을 사용해야 합니다.

다음 예는 거부 중인 인증에 대한 EAP 요청을 보여줍니다.

```
ciscoasa(config-tunnel-ipsec)# ikev2 remote-authentication eap query-identity
ciscoasa(config-tunnel-ipsec)# ikev2 remote-authentication certificate
ciscoasa(config-tunnel-ipsec)# ikev2 local-authentication pre-shared-key 12345678
ERROR: The local-authentication method is required to be certificate based
if remote-authentication allows EAP
ciscoasa(config-tunnel-ipsec)# ikev2 local-authentication certificate myIDcert
```

단계 **3** 변경 내용을 저장합니다.

```
hostname(config)# write memory
hostname(config)#
```

터널이 작동 및 실행 중인지 확인하려면 **show vpn-sessiondb summary** 또는 **show crypto ipsec sa** 명령을 사용합니다.

비밀번호 관리를 위한 Microsoft Active Directory 설정 구성

인증을 위해 LDAP 디렉토리 서버를 사용 중인 경우, 비밀번호 관리가 Sun Microsystems JAVA System Directory Server(이전 이름은 Sun ONE Directory Server) 및 Microsoft Active Directory에서 지원됩니다.

- Sun - Sun 디렉토리 서버에 액세스하려면 ASA에 구성된 DN이 이 서버의 기본 비밀번호 정책에 액세스할 수 있어야 합니다. 디렉토리 관리자 또는 디렉토리 관리자 권한이 있는 사용자를 DN으로 사용할 것을 권장합니다. 또는 기본 비밀번호 정책에 ACI를 배치할 수 있습니다.
- Microsoft - Microsoft Active Directory에서 비밀번호 관리를 활성화하려면 LDAP over SSL을 구성해야 합니다.

Microsoft Active Directory에서 비밀번호 관리를 사용하려면 ASA에서 특정 Active Directory 매개변수뿐만 아니라 비밀번호 관리 구성을 설정해야 합니다. 이 섹션에서는 다양한 비밀번호 관리 작업과 연계된 Active Directory 설정에 대해 설명합니다. 다음 설명에서는 ASA에서 비밀번호 관리를 활성화했으며 해당하는 비밀번호 관리 속성을 구성했다고 가정합니다. 이 섹션의 특정 단계에서 Windows 2000 이하 버전의 Active Directory 용어를 참조합니다. 이 섹션에서는 인증을 위해 LDAP 디렉토리 서버를 사용한다고 가정합니다.

Active Directory를 사용하여 다음 로그온 시 사용자가 비밀번호를 변경하도록 설정

다음 로그온 시 사용자가 비밀번호를 변경하도록 설정하려면 ASA의 터널 그룹 일반 속성 구성 모드에서 **password-management** 명령을 지정하고 Active Directory 아래에서 다음 단계를 수행하십시오.

프로시저

단계 **1** **Start(**시작**)** > **Programs(**프로그램**)** > **Administrative Tools(**관리 툴**)** > **Active Directory Users and Computers(Active Directory** 사용자 및 컴퓨터**)**를 선택합니다.

단계 **2** 마우스 오른쪽 버튼을 클릭하여 **Username(**사용자 이름**)** > **Properties(**속성**)** > **Account(**계정**)**를 선택합니다.

단계 **3** **User must change password at next logon(**다음 로그온 시 사용자가 비밀번호를 변경해야 함**)** 확인란을 선택합니다.

이 사용자가 다음에 로그온하면, ASA에 다음 확인 상자가 표시됩니다. "새 비밀번호가 필요합니다. 비밀번호를 변경해야 합니다. 계속하려면 *n*자 이상의 새 비밀번호를 입력하십시오." Active Directory 구성의 일부로, Start(시작) > Programs(프로그램) > Administrative Tools(관리 툴) > Domain Security Policy(도메인 보안 정책) > Windows Settings(Windows 설정) > Security Settings(보안 설정) > Account Policies(계정 정책) > Password Policy(비밀번호 정책)에서 최소한의 필수 비밀번호 길이로 *n*을 설정할 수 있습니다. **Minimum password length(**최소 비밀번호 길이**)**를 선택합니다.

Active Directory를 사용하여 최대 비밀번호 사용 기간 지정

보안 강화를 위해 특정한 날짜 수 이후에 비밀번호가 만료되도록 지정할 수 있습니다. 사용자 비밀번호에 대해 최대 비밀번호 사용 기간을 지정하려면 ASA의 터널 그룹 일반 속성 구성 모드에서 **password-management** 명령을 지정하고 Active Directory 아래에서 다음 단계를 수행하십시오.

참고 비밀번호 사용 기간 기능을 수행하기 위해 터널 그룹 원격 액세스 구성의 일부로 이전에 구성한 **radius-with-expiry** 명령은 더 이상 사용되지 않습니다. 터널 그룹 일반 속성 모드에서 입력한 **password-management** 명령이 이 명령을 대체합니다.

프로시저

단계 **1** **Start**(시작) > **Programs**(프로그램) > **Administrative Tools**(관리 툴) > **Domain Security Policy**(도메인 보안 정책) > **Windows Settings**(Windows 설정) > **Security Settings**(보안 설정) > **Account Policies**(계정 정책) > **Password Policy**(비밀번호 정책)를 선택합니다.

단계 **2** 최대 비밀번호 사용 기간을 두 번 클릭합니다.

단계 **3** **Define this policy setting**(이 정책 설정 정의) 확인란을 선택하고 허용할 최대 비밀번호 사용 기간(날짜 단위)을 지정합니다.

Active Directory를 사용하여 최소 비밀번호 길이 적용

비밀번호에 대해 최소 길이를 적용하려면 ASA의 터널 그룹 일반 속성 구성 모드에서 **password-management** 명령을 지정하고 Active Directory 아래에서 다음 단계를 수행하십시오.

프로시저

단계 **1** **Start**(시작) > **Programs**(프로그램) > **Administrative Tools**(관리 툴) > **Domain Security Policy**(도메인 보안 정책)를 선택합니다.

단계 **2** **Windows Settings**(Windows 설정) > **Security Settings**(보안 설정) > **Account Policies**(계정 정책) > **Password Policy**(비밀번호 정책)를 선택합니다.

단계 **3** **Minimum Password Length**(최소 비밀번호 길이)를 두 번 클릭합니다.

단계 **4** **Define this policy setting**(이 정책 설정 정의) 확인란을 선택하고 비밀번호가 포함해야 할 최소 문자 수를 지정합니다.

Active Directory를 사용하여 비밀번호 복잡성 적용

복잡한 비밀번호를 적용하려면 예를 들어 대문자, 소문자, 숫자 및 특수 문자가 포함된 비밀번호가 필요한 경우, ASA의 터널 그룹 일반 속성 구성 모드에서 **password-management** 명령을 입력하고 Active Directory 아래에서 다음 단계를 수행하십시오.

프로시저

단계 1 **Start**(시작) > **Programs**(프로그램) > **Administrative Tools**(관리 툴) > **Domain Security Policy**(도메인 보안 정책)를 선택합니다. **Windows Settings**(Windows 설정) > **Security Settings**(보안 설정) > **Account Policies**(계정 정책) > **Password Policy**(비밀번호 정책)를 선택합니다.

단계 2 보안 정책 설정 대화 상자를 열려면 두 번 클릭한 비밀번호가 복잡성 요건을 충족해야 합니다.

단계 3 Define this policy setting(이 정책 설정 정의) 확인란을 선택하고 **Enable**(활성화)을 선택합니다.

비밀번호 복잡성은 다음 로그인 시 비밀번호 변경 적용 또는 비밀번호가 *n*일 이내에 만료됨을 구성한 경우와 같이 사용자가 비밀번호를 변경하는 경우에만 적용됩니다. 로그인 시 사용자가 새 비밀번호를 입력하라는 확인 상자 메시지를 수신하면 시스템은 복잡한 비밀번호만 수락합니다.

AnyConnect 클라이언트에 대한 RADIUS/SDI 메시지 지원을 위한 연결 프로파일 구성

이 섹션에서는 RSA SecureID 소프트웨어 토큰을 사용하는 AnyConnect VPN 클라이언트가 SDI 서버로 프록시 연결하는 RADIUS 서버를 통해 클라이언트에 제공되는 사용자 확인 상자에 대해 제대로 응답할 수 있도록 하는 절차를 설명합니다.

참고 이중 인증 기능을 구성한 경우, SDI 인증은 1차 인증 서버에서만 지원됩니다.

원격 사용자가 AnyConnect VPN 클라이언트를 사용하는 ASA에 연결하고 RSA SecurID 토큰을 사용하여 인증을 시도하는 경우, ASA는 인증에 대해 RADIUS 서버 및 SDI 서버와 차례대로 통신합니다.

인증 시 RADIUS 서버는 ASA에 대한 액세스 요청 메시지를 제공합니다. 이러한 챌린지 메시지 안에는 SDI 서버의 텍스트를 포함하는 응답 메시지가 있습니다. 메시지 텍스트는 ASA가 SDI 서버와 직접 통신하는 경우에 RADIUS 프록시를 통해 통신하는 경우와 서로 다릅니다. 따라서 AnyConnect 클라이언트에 대한 네이티브 SDI 서버로 표시되도록 ASA는 RADIUS 서버의 메시지를 해석해야 합니다.

또한 SDI 메시지는 SDI 서버에 구성할 수 있으므로 ASA의 메시지 텍스트는 SDI 서버의 메시지 텍스트와 전체 또는 부분적으로 일치해야 합니다. 그렇지 않으면 인증 시 필요한 작업에 적합하지 않은 프롬프트가 원격 클라이언트 사용자에게 표시될 수 있습니다. AnyConnect 클라이언트는 응답하지 못하고 인증에 실패할 수 있습니다.

RADIUS/SDI 메시지를 지원하도록 보안 어플라이언스 구성, 138 페이지 ASA에서는 클라이언트와 SDI 서버 간에 성공적인 인증을 위해 ASA를 구성하는 방법을 설명합니다.

RADIUS/SDI 메시지를 지원하도록 보안 어플라이언스 구성

SDI별 RADIUS 응답 메시지를 해석하고 AnyConnect 사용자에게 적절한 조치에 대해 확인 상자를 표시하도록 ASA를 구성하려면 다음 단계를 수행하십시오.

프로시저

단계 1 터널 그룹 webvpn 구성 모드에서 **proxy-auth sdi** 명령을 사용하여 SDI 서버와의 직접적인 통신을 시뮬레이션하는 방식으로 RADIUS 응답 메시지를 전달하도록 연결 프로파일(터널 그룹)을 구성합니다. SDI 서버에 대해 인증 중인 사용자는 이 연결 프로파일을 통해 연결해야 합니다.

예제:

```
hostname(config)# tunnel-group sales webvpn attributes
hostname(tunnel-group-webvpn)# proxy-auth sdi
```

단계 2 터널 그룹 webvpn 구성 모드에서 **proxy-auth_map sdi** 명령을 사용하여 ASA에 있는 RADIUS 응답 메시지 텍스트를 RADIUS 서버에서 전송된 메시지 텍스트와 전체 또는 부분적으로 일치하도록 구성합니다.

ASA에서 사용하는 기본 메시지 텍스트는 Cisco Secure Access Control Server(ACS)에서 사용하는 기본 메시지 텍스트입니다. Cisco Secure ACS를 사용 중이며 Cisco Secure ACS에서 기본 메시지 텍스트를 사용 중인 경우, ASA에서 메시지 텍스트를 구성할 필요가 없습니다. 그렇지 않은 경우 **proxy-auth_map sdi** 명령을 사용하여 메시지 텍스트가 일치하는지 확인합니다.

아래 표에는 각 메시지의 메시지 코드, 기본 RADIUS 응답 메시지 텍스트 및 기능이 나와 있습니다. 보안 어플라이언스는 이 표에 나타나는 순서대로 문자열을 검색하므로 메시지 텍스트에 사용하는 문자열이 다른 문자열의 하위 집합이 아닌지 확인해야 합니다.

예를 들어 "new PIN"은 new-pin-sup 및 next-ccode-and-reauth 모두에 대한 기본 메시지 텍스트의 하위 집합입니다. new-pin-sup를 "새 PIN"으로 구성한 경우, 보안 어플라이언스가 RADIUS 서버에서 "다음 카드 코드가 있는 새 PIN"을 수신할 때 텍스트를 next-ccode-and-reauth 코드 대신 new-pin-sup 코드에 일치시킵니다.

SDI Op 코드, 기본 메시지 텍스트 및 메시지 기능

메시지 코드	기본 **RADIUS** 응답 메시지 텍스트	기능
next-code	다음 암호를 입력하십시오.	사용자가 PIN 없이 다음 토큰 코드를 입력해야 함을 나타냅니다.
new-pin-sup	새 PIN을 기억하십시오.	새 시스템 PIN이 제공되었음을 나타내며 해당 사용자용 PIN을 표시합니다.
new-pin-meth	사용자 고유의 PIN을 입력하시겠습니까?	새 PIN을 생성하기 위해 새 PIN 방법을 사용하는 사용자로부터의 요청입니다.
new-pin-req	새 영숫자 PIN을 입력하십시오.	사용자가 생성한 PIN을 나타내며 사용자에게 PIN을 입력하도록 요청합니다.

메시지 코드	기본 **RADIUS** 응답 메시지 텍스트	기능
new-pin-reenter	PIN 다시 입력:	사용자 제공 PIN 확인을 위해 ASA에서 내부적으로 사용됩니다. 클라이언트는 사용자에게 프롬프트를 표시하지 않고 PIN을 확인합니다.
new-pin-sys-ok	새 PIN이 승인되었습니다.	사용자 제공 PIN이 승인되었음을 나타냅니다.
next-ccode-and-reauth	다음 카드 코드가 있는 새 PIN입니다.	PIN 작업에 따라 사용자가 다음 토큰 코드를 기다려야 하며 인증을 위해 새 PIN과 다음 토큰 코드를 모두 입력해야 함을 나타냅니다.
ready-for-sys- pin	시스템에서 생성한 PIN을 승인합니다.	사용자가 시스템에서 생성한 PIN을 사용할 준비가 되었음을 나타내기 위해 ASA에서 내부적으로 사용됩니다.

다음 예에서는 aaa-server-host 모드를 시작하며 RADIUS 응답 메시지 new-pin-sup에 대해 텍스트를 변경합니다.

```
hostname(config)# aaa-server radius_sales host 10.10.10.1
hostname(config-aaa-server-host)# proxy-auth_map sdi new-pin-sup "This is your new PIN"
```

그룹 정책

이 섹션에서는 그룹 정책 및 그룹 정책을 구성하는 방법에 대해 설명합니다.

그룹 정책은 디바이스에서 내부적(로컬)으로 또는 RADIUS 서버에서 외부적으로 저장된 IPsec 연결에 대한 사용자 중심 특성/값 쌍의 집합입니다. 연결 프로파일은 터널이 설정된 이후에 사용자 연결을 위한 조건을 설정하는 그룹 정책을 사용합니다. 그룹 정책을 사용하면 각 사용자에 대해 개별적으로 각 특성을 지정할 필요 없이 사용자 또는 사용자 그룹에 전체 특성 집합을 적용할 수 있습니다.

전역 구성 모드에서 **group-policy** 명령을 입력하여 그룹 정책을 사용자에게 할당하거나 특정 사용자에 대해 그룹 정책을 수정합니다.

ASA에는 기본 그룹 정책이 포함됩니다. 수정할 수 있지만 삭제는 할 수 없는 기본 그룹 정책 외에, 환경에 고유한 하나 이상의 그룹 정책을 생성할 수 있습니다.

내부 및 외부 그룹 정책을 구성할 수 있습니다. 내부 그룹은 ASA의 내부 데이터베이스에 구성됩니다. 외부 그룹은 RADIUS와 같은 외부 인증 서버에 구성됩니다. 그룹 정책은 다음 특성을 포함합니다.

- ID
- 서버 정의
- 클라이언트 방화벽 설정
- 터널링 프로토콜
- IPsec 설정
- 하드웨어 클라이언트 설정
- 필터
- 클라이언트 구성 설정
- 연결 설정

기본 그룹 정책 수정

ASA는 기본 그룹 정책을 제공합니다. 이 기본 그룹 정책을 수정할 수 있지만 삭제할 수는 없습니다. 이름이 DfltGrpPolicy인 기본 그룹 정책은 항상 ASA에 존재하지만 이 기본 그룹 정책은 이 정책을 사용하도록 ASA를 구성한 이후에만 적용됩니다. 다른 그룹 정책을 구성하는 경우, 명시적으로 지정하지 않은 모든 특성은 기본 그룹 정책에서 값을 가져옵니다. 기본 그룹 정책을 확인하려면 다음 명령을 입력합니다.

```
hostname(config)# show running-config all group-policy DfltGrpPolicy
hostname(config)#
```

기본 그룹 정책을 구성하려면 다음 명령을 입력합니다.

```
hostname(config)# group-policy DfltGrpPolicy internal
hostname(config)#
```

참고 기본 그룹 정책은 항상 내부 형식입니다. 명령 구문이 hostname(config)# group-policy DfltGrpPolicy {internal | external}이라는 사실에도 불구하고 정책 형식을 외부로 변경할 수 없습니다.

기본 그룹 정책의 속성을 변경하려면 다음과 같이 **group-policy attributes** 명령을 사용하여 속성 모드를 시작한 다음 수정하려는 속성을 변경하도록 명령을 지정합니다.

```
hostname(config)# group-policy DfltGrpPolicy attributes
```

참고 특성 모드는 내부 그룹 정책에만 적용됩니다.

ASA가 제공하는 기본 그룹 정책인 DfltGrpPolicy는 다음과 같습니다.

```
hostname# show run all group-policy DfltGrpPolicy
group-policy DfltGrpPolicy internal
group-policy DfltGrpPolicy attributes
 banner none
 wins-server none
 dns-server value 10.10.10.1.1
 dhcp-network-scope none
 vpn-access-hours none
 vpn-simultaneous-logins 3
 vpn-idle-timeout 30
 vpn-idle-timeout alert-interval 1
 vpn-session-timeout none
 vpn-session-timeout alert-interval 1
 vpn-filter none
 vpn-tunnel-protocol ikev1 ikev2 l2tp-ipsec ssl-client ssl-clientless
 password-storage disable
 ip-comp disable
 re-xauth disable
 group-lock none
 pfs disable
 ipsec-udp disable
 ipsec-udp-port 10000
 split-tunnel-policy tunnelall
 ipv6-split-tunnel-policy tunnelall
 split-tunnel-network-list none
 default-domain value cisco.com
 split-dns none
 split-tunnel-all-dns disable
 intercept-dhcp 255.255.255.255 disable
 secure-unit-authentication disable
 user-authentication disable
 user-authentication-idle-timeout 30
 ip-phone-bypass disable
 client-bypass-protocol disable
 gateway-fqdn none
 leap-bypass disable
 nem disable
 backup-servers keep-client-config
 msie-proxy server none
 msie-proxy method no-modify
 msie-proxy except-list none
 msie-proxy local-bypass disable
 msie-proxy pac-url none
 msie-proxy lockdown enable
 vlan none
 nac-settings none
 address-pools none
 ipv6-address-pools none
 smartcard-removal-disconnect enable
 scep-forwarding-url none
 client-firewall none
 client-access-rule none
 webvpn
  url-list none
  filter none
  homepage none
```

```
  html-content-filter none
  port-forward name Application Access
  port-forward disable
  http-proxy disable

  anyconnect ssl dtls enable
  anyconnect mtu 1406
  anyconnect firewall-rule client-interface private none
  anyconnect firewall-rule client-interface public none
  anyconnect keep-installer installed
  anyconnect ssl keepalive 20
  anyconnect ssl rekey time none
  anyconnect ssl rekey method none
  anyconnect dpd-interval client 30
  anyconnect dpd-interval gateway 30
  anyconnect ssl compression none
  anyconnect dtls compression lzs
  anyconnect modules none
  anyconnect profiles none
  anyconnect ask none
  customization none
  keep-alive-ignore 4
  http-comp gzip
  download-max-size 2147483647
  upload-max-size 2147483647
  post-max-size 2147483647
  user-storage none
  storage-objects value cookies,credentials
  storage-key none
  hidden-shares none
  smart-tunnel disable
  activex-relay enable
  unix-auth-uid 65534
  unix-auth-gid 65534
  file-entry enable
  file-browsing enable
  url-entry enable
  deny-message value Login was successful, but because certain criteria have not been met
or due to some specific group policy, you do not have permission to use any of the VPN
features. Contact your IT administrator for more information
  smart-tunnel auto-signon disable
  anyconnect ssl df-bit-ignore disable
  anyconnect routing-filtering-ignore disable
  smart-tunnel tunnel-policy tunnelall
  always-on-vpn profile-setting
```

기본 그룹 정책을 수정하고 환경에 고유한 하나 이상의 그룹 정책을 생성할 수도 있습니다.

그룹 정책 구성

그룹 정책은 모든 종류의 터널에 적용할 수 있습니다. 각각의 경우 명시적으로 매개변수를 정의하지 않으면 그룹은 기본 그룹 정책에서 값을 가져옵니다.

단일 상황 모드 또는 다중 상황 모드 두 가지에서 이 구성 작업을 수행할 수 있습니다.

참고 다중 상황 모드는 IKEv2 및 IKEv1 사이트 간에만 적용되며 AnyConnect, 클라이언트리스 SSL VPN, Apple 네이티브 VPN 클라이언트, Microsoft 네이티브 VPN 클라이언트 또는 IKEv1 IPsec용 cTCP에는 적용되지 않습니다.

외부 그룹 정책 구성

외부 그룹 정책은 사용자가 지정하는 외부 서버에서 특성 값을 가져옵니다. 외부 그룹 정책의 경우 ASA가 속성에 대해 쿼리할 수 있는 AAA 서버 그룹을 식별해야 하며 외부 AAA 서버 그룹에서 이 속성을 검색할 때 사용할 비밀번호를 지정해야 합니다. 외부 인증 서버를 사용 중이며 외부 그룹 정책 특성이 인증하려는 사용자와 동일한 RADIUS 서버에 존재하는 경우, 이 둘 간에 이름이 중복되지 않았는지 확인해야 합니다.

참고 ASA에 있는 외부 그룹 이름은 RADIUS 서버의 사용자 이름을 나타냅니다. 즉 외부 그룹 X를 ASA에 구성하는 경우, RADIUS 서버는 쿼리를 사용자 X에 대한 인증 요청으로 간주합니다. 따라서 외부 그룹은 ASA에 특별한 의미가 있는 RADIUS 서버의 사용자 어카운트입니다. 외부 그룹 특성이 인증하려는 사용자와 동일한 RADIUS 서버에 존재하는 경우, 이 둘 간에 이름이 중복되지 않아야 합니다.

ASA는 외부 LDAP 또는 RADIUS 서버에서 사용자 권한 부여를 지원합니다. 외부 서버를 사용하도록 ASA를 구성하려면 먼저 올바른 ASA 권한 부여 속성을 사용하여 해당 서버를 구성해야 하며 이러한 속성의 하위 집합에서 특정한 권한을 개별 사용자에게 할당해야 합니다. 외부 서버를 구성하려면 VPN을 위한 외부 AAA 서버 구성, 289 페이지의 지침을 따르십시오.

프로시저

외부 그룹 정책을 구성하려면 다음 단계를 수행하여 서버 그룹 이름 및 비밀번호와 함께 그룹 정책에 대해 이름 및 유형을 지정합니다.

```
hostname(config)# group-policy group_policy_name type server-group server_group_name password
 server_password
hostname(config)#
```

참고 외부 그룹 정책의 경우 RADIUS는 지원되는 유일한 AAA 서버 유형입니다.

예를 들어 다음 명령은 이름이 ExtRAD인 외부 RADIUS 서버에서 특성을 가져오는 이름이 ExtGroup인 외부 그룹 정책을 생성하며 이 특성을 검색할 때 사용할 비밀번호인 newpassword를 지정합니다.

```
hostname(config)# group-policy ExtGroup external server-group ExtRAD password newpassword
hostname(config)#
```

참고 VPN을 위한 외부 AAA 서버 구성, 289 페이지에 설명된 대로 여러 VSA(Vendor-Specific Attributes: 공급업체별 특성)를 구성할 수 있습니다. RADIUS 서버가 클래스 속성(#25)을 반환하도록 구성된 경우 ASA는 이 속성을 사용하여 그룹 이름을 인증합니다. RADIUS 서버에서 속성은 OU=*groupname*과 같은 형식이어야 합니다. 이때 *groupname*은 ASA에 구성된 그룹 이름과 일치합니다(예: OU=Finance).

내부 그룹 정책 생성

내부 그룹 정책을 구성하려면 구성 모드를 시작하고 다음과 같이 group-policy 명령을 사용하여 그룹 정책에 대해 이름 및 내부 유형을 지정하십시오.

```
hostname(config)# group-policy group_policy_name internal
hostname(config)#
```

예를 들어 다음 명령은 이름이 GroupPolicy1인 내부 그룹 정책을 생성합니다.

```
hostname(config)# group-policy GroupPolicy1 internal
hostname(config)#
```

참고 그룹 정책을 생성한 후에는 이름을 변경할 수 없습니다.

다음과 같이 키워드 **from**을 추가하고 기존 정책의 이름을 지정하여 기존의 그룹 정책 값을 복사하는 방법으로 내부 그룹 정책의 속성을 구성할 수 있습니다.

```
hostname(config)# group-policy group_policy_name internal from group_policy_name
hostname(config-group-policy)#
```

예를 들어 다음 명령은 GroupPolicy1의 특성을 복사하여 이름이 GroupPolicy2인 내부 그룹 정책을 생성합니다.

```
hostname(config)# group-policy GroupPolicy2 internal from GroupPolicy1
hostname(config-group-policy)#
```

일반 내부 그룹 정책 속성 구성

그룹 정책 이름

그룹 정책 이름은 내부 그룹 정책이 생성될 때 선택됩니다. 그룹 정책이 생성된 후에는 이름을 변경할 수 없습니다. 자세한 내용은 내부 그룹 정책 생성, 145 페이지를 참조하십시오.

그룹 정책 배너 메시지 구성

표시할 배너 또는 환영 메시지(있는 경우)를 지정합니다. 기본값은 배너 없음입니다. 지정하는 메시지는 원격 클라이언트가 연결될 때 표시됩니다. 배너를 지정하려면 그룹 정책 구성 모드에서 **banner** 명령을 입력합니다. 배너 텍스트는 최대 500자까지 입력할 수 있습니다. 캐리지 리턴을 삽입하려면 "\n" 시퀀스를 입력합니다.

ASA 버전 9.5.1에서, 로그인 후 VPN 원격 클라이언트에 표시되는 전체 배너 길이가 510에서 4000자로 증가했습니다.

참고 배너에 포함된 캐리지 리턴 및 라인 피드는 두 글자로 셉니다.

배너를 삭제하려면 이 명령의 **no** 형식을 입력합니다. **no** 버전의 명령을 사용하면 그룹 정책에 대한 모든 배너가 삭제된다는 점에 주의하십시오.

그룹 정책은 다른 그룹 정책에서 이 값을 상속받을 수 있습니다. 값 상속을 방지하려면 다음과 같이 배너 문자열에 대해 값을 지정하는 대신 **none** 키워드를 입력합니다.

```
hostname(config-group-policy)# banner {value banner_string | none}
```

다음 예는 이름이 FirstGroup인 그룹 정책에 대해 배너를 생성하는 방법을 보여줍니다.

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# banner value Welcome to Cisco Systems ASA 9.0.
```

원격 액세스 연결에 대해 주소 풀 지정

원격 액세스 클라이언트에서 ASA에 연결하는 경우, ASA는 연결을 위해 지정된 그룹 정책을 기반으로 IPv4 또는 IPv6 주소를 클라이언트에 할당할 수 있습니다.

로컬 주소 할당에 사용할 최대 6개의 로컬 주소 풀 목록을 지정할 수 있습니다. 풀을 지정하는 순서는 중요합니다. ASA는 이 명령에 나타나는 풀의 순서에 따라 이 풀에서 주소를 할당합니다.

내부 그룹 정책에 **IPv4** 주소 풀 할당

시작하기 전에

IPv4 주소 풀을 생성합니다.

프로시저

단계 **1** 그룹 정책 구성 모드를 시작합니다.

group-policy 값 **attributes**

예제:

```
hostname> en
hostname# config t
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)#
```

단계 2 이름이 ipv4-pool1, ipv4-pool2 및 ipv4pool3인 주소 풀을 FirstGroup 그룹 정책에 할당합니다. 그룹 정책에 대해 최대 6개의 주소 풀을 지정할 수 있습니다.

address-pools value *pool-name1 pool-name2 pool-name6*

예제:

```
asa4(config-group-policy)# address-pools value ipv4-pool1 ipv4-pool2 ipv4-pool3
asa4(config-group-policy)#
```

단계 3 (선택 사항) **no address-pools value pool-name** 명령을 사용하여 그룹 정책 구성에서 주소 풀을 제거하고 DefltGroupPolicy 같은 다른 소스에서 주소 풀 정보를 상속받도록 주소 풀 설정을 되돌립니다.

no address-pools value *pool-name1 pool-name2 pool-name6*

예제:

```
hostname(config-group-policy)# no address-pools value ipv4-pool1 ipv4-pool2 ipv4-pool3
hostname(config-group-policy)#
```

단계 4 (선택 사항) **address-pools none** 명령은 DefltGrpPolicy 같은 정책의 다른 소스에서 이 속성을 상속받는 것을 비활성화합니다.

```
hostname(config-group-policy)# address-pools none
hostname(config-group-policy)#
```

단계 5 (선택 사항) **no address pools none** 명령은 그룹 정책에서 **address-pools none** 명령을 제거하여 상속을 허용하는 기본값을 복원합니다.

```
hostname(config-group-policy)# no address-pools none
hostname(config-group-policy)#
```

내부 그룹 정책에 IPv6 주소 풀 할당

시작하기 전에

IPv6 주소 풀을 생성합니다. VPN용 IP 주소, 199 페이지를 참고하십시오.

프로시저

단계 1 그룹 정책 구성 모드를 시작합니다.

group-policy *value* **attributes**

예제:

```
hostname> en
hostname# config t
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)#
```

단계 **2** 이름이 ipv6-pool인 주소 풀을 FirstGroup 그룹 정책에 할당합니다. 그룹 정책에 최대 6개의 ipv6 주소 풀을 할당할 수 있습니다.

예제:

이 예는 ipv6-pool1, ipv6-pool2 및 ipv6-pool3를 FirstGroup 그룹 정책에 할당하는 내용을 보여줍니다.

```
hostname(config-group-policy)# ipv6-address-pools value ipv6-pool1 ipv6-pool2 ipv6-pool3
hostname(config-group-policy)#
```

단계 **3** (선택 사항) **no ipv6-address-pools value pool-name** 명령을 사용하여 그룹 정책 구성에서 주소 풀을 제거하고 DfltGroupPolicy 같은 다른 소스에서 주소 풀 정보를 상속받도록 주소 풀 설정을 되돌립니다.

no ipv6-address-pools value pool-name1 pool-name2 pool-name6

예제:

```
hostname(config-group-policy)# no ipv6-address-pools value ipv6-pool1 ipv6-pool2 ipv6-pool3
hostname(config-group-policy)#
```

단계 **4** (선택 사항) **ipv6-address-pools none** 명령을 사용하여 DfltGrpPolicy 같은 정책의 다른 소스에서 이 속성을 상속받는 것을 비활성화합니다.

```
hostname(config-group-policy)# ipv6-address-pools none
hostname(config-group-policy)#
```

단계 **5** (선택 사항) **no ipv6-address pools none** 명령을 사용해 그룹 정책에서 **ipv6-address-pools none** 명령을 제거하여 상속을 허용하는 기본값을 복원합니다.

```
hostname(config-group-policy)# no ipv6-address-pools none
hostname(config-group-policy)#
```

그룹 정책에 대해 터널링 프로토콜 지정

그룹 정책 구성 모드에서 **vpn-tunnel-protocol** {ikev1 | ikev2 | l2tp-ipsec | ssl-client | ssl-clientless} 명령을 입력하여 이 그룹 정책에 대해 VPN 터널 유형을 지정합니다.

기본값은 기본 그룹 정책의 특성을 상속받는 것입니다. 실행 중인 구성에서 특성을 제거하려면 **no** 형식의 이 명령을 입력합니다.

이 명령에 대한 매개변수 값은 다음과 같습니다.

- ikev1 — 2개의 피어(Cisco VPN 클라이언트 또는 다른 보안 게이트웨이) 사이에서 IPsec IKEv1 터널을 협상합니다. 인증, 암호화, 캡슐화 및 키 관리를 제어하는 보안 연계를 생성합니다.
- ikev2 — 2개의 피어(AnyConnect Secure Mobility Client 또는 다른 보안 게이트웨이) 사이에서 IPsec IKEv2 터널을 협상합니다. 인증, 암호화, 캡슐화 및 키 관리를 제어하는 보안 연계를 생성합니다.
- **l2tp-ipsec**- L2TP 연결에 대해 IPsec 터널을 협상합니다.
- ssl-client — AnyConnect Secure Mobility Client에서 TLS 또는 DTLS를 사용하는 SSL 터널을 협상합니다.
- **ssl-clientless**- HTTPS 활성화 웹 브라우저를 통해 원격 사용자에게 VPN 서비스를 제공하며 클라이언트가 필요하지 않습니다.

하나 이상의 터널링 모드를 구성하려면 다음 명령을 입력합니다. 사용자가 VPN 터널을 통해 연결하려면 하나 이상의 터널링 모드를 구성해야 합니다.

다음 예는 이름이 FirstGroup인 그룹 정책에 대해 IPsec IKEv1 터널링 모드를 구성하는 방법을 보여줍니다.

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# vpn-tunnel-protocol ikev1
hostname(config-group-policy)#
```

Specify a VLAN for Remote Access or Apply a Unified Access Control Rule to the Group Policy

필터는 소스 주소, 수신 주소 및 프로토콜 등의 기준에 따라 ASA를 통해 수신하는 터널링된 데이터 패킷의 허용 또는 거부 여부를 결정하는 규칙으로 구성됩니다. 그룹 정책에 대해 IPv4 또는 IPv6 통합 액세스 제어 목록을 지정하거나 기본 그룹 정책에 지정된 ACL을 상속받도록 허용할 수 있습니다.

다음 옵션 중 하나를 선택하여 원격 액세스에 대해 이그레스(egress) VLAN("VLAN 매핑"이라고 함)을 지정하거나 트래픽을 필터링하도록 ACL을 지정하십시오.

- 이 그룹 정책 또는 이 그룹 정책을 상속받는 그룹 정책에 할당된 원격 액세스 VPN 세션에 대해 이그레스(egress) VLAN을 지정하려면 그룹 정책 구성 모드에서 다음 명령을 입력합니다.

  [**no**] **vlan** {*vlan_id* |**none**}

  *no vlan*은 그룹 정책에서 *vlan_id*를 제거합니다. 그룹 정책은 기본 그룹 정책에서 vlan 값을 상속받습니다.

  *none*은 그룹 정책에서 *vlan_id*를 제거하고 이 그룹 정책에 대해 VLAN 매핑을 비활성화합니다. 그룹 정책은 기본 그룹 정책에서 vlan 값을 상속하지 않습니다.

  *vlan_id*는 10진수 형식의 VLAN 개수로 이 그룹 정책에서 사용하는 원격 액세스 VPN 세션에 할당됩니다. VLAN은 일반 작업 구성 가이드에 있는 "VLAN 서브 인터페이스 및 802.1Q 트렁킹 구성"의 지침에 따라 이 ASA에 구성되어야 합니다.

참고 이그레스(egress) VLAN 기능은 HTTP 연결용으로는 작동하지만 FTP와 CIFS용으로는 작동하지 않습니다.

- 그룹 정책 모드에서 **vpn-filter** 명령을 사용하여 VPN 세션에 적용할 ACL(Access Control Rule: 액세스 제어 규칙)의 이름을 지정합니다. vpn-filter 명령을 사용하여 IPv4 또는 IPv6 ACL을 지정할 수 있습니다.

참고 이전 릴리스에서 vpn-filter에서 지정한 IPv6 항목이 없는 경우, 더 이상 사용되지 않는 ipv6-vpn-filter 명령을 사용하여 IPv6 ACL을 지정할 수 있습니다. ASA 9.1(4)부터 ipv6-vpn-filter가 비활성화되었으며 vpn-filter 명령을 사용하여 IPv6 ACL 항목을 지정해야 합니다. ipv6-vpn-filter가 설정된 경우 VPN 연결이 종료됩니다.

참고 또한 사용자 이름 모드에서 이 특성을 구성할 수 있으며 이 경우, 사용자 이름 아래에서 구성한 값이 그룹 정책 값을 대체합니다.

```
hostname(config-group-policy)# vpn-filter {value ACL name | none}
hostname(config-group-policy)#
```

이 그룹 정책에 대한 다양한 유형의 트래픽을 허용하거나 거부하도록 ACL을 구성합니다. 그런 다음 해당 ACL을 적용하도록 **vpn-filter** 명령을 입력합니다.

vpn-filter none 명령을 입력하여 생성한 null 값을 포함하는 ACL을 제거하려면 이 명령의 **no** 형식을 입력합니다. **no** 옵션을 사용하면 다른 그룹 정책에서 값을 상속받을 수 있습니다.

그룹 정책은 다른 그룹 정책에서 이 값을 상속받을 수 있습니다. 값 상속을 방지하려면 ACL 이름을 지정하는 대신 **none** 키워드를 입력합니다. **none** 키워드는 ACL이 없으며 null 값이 설정되므로 ACL이 허용되지 않음을 나타냅니다.

다음 예는 이름이 FirstGroup인 그룹 정책에 대해 acl_vpn이라는 ACL을 호출하는 필터를 설정하는 방법을 보여줍니다.

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# vpn-filter acl_vpn
hostname(config-group-policy)#
```

vpn-filter 명령은 터널에서 나간 이후 사후 암호 해독 트래픽에 적용되며 터널에 들어가기 전에 사전 암호화 트래픽에 적용됩니다. vpn-filter에 사용된 ACL은 또한 인터페이스 액세스 그룹에 사용할 수 없습니다. **vpn-filter** 명령이 원격 액세스 VPN 클라이언트 연결을 제어하는 그룹 정책에 적용되는 경우, ACL의 **src_ip** 위치에 있는 클라이언트 할당 IP 주소 및 ACL의 **dest_ip** 위치에 있는 로컬 네트워크를 사용하여 ACL을 구성해야 합니다.

vpn-filter 명령이 LAN to LAN VPN 연결을 제어하는 그룹 정책에 적용되는 경우, ACL의 **src_ip** 위치에 있는 원격 네트워크 및 ACL의 **dest_ip** 위치에 있는 로컬 네트워크를 사용하여 ACL을 구성해야 합니다.

vpn-filter 기능에 사용하기 위해 ACL을 구성하는 경우 주의하십시오. ACL이 사후 암호 해독 트래픽에 구성된다는 점을 기억하십시오. 그러나 ACL은 반대 방향의 트래픽에도 적용됩니다. 터널로 오는 사전 암호화 트래픽의 경우, ACL은 대체된 **src_ip** 및 **dest_ip** 위치에 구성됩니다.

다음 예에서 vpn-filter는 원격 액세스 VPN 클라이언트에 사용됩니다. 이 예에서는 클라이언트 할당 IP 주소가 10.10.10.1/24이고 로컬 네트워크는 192.168.1.0/24라고 가정합니다.

다음 ACE는 원격 액세스 VPN 클라이언트에서 로컬 네트워크에 텔넷 연결하도록 허용합니다.

```
hostname(config-group-policy)# access-list vpnfilt-ra permit 10.10.10.1 255.255.255.255
192.168.1.0 255.255.255.0 eq 23
```

다음 ACE는 로컬 네트워크에서 원격 액세스 클라이언트에 텔넷 연결하도록 허용합니다.

```
hostname(config-group-policy)# access-list vpnfilt-ra permit 10.10.10.1 255.255.255.255 eq
 23 192.168.1.0 255.255.255.0
```

참고 ACE **access-list vpnfilt-ra permit 10.10.10.1 255.255.255.255 192.168.1.0 255.255.255.0 eq 23**은 로컬 네트워크가 소스 포트 23을 사용하는 경우 모든 TCP 포트에서 원격 액세스 클라이언트에 대한 연결을 시작하도록 허용합니다. ACE **access-list vpnfilt-ra permit 10.10.10.1 255.255.255.255 eq 23 192.168.1.0 255.255.255.0**은 원격 액세스 클라이언트가 소스 포트 23을 사용하는 경우 모든 TCP 포트에서 로컬 네트워크에 대한 연결을 시작하도록 허용합니다.

다음 예에서 vpn-filter는 LAN to LAN VPN 연결에 사용됩니다. 이 예에서는 원격 네트워크가 10.0.0.0/24이고 로컬 네트워크가 192.168.1.0/24라고 가정합니다. 다음 ACE는 원격 네트워크에서 로컬 네트워크에 텔넷 연결하도록 허용합니다.

```
hostname(config-group-policy)# access-list vpnfilt-l2l permit 10.0.0.0 255.255.255.0
192.168.1.0 255.255.255.0 eq 23
```

다음 ACE는 로컬 네트워크에서 원격 네트워크에 텔넷 연결하도록 허용합니다.

```
hostname(config-group-policy)# access-list vpnfilt-l2l permit 10.0.0.0 255.255.255.0 eq 23
 192.168.1.0 255.255.255.0
```

참고 ACE **access-list vpnfilt-l2l permit 10.0.0.0 255.255.255.0 192.168.1.0 255.255.255.0 eq 23**은 로컬 네트워크가 소스 포트 23을 사용하는 경우 모든 TCP 포트에서 원격 네트워크에 대한 연결을 시작하도록 허용합니다. ACE **access-list vpnfilt-l2l permit 10.0.0.0 255.255.255.0 eq 23 192.168.1.0 255.255.255.0**은 원격 네트워크가 소스 포트 23을 사용하는 경우 모든 TCP 포트에서 로컬 네트워크에 대한 연결을 시작하도록 허용합니다.

그룹 정책에 대해 VPN 액세스 시간 지정

시작하기 전에

시간 범위를 생성합니다. 일반 작업 구성 가이드에서 "구성 시간 범위"를 참조하십시오.

프로시저

단계 **1** 그룹 정책 구성 모드를 시작합니다.

group-policy *value* **attributes**

예제:

```
hostname> en
hostname# config t
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)#
```

단계 **2** 그룹 정책 구성 모드에서 **vpn-access-hours** 명령을 사용하여 구성된 시간 범위 정책을 그룹 정책과 연계하는 방법으로 VPN 액세스 시간을 설정할 수 있습니다. 이 명령은 이름이 business-hours인 VPN 액세스 시간 범위를 이름이 FirstGroup인 그룹 정책에 할당합니다.

그룹 정책은 기본값 또는 지정된 그룹 정책에서 시간 범위 값을 상속받을 수 있습니다. 상속을 방지하려면 이 명령에서 시간 범위의 이름 대신 **none** 키워드를 입력합니다. 이 키워드는 시간 범위 정책을 허용하지 않는 null 값에 VPN 액세스 시간을 설정합니다.

vpn-access-hours value {*time-range-name* | **none**}

예제:

```
hostname(config-group-policy)# vpn-access-hours value business-hours
hostname(config-group-policy)#
```

그룹 정책에 대해 동시 VPN 로그인 지정

그룹 정책 구성 모드에서 **vpn-simultaneous-logins** *integer* 명령을 사용하여 모든 사용자에게 허용되는 동시 로그인 수를 지정합니다.

기본값은 3입니다. 범위는 0부터 2147483647 사이의 정수입니다. 그룹 정책은 다른 그룹 정책에서 이 값을 상속받을 수 있습니다. 0을 입력하여 로그인을 비활성화하고 사용자 액세스를 방지합니다. 다음 예는 이름이 FirstGroup인 그룹 정책에 대해 최대 4개의 동시 로그인을 허용하는 방법을 보여줍니다.

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# vpn-simultaneous-logins 4
hostname(config-group-policy)#
```

참고 동시 로그인 수에 대한 최대 한계치는 매우 높지만 여러 개의 동시 로그인을 허용하면 보안이 손상되고 성능에 영향을 미칠 수 있습니다.

"새" 세션이 동일한 사용자 이름으로 설정된 경우에도 기존 AnyConnect, IPsec 클라이언트 또는 클라이언트리스 세션(비정상적으로 종료된 세션)이 세션 데이터베이스에 그대로 남을 수 있습니다.

vpn-simultaneous-logins 값이 1인 경우 비정상 종료 후 동일한 사용자가 다시 로그인하면 시간이 경과된 세션이 데이터베이스에서 제거되고 새 세션이 설정됩니다. 그러나 기존 세션이 계속 활성 연결 상태이며 동일한 사용자가 다른 PC에서 다시 로그인하는 경우, 첫 번째 세션이 로그오프되고 데이터베이스에서 제거되며 새 세션이 설정됩니다.

동시 로그인 수가 1보다 큰 값인 경우 최대 수에 도달한 후에 다시 로그인을 시도하면 유휴 시간이 가장 긴 세션이 로그오프됩니다. 모든 현재 세션이 동일하게 오랜 시간 동안 유휴 상태인 경우 가장 오래된 세션이 로그오프됩니다. 이 동작은 세션을 비우고 새 로그인을 허용합니다.

특정 연결 프로파일에 대한 액세스 제한

그룹 정책 구성 모드에서 **group-lock** 명령을 사용하여 연결 프로파일을 통해서만 액세스하도록 원격 사용자를 제한할지 지정하십시오.

```
hostname(config-group-policy)# group-lock {value tunnel-grp-name | none}
hostname(config-group-policy)# no group-lock
hostname(config-group-policy)#
```

tunnel-grp-name 변수는 ASA가 사용자 연결을 위해 필요로 하는 기존 연결 프로파일의 이름을 지정합니다. 그룹 잠금은 VPN 클라이언트에 구성된 그룹이 사용자가 할당된 연결 프로파일과 동일한지 여부를 확인하여 사용자를 제한합니다. 동일하지 않으면 ASA에서 사용자의 연결을 차단합니다. 그룹 잠금을 구성하지 않은 경우 ASA는 할당된 그룹에 상관없이 사용자를 인증합니다. 그룹 잠금은 기본적으로 비활성화되어 있습니다.

실행 중인 구성에서 **group-lock** 특성을 제거하려면 **no** 형식의 이 명령을 입력합니다. 이 옵션을 사용하면 다른 그룹 정책에서 값을 상속받을 수 있습니다.

그룹 잠금을 비활성화하려면 **none** 키워드와 함께 **group-lock** 명령을 입력합니다. none 키워드는 그룹 잠금을 null 값으로 설정하므로 그룹 잠금 제한이 허용되지 않습니다. 또한 기본 또는 지정된 그룹 정책에서 그룹 잠금 값을 상속받는 것을 방지합니다.

그룹 정책에서 최대 VPN 연결 시간 지정

프로시저

단계 1 (선택 사항) 그룹 정책 구성 모드 또는 사용자 이름 구성 모드에서 **vpn-session-timeout** *minutes* 명령을 사용하여 VPN 연결의 최대 시간을 구성합니다.

최소 시간은 1분이고 최대 시간은 35791394분입니다. 기본값은 없습니다. 구성된 기간의 마지막에서 ASA는 연결을 종료합니다.

다음 예는 이름이 FirstGroup인 그룹 정책에 대해 180분의 VPN 세션 시간 제한을 설정하는 방법을 보여줍니다.

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# vpn-session-timeout 180
hostname(config-group-policy)#
```

다음 예는 이름이 anyuser인 사용자에 대해 180분의 VPN 세션 시간 제한을 설정하는 방법을 보여줍니다.

```
hostname(config)# username anyuser attributes
hostname(config-username)# vpn-session-timeout 180
hostname(config-username)#
```

[**no**] **vpn-session-timeout** {*minutes* | **none**} 명령을 사용하는 다른 작업:

- 이 정책에서 속성을 제거하고 상속을 허용하려면 이 명령의 **no vpn-session-timeout** 형식을 입력합니다.
- 무제한 시간 제한 기간을 허용하여 시간 제한 값의 상속을 방지하려면 **vpn-session-timeout none**을 입력합니다.

단계 2 필요에 따라**vpn-session-timeout alert-interval** {*minutes* | } 명령을 사용하여 사용자에게 유휴 시간 제한 알림 메시지가 표시되는 시간을 구성할 수 있습니다.

이러한 알림 메시지는 VPN 세션이 자동으로 연결이 끊어질 때까지 몇 분이 남았는지 사용자에게 알려줍니다. 다음 예는 VPN 세션의 연결이 끊어지기 20분 전에 사용자에게 알려주도록 지정하는 방법을 보여줍니다. 1분-30분의 범위를 지정할 수 있습니다.

```
hostname(config-webvpn)# vpn-session-timeout alert-interval 20
```

[**no**] **vpn-session-timeout alert-interval** {*minutes* | **none**} 명령을 사용하는 다른 작업:

- 다음과 같이 no 형식의 명령을 사용하여 VPN 세션 시간 제한 알림 간격 특성을 기본 그룹 정책에서 상속받음을 나타냅니다.

  ```
  hostname(config-webvpn)# no vpn-session-timeout alert-interval
  ```

- **vpn-session-timeout alert-interval none**은 사용자가 알림을 수신하지 않음을 나타냅니다.

그룹 정책에 대해 VPN 세션 유휴 시간 제한 지정

프로시저

단계 1 (선택 사항) VPN 유휴 시간 제한 기간을 구성하려면 그룹 정책 구성 모드 또는 사용자 이름 구성 모드에서 **vpn-idle-timeout** *minutes* 명령을 사용합니다.

이 기간 동안 연결을 통한 통신 활동이 없는 경우 ASA는 연결을 종료합니다. 최소 시간은 1분, 최대 시간은 35791394분, 기본값은 30분입니다.

다음 예는 이름이 FirstGroup인 그룹 정책에 대해 15분의 VPN 유휴 시간 제한을 설정하는 방법을 보여줍니다.

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# vpn-idle-timeout 15
hostname(config-group-policy)#
```

[**no**] **vpn-idle-timeout** {*minutes* | **none**} 명령을 사용하는 다른 작업:

- **vpn-idle-timeout none**을 입력하여 VPN 유휴 시간 제한을 비활성화하고 시간 제한 값이 상속되지 않도록 합니다.

  ```
  hostname(config)# group-policy FirstGroup attributes
  hostname(config-group-policy)# vpn-idle-timeout none
  hostname(config-group-policy)#
  ```

  그러면 전역 webvpn **default-idle-timeout** 초 값을 사용하는 AnyConnect(SSL 및 IPsec/IKEv2) 및 클라이언트리스 VPN이 됩니다. 이 명령은 webvpn-config 모드에 입력됩니다(예: `hostnamee(config-webvpn)# default-idle-timeout 300`). 기본값은 1800초(30분), 범위는 60-86400초입니다.

  모든 webvon 연결에서 **vpn-idle-timeout none**이 그룹 정책/사용자 이름 속성에 설정된 경우에만 **default-idle-timeout** 값이 적용됩니다. 0이 아닌 유휴 시간 제한 값은 모든 AnyConnect 연결을 위한 ASA에 필요합니다.

  사이트 대 사이트(IKEv1, IKEv2) 및 IKEv1 원격 액세스 VPN: 시간 제한을 비활성화하고 무제한 유휴 기간을 허용하는 것이 좋습니다.

- 이 그룹 정책 또는 사용자 정책에 대한 유휴 시간 제한을 비활성화하려면 **no vpn-idle-timeout**을 입력합니다. 값이 상속됩니다.

- **vpn-idle-timeout**을 전혀 설정하지 않은 경우, 값이 상속되며 기본값은 30분입니다.

단계 2 (선택 사항) 필요에 따라 **vpn-idle-timeout alert-interval** {*minutes*} 명령을 사용하여 사용자에게 유휴 시간 제한 알림 메시지가 표시되는 시간을 구성할 수 있습니다.

이러한 알림 메시지는 VPN 세션이 비활성화로 인해 연결이 끊어질 때까지 몇 분이 남았는지 사용자에게 알려줍니다. 기본 알림 간격은 1분입니다.

다음 예는 이름이 anyuser인 사용자에 대해 VPN 유휴 시간 제한 및 3분의 알림 간격을 설정하는 방법을 보여줍니다.

```
hostname(config)# username anyuser attributes
hostname(config-username)# vpn-idle-timeout alert-interval 3
hostname(config-username)#
```

[**no**] **vpn-idle-timeout alert-interval** {*minutes* | **none**} 명령을 사용하는 다른 작업:

- **none** 매개변수는 사용자가 알림을 수신하지 않음을 나타냅니다.

```
hostname(config)# username anyuser attributes
hostname(config-username)# vpn-idle-timeout none
hostname(config-username)#
```

- 이 그룹 또는 사용자 정책에 대한 알림 간격을 제거하려면 **no vpn-idle-timeout alert-interval**을 입력합니다. 값이 상속됩니다.
- 이 매개변수를 설정하지 않을 경우 기본 알림 간격은 1분입니다.

그룹 정책에 대해 WINS 및 DNS 서버 구성

1차 및 2차 WINS 서버와 DNS 서버를 지정할 수 있습니다. 각각의 경우 기본값은 none(없음)입니다. 이 서버를 지정하려면 다음 단계를 수행하십시오.

프로시저

단계 **1** 다음과 같이 1차 및 2차 WINS 서버를 지정합니다.

```
hostname(config-group-policy)# wins-server value {ip_address [ip_address] | none}
hostname(config-group-policy)#
```

지정된 첫 번째 IP 주소는 1차 WINS 서버의 IP 주소입니다. 두 번째(선택 사항) IP 주소는 2차 WINS 서버의 IP 주소입니다. IP 주소 대신 **none** 키워드를 지정하면 WINS 서버가 null 값으로 설정되어 WINS 서버를 사용할 수 없으며 기본 또는 지정된 그룹 정책에서 값을 상속받는 것을 방지합니다.

wins-server 명령을 입력할 때마다 기존 설정이 덮어쓰기됩니다. 예를 들어 WINS 서버 x.x.x.x를 구성한 후 WINS 서버 y.y.y.y를 구성하는 경우 두 번째 명령이 첫 번째 명령을 덮어쓰고, y.y.y.y가 유일한 WINS 서버가 됩니다. 여러 서버의 경우에도 마찬가지입니다. 이전에 구성한 서버를 덮어쓰지 않고 WINS 서버를 추가하려면 이 명령을 입력할 때 모든 WINS 서버의 IP 주소를 포함하십시오.

다음 예는 이름이 FirstGroup인 그룹 정책에 대해 IP 주소 10.10.10.15 및 10.10.10.30을 사용하여 WINS 서버를 구성하는 방법을 보여줍니다.

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# wins-server value 10.10.10.15 10.10.10.30
hostname(config-group-policy)#
```

단계 **2** 다음과 같이 1차 및 2차 DNS 서버를 지정합니다.

```
hostname(config-group-policy)# dns-server value {ip_address [ip_address] | none}
hostname(config-group-policy)#
```

지정된 첫 번째 IP 주소는 1차 DNS 서버의 IP 주소입니다. 두 번째(선택 사항) IP 주소는 2차 DNS 서버의 IP 주소입니다. IP 주소 대신 **none** 키워드를 지정하면 DNS 서버가 null 값으로 설정되어 DNS 서버를 사용할 수 없으며 기본 또는 지정된 그룹 정책에서 값을 상속받는 것을 방지합니다. DNS 서버 주소는 최대 4개까지 지정할 수 있으며, IPv4 주소와 IPv6 주소는 각각 최대 2개까지 지정할 수 있습니다.

dns-server 명령을 입력할 때마다 기존 설정이 덮어쓰기됩니다. 예를 들어 DNS 서버 x.x.x.x를 구성한 다음 DNS 서버 y.y.y.y를 구성할 경우, 두 번째 명령이 첫 번째 명령을 덮어쓰므로 y.y.y.y가 유일한 DNS 서버가 됩니다. 여러 서버의 경우에도 마찬가지입니다. 이전에 구성한 서버를 덮어쓰지 않고 DNS 서버를 추가하려면 이 명령을 입력할 때 모든 DNS 서버의 IP 주소를 포함시키십시오.

다음 예는 이름이 FirstGroup인 그룹 정책에 대해 IP 주소 10.10.10.15, 10.10.10.30, 2001:DB8::1 및 2001:DB8::2를 사용하여 DNS 서버를 구성하는 방법을 보여줍니다.

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# dns-server value 10.10.10.15 10.10.10.30
2001:DB8::1 2001:DB8::2
hostname(config-group-policy)#
```

단계 **3** **DefaultDNS DNS** 서버 그룹에 지정된 기본 도메인 이름이 없는 경우, 기본 도메인을 지정해야 합니다. 예를 들어 **example.com**과 같은 도메인 이름과 최상위 도메인을 사용하십시오.

```
asa4(config)# group-policy FirstGroup attributes
asa4(config-group-policy)# default-domain value example.com
asa4(config-group-policy)#
```

단계 **4** 다음과 같이 DHCP 네트워크 범위를 구성합니다.

```
hostname(config-group-policy)# dhcp-network-scope {ip_address | none}
hostname(config-group-policy)#
```

DHCP 범위는 ASA DHCP 서버가 이 그룹 정책 사용자에게 주소를 할당하기 위해 사용해야 하는 IP 주소(즉, 서브네트워크) 범위를 지정합니다.

다음 예는 이름이 FirstGroup인 그룹 정책에 대해 10.10.85.0의 IP 서브네트워크(주소 범위를 10.10.85.0부터 10.10.85.255까지 지정)를 설정하는 방법을 보여줍니다.

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# dhcp-network-scope 10.10.85.0
```

스플릿 터널링 정책 설정

다음과 같이 IPv4 트래픽에 대해 스플릿 터널링 정책을 지정하여 터널링 트래픽에 대한 규칙을 설정합니다.

split-tunnel-policy{**tunnelall** | **tunnelspecified** | **excludespecified**}

no split-tunnel-policy

다음과 같이 IPv6 트래픽에 대해 스플릿 터널링 정책을 지정하여 터널링 트래픽에 대한 규칙을 설정합니다.

ipv6-split-tunnel-policy{**tunnelall** | **tunnelspecified** | **excludespecified**}

no ipv6-split-tunnel-policy

정책 옵션은 다음과 같습니다.

- **tunnelspecified** — 터널을 통해 네트워크 목록에 지정된 네트워크로 또는 네트워크로부터 모든 트래픽을 터널링합니다. 기타 모든 주소에 대한 데이터는 암호화되지 않고 이동하며 원격 사용자의 인터넷 서비스 공급자를 통해 라우팅됩니다.

  ASA 9.1.4 이상 버전의 경우 포함 목록을 지정할 때 포함 범위 내에 있는 서브넷에 대해 제외 목록을 지정할 수 있습니다. 제외된 서브넷에 있는 주소는 터널링되지 않으며 포함 목록의 나머지는 터널링됩니다. 제외 목록의 네트워크는 터널을 통해 전송되지 않습니다. 제외 목록은 거부 항목을 사용하여 지정되며 포함 목록은 허용 항목을 사용하여 지정됩니다.

- **excludespecified** — 네트워크 목록에 지정된 네트워크로 또는 해당 네트워크로부터 트래픽을 터널링하지 않습니다. 기타 모든 주소로부터 또는 주소로의 트래픽은 터널링됩니다. 클라이언트에서 활성화된 VPN 클라이언트 프로파일은 로컬 LAN 액세스가 활성화되어 있어야 합니다.

  참고 포함 목록의 하위 집합이 아닌 제외 목록에 있는 네트워크는 클라이언트에서 무시됩니다.

- **tunnelall** —모든 트래픽이 터널을 통과할지 지정합니다. 이 정책은 스플릿 터널링을 비활성화합니다. 원격 사용자는 기업 네트워크에 액세스할 수 있지만, 로컬 네트워크에는 액세스할 수 없습니다. 이것이 기본 옵션입니다.

참고 스플릿 터널링은 보안 기능이 아니라 트래픽 관리 기능입니다. 최상의 보안을 위해 스플릿 터널링을 활성화하지 않는 것이 좋습니다.

예

다음 예는 IPv4 및 IPv6용으로 이름이 FirstGroup인 그룹 정책에 대해 터널링만 지정된 네트워크의 스플릿 터널링 정책을 설정하는 방법을 보여줍니다.

```
hostname(config)# group-policy FirstGroup attributes
```

```
hostname(config-group-policy)# split-tunnel-policy tunnelspecified

hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# ipv6-split-tunnel-policy tunnelspecified
```

스플릿 터널링을 위한 네트워크 목록 지정

스플릿 터널링에서 네트워크 목록은 터널을 통해 어떤 네트워크 트래픽이 이동하는지 결정합니다. AnyConnect는 ACL인 네트워크 목록을 기준으로 스플릿 터널링을 결정합니다.

```
hostname(config-group-policy)# split-tunnel-network-list {value access-list_name | none}
hostname(config-group-policy)# no split-tunnel-network-list value [access-list_name]
```

- **value** access-list name - 터널링 또는 터널링하지 않는 네트워크를 열거하는 ACL을 식별합니다. ACL은 IPv4와 IPv6 주소를 모두 지정하는 ACE가 있는 통합 ACL이 될 수 있습니다.
- **none** - 스플릿 터널링을 위한 네트워크 목록이 없음을 나타내며 ASA는 모든 트래픽을 터널링합니다. **none** 키워드를 지정하면 스플릿 터널링 네트워크 목록이 null 값으로 설정되므로 스플릿 터널링이 허용되지 않습니다. 또한 기본 또는 지정된 그룹 정책에서 기본 스플릿 터널링 네트워크 목록을 상속받는 것을 방지합니다.

네트워크 목록을 삭제하려면 이 명령의 **no** 형식을 입력합니다. 모든 스플릿 터널링 네트워크 목록을 삭제하려면 인수 없이 **no split-tunnel-network-list** 명령을 입력합니다. 이 명령은 **none** 키워드를 입력하여 목록을 생성한 경우 null 목록을 포함하여 모든 구성된 네트워크 목록을 삭제합니다.

스플릿 터널링 네트워크 목록이 없는 경우 사용자는 기본 지정된 그룹 정책에 존재하는 모든 네트워크 목록을 상속받습니다. 사용자가 이 네트워크 목록에서 상속받는 것을 방지하려면 **split-tunnel-network-list none** 명령을 입력합니다.

예

다음 예는 이름이 FirstList인 네트워크 목록을 생성하고 이름이 FirstGroup인 그룹 정책에 이 목록을 추가하는 방법을 보여줍니다. FirstList는 제외 목록 및 이 제외 목록의 서브넷인 포함 목록입니다.

```
hostname(config)# split-tunnel-policy tunnelspecified
hostname(config)# access-list FirstList deny ip 10.10.10.0 255.255.255.0 any
hostname(config)# access-list FirstList permit ip 10.0.0.0 255.0.0.0 any

hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# split-tunnel-network-list value FirstList
```

다음 예는 이름이 v6인 네트워크 목록을 생성하고 이름이 GroupPolicy_ipv6-ikev2인 그룹 정책에 v6 스플릿 터널 정책을 추가하는 방법을 보여줍니다. v6는 제외 목록 및 이 제외 목록의 서브넷인 포함 목록입니다.

```
hostname(config)# access-list v6 extended permit ip fd90:5000::/32 any6
hostname(config)# access-list v6 extended deny ip fd90:5000:3000:2880::/64 any6

hostname(config)# group-policy GroupPolicy_ipv6-ikev2 internal
hostname(config)# group-policy GroupPolicy_ipv6-ikev2 attributes
hostname(config-group-policy)# vpn-tunnel-protocol ikev2 ssl-client
hostname(config-group-policy)# ipv6-split-tunnel-policy tunnelspecified
```

```
hostname(config-group-policy)# split-tunnel-network-list value v6
```

스플릿 터널 구성 확인

show runn group-policy attributes 명령을 실행하여 구성을 확인하십시오. 이 예는 관리자가 IPv4 및 IPv6 네트워크 정책 모두를 설정하고 이 두 가지 정책에 대해 네트워크 목록(통합 ACL)인 **FirstList**를 사용했는지 보여줍니다.

```
hostname(config-group-policy)# show runn group-policy FirstGroup attributes
group-policy FirstGroup attributes
 split-tunnel-policy tunnelspecified
 ipv6-split-tunnel-policy tunnelspecified
 split-tunnel-network-list value FirstList
```

스플릿 터널링을 위한 도메인 특성 구성

스플릿 터널을 통해 확인해야 할 기본 도메인 이름 또는 도메인 목록을 지정할 수 있으며 이를 스플릿 DNS라고도 합니다.

AnyConnect 3.1은 Windows와 Mac OS X 플랫폼에 대해 정확한 스플릿 DNS 기능을 지원합니다. 보안 어플라이언스에 있는 그룹 정책이 스플릿 포함 터널링을 활성화하고 터널링할 DNS 이름을 지정하는 경우, AnyConnect는 이 이름과 일치하는 모든 DNS 쿼리를 개별 DNS 서버에 터널링합니다. 정확한 스플릿 DNS는 ASA에서 클라이언트에 푸시한 도메인과 일치하는 DNS 요청에 대해서만 터널 액세스를 허용합니다. 이 요청은 암호화되지 않은 상태로 전송되지 않습니다. 반면에 DNS 요청이 ASA에서 푸시다운한 도메인과 일치하지 않는 경우, AnyConnect는 클라이언트 운영 체제에 있는 DNS 확인자가 DNS 확인을 위해 호스트 이름을 암호화되지 않은 상태로 전송하도록 할 수 있습니다.

참고 스플릿 DNS는 표준 및 업데이트 쿼리(A, AAAA, NS, TXT, MX SOA, ANY, SRV, PTR 및 CNAME)를 지원합니다. 터널링된 네트워크의 쿼리와 일치하는 PTR 쿼리는 터널을 통해 사용할 수 있습니다.

Mac OS X에서 AnyConnect는 다음 조건 중 하나를 충족하는 경우에만 특정 IP 프로토콜에 정확한 스플릿 DNS를 사용할 수 있습니다.

- 스플릿 DNS는 하나의 IP 프로토콜(IPv4 등)용으로 구성되었으며 클라이언트 우회 프로토콜은 그룹 정책에서 기타 IP 프로토콜(IPv6 등)용으로 구성되었습니다(기타 IP 프로토콜용으로 구성된 주소 풀 없음).
- 스플릿 DNS는 이 두 가지 IP 프로토콜용으로 구성됩니다.

기본 도메인 이름 정의

ASA는 AnyConnect 클라이언트에 기본 도메인 이름을 전달합니다. 클라이언트는 도메인 필드를 생략하는 DNS 쿼리에 도메인 이름을 추가합니다. 이 도메인 이름은 터널링 패킷에만 적용됩니다. 기본 도메인 이름이 없는 경우, 사용자는 기본 그룹 정책의 기본 도메인 이름을 상속받습니다.

그룹 정책의 사용자에 대해 기본 도메인 이름을 지정하려면 그룹 정책 구성 모드에서 **default-domain** 명령을 입력합니다. 도메인 이름을 삭제하려면 이 명령의 **no** 형식을 입력합니다.

```
hostname(config-group-policy)# default-domain {value domain-name | none}
hostname(config-group-policy)# no default-domain [domain-name]
```

value domain-name 매개변수는 그룹에 대한 기본 도메인 이름을 식별합니다. 기본 도메인 이름이 없도록 지정하려면 **none** 키워드를 입력합니다. 이 명령은 기본 도메인 이름을 null 값으로 설정하여 기본 도메인 이름을 허용하지 않고 기본 또는 지정된 그룹 정책에서 기본 도메인 이름을 상속받는 것을 방지합니다.

모든 기본 도메인 이름을 삭제하려면 인수 없이 **no default-domain** 명령을 입력합니다. 이 명령은 **none** 키워드와 함께 **default-domain** 명령을 입력하여 목록을 생성한 경우 null 목록을 포함하여 모든 구성된 기본 도메인 이름을 삭제합니다. **no** 형식은 도메인 이름을 상속받도록 허용합니다.

다음 예는 이름이 FirstGroup인 그룹 정책에 대해 FirstDomain의 기본 도메인 이름을 설정하는 방법을 보여줍니다.

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# default-domain value FirstDomain
```

스플릿 터널링을 위한 도메인 목록 정의

기본 도메인 이외에 스플릿 터널을 통해 확인할 도메인 목록을 입력합니다. 그룹 정책 구성 모드에서 **split-dns** 명령을 입력합니다. 목록을 삭제하려면 이 명령의 **no** 형식을 입력합니다.

스플릿 터널링 도메인 목록이 없는 경우 사용자는 기본 그룹 정책에 있는 항목을 상속합니다. 사용자가 해당 스플릿 터널링 도메인 목록을 상속받는 것을 방지하려면 **none** 키워드와 함께 **split-dns** 명령을 입력합니다.

모든 스플릿 터널링 도메인 목록을 삭제하려면 인수 없이 **no split-dns** 명령을 입력합니다. 이렇게 하면 **none** 키워드와 함께 **split-dns** 명령을 발행하여 생성한 null 목록을 포함하여 구성된 모든 스플릿 터널링 도메인 목록이 삭제됩니다.

매개변수인 **value** domain-name은 스플릿 터널을 통해 ASA가 확인하는 도메인 이름을 제공합니다. **none** 키워드는 스플릿 DNS 목록이 없음을 나타냅니다. 또한 스플릿 DNS 목록을 null 값으로 설정하므로 스플릿 DNS 목록을 허용하지 않고 기본 또는 지정된 그룹 정책에서 스플릿 DNS 목록을 상속받는 것을 방지합니다. 명령의 구문은 다음과 같습니다.

```
hostname(config-group-policy)# split-dns {value domain-name1 [domain-name2... domain-nameN]
 | none}
hostname(config-group-policy)# no split-dns [domain-name domain-name2 domain-nameN]
```

도메인 목록에 포함된 각 항목을 구분하려면 공백 한 칸을 입력합니다. 항목 수에 대한 제한은 없지만 전체 문자열이 255자를 초과할 수 없습니다. 영숫자 문자, 하이픈(-) 및 마침표(.)만 사용할 수 있습니다. 기본 도메인 이름을 터널을 통해 확인하려는 경우, 이 목록에 해당 이름을 명시적으로 포함시켜야 합니다.

다음 예는 이름이 FirstGroup인 그룹 정책에 대해 스플릿 터널링을 통해 도메인 Domain1, Domain2, Domain3 및 Domain4를 확인하도록 구성하는 방법을 보여줍니다.

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# split-dns value Domain1 Domain2 Domain3 Domain4
```

참고 스플릿 DNS를 구성하는 경우, 지정된 개별 DNS 서버가 클라이언트 플랫폼용으로 구성된 DNS 서버와 중복되지 않는지 확인하십시오. 중복되는 경우, 이름 확인 기능이 제대로 작동하지 않으며 쿼리가 삭제될 수 있습니다.

Windows XP 및 스플릿 터널링에 대한 DHCP 가로채기 구성

스플릿 터널 옵션이 255바이트를 초과하면 Microsoft XP에서 비정상적으로 도메인 이름이 손상될 수 있습니다. 이 문제를 방지하기 위해 ASA는 전송하는 경로 수를 27개에서 40개 경로로 제한합니다(경로 클래스에 종속된 경로 수 포함).

DHCP 가로채기를 통해 Microsoft Windows XP 클라이언트가 ASA에서 스플릿 터널링을 사용할 수 있습니다. ASA는 Microsoft Windows XP 클라이언트 DHCP Inform 메시지에 직접 응답하여, 해당 클라이언트에 터널 IP 주소의 서브넷 마스크, 도메인 이름 및 클래스리스 고정 경로를 제공합니다. Windows XP 이전 Windows 클라이언트의 경우 DHCP 가로채기는 도메인 이름 및 서브넷 마스크를 제공합니다. 이는 DHCP 서버 사용이 유리하지 않은 환경에서 유용합니다.

intercept-dhcp 명령은 DHCP 가로채기를 활성화 또는 비활성화합니다.

```
hostname(config-group-policy)# intercept-dhcp netmask {enable | disable}
hostname(config-group-policy)#
```

netmask 변수는 터널 IP 주소에 대한 서브넷 마스크를 제공합니다. 이 명령의 **no** 형식을 사용하면 구성에서 DHCP 가로채기가 제거됩니다.

[**no**] **intercept-dhcp**

다음 예는 이름이 FirstGroup인 그룹 정책에 대해 DHCP 가로채기를 설정하는 방법을 보여줍니다.

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# intercept-dhcp enable
```

원격 액세스 클라이언트에 사용할 브라우저 프록시 설정 구성

클라이언트에 대한 프록시 서버 매개변수를 구성하려면 다음 단계를 수행하십시오.

프로시저

단계 **1** 다음과 같이 그룹 정책 구성 모드에서 **msie-proxy server** 명령을 입력하여 클라이언트 기기에 대해 브라우저 프록시 서버 및 포트를 구성합니다.

```
hostname(config-group-policy)# msie-proxy server {value server[:port] | none}
hostname(config-group-policy)#
```

기본값은 **none**이며, 이는 클라이언트 디바이스의 브라우저에 대한 프록시 서버 설정을 지정하지 않습니다. 구성에서 속성을 제거하려면 명령의 **no** 형식을 사용합니다.

```
hostname(config-group-policy)# no msie-proxy server
hostname(config-group-policy)#
```

프록시 서버 IP 주소 또는 호스트 이름과 포트 번호를 포함하는 줄은 길이가 100자 미만이어야 합니다.

다음 예는 이름이 FirstGroup인 그룹 정책에 대해 포트 880을 사용하여 IP 주소 192.168.10.1을 브라우저 프록시 서버로 구성하는 방법을 보여줍니다.

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# msie-proxy server value 192.168.21.1:880
hostname(config-group-policy)#
```

단계 **2** 그룹 정책 구성 모드에서 **msie-proxy method** 명령을 입력하여 클라이언트 기기에 대해 브라우저 프록시 작업("방법")을 구성합니다.

```
hostname(config-group-policy)# msie-proxy method [auto-detect | no-modify |
no-proxy | use-server]
hostname(config-group-policy)#
```

기본값은 **no-modify**입니다. 구성에서 특성을 제거하려면 다음과 같이 **no** 형식의 명령을 사용합니다.

```
hostname(config-group-policy)# no msie-proxy method [auto-detect | no-modify |
no-proxy | use-server]
hostname(config-group-policy)#
```

사용 가능한 방법은 다음과 같습니다.

- **auto-detect** — 클라이언트 기기에 대해 브라우저에서 자동 프록시 서버 감지를 사용하도록 활성화합니다.
- **no-modify** — 브라우저에서 HTTP 브라우저 프록시 서버 설정을 이 클라이언트 기기에 대해 변경하지 않습니다.
- **no-proxy**—클라이언트 기기에 대해 브라우저에서 HTTP 프록시 설정을 비활성화합니다.
- **use-server**—브라우저의 HTTP 프록시 서버 설정에서 **msie-proxy server** 명령에 구성된 값을 사용하도록 설정합니다.

프록시 서버 IP 주소 또는 호스트 이름과 포트 번호를 포함하는 줄은 길이가 100자 미만이어야 합니다.

다음 예는 이름이 FirstGroup인 그룹 정책에 대해 브라우저 프록시 설정으로 auto-detect(자동 감지)를 구성하는 방법을 보여줍니다.

```
hostname(config)# group-policy FirstGroup attributes
```

```
hostname(config-group-policy)# msie-proxy method auto-detect
hostname(config-group-policy)#
```

다음은 서버 QAserver, 포트 1001을 클라이언트 기기에 대한 서버로 사용하도록 이름이 FirstGroup인 그룹 정책에 대해 브라우저 프록시 설정을 구성하는 예입니다.

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# msie-proxy server QAserver:port 1001
hostname(config-group-policy)# msie-proxy method use-server
hostname(config-group-policy)#
```

단계 **3** 그룹 정책 구성 모드에서 **msie-proxy except-list** 명령을 입력하여 클라이언트 기기에서 로컬 우회를 위해 브라우저 프록시 예외 목록 설정을 구성합니다. 이 주소는 프록시 서버에서 액세스되지 않습니다. 이 목록은 프록시 설정 대화 상자의 예외 상자에 해당합니다.

```
hostname(config-group-policy)# msie-proxy except-list {value server[:port] | none}
hostname(config-group-policy)#
```

구성에서 속성을 제거하려면 명령의 **no** 형식을 사용합니다.

```
hostname(config-group-policy)# no msie-proxy except-list
hostname(config-group-policy)#
```

- **value** server:port - 이 클라이언트 기기에 적용된 MSIE 서버와 포트의 IP 주소 또는 이름을 지정합니다. 포트 번호는 선택 사항입니다.
- **none**- IP 주소/호스트 이름 또는 포트가 없음을 나타내며 예외 목록을 상속받는 것을 방지합니다.

기본적으로 msie-proxy except-list는 비활성화되어 있습니다.

프록시 서버 IP 주소 또는 호스트 이름과 포트 번호를 포함하는 줄은 길이가 100자 미만이어야 합니다.

다음 예는 이름이 FirstGroup인 그룹 정책에 대해 포트 880을 사용하여 IP 주소 192.168.20.1에서 서버로 구성되는 브라우저 프록시 예외 목록을 설정하는 방법을 보여줍니다.

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# msie-proxy except-list value 192.168.20.1:880
hostname(config-group-policy)#
```

단계 **4** 그룹 정책 구성 모드에서 **msie-proxy local-bypass** 명령을 입력하여 클라이언트 기기에 대해 브라우저 프록시 로컬 우회 설정을 활성화하거나 비활성화합니다.

```
hostname(config-group-policy)# msie-proxy local-bypass {enable | disable}
hostname(config-group-policy)#
```

구성에서 특성을 제거하려면 다음과 같이 **no** 형식의 명령을 사용합니다.

```
hostname(config-group-policy)# no msie-proxy local-bypass {enable | disable}
hostname(config-group-policy)#
```

기본적으로 msie-proxy local-bypass는 비활성화되어 있습니다.

다음 예는 이름이 FirstGroup인 그룹 정책에 대해 브라우저 프록시 로컬 우회를 활성화하는 방법을 보여줍니다.

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# msie-proxy local-bypass enable
hostname(config-group-policy)#
```

IPsec(IKEv1) 클라이언트에 대한 보안 특성 구성

그룹에 대해 보안 설정을 지정하려면 다음 단계를 수행하십시오.

프로시저

단계 **1** 그룹 정책 구성 모드에서 **enable** 키워드와 함께 **password-storage** 명령을 사용하여 사용자가 클라이언트 시스템에 자신의 로그인 비밀번호를 저장하도록 허용할지 여부를 지정합니다. 비밀번호 저장을 비활성화하려면 **disable** 키워드와 함께 **password-storage** 명령을 사용합니다.

```
hostname(config-group-policy)# password-storage {enable | disable}
hostname(config-group-policy)#
```

보안상의 이유로 비밀번호 저장은 기본적으로 비활성화되어 있습니다. 안전한 사이트라고 간주되는 시스템에만 비밀번호 저장을 활성화합니다.

실행 중인 구성에서 password-storage 속성을 제거하려면 이 명령의 **no** 형식을 입력합니다.

```
hostname(config-group-policy)# no password-storage
hostname(config-group-policy)#
```

no 형식을 지정하면 다른 그룹 정책에서의 password-storage 값의 상속을 활성화합니다.

이 명령은 하드웨어 클라이언트를 위한 인터랙티브 하드웨어 클라이언트 인증 또는 개별 사용자 인증에 적용되지 않습니다.

다음 예는 이름이 FirstGroup인 그룹 정책에 대해 비밀번호 저장을 활성화하는 방법을 보여줍니다.

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# password-storage enable
hostname(config-group-policy)#
```

단계 **2** IP 압축을 활성화할지 지정합니다(기본적으로는 비활성화됨).

참고 IP 압축은 IPsec IKEv2 연결에 지원되지 않습니다.

```
hostname(config-group-policy)# ip-comp {enable | disable}
hostname(config-group-policy)#
```

LZS IP 압축을 활성화하려면 그룹 정책 구성 모드에서 **enable** 키워드와 함께 **ip-comp** 명령을 입력합니다. IP 압축을 비활성화하려면 **disable** 키워드와 함께 **ip-comp** 명령을 입력합니다.

실행 중인 구성에서 **ip-comp** 속성을 제거하려면 이 명령의 **no** 형식을 입력합니다. 이렇게 하면 다른 그룹 정책에서 값을 상속받을 수 있습니다.

```
hostname(config-group-policy)# no ip-comp
hostname(config-group-policy)#
```

데이터 압축을 활성화하면 모뎀으로 연결하는 원격 전화 접속 사용자의 데이터 전송 속도가 빨라질 수 있습니다.

팁 데이터 압축은 각 사용자 세션의 메모리 요건 및 CPU 사용률을 높이므로 결과적으로 ASA의 전체적인 처리량이 줄어듭니다. 이러한 이유로 모뎀에 연결하는 원격 사용자용으로만 데이터 압축을 활성화하는 것이 좋습니다. 모뎀 사용자에게 특정한 그룹 정책을 설계하고 모뎀 사용자용으로만 압축을 활성화합니다.

단계 **3** 그룹 정책 구성 모드에서 **enable** 키워드와 함께 **re-xauth** 명령을 사용하여 사용자가 IKE 키 재설정을 재인증해야 하는지 지정합니다.

참고 IKE 키 재설정은 IKEv2 연결에 지원되지 않습니다.

IKE 키 재설정에서 재인증을 활성화한 경우, ASA는 초기 1단계 IKE 협상 중에 사용자 이름과 비밀번호를 입력하도록 사용자에게 확인 상자를 표시하며 IKE 키 재설정이 발생할 때마다 사용자 인증을 위해 사용자에게 확인 상자를 표시합니다. 재인증은 추가 보안을 제공합니다.

구성된 키 재설정 간격이 매우 짧은 경우, 반복되는 권한 부여 요청이 불편할 수 있습니다. 반복되는 권한 부여 요청을 방지하려면 재인증을 비활성화하십시오. 구성된 키 재설정 간격을 확인하려면 모니터링 모드에서 **show crypto ipsec sa** 명령을 입력하여 보안 연계 수명(초 단위) 및 데이터 수명(킬로바이트 단위)을 확인합니다. IKE 키 재설정에서 사용자 재인증을 비활성화하려면 **disable** 키워드를 입력합니다. IKE 키 재설정에서 재인증은 기본적으로 비활성화되어 있습니다.

```
hostname(config-group-policy)# re-xauth {enable | disable}
hostname(config-group-policy)#
```

다른 그룹 정책으로부터 IKE 키 재설정에서의 재인증을 위해 값 상속을 활성화하려면, 다음과 같이 이 명령의 **no** 형식을 입력하여 실행 중인 구성에서 re-xauth 속성을 제거합니다.

```
hostname(config-group-policy)# no re-xauth
```

```
hostname(config-group-policy)#
```

참고 연결의 반대편에 사용자가 없는 경우 재인증이 실패합니다.

단계 4 완전 순방향 비밀성을 활성화할지 지정합니다. IPsec 협상에서 완전 순방향 비밀성은 각각의 새 암호화 키가 이전 키와 관련이 없도록 보장합니다. 그룹 정책은 다른 그룹 정책에서 완전 순방향 비밀성을 위한 값을 상속받을 수 있습니다. 완전 순방향 비밀성은 기본적으로 비활성화되어 있습니다. 완전 순방향 비밀성을 활성화하려면 그룹 정책 구성 모드에서 **enable** 키워드와 함께 **pfs** 명령을 사용합니다.

```
hostname(config-group-policy)# pfs {enable | disable}
hostname(config-group-policy)#
```

완전 순방향 비밀성을 비활성화하려면 **disable** 키워드와 함께 **pfs** 명령을 입력합니다.

실행 중인 구성에서 완전 순방향 비밀성 속성을 제거하고 값 상속을 방지하려면 이 명령의 **no** 형식을 입력합니다.

```
hostname(config-group-policy)# no pfs
hostname(config-group-policy)#
```

IKEv1 클라이언트에 대한 IPsec-UDP 특성 구성

UDP를 통한 IPsec(경우에 따라 NAT를 통한 IPsec이라고 함)을 사용하면 하드웨어 클라이언트가 NAT를 실행 중인 ASA에 UDP를 통해 연결될 수 있습니다. 기본적으로 비활성화되어 있습니다. UDP를 통한 IPsec은 전용 특성이며 원격 액세스 연결에만 적용되고 모드 구성을 필요로 합니다. ASA는 SA를 협상하는 동안 클라이언트와 구성 매개변수를 교환합니다. UDP를 통한 IPsec을 사용하면 시스템 성능이 약간 저하될 수 있습니다.

UDP를 통한 IPsec을 활성화하려면 다음과 같이 그룹 정책 구성 모드에서 **enable** 키워드와 함께 **ipsec-udp** 명령을 구성합니다.

```
hostname(config-group-policy)# ipsec-udp {enable | disable}
hostname(config-group-policy)# no ipsec-udp
```

UDP를 통한 IPsec을 사용하려면 이 섹션에 설명된 대로 **ipsec-udp-port** 명령도 구성해야 합니다.

UDP를 통한 IPsec을 비활성화하려면 **disable** 키워드를 입력합니다. 실행 중인 구성에서 UDP를 통한 IPsec을 제거하려면 이 명령의 **no** 형식을 입력합니다. 이렇게 하면 다른 그룹 정책에서 UDP를 통한 IPsec의 값을 상속받을 수 있습니다.

다음 예는 이름이 FirstGroup인 그룹 정책에 대해 UDP를 통한 IPsec을 설정하는 방법을 보여줍니다.

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# ipsec-udp enable
```

UDP를 통한 IPsec을 활성화한 경우, 그룹 정책 구성 모드에서 **ipsec-udp-port** 명령도 구성해야 합니다. 이 명령은 UDP를 통한 IPsec에 대해 UDP 포트 번호를 설정합니다. IPsec 협상에서 ASA는 구성된 포트에서 수신 대기하며 다른 필터 규칙이 UDP 트래픽을 삭제한 경우에도 해당 포트에 대해 UDP 트래픽을 전달합니다. 포트 번호는 4001부터 49151까지의 범위에서 가능합니다. 기본 포트 값은 10000입니다.

UDP 포트를 비활성화하려면 이 명령의 **no** 형식을 입력합니다. 이렇게 하면 다른 그룹 정책에서 UDP 포트를 통한 IPsec의 값을 상속받을 수 있습니다.

```
hostname(config-group-policy)# ipsec-udp-port port
```

다음 예는 이름이 FirstGroup인 그룹 정책에 대해 IPsec UDP 포트를 포트 4025로 설정하는 방법을 보여줍니다.

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# ipsec-udp-port 4025
```

VPN 하드웨어 클라이언트에 대한 속성 구성

프로시저

단계 **1** (선택 사항) 다음 명령을 사용하여 네트워크 확장 모드를 구성합니다.

[**no**] **nem** [**enable** | **disable**]

네트워크 확장 모드에서는 하드웨어 클라이언트가 VPN 터널을 통해 원격 사설 네트워크에 라우팅 가능한 단일 네트워크를 제공할 수 있습니다. PAT는 적용되지 않습니다. 따라서 Easy VPN Server 뒤에 있는 디바이스는 터널을 통해 Easy VPN Remote 뒤에 있는 프라이빗 네트워크의 디바이스에 직접 액세스할 수 있으며 이와 반대의 경우에는 터널을 통해서만 가능합니다. 하드웨어 클라이언트가 터널을 시작해야 하지만 터널이 끝나면 양측에서 데이터 교환을 시작할 수 있습니다.

예제**:**

다음 예는 이름이 FirstGroup인 그룹 정책에 대해 NEM을 설정하는 방법을 보여줍니다.

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# nem enable
```

NEM을 비활성화하려면 **disable** 키워드를 입력합니다. 실행 중인 구성에서 NEM 속성을 제거하려면 이 명령의 **no** 형식을 입력합니다. 이 옵션을 사용하면 다른 그룹 정책에서 값을 상속받을 수 있습니다.

단계 **2** (선택 사항) 다음 명령을 사용하여 Secure Unit Authentication(보안 유닛 인증)을 구성합니다.

[**no**] **secure-unit-authentication** [**enable** | **disable**]

보안 유닛 인증은 VPN 하드웨어 클라이언트가 터널을 시작할 때마다 사용자 이름 및 비밀번호를 사용하여 인증하도록 요구하는 방법을 통해 추가 보안을 제공합니다. 이 기능이 활성화되면 하드웨어

클라이언트에 저장된 사용자 이름 및 비밀번호를 사용하지 않습니다. 보안 유닛 인증은 기본적으로 비활성화되어 있습니다.

보안 유닛 인증에서는 하드웨어 클라이언트가 사용하는 연결 프로필에 대해 인증 서버 그룹을 구성해야 합니다. 1차 ASA에서 보안 유닛 인증이 필요한 경우, 백업 서버에서도 이를 구성했는지 확인하십시오.

참고 이 기능을 활성화한 경우 VPN 터널을 호출하려면 사용자가 사용자 이름 및 비밀번호를 입력해야 합니다.

예제:

다음 예는 이름이 FirstGroup인 그룹 정책에 대해 보안 유닛 인증을 활성화하는 방법을 보여줍니다.

```
hostname(config)#group-policy FirstGroup attributes
hostname(config-group-policy)# secure-unit-authentication enable
```

보안 유닛 인증을 비활성화하려면 **disable** 키워드를 입력합니다. 실행 중인 구성에서 보안 유닛 인증 속성을 제거하려면 이 명령의 **no** 형식을 입력합니다. 이 옵션을 사용하면 다른 그룹 정책에서 보안 유닛 인증을 위한 값을 상속받을 수 있습니다.

단계 **3** (선택 사항) 다음 명령을 사용하여 User Authentication(사용자 인증)을 구성합니다.

[**no**] **user-authentication** [**enable** | **disable**]

활성화되어 있는 경우, 사용자 인증을 하려면 하드웨어 클라이언트 뒤에 있는 개별 사용자가 인증하여 터널을 통과하는 네트워크에 대한 액세스 권한을 획득해야 합니다. 개별 사용자는 구성된 인증 서버의 순서에 따라 인증됩니다. 사용자 인증은 기본적으로 비활성화되어 있습니다.

1차 ASA에서 사용자 인증이 필요한 경우, 모든 백업 서버에서도 이를 구성했는지 확인하십시오.

예제:

다음 예는 이름이 FirstGroup인 그룹 정책에 대해 사용자 인증을 활성화하는 방법을 보여줍니다.

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# user-authentication enable
```

사용자 인증을 비활성화하려면 **disable** 키워드를 입력합니다. 실행 중인 구성에서 사용자 인증 속성을 제거하려면 이 명령의 **no** 형식을 입력합니다. 이 옵션을 사용하면 다른 그룹 정책에서 사용자 인증을 위한 값을 상속받을 수 있습니다.

단계 **4** 다음 명령을 사용하여 인증된 개별 사용자에 대한 유휴 시간 제한을 설정합니다.

[**no**] **user-authentication-idle-timeout** *minutes* | **none**]

minutes 매개변수는 유휴 시간 제한 동안의 시간(분)을 지정합니다. 최소값은 1분, 기본값은 30분, 최대값은 35791394분입니다.

유휴 시간 제한 동안 하드웨어 클라이언트 뒤에 있는 사용자가 통신 활동을 수행하지 않으면 다음과 같이 ASA는 클라이언트 액세스를 종료합니다. 이 타이머는 VPN 터널 자체가 아니라 VPN 터널을 통한 클라이언트 액세스만 종료합니다.

예제:

다음 예는 이름이 FirstGroup인 그룹 정책에 대해 45분의 유휴 시간 제한 값을 설정하는 방법을 보여 줍니다.

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# user-authentication enable
hostname(config-group-policy)#user-authentication-idle-timeout 45
```

유휴 시간 제한 값을 삭제하려면 이 명령의 **no** 형식을 입력합니다. 이 옵션을 사용하면 다른 그룹 정책에서 유휴 시간 제한 값을 상속받을 수 있습니다. 유휴 시간 제한 값의 상속을 방지하려면 **none** 키워드와 함께 **user-authentication-idle-timeout** 명령을 입력합니다. 이 명령은 유휴 시간 제한을 null 값으로 설정하여 유휴 시간 제한을 허용하지 않고 기본 또는 지정된 그룹 정책에서 사용자 인증 유휴 시간 제한 값을 상속받는 것을 방지합니다.

참고 **show uauth** 명령에 대한 응답으로 표시되는 유휴 시간 제한은 항상 Cisco Easy VPN 원격 디바이스의 터널에 인증된 사용자의 유휴 시간 제한 값입니다.

단계 **5** 다음 명령을 사용하여 IP Phone Bypass(IP 전화기 우회)를 구성합니다.

ip-phone-bypass enable

IP 전화기 우회를 사용하면 하드웨어 클라이언트 뒤에 있는 IP 전화기가 사용자 인증 프로세스 없이 연결됩니다. IP 전화기 우회는 기본적으로 비활성화되어 있습니다. IUA가 활성화된 경우에만 적용됩니다.

참고 클라이언트를 인증에서 면제하려면 클라이언트에서 MAC 주소 면제를 구성해야 합니다.

IP Phone Bypass(IP 전화기 우회)를 비활성화하려면 **disable** 키워드를 입력합니다. 실행 중인 구성에서 IP 전화기 우회 속성을 제거하려면 이 명령의 **no** 형식을 입력합니다. 이 옵션을 사용하면 다른 그룹 정책에서 IP Phone Bypass(IP 전화기 우회)를 위한 값을 상속 받을 수 있습니다.

단계 **6** 다음 명령을 사용하여 LEAP Bypass(LEAP 우회)를 구성합니다.

leap-bypass enable

user-authentication이 활성화된 경우에만 LEAP Bypass(LEAP 우회)가 적용됩니다. 이 명령을 사용하면 Cisco 무선 액세스 포인트 디바이스를 사용하는 LEAP 패킷이 LEAP 인증을 설정한 다음 사용자별 인증을 다시 인증합니다. LEAP 우회는 기본적으로 비활성화되어 있습니다.

하드웨어 클라이언트를 지원하는 LEAP 사용자에게는 상충하는 문제가 발생합니다. 터널을 통해 중앙 사이트 디바이스를 지원하는 RADIUS 서버로 크리덴셜을 전송할 수 없으므로 LEAP 인증을 협상할 수 없습니다. 터널을 통해 크리덴셜을 전송할 수 없는 이유는 무선 네트워크에서 인증되지 않았기 때문입니다. LEAP Bypass(LEAP 우회)는 이 문제를 해결하기 위해 LEAP 패킷이(LEAP 패킷만) 터널을 통과하도록 허용하여 개별 사용자 인증에 앞서 RADIUS 서버에 대한 무선 연결을 인증하도록 합니다. 그러면 사용자가 개별 사용자 인증을 진행할 수 있습니다.

LEAP Bypass(LEAP 우회)는 다음 조건에서 제대로 작동합니다.

- **secure-unit-authentication** 비활성화해야 합니다. 인터랙티브 유닛 인증이 활성화되면 비 LEAP(유선) 디바이스에서 하드웨어 클라이언트를 인증해야 LEAP 디바이스가 해당 터널을 사용하여 연결할 수 있습니다.

- **user-authentication** 활성화되어 있습니다. 그렇지 않으면, LEAP Bypass(LEAP 우회)가 적용되지 않습니다.
- 무선 환경에서 액세스 포인트는 CDP(Cisco Discovery Protocol)를 실행하는 Cisco Aironet Access Point여야 합니다. PC용 무선 NIC 카드는 다른 브랜드여도 됩니다.

예제:

다음 예는 이름이 FirstGroup인 그룹 정책에 대해 LEAP 우회를 설정하는 방법을 보여줍니다.

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# user-authentication enable
hostname(config-group-policy)# leap-bypass enable
```

LEAP 우회를 비활성화하려면 **disable** 키워드를 입력합니다. 실행 중인 구성에서 LEAP 우회 속성을 제거하려면 이 명령의 **no** 형식을 입력합니다. 이 옵션을 사용하면 다른 그룹 정책에서 LEAP 우회를 위한 값을 상속받을 수 있습니다.

AnyConnect Secure Mobility Client 연결에 대한 그룹 정책 특성 구성

AnyConnect VPN 클라이언트 연결, 237 페이지에 설명된 대로 AnyConnect 클라이언트 연결을 활성화한 후 그룹 정책에 대해 AnyConnect 기능을 활성화하거나 요청할 수 있습니다. 그룹 정책 webvpn 구성 모드에서 다음 단계를 수행하십시오.

프로시저

단계 **1** 그룹 정책 webvpn 구성 모드를 시작합니다. 예를 들면 다음과 같습니다.

```
hostname(config)# group-policy sales attributes
hostname(config-group-policy)# webvpn
```

단계 **2** 엔드포인트 컴퓨터에서 AnyConnect 클라이언트의 영구 설치를 비활성화하려면 **none** 키워드와 함께 anyconnect keep-installer 명령을 사용합니다. 예를 들면 다음과 같습니다.

```
hostname(config-group-webvpn)# anyconnect keep-installer none
hostname(config-group-webvpn)#
```

기본값은 클라이언트의 영구 설치를 활성화하는 것입니다. AnyConnect 세션 마지막에 클라이언트는 엔드포인트에 설치된 상태로 있습니다.

단계 **3** 그룹 정책을 위해 AnyConnect SSL 연결을 통해 HTTP 데이터의 압축을 활성화하려면 anyconnect ssl compression 명령을 입력합니다. 기본적으로 압축은 **none**(비활성화됨)으로 설정되어 있습니다. 압축을 활성화하려면 **deflate** 키워드를 사용합니다. 예를 들면 다음과 같습니다.

```
hostname(config-group-webvpn)# anyconnect compression deflate
```

```
hostname(config-group-webvpn)#
```

단계 **4** 데드 피어 감지 구성, 254 페이지

단계 **5** 다음과 같이 디바이스에서 다음 명령을 사용하여 킵얼라이브 메시지 빈도를 조정함으로써 연결이 유휴될 수 있는 시간을 제한하는 경우에도 프록시, 방화벽 또는 NAT 디바이스를 통해 AnyConnect 연결이 열린 상태인지 확인할 수 있습니다. **anyconnect ssl keepalive command:**

anyconnect ssl keepalive {none | *seconds***}**

킵얼라이브를 조정하면 원격 사용자가 소켓 기반 애플리케이션(예: Microsoft Outlook 또는 Microsoft Internet Explorer)을 활발하게 실행 중이지 않은 경우에도 AnyConnect 클라이언트가 연결 끊기 및 재연결하지 않습니다.

다음은 킵얼라이브 메시지를 300초(5분) 빈도로 전송하도록 AnyConnect 클라이언트를 활성화하기 위해 보안 어플라이언스를 구성하는 예입니다.

```
hostname(config-group-webvpn)# anyconnect ssl keepalive 300
hostname(config-group-webvpn)#
```

단계 **6** SSL 세션에서 키 재설정을 수행하도록 AnyConnect 클라이언트를 활성화하려면 다음과 같이 anyconnect ssl rekey 명령을 사용합니다.

anyconnect ssl rekey {**method** {**ssl** | **new-tunnel**} | **time** *minutes* | **none**}}

기본적으로 키 재설정은 비활성화되어 있습니다.

방법을 new-tunnel로 지정하면 AnyConnect 클라이언트가 SSL 키 재설정 동안 새 터널을 설정하도록 지정합니다. none으로 방법을 지정하면 키 재설정이 비활성화됩니다. ssl로 방법을 지정하면 SSL 재협상이 키 재설정 동안 발생함을 지정합니다. 방법을 지정하는 대신 시간 즉, 세션 시작부터 키 재설정이 발생할 때까지의 시간(분)을 1부터 10080(일주일)까지 지정할 수 있습니다.

다음은 키 재설정 동안 SSL과 재협상하도록 AnyConnect 클라이언트를 구성하고 키 재설정이 세션 시작 30분 후에 발생하도록 구성하는 예입니다.

```
hostname(config-group-webvpn)# anyconnect ssl rekey method ssl
hostname(config-group-webvpn)# anyconnect ssl rekey time 30
hostname(config-group-webvpn)#
```

단계 **7** 클라이언트 우회 프로토콜 기능을 사용하면 ASA에서 IPv6 트래픽만 예상하고 있을 때 IPv4 트래픽을 다루는 방법 또는 IPv4 트래픽만 예상하고 있을 때 IPv6 트래픽을 다루는 방법을 구성할 수 있습니다.

AnyConnect 클라이언트가 ASA와의 VPN 연결을 수행할 때 ASA는 IPv4, IPv6 주소를 또는 IPv4 및 IPv6 주소 모두 지정할 수 있습니다. ASA가 AnyConnect 연결에 IPv4 주소만 또는 IPv6 주소만 지정할 경우, ASA에서 IP 주소를 지정하지 않은 네트워크 트래픽을 삭제하거나 이 트래픽이 ASA를 우회하여 암호화되지 않은 "일반 텍스트" 형태로 클라이언트에서 전송되는 것을 허용하도록 클라이언트 우회 프로토콜을 구성할 수 있습니다.

예를 들어, ASA에서 AnyConnect 연결에 IPv4 주소만 지정하고 엔드포인트가 이중 스택이라고 가정합니다. 엔드포인트가 IPv6 주소에 연결하려고 시도할 때 클라이언트 우회 프로토콜이 비활성화된

경우 IPv6 트래픽이 끊기지만 클라이언트 우회 프로토콜이 활성화된 경우, IPv6 트래픽은 클라이언트에서 암호화되지 않은 상태로 전송됩니다.

클라이언트 우회 프로토콜 명령을 사용하여 클라이언트 우회 프로토콜 기능을 활성화 또는 비활성화합니다. 다음은 명령 구문입니다.

client-bypass-protocol {enable | disable}

다음 예는 클라이언트 우회 프로토콜을 활성화합니다.

```
hostname(config-group-policy)# client-bypass-protocol enable
hostname(config-group-policy)#
```

다음 예는 클라이언트 우회 프로토콜을 비활성화합니다.

```
hostname(config-group-policy)# client-bypass-protocol disable
hostname(config-group-policy)#
```

다음 예는 활성화 또는 비활성화된 클라이언트 우회 프로토콜 설정을 제거합니다.

```
hostname(config-group-policy)# no client-bypass-protocol enable
hostname(config-group-policy)#
```

단계 **8** ASA 간에 부하 균형을 구성한 경우, VPN 세션 재설정에 사용된 ASA IP 주소를 확인하도록 ASA의 FQDN을 지정합니다. 이 설정은 다른 IP 프로토콜의 네트워크 간(예: IPv4에서 IPv6)에 클라이언트 로밍을 지원하는 핵심 설정입니다.

AnyConnect 프로파일에 있는 ASA FQDN을 사용하여 로밍 후에 ASA IP 주소를 얻을 수 없습니다. 주소가 부하 균형 시나리오에 있는 올바른 디바이스(터널이 설정된 디바이스)와 일치하지 않을 수 있습니다.

FQDN 디바이스가 클라이언트에 푸시되지 않은 경우, 클라이언트는 터널에서 이전에 설정한 모든 IP 주소에 재연결하려고 시도합니다. 서로 다른 IP 프로토콜로 구성된 네트워크 사이의 로밍(예: IPv4에서 IPv6로)을 지원하려면 터널 재설정에 사용할 ASA 주소를 확인할 수 있도록 로밍 후에 AnyConnect에서 디바이스 FQDN의 이름 확인 작업을 수행해야 합니다. 클라이언트는 초기 연결 동안 프로파일에 있는 ASA FQDN을 사용합니다. 후속 세션 재연결 동안 사용 가능한 경우 ASA에서 푸시하고 그룹 정책에서 관리자가 구성한 디바이스 FQDN을 항상 사용합니다. FQDN이 구성되지 않은 경우, ASA는 Device Setup(디바이스 설정) > Device Name/Password and Domain Name(디바이스 이름/비밀번호 및 도메인 이름) 아래 설정에서 디바이스 FQDN을 파생시키고 이를 클라이언트에 전송합니다.

디바이스 FQDN이 ASA에서 푸시되지 않은 경우, 클라이언트는 여러 IP 프로토콜의 네트워크 간 로밍 후에 VPN 세션을 재설정할 수 없습니다.

gateway-fqdn 명령을 사용하여 ASA의 FQDN을 구성합니다. 다음은 명령 구문입니다.

gateway-fqdn { **value** *FQDN_Name* | **none**} 또는 **no gateway-fqdn**

다음은 ASAName.example.cisco.com으로 ASA의 FQDN을 정의한 예입니다.

```
hostname(config-group-policy)# gateway-fqdn value ASAName.example.cisco.com
hostname(config-group-policy)#
```

다음은 그룹 정책에서 ASA의 FQDN을 제거한 예입니다. 그룹 정책은 기본 그룹 정책에서 이 값을 상속받습니다.

```
hostname(config-group-policy)# no gateway-fqdn
hostname(config-group-policy)#
```

다음은 FQDN을 빈 값으로 정의하는 예입니다. hostname 및 domain-name 명령으로 구성된 전역 FQDN이 있으면 이 FQDN이 사용됩니다.

```
hostname(config-group-policy)# gateway-fqdn none
hostname(config-group-policy)#
```

백업 서버 특성 구성

백업 서버 특성을 사용할 계획인 경우 백업 서버를 구성하십시오. IPsec 백업 서버를 사용하면 기본 ASA를 사용할 수 없는 경우 VPN 클라이언트에서 중앙 사이트에 연결할 수 있습니다. 백업 서버를 구성하는 경우 ASA는 IPsec 터널이 설정되어 서버 목록을 클라이언트에 푸시합니다. 백업 서버는 클라이언트 또는 기본 ASA 중 하나에 이를 구성해야 존재합니다.

클라이언트 또는 기본 ASA 중 하나에 백업 서버를 구성하십시오. ASA에 백업 서버를 구성하는 경우, 백업 서버 정책을 그룹에 있는 클라이언트에 푸시하여 백업 서버가 구성된 경우 클라이언트에 있는 백업 서버 목록을 대체합니다.

참고 호스트 이름을 사용 중인 경우, 백업 DNS와 WINS 서버를 1차 DNS와 WINS 서버가 있는 네트워크와 다른 별도의 네트워크에 두는 것이 좋습니다. 그렇지 않으면 하드웨어 클라이언트 뒤에 있는 클라이언트가 DHCP를 통해 하드웨어 클라이언트에서 DNS 및 WINS 정보를 가져오는 경우, 1차 서버에 대한 연결이 손실되고 백업 서버가 다른 DNS 및 WINS 정보를 갖게 되며 DHCP 리스 기간이 만료될 때까지 클라이언트를 업데이트할 수 없습니다. 또한 사용할 수 없는 호스트 이름 및 DNS 서버를 사용하는 경우 시간이 상당히 지연될 수 있습니다.

백업 서버를 구성하려면 다음과 같이 그룹 정책 구성 모드에서 **backup-servers** 명령을 입력합니다.

```
hostname(config-group-policy)# backup-servers {server1 server2... server10 |
clear-client-config | keep-client-config}
```

백업 서버를 제거하려면 지정된 백업 서버에 이 명령의 **no** 형식을 입력합니다. 실행 중인 구성에서 백업 서버 속성을 제거하고 다른 그룹 정책으로부터의 백업 서버에 대한 값 상속을 활성화하려면 인수 없이 이 명령의 **no** 형식을 입력합니다.

```
hostname(config-group-policy)# no backup-servers [server1 server2... server10 |
clear-client-config | keep-client-config]
```

clear-client-config 키워드는 클라이언트가 백업 서버를 사용하지 않음을 지정합니다. ASA는 null 서버 목록을 푸시합니다.

keep-client-config 키워드는 ASA가 클라이언트에 백업 서버 정보를 전송하지 않음을 지정합니다. 클라이언트는 구성되어 있는 자신의 백업 서버 목록을 사용합니다. 이는 기본값입니다.

*server1 server 2.... server10*매개변수 목록은 기본 ASA를 사용할 수 없는 경우, 공백으로 구분되고 우선순위에 따라 나열된 사용할 VPN 클라이언트에 대한 서버 목록입니다. 이 목록은 IP 주소 또는 호스트 이름에 따라 서버를 식별합니다. 목록의 길이는 500자까지 가능하며 최대 10개의 항목이 포함될 수 있습니다.

다음 예는 이름이 FirstGroup인 그룹 정책에 대해 IP 주소 10.10.10.1 및 192.168.10.14를 사용하여 백업 서버를 구성하는 방법을 보여줍니다.

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# backup-servers 10.10.10.1 192.168.10.14
```

Network Admission Control 매개변수 구성

이 섹션에서 그룹 정책 NAC 명령에는 모두 기본값이 있습니다. 기본값을 변경할 합당한 이유가 있지 않은 한, 매개변수에 대해 이 기본값을 사용하십시오.

ASA는 UDP(EAPoUDP)를 통한 EAP(Extensible Authentication Protocol: 확장 가능 인증 프로토콜) 메시징을 사용하여 원격 호스트의 상태를 확인합니다. 보안 상태 검증에는 네트워크 액세스 정책을 할당하기 전에 보안 요건 컴플라이언스를 위해 원격 호스트를 확인하는 내용이 포함되어 있습니다. 보안 어플라이언스에서 NAC를 구성하기 전에 Network Admission Control을 위해 Access Control Server를 구성해야 합니다.

Access Control Server는 시스템 모니터링, 보고, 디버깅 및 로깅을 지원하기 위해 상태 토큰, ACS에서 구성 가능한 정보 텍스트 문자열을 보안 어플라이언스에 다운로드합니다. 일반적인 상태 토큰은 Healthy, Checkup, Quarantine, Infected 또는 Unknown입니다. 보안 상태 검증 또는 클라이언트리스 인증에 따라 ACS는 세션에 대한 액세스 정책을 보안 어플라이언스에 다운로드합니다.

기본 그룹 정책 또는 대체 그룹 정책에 대해 Network Admission Control 설정을 구성하려면 다음 단계를 수행하십시오.

프로시저

단계 **1** (선택 사항) 상태 쿼리 타이머 기간을 구성합니다. 보안 어플라이언스는 성공적인 보안 상태 검증 및 상태 쿼리 응답 이후에 상태 쿼리 타이머를 시작합니다. 이 타이머가 만료되면 호스트 상태의 변경사항에 대한 쿼리가 시작됩니다(상태 쿼리라고 함). 30에서 1800까지의 범위에서 시간(초)을 입력합니다. 기본 설정은 300입니다.

Network Admission Control 세션에서의 성공적인 각 보안 상태 검증과 호스트 상태의 변경사항에 대한 다음 쿼리 간에 간격을 지정하려면 다음과 같이 그룹 정책 구성 모드에서 **nac-sq-period** 명령을 사용합니다.

```
hostname(config-group-policy)# nac-sq-period seconds
```

```
hostname(config-group-policy)#
```

기본 그룹 정책에서 상태 쿼리 타이머의 값을 상속받으려면 이 값을 상속하는 대체 그룹 정책에 액세스한 다음 **no** 형식의 다음 명령을 사용합니다.

```
hostname(config-group-policy)# no nac-sq-period [seconds]
hostname(config-group-policy
```

다음은 상태 쿼리 타이머의 값을 1800초로 변경하는 예입니다.

```
hostname(config-group-policy)# nac-sq-period 1800
hostname(config-group-policy)#
```

다음은 기본 그룹 정책에서 상태 쿼리 타이머의 값을 상속받는 예입니다.

```
hostname(config-group-policy)# no nac-sq-period
hostname(config-group-policy)#
```

단계 **2** (선택 사항) NAC 재인증 기간을 구성합니다. 보안 어플라이언스는 성공적인 보안 상태 검증 이후에 재인증 타이머를 시작합니다. 이 타이머가 만료되면 다음의 무조건부 보안 상태 검증이 시작됩니다. 보안 어플라이언스는 재인증 동안 보안 상태 검증을 유지 관리합니다. 기본 그룹 정책은 보안 상태 검증 또는 재인증 동안 Access Control Server를 사용할 수 없는 경우 적용됩니다. 성공적인 보안 상태 검증 간격(초)을 입력합니다. 범위는 300에서 86400입니다. 기본 설정은 36000입니다.

Network Admission Control 세션에서 성공적인 보안 상태 검증 간 간격을 지정하려면 다음과 같이 그룹 정책 구성 모드에서 **nac-reval-period** 명령을 사용합니다.

```
hostname(config-group-policy)# nac-reval-period seconds
hostname(config-group-policy)#
```

기본 그룹 정책에서 재인증 타이머의 값을 상속받으려면 이 값을 상속하는 대체 그룹 정책에 액세스한 다음 **no** 형식의 다음 명령을 사용합니다.

```
hostname(config-group-policy)# no nac-reval-period [seconds]
hostname(config-group-policy)#
```

다음은 재인증 타이머를 86400초로 변경하는 예입니다.

```
hostname(config-group-policy)# nac-reval-period 86400
hostname(config-group-policy)
```

다음은 기본 그룹 정책에서 재인증 타이머의 값을 상속받는 예입니다.

```
hostname(config-group-policy)# no nac-reval-period
hostname(config-group-policy)#
```

단계 **3** (선택 사항) NAC에 대해 기본 ACL을 구성합니다. 보안 어플라이언스는 보안 상태 검증이 실패하는 경우 선택한 ACL과 연계된 보안 정책을 적용합니다. **none** 또는 확장 ACL을 지정합니다. 기본 설정

은 **none**입니다. 설정이 **none**이고 보안 상태 검증이 실패하면 보안 어플라이언스는 기본 그룹 정책을 적용합니다.

ACL을 보안 상태 검증에 실패하는 Network Admission Control 세션에 대한 기본 ACL로 사용되도록 지정하려면 다음과 같이 그룹 정책 구성 모드에서 **nac-default-acl** 명령을 사용합니다.

```
hostname(config-group-policy)# nac-default-acl {acl-name | none}
hostname(config-group-policy)#
```

기본 그룹 정책에서 ACL을 상속받으려면 이 값을 상속하는 대체 그룹 정책에 액세스한 다음 **no** 형식의 다음 명령을 사용합니다.

```
hostname(config-group-policy)# no nac-default-acl [acl-name | none]
hostname(config-group-policy)#
```

이 명령의 요소는 다음과 같습니다.

- *acl-name* - **aaa-server host** 명령을 사용하여 ASA에 구성된 대로 보안 상태 검증 서버 그룹의 이름을 지정합니다. 이 이름은 이 명령에 지정된 서버 태그 변수와 일치해야 합니다.
- **none** — 기본 그룹 정책에서의 ACL 상속을 비활성화하며 보안 상태 검증에 실패한 NAC 세션에 ACL을 적용하지 않습니다.

NAC는 기본적으로 비활성화되어 있으므로 ASA를 통과하는 VPN 트래픽은 NAC가 활성화될 때까지 NAC 기본 ACL의 적용을 받지 않습니다.

다음은 보안 상태 검증이 실패하는 경우 acl-1을 적용할 ACL로 식별하는 예입니다.

```
hostname(config-group-policy)# nac-default-acl acl-1
hostname(config-group-policy)#
```

다음은 기본 그룹 정책에서 ACL을 상속받는 예입니다.

```
hostname(config-group-policy)# no nac-default-acl
hostname(config-group-policy)#
```

다음은 기본 그룹 정책에서의 ACL 상속을 비활성화하며 보안 상태 검증에 실패한 NAC 세션에 ACL을 적용하지 않는 예입니다.

```
hostname(config-group-policy)# nac-default-acl none
hostname(config-group-policy)#
```

단계 **4** VPN에 NAC 면제를 구성합니다. 기본적으로 면제 목록은 비어 있습니다. 필터 속성의 기본값은 **none**입니다. 보안 상태 검증에서 원격 호스트를 면제하기 위해 일치하는 각 운영 체제(및 ACL)에 대해 **vpn-nac-exempt** 명령을 한 번 입력합니다.

보안 상태 검증에서 면제된 원격 컴퓨터 유형의 목록에 항목을 추가하려면 다음과 같이 그룹 정책 구성 모드에서 **vpn-nac-exempt** 명령을 사용합니다.

```
hostname(config-group-policy)# vpn-nac-exempt os "os name" [filter {acl-name | none}]
```

```
[disable]
hostname(config-group-policy)#
```

상속을 비활성화하고 모든 호스트가 보안 상태 검증의 적용을 받게 하려면 다음과 같이 **none** 키워드를 **vpn-nac-exempt** 명령 바로 다음에 사용합니다.

```
hostname(config-group-policy)# vpn-nac-exempt none
hostname(config-group-policy)#
```

면제 목록에서 항목을 제거하려면 다음과 같이 **no** 형식의 명령을 사용하고 제거할 항목에서 운영 체제(및 ACL)의 이름을 지정합니다.

```
hostname(config-group-policy)# no vpn-nac-exempt [os "os name"] [filter {acl-name | none}]
 [disable]
hostname(config-group-policy)#
```

이 그룹 정책과 연계된 면제 목록에서 모든 항목을 제거하고 기본 그룹 정책에서 목록을 상속받으려면 다음과 같이 추가 키워드를 지정하지 않고 **no** 형식의 이 명령을 사용합니다.

```
hostname(config-group-policy)# no vpn-nac-exempt
hostname(config-group-policy)#
```

이 명령의 구문 요소는 다음과 같습니다.

- *acl-name* - ASA 구성에 있는 ACL의 이름입니다.
- disable — 목록에서 항목을 제거하지 않고 면제 목록의 항목을 비활성화합니다.
- **filter**- (선택 사항) 컴퓨터가 운영 체제 이름과 일치하는 경우, ACL을 적용하여 트래픽을 필터링합니다.
- **none - vpn-nac-exempt** 이후에 바로 입력하면 이 키워드는 상속을 비활성화하고 모든 호스트가 보안 상태 검증의 적용을 받도록 지정합니다. **filter** 이후에 바로 입력하면 이 키워드는 항목이 ACL을 지정하지 않음을 나타냅니다.
- **OS -** 보안 상태 검증에서 운영 체제를 면제합니다.
- *os name* — 운영 체제 이름입니다. 따옴표는 이름에 공백이 포함되는 경우에만 필요합니다(예: "Windows XP").

다음은 상속을 비활성화하고 모든 호스트가 보안 상태 검증의 적용을 받도록 지정하는 예입니다.

```
hostname(config-group-policy)# no vpn-nac-exempt none
hostname(config-group-policy)
```

다음은 면제 목록에서 모든 항목을 제거하는 예입니다.

```
hostname(config-group-policy)# no vpn-nac-exempt
hostname(config-group-policy)
```

단계 **5** 다음 명령을 입력하여 Network Admission Control을 활성화 또는 비활성화합니다.

```
hostname(config-group-policy)# nac {enable | disable}
hostname(config-group-policy)#
```

기본 그룹 정책에서 NAC 설정을 상속받으려면 이 값을 상속하는 대체 그룹 정책에 액세스한 다음 **no** 형식의 다음 명령을 사용합니다.

```
hostname(config-group-policy)# no nac [enable | disable]
hostname(config-group-policy)#
```

기본적으로 NAC는 비활성화되어 있습니다. NAC를 활성화하려면 원격 액세스에 대한 보안 상태 검증이 필요합니다. 원격 컴퓨터가 검증 확인에 통과하는 경우, ACS 서버는 ASA에 적용할 액세스 정책을 다운로드합니다. NAC는 기본적으로 비활성화되어 있습니다.

Access Control Server는 네트워크 상에 있어야 합니다.

다음은 그룹 정책에 대해 NAC를 활성화하는 예입니다.

```
hostname(config-group-policy)# nac enable
hostname(config-group-policy)#
```

VPN 클라이언트 방화벽 정책 구성

방화벽은 데이터의 방화벽 통과를 허용할지 또는 삭제할지 판단하기 위해 데이터의 각 인바운드 및 아웃바운드 패킷을 검사하여 컴퓨터를 인터넷으로부터 격리시키고 보호합니다. 방화벽은 그룹에 있는 원격 사용자가 스플릿 터널링을 구성한 경우, 추가 보안을 제공합니다. 이 경우 방화벽은 인터넷 또는 사용자의 로컬 LAN을 사용하는 침입으로부터 사용자의 컴퓨터를 보호하므로 기업 네트워크도 보호됩니다. VPN 클라이언트를 사용하여 ASA에 연결하는 원격 사용자는 적절한 방화벽 옵션을 선택할 수 있습니다.

그룹 정책 구성 모드에서 **client-firewall** 명령을 사용하여 IKE 터널 협상 동안 ASA가 VPN 클라이언트에 푸시하는 개인 방화벽 정책을 설정합니다. 방화벽 정책을 삭제하려면 이 명령의 **no** 형식을 입력합니다.

모든 방화벽 정책을 삭제하려면 인수 없이 **no client-firewall** 명령을 입력합니다. 이 명령은 **none** 키워드와 함께 **client-firewall** 명령을 입력하여 정책을 생성한 경우 null 정책을 포함하여 모든 구성된 방화벽 정책을 삭제합니다.

방화벽 정책이 없는 경우 사용자는 기본 또는 기타 그룹 정책에 있는 방화벽 정책을 상속받습니다. 사용자가 해당 방화벽 정책을 상속받는 것을 방지하려면 **none** 키워드와 함께 **client-firewall** 명령을 입력합니다.

클라이언트 방화벽 탭에서 그룹 정책 추가 또는 수정 대화 상자를 사용하면 추가 또는 수정할 그룹 정책에 대해 VPN 클라이언트의 방화벽 설정을 구성할 수 있습니다.

참고 Microsoft Windows를 실행하는 VPN 클라이언트만 이러한 방화벽 기능을 사용할 수 있습니다. 이 기능은 하드웨어 클라이언트 또는 기타(Windows 이외) 소프트웨어 클라이언트에서는 현재 사용할 수 없습니다.

첫 번째 시나리오에서 원격 사용자의 PC에 개인 방화벽이 설치되어 있습니다. VPN 클라이언트는 로컬 방화벽에 정의된 방화벽 정책을 적용하고 방화벽이 실행 중인지 확인하기 위해 이를 모니터링합니다. 방화벽 실행이 중지되는 경우, VPN 클라이언트는 ASA에 대한 연결을 삭제합니다. (이 방화벽 적용 메커니즘은 VPN 클라이언트가 정기적으로 "are you there?"라는 메시지를 전송하여 방화벽을 모니터링하고 응답이 오지 않으면 방화벽이 다운된 것으로 알고 ASA에 대한 연결을 종료하므로 Are You There(AYT)라고 합니다.) 네트워크 관리자는 이러한 PC 방화벽을 초기 설정대로 구성할 수 있지만 이 접근 방식을 통해 각 사용자가 고유한 구성을 사용자 지정할 수 있습니다.

두 번째 시나리오에서는 VPN 클라이언트 PC의 개인 방화벽에 중앙 집중식 방화벽 정책을 적용하려고 합니다. 일반적인 예는 스플릿 터널링을 사용하여 그룹에 있는 원격 PC에 인터넷 트래픽을 차단하는 것입니다. 이러한 접근 방식은 터널을 설정하는 동안 인터넷을 통한 침입으로부터 PC와 중앙 사이트를 보호합니다. 이 방화벽 시나리오는 푸시 정책 또는 CPP(Central Protection Policy:중앙 보호 정책)라고 합니다. ASA에서 VPN 클라이언트에 적용할 트래픽 관리 규칙 집합을 만들어서 필터와 연결하고, 해당 필터를 방화벽 정책으로 지정합니다. ASA는 이 정책을 VPN 클라이언트에 푸시다운합니다. 그런 다음 VPN 클라이언트가 이 정책을 적용하는 로컬 방화벽에 차례대로 전달합니다.

AnyConnect 클라이언트 방화벽 정책 구성

AnyConnect 클라이언트에 대한 방화벽 규칙은 IPv4 및 IPv6 주소를 지정할 수 있습니다.

시작하기 전에

지정된 IPv6 주소를 사용하여 통합 액세스 규칙을 생성해야 합니다.

프로시저

단계 **1** webvpn 그룹 정책 구성 모드를 시작합니다.

webvpn

예제:

```
hostname(config)# group-policy ac-client-group attributes
hostname(config-group-policy)# webvpn
```

단계 **2** 프라이빗 또는 퍼블릭 네트워크 규칙에 대해 액세스 제어 규칙을 지정합니다. 프라이빗 네트워크 규칙은 클라이언트에 있는 VPN 가상 어댑터 인터페이스에 적용되는 규칙입니다.

anyconnect firewall-rule client-interface {private | public} value *[RuleName]*

```
hostname(config-group-webvpn)# anyconnect firewall-rule client-interface private value
ClientFWRule
```

단계 **3** 그룹 정책 속성과 그룹 정책에 대한 webvpn 정책 속성을 표시합니다.

show runn group-policy [value]

예제**:**

```
hostname(config-group-webvpn)# show run group-policy FirstGroup
group-policy FirstGroup internal
group-policy FirstGroup attributes
webvpn
  anyconnect firewall-rule client-interface private value ClientFWRule
```

단계 **4** 프라이빗 네트워크 규칙에서 클라이언트 방화벽 규칙을 제거합니다.

no anyconnect firewall-rule client-interface private value [*RuleName*]

예제**:**

```
hostname(config-group-webvpn)# no anyconnect firewall-rule client-interface private value
hostname(config-group-webvpn)#
```

Zone Labs Integrity 서버 사용

이 섹션에서는 Check Point Integrity 서버라고 불리는 Zone Labs Integrity 서버를 소개하고 Zone Labs Integrity 서버를 지원하도록 ASA를 구성하는 절차에 대한 예를 보여줍니다. Integrity 서버는 원격 PC에서 보안 정책을 구성하고 적용하기 위한 중앙 관리 스테이션입니다. 원격 PC가 Integrity 서버에서 지시한 보안 정책에 부합하지 않는 경우, Integrity 서버 및 ASA를 통해 보호하는 프라이빗 네트워크에 대한 액세스 권한이 부여되지 않습니다.

VPN 클라이언트 소프트웨어 및 Integrity 클라이언트 소프트웨어는 원격 PC에 공존합니다. 다음 단계는 PC와 기업 프라이빗 네트워크 간에 세션 설정 시 원격 PC, ASA 및 Integrity 서버의 작업을 요약한 것입니다.

1. Integrity 클라이언트 소프트웨어와 동일한 원격 PC에 있는 VPN 클라이언트 소프트웨어는 ASA에 연결하고 어떤 유형의 방화벽 클라이언트인지에 ASA에 정보를 제공합니다.
2. ASA가 클라이언트 방화벽 유형을 승인하면 ASA는 Integrity 서버 주소 정보를 Integrity 클라이언트에 다시 전달합니다.
3. 프록시 역할을 하는 ASA를 사용하여 Integrity 클라이언트는 Integrity 서버에 제한된 연결을 설정합니다. 제한된 연결은 Integrity 클라이언트와 Integrity 서버 간에만 적용됩니다.
4. Integrity 서버는 Integrity 클라이언트가 의무적인 보안 정책을 준수하는지 판단합니다. Integrity 클라이언트가 보안 정책 규정을 준수하는 경우, Integrity 서버는 연결을 열고 Integrity 클라이언트에 연결 세부 정보를 제공하도록 ASA에 지시합니다.
5. 원격 PC에서 VPN 클라이언트는 연결 세부사항을 Integrity 클라이언트에 전달하고 정책을 즉시 적용해야 한다고 신호를 보내면 Integrity 클라이언트가 사설 네트워크를 시작할 수 있습니다.

6. VPN 연결이 설정되면 Integrity 서버는 클라이언트 하트비트 메시지를 사용하여 Integrity 클라이언트의 상태를 계속해서 모니터링합니다.

참고 사용자 인터페이스에서 최대 5개의 Integrity 서버 구성을 지원하지만 ASA의 현재 릴리스는 한 번에 하나의 Integrity 서버를 지원합니다. 활성 Integrity 서버에서 장애가 발생하는 경우, ASA에 다른 Integrity 서버를 구성한 다음 VPN 클라이언트 세션을 재설정하십시오.

Integrity 서버를 구성하려면 다음 단계를 수행하십시오.

프로시저

단계 **1** IP 주소 10.0.0.5를 사용하여 Integrity 서버를 구성합니다.

```
zonelabs-Integrity server-address {hostname1 | ip-address1}
```

예제:

```
hostname(config)# zonelabs-Integrity server-address 10.0.0.5
```

단계 **2** 포트 300(기본 포트는 5054)을 지정합니다.

```
zonelabs-integrity port port-number
```

예제:

```
hostname(config)# zonelabs-integrity port 300
```

단계 **3** Integrity 서버와 통신하도록 내부 인터페이스를 지정합니다.

```
zonelabs-integrity interface interface
```

예제:

```
hostname(config)# zonelabs-integrity interface inside
```

단계 **4** Integrity 서버를 실패로 선언하고 VPN 클라이언트 연결을 닫기 전에 활성 또는 대기 Integrity 서버 중 하나로부터 응답을 받기 위해 ASA가 12초 동안 대기했는지 확인합니다.

참고 ASA와 Integrity 서버 간의 연결이 실패할 경우, 엔터프라이즈 VPN이 Integrity 서버의 실패로 인해 중단되지 않도록 VPN 클라이언트 연결이 기본적으로 열린 상태를 유지합니다. 하지만 Zone Labs Integrity 서버가 실패할 경우 VPN 연결을 닫을 수도 있습니다.

```
zonelabs-integrity fail-timeout timeout
```

예제:

```
hostname(config)# zonelabs-integrity fail-timeout 12
```

단계 **5** ASA와 Zone Labs Integrity 서버 간의 연결이 실패할 경우, VPN 클라이언트에 대한 연결이 닫히도록 ASA를 구성합니다.

zonelabs-integrity fail-close

예제:

```
hostname(config)# zonelabs-integrity fail-close
```

단계 **6** 구성된 VPN 클라이언트 연결 실패 상태를 기본값으로 되돌리고 클라이언트 연결이 열려 있는지 확인합니다.

zonelabs-integrity fail-open

예제:

```
hostname(config)# zonelabs-integrity fail-open
```

단계 **7** 서버 SSL 인증서를 요청하기 위해 ASA에 있는 포트 300(기본값은 포트 80)에 Integrity 서버를 연결하도록 지정합니다.

zonelabs-integrity ssl-certificate-port cert-port-number

예제:

```
hostname(config)# zonelabs-integrity ssl-certificate-port 300
```

단계 **8** 서버 SSL 인증서가 항상 인증된 상태이며 Integrity 서버의 클라이언트 SSL 인증서가 인증되도록 지정합니다.

zonelabs-integrity ssl-client-authentication {enable | disable}

예제:

```
hostname(config)# zonelabs-integrity ssl-client-authentication enable
```

방화벽 클라이언트 유형을 Zone Labs로 설정

프로시저

	명령 또는 동작	목적
단계 **1**	Zone Labs Integrity 유형의 방화벽 클라이언트 유형을 설정하려면 다음 명령을 입력합니다. 예제: `hostname(config)# client-firewall req zonelabs-integrity`	**client-firewall {opt | req} zonelabs-integrity**

다음에 수행할 작업

자세한 내용은 VPN 클라이언트 방화벽 정책 구성, 179 페이지를 참조하십시오. Integrity 서버가 방화벽 정책을 결정하므로 방화벽 유형이 **zonelabs-integrity**인 경우, 방화벽 정책을 지정하는 명령 인수가 사용되지 않습니다.

클라이언트 방화벽 매개변수 설정

적절한 클라이언트 방화벽 매개변수를 설정하려면 다음 명령을 입력합니다. 각 명령에 하나의 인스턴스만 구성할 수 있습니다. 자세한 내용은 VPN 클라이언트 방화벽 정책 구성, 179 페이지를 참조하십시오.

- Cisco 통합 방화벽

```
hostname(config-group-policy)# client-firewall {opt | req} cisco-integrated
acl-in ACL acl-out ACL
```

- Cisco Security Agent

```
hostname(config-group-policy)# client-firewall {opt | req} cisco-security-agent
```

- 방화벽 없음

```
hostname(config-group-policy)# client-firewall none
```

- 사용자 지정 방화벽

```
hostname(config-group-policy)# client-firewall {opt | req} custom vendor-id num product-id
 num policy {AYT | CPP acl-in ACL acl-out ACL} [description string]
```

- Zone Labs 방화벽

```
hostname(config-group-policy)# client-firewall {opt | req} zonelabs-integrity
```

참고 방화벽 유형이 **zonelabs-integrity**라면 인수를 포함하지 않습니다. Zone Labs Integrity 서버가 정책을 결정합니다.

```
hostname(config-group-policy)# client-firewall {opt | req} zonelabs-zonealarm
 policy {AYT | CPP acl-in ACL acl-out ACL}

hostname(config-group-policy)# client-firewall {opt | req}
zonelabs-zonealarmorpro policy {AYT | CPP acl-in ACL acl-out ACL}

client-firewall {opt | req} zonelabs-zonealarmpro policy {AYT | CPP acl-in
 ACL acl-out ACL}
```

- Sygate 개인용 방화벽

```
hostname(config-group-policy)# client-firewall {opt | req} sygate-personal

hostname(config-group-policy)# client-firewall {opt | req} sygate-personal-pro

hostname(config-group-policy)# client-firewall {opt | req} sygate-security-agent
```

- Network Ice,Black Ice 방화벽

```
hostname(config-group-policy)# client-firewall {opt | req} networkice-blackice
```

표 6: 클라이언트 방화벽 명령 키워드 및 변수

파라미터	설명
acl-in ACL	클라이언트가 인바운드 트래픽에 사용하는 정책을 제공합니다.
acl-out ACL	클라이언트가 아웃바운드 트래픽에 사용하는 정책을 제공합니다.
AYT	클라이언트 PC 방화벽 애플리케이션이 방화벽 정책을 제어하도록 지정합니다. ASA는 방화벽이 실행되고 있는지 확인합니다. "Are You There?"라고 물은 경우 응답이 없으면 ASA는 터널을 해체합니다.
cisco-integrated	Cisco 통합 방화벽 유형을 지정합니다.
cisco-security-agent	Cisco Intrusion Prevention Security Agent 방화벽 유형을 지정합니다.
CPP	푸시된 정책을 VPN 클라이언트 방화벽 정책의 소스로 지정합니다.
custom	사용자 지정 방화벽 유형을 지정합니다.
description 문자열	방화벽에 대해 설명합니다.
networkice-blackice	Network ICE Black ICE 방화벽 유형을 지정합니다.
none	클라이언트 방화벽 정책이 없음을 나타냅니다. 방화벽 정책을 null 값으로 설정하므로 방화벽 정책을 허용하지 않습니다. 기본 또는 지정된 그룹 정책에서 방화벽 정책을 상속받는 것을 방지합니다.
opt	선택적인 방화벽 유형을 나타냅니다.
product-id	방화벽 제품을 식별합니다.
req	필수 방화벽 유형을 나타냅니다.
sygate-personal	Sygate 개인용 방화벽 유형을 지정합니다.
sygate-personal-pro	Sygate 개인용 Pro 버전 방화벽 유형을 지정합니다.

sygate-security-agent	Sygate Security Agent 방화벽 유형을 지정합니다.
vendor-id	방화벽 공급업체를 식별합니다.
zonelabs-integrity	Zone Labs Integrity 서버 방화벽 유형을 지정합니다.
zonelabs-zonealarm	Zone Labs Zone Alarm 방화벽 유형을 지정합니다.
zonelabs-zonealarmorpro policy	Zone Labs Zone Alarm 또는 Pro 방화벽 유형을 지정합니다.
zonelabs-zonealarmpro policy	Zone Labs Zone Alarm Pro 방화벽 유형을 지정합니다.

다음 예는 이름이 FirstGroup인 그룹 정책에 대해 Cisco Intrusion Prevention Security Agent를 필요로 하는 클라이언트 방화벽 정책을 설정하는 방법을 보여줍니다.

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# client-firewall req cisco-security-agent
hostname(config-group-policy)#
```

클라이언트 액세스 규칙 구성

그룹 정책 구성 모드에서 **client-access-rule** 명령을 사용하여 ASA에서 IPsec을 통해 연결할 수 있는 버전 및 원격 액세스 클라이언트 유형을 제한하는 규칙을 구성합니다. 다음 지침에 따라 규칙을 구성하십시오.

- 어떤 규칙도 정의하지 않은 경우, ASA는 모든 연결 유형을 허용합니다.
- 클라이언트가 어떤 규칙과도 일치하지 않는 경우, ASA는 연결을 거부합니다. 거부 규칙을 정의하는 경우, 최소한 하나의 허용 규칙을 정의해야 하며 그렇지 않은 경우, ASA는 모든 연결을 거부합니다.
- 소프트웨어 및 하드웨어 클라이언트 모두에 대해 유형과 버전이 **show vpn-sessiondb remote** 표시의 모양과 정확하게 일치해야 합니다.
- ***** 문자는 각 규칙에서 여러 번 입력할 수 있는 와일드카드입니다. 예를 들어 **client-access rule 3 deny type * version 3.***는 3.x 버전 소프트웨어를 실행하는 모든 클라이언트 유형을 거부하는 우선순위 3의 클라이언트 액세스 규칙을 생성합니다.
- 그룹 정책당 최대 25개의 규칙을 구성할 수 있습니다.
- 전체 규칙 집합의 문자 수는 255자로 제한됩니다.
- 클라이언트 유형 및/또는 버전을 전송하지 않는 클라이언트에 대해 n/a를 입력할 수 있습니다.

규칙을 삭제하려면 이 명령의 **no** 형식을 입력합니다. 이 명령은 다음 명령과 동일합니다.

```
hostname(config-group-policy)# client-access-rule 1 deny type "Cisco VPN Client" version
```

4.0

모든 규칙을 삭제하려면 인수 없이 **no client-access-rule command**을 입력합니다. 이 명령은 **none** 키워드와 함께 **client-access-rule** 명령을 발행하여 규칙을 생성한 경우 null 규칙을 포함하여 모든 구성된 규칙을 삭제합니다.

기본적으로 액세스 규칙은 없습니다. 클라이언트 액세스 규칙이 없는 경우 사용자는 기본 그룹 정책에 있는 규칙을 상속받습니다.

사용자가 클라이언트 액세스 규칙을 상속받는 것을 방지하려면 **none** 키워드와 함께 **client-access-rule** 명령을 입력합니다. 이 명령을 사용하면 모든 클라이언트 유형 및 버전에서 연결할 수 있습니다.

```
hostname(config-group-policy)# client-access rule priority {permit | deny} type
type version {version | none}

hostname(config-group-policy)# no client-access rule [priority {permit | deny} type
 type version version]
```

아래 표에는 이 명령에 포함된 키워드 및 매개변수의 의미가 설명되어 있습니다.

표 *7:* 클라이언트 액세스 규칙 명령 키워드 및 변수

파라미터	설명
deny	특정 유형 및/또는 버전의 디바이스에 대해 연결을 거부합니다.
none	클라이언트 액세스 규칙을 허용하지 않습니다. client-access-rule을 null 값으로 설정하므로 제한이 없습니다. 기본 또는 지정된 그룹 정책에서 값을 상속받는 것을 방지합니다.
permit	특정 유형 및/또는 버전의 디바이스에 대해 연결을 허용합니다.
priority	규칙의 우선순위를 결정합니다. 가장 낮은 정수가 포함된 규칙이 우선순위가 가장 높습니다. 따라서 클라이언트 유형 및/또는 버전과 일치하는 가장 낮은 정수가 포함된 규칙이 적용되는 규칙입니다. 우선순위가 낮은 규칙이 일치하지 않는 경우 ASA는 이 규칙을 무시합니다.
type *type*	자유 형식 문자열로 디바이스 유형을 나타냅니다. * 문자를 와일드카드로 입력할 수 있다는 점을 제외하고 문자열은 **show vpn-sessiondb remote** 표시의 모양과 정확하게 일치해야 합니다.

파라미터	설명
version version	자유 형식 문자열로 디바이스 버전을 나타냅니다(예: 7.0). * 문자를 와일드카드로 입력할 수 있다는 점을 제외하고 문자열은 **show vpn-sessiondb remote** 표시의 모양과 정확하게 일치해야 합니다.

다음 예는 이름이 FirstGroup인 그룹 정책에 대해 클라이언트 액세스 규칙을 생성하는 방법을 보여줍니다. 이 규칙은 다음과 같이 모든 Windows NT 클라이언트는 거부하지만 소프트웨어 버전 4.x를 실행하는 Cisco VPN 클라이언트는 허용합니다.

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# client-access-rule 1 deny type WinNT version *
hostname(config-group-policy)# client-access-rule 2 permit "Cisco VPN Client"
version 4.*
```

참고 "type" 필드는 어떤 값이든 허용하는 자유 형식 문자열이지만 이때 값은 연결 시간에 클라이언트가 ASA에 전송하는 고정 값과 일치해야 합니다.

사용자 속성 구성

이 섹션에서는 사용자 특성 및 사용자 특성을 구성하는 방법에 대해 설명합니다.

기본적으로 사용자는 할당된 그룹 정책에서 모든 사용자 특성을 상속받습니다. 또한 ASA를 사용하면 사용자 수준에서 개별 속성을 할당할 수 있어 해당 사용자에게 적용되는 그룹 정책에서 값을 재정의합니다. 예를 들어 업무 시간 동안 모든 사용자 액세스를 제공하는 그룹 정책을 지정할 수 있지만 특정 사용자에게 24시간 액세스를 제공합니다.

사용자 이름 구성 보기

그룹 정책에서 상속받은 기본값을 포함하여 모든 사용자 이름에 대해 구성을 표시하려면 다음과 같이 **show running-config username** 명령과 함께 **all** 키워드를 입력합니다.

```
hostname# show running-config all username
hostname#
```

이것은 모든 사용자에 대해 암호화된 비밀번호 및 권한 수준을 표시하며 사용자 이름을 제공하는 경우 특정 사용자에 대해 표시합니다. **all** 키워드를 생략하는 경우 명시적으로 구성된 값만 이 목록에 나타납니다. 다음 예는 이름이 testuser인 사용자에 대해 명령의 출력을 표시합니다.

```
hostname# show running-config all username testuse
username testuser password 12RsxXQnphyr/I9Z encrypted privilege 15
```

개별 사용자를 위한 특성 구성

특정한 사용자를 구성하려면 사용자 이름 모드를 시작하는 **username** 명령을 사용하여 비밀번호(또는 비밀번호 없음) 및 특성을 사용자에게 할당합니다. 지정하지 않은 모든 특성은 그룹 정책에서 상속받습니다.

내부 사용자 인증 데이터베이스는 **username** 명령을 사용하여 입력된 사용자로 구성됩니다. **login** 명령은 인증을 위해 이 데이터베이스를 사용합니다. ASA 데이터베이스에 사용자를 추가하려면 전역 구성 모드에서 **username** 명령을 입력합니다. 사용자를 제거하려면 제거할 사용자 이름과 함께 **no** 버전의 명령을 사용합니다. 모든 사용자 이름을 제거하려면 사용자 이름을 추가하지 않고 **clear configure username** 명령을 사용합니다.

사용자 비밀번호 및 권한 수준 설정

사용자에게 비밀번호 및 권한 수준을 할당하려면 **username** 명령을 입력합니다. 이 사용자에게 비밀번호가 필요하지 않음을 지정하려면 **nopassword** 키워드를 입력할 수 있습니다. 비밀번호를 지정한 경우 암호화된 형식으로 해당 비밀번호를 저장할지 지정할 수 있습니다.

선택 사항인 **privilege** 키워드를 사용하여 이 사용자의 권한 수준을 설정할 수 있습니다. 권한 수준은 0(최저)부터 15까지입니다. 시스템 관리자는 일반적으로 가장 높은 수준의 권한을 지닙니다. 기본 수준은 2입니다.

```
hostname(config)# username name {nopassword | password password [encrypted]}
[privilege priv_level]}
```

```
hostname(config)# no username [name]
```

아래 표에서는 이 명령에서 사용되는 키워드 및 변수의 의미를 설명합니다.

사용자 이름 명령 키워드 및 변수

키워드/변수	의미
encrypted	비밀번호가 암호화되어 있음을 나타냅니다.
name	사용자의 이름을 제공합니다.
nopassword	이 사용자에게 비밀번호가 필요하지 않음을 나타냅니다.
password password	이 사용자에게는 비밀번호가 있음을 표시하며 비밀번호를 제공합니다.
privilege priv_level	이 사용자의 권한 수준을 설정합니다. 범위는 0에서 15까지이며, 숫자가 낮을수록 명령을 사용하고 ASA를 관리하는 능력이 낮습니다. 기본 권한 수준은 2입니다. 시스템 관리자의 일반적인 권한 수준은 15입니다.

기본적으로 이 명령을 사용하여 추가하는 VPN 사용자에게는 특성 또는 그룹 정책 연결이 없습니다. 명시적으로 모든 값을 구성해야 합니다.

다음 예는 이름이 anyuser인 사용자를 암호화된 비밀번호인 pw_12345678과 권한 수준 12로 구성하는 방법을 보여줍니다.

```
hostname(config)# username anyuser password pw_12345678 encrypted privilege
 12
hostname(config)#
```

사용자 속성 구성

사용자의 비밀번호(있는 경우) 및 권한 수준을 구성한 후 다른 특성을 설정합니다. 특성은 어떤 순서로도 설정 가능합니다. 모든 속성 값 쌍을 제거하려면 **no** 형식의 명령을 입력합니다.

다음과 같이 **attributes** 키워드와 함께 **username** 명령을 입력하여 사용자 이름 모드를 시작합니다.

```
hostname(config)# username name attributes
hostname(config-username)#
```

확인 상자가 변경되어 새 모드를 나타냅니다. 이제 특성을 구성할 수 있습니다.

VPN 사용자 속성 구성

다음 섹션에서 설명한 대로 VPN 사용자 특성은 VPN 연결에 특정한 값을 설정합니다.

상속 구성

사용자가 그룹 정책으로부터 사용자 이름 수준에서 구성하지 않은 특성 값을 상속받도록 설정할 수 있습니다. 이 사용자가 속성을 상속받을 그룹 정책의 이름을 지정하려면 **vpn-group-policy** 명령을 입력합니다. 다음과 같이 VPN 사용자는 기본적으로 그룹 정책 연계가 없습니다.

```
hostname(config-username)# vpn-group-policy group-policy-name
hostname(config-username)# no vpn-group-policy group-policy-name
```

사용자 이름 모드에서 사용할 수 있는 특성의 경우, 사용자 이름 모드로 구성하여 특정 사용자에 대한 그룹 정책의 특성 값을 재정의할 수 있습니다.

다음 예는 이름이 FirstGroup인 그룹 정책의 특성을 사용하도록 이름이 anyuser인 사용자를 구성하는 방법을 보여줍니다.

```
hostname(config)# username anyuser attributes
hostname(config-username)# vpn-group-policy FirstGroup
hostname(config-username)#
```

액세스 시간 구성

다음과 같이 구성된 시간 범위 정책의 이름을 지정하여 이 사용자가 시스템에 액세스하는 데 허용된 시간을 연계하십시오.

실행 중인 구성에서 특성을 제거하려면 **no** 형식의 이 명령을 입력합니다. 이 옵션을 사용하면 다른 그룹 정책에서 시간 범위 값을 상속받을 수 있습니다. 값 상속을 방지하려면 **vpn-access-hours none** 명령을 입력합니다. 기본값은 무제한 액세스입니다.

```
hostname(config-username)# vpn-access-hours value {time-range | none}
hostname(config-username)# vpn-access-hours value none
hostname(config)#
```

다음 예는 이름이 anyuser인 사용자를 824라는 시간 범위 정책과 연계하는 방법을 보여줍니다.

```
hostname(config)# username anyuser attributes
hostname(config-username)# vpn-access-hours 824
hostname(config-username)#
```

최대 동시 로그인 구성

이 사용자에게 허용되는 동시 로그인의 최대 수를 지정합니다. 범위는 0부터 2147483647까지입니다. 기본값은 3개의 동시 로그인입니다. 실행 중인 구성에서 특성을 제거하려면 **no** 형식의 이 명령을 입력합니다. 0을 입력하여 로그인을 비활성화하고 사용자 액세스를 방지합니다.

```
hostname(config-username)# vpn-simultaneous-logins integer
hostname(config-username)# no vpn-simultaneous-logins
hostname(config-username)# vpn-session-timeout alert-interval none
```

참고 동시 로그인 수에 대한 최대 한계치는 매우 높지만 여러 개의 동시 로그인을 허용하면 보안이 손상되고 성능에 영향을 미칠 수 있습니다.

다음 예는 이름이 anyuser인 사용자에 대해 최대 4개의 동시 로그인을 허용하는 방법을 보여줍니다.

```
hostname(config)# username anyuser attributes
hostname(config-username)# vpn-simultaneous-logins 4
hostname(config-username)#
```

유휴 시간 제한 구성

프로시저

단계 **1** (선택 사항) VPN 유휴 시간 제한 기간을 구성하려면 그룹 정책 구성 모드 또는 사용자 이름 구성 모드에서 **vpn-idle-timeout** *minutes* 명령을 사용합니다.

이 기간 동안 연결을 통한 통신 활동이 없는 경우 ASA는 연결을 종료합니다. 최소 시간은 1분, 최대 시간은 35791394분, 기본값은 30분입니다.

다음 예는 이름이 FirstGroup인 그룹 정책에 대해 15분의 VPN 유휴 시간 제한을 설정하는 방법을 보여줍니다.

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# vpn-idle-timeout 15
hostname(config-group-policy)#
```

[**no**] **vpn-idle-timeout** {*minutes* | **none**} 명령을 사용하는 다른 작업:

- **vpn-idle-timeout none**을 입력하여 VPN 유휴 시간 제한을 비활성화하고 시간 제한 값이 상속되지 않도록 합니다.

  ```
  hostname(config)# group-policy FirstGroup attributes
  hostname(config-group-policy)# vpn-idle-timeout none
  hostname(config-group-policy)#
  ```

  그러면 전역 webvpn **default-idle-timeout** 초 값을 사용하는 AnyConnect(SSL 및 IPsec/IKEv2) 및 클라이언트리스 VPN이 됩니다. 이 명령은 webvpn-config 모드에 입력됩니다(예: `hostnamee(config-webvpn)# default-idle-timeout 300`). 기본값은 1800초(30분), 범위는 60-86400초입니다.

  모든 webvon 연결에서 **vpn-idle-timeout none**이 그룹 정책/사용자 이름 속성에 설정된 경우에만 **default-idle-timeout** 값이 적용됩니다. 0이 아닌 유휴 시간 제한 값은 모든 AnyConnect 연결을 위한 ASA에 필요합니다.

  사이트 대 사이트(IKEv1, IKEv2) 및 IKEv1 원격 액세스 VPN: 시간 제한을 비활성화하고 무제한 유휴 기간을 허용하는 것이 좋습니다.

- 이 그룹 정책 또는 사용자 정책에 대한 유휴 시간 제한을 비활성화하려면 **no vpn-idle-timeout**을 입력합니다. 값이 상속됩니다.

- **vpn-idle-timeout**을 전혀 설정하지 않은 경우, 값이 상속되며 기본값은 30분입니다.

단계 **2** (선택 사항) 필요에 따라 **vpn-idle-timeout alert-interval** {*minutes*} 명령을 사용하여 사용자에게 유휴 시간 제한 알림 메시지가 표시되는 시간을 구성할 수 있습니다.

이러한 알림 메시지는 VPN 세션이 비활성화로 인해 연결이 끊어질 때까지 몇 분이 남았는지 사용자에게 알려줍니다. 기본 알림 간격은 1분입니다.

다음 예는 이름이 anyuser인 사용자에 대해 VPN 유휴 시간 제한 및 3분의 알림 간격을 설정하는 방법을 보여줍니다.

```
hostname(config)# username anyuser attributes
hostname(config-username)# vpn-idle-timeout alert-interval 3
hostname(config-username)#
```

[**no**] **vpn-idle-timeout alert-interval** {*minutes* | **none**} 명령을 사용하는 다른 작업:

- **none** 매개변수는 사용자가 알림을 수신하지 않음을 나타냅니다.

  ```
  hostname(config)# username anyuser attributes
  hostname(config-username)# vpn-idle-timeout none
  hostname(config-username)#
  ```

- 이 그룹 또는 사용자 정책에 대한 알림 간격을 제거하려면 **no vpn-idle-timeout alert-interval**을 입력합니다. 값이 상속됩니다.

- 이 매개변수를 설정하지 않을 경우 기본 알림 간격은 1분입니다.

최대 연결 시간 구성

프로시저

단계 **1** (선택 사항) 그룹 정책 구성 모드 또는 사용자 이름 구성 모드에서 **vpn-session-timeout** *minutes* 명령을 사용하여 VPN 연결의 최대 시간을 구성합니다.

최소 시간은 1분이고 최대 시간은 35791394분입니다. 기본값은 없습니다. 구성된 기간의 마지막에서 ASA는 연결을 종료합니다.

다음 예는 이름이 FirstGroup인 그룹 정책에 대해 180분의 VPN 세션 시간 제한을 설정하는 방법을 보여줍니다.

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# vpn-session-timeout 180
hostname(config-group-policy)#
```

다음 예는 이름이 anyuser인 사용자에 대해 180분의 VPN 세션 시간 제한을 설정하는 방법을 보여줍니다.

```
hostname(config)# username anyuser attributes
hostname(config-username)# vpn-session-timeout 180
hostname(config-username)#
```

[**no**] **vpn-session-timeout** {*minutes* | **none**} 명령을 사용하는 다른 작업:

- 이 정책에서 속성을 제거하고 상속을 허용하려면 이 명령의 **no vpn-session-timeout** 형식을 입력합니다.
- 무제한 시간 제한 기간을 허용하여 시간 제한 값의 상속을 방지하려면 **vpn-session-timeout none**을 입력합니다.

단계 **2** 필요에 따라**vpn-session-timeout alert-interval** {*minutes* | } 명령을 사용하여 사용자에게 유휴 시간 제한 알림 메시지가 표시되는 시간을 구성할 수 있습니다.

이러한 알림 메시지는 VPN 세션이 자동으로 연결이 끊어질 때까지 몇 분이 남았는지 사용자에게 알려줍니다. 다음 예는 VPN 세션의 연결이 끊어지기 20분 전에 사용자에게 알려주도록 지정하는 방법을 보여줍니다. 1분-30분의 범위를 지정할 수 있습니다.

```
hostname(config-webvpn)# vpn-session-timeout alert-interval 20
```

[**no**] **vpn-session-timeout alert-interval** {*minutes* | **none**} 명령을 사용하는 다른 작업:

- 다음과 같이 no 형식의 명령을 사용하여 VPN 세션 시간 제한 알림 간격 특성을 기본 그룹 정책에서 상속받음을 나타냅니다.

```
hostname(config-webvpn)# no vpn-session-timeout alert-interval
```

- **vpn-session-timeout alert-interval none**은 사용자가 알림을 수신하지 않음을 나타냅니다.

ACL 필터 적용

VPN 연결에 필터로 사용하기 위해 이전에 구성한 사용자별 ACL의 이름을 지정합니다. ACL을 허용하지 않고 그룹 정책에서의 ACL 상속을 방지하려면 none 키워드와 함께 **vpn-filter** 명령을 입력합니다. **vpn-filter none** 명령을 발행하여 생성한 null 값을 포함하는 ACL을 제거하려면 이 명령의 **no** 형식을 입력합니다. **no** 옵션을 사용하면 그룹 정책에서 값을 상속받을 수 있습니다. 이 명령에 대한 기본 동작이나 값이 없습니다.

이 사용자에 대한 다양한 유형의 트래픽을 허용하거나 거부하도록 ACL을 구성합니다. 그런 다음 **vpn-filter** 명령을 사용하여 이러한 ACL을 적용합니다.

```
hostname(config-username)# vpn-filter {value ACL_name | none}
hostname(config-username)# no vpn-filter
hostname(config-username)#
```

참고 클라이언트리스 SSL VPN은 **vpn-filter** 명령에 정의된 ACL을 사용하지 않습니다.

다음 예는 이름이 anyuser인 사용자 대해 acl_vpn이라는 ACL을 호출하는 필터를 설정하는 방법을 보여줍니다.

```
hostname(config)# username anyuser attributes
hostname(config-username)# vpn-filter value acl_vpn
hostname(config-username)#
```

IPv4 주소 및 넷마스크 지정

특정 사용자에게 할당하도록 IP 주소와 넷마스크를 지정합니다. IP 주소를 제거하려면 이 명령의 **no** 형식을 입력합니다.

```
hostname(config-username)# vpn-framed-ip-address {ip_address}
hostname(config-username)# no vpn-framed-ip-address
hostname(config-username)
```

다음 예에서는 anyuser라는 사용자에 대한 IP 주소를 10.92.166.7로 설정하는 방법을 보여줍니다.

```
hostname(config)# username anyuser attributes
hostname(config-username)# vpn-framed-ip-address 10.92.166.7
hostname(config-username)
```

이전 단계에서 지정된 IP 주소와 함께 사용할 네트워크 마스크를 지정합니다. **no vpn-framed-ip-address** 명령을 사용한 경우, 네트워크 마스크를 지정하지 마십시오. 서브넷 마스크를 제거하려면 이 명령의 **no** 형식을 입력합니다. 기본 동작 또는 값이 없습니다.

```
hostname(config-username)# vpn-framed-ip-netmask {netmask}
hostname(config-username)# no vpn-framed-ip-netmask
hostname(config-username)
```

다음 예는 이름이 anyuser인 사용자에 대해 255.255.255. 254의 서브넷 마스크를 설정하는 방법을 보여줍니다.

```
hostname(config)# username anyuser attributes
hostname(config-username)# vpn-framed-ip-netmask 255.255.255.254
hostname(config-username)
```

IPv6 주소 및 넷마스크 지정

특정 사용자에게 할당하도록 IPv6 주소와 넷마스크를 지정합니다. IP 주소를 제거하려면 **no** 형식의 이 명령을 입력합니다.

```
hostname(config-username)# vpn-framed-ipv6-address {ip_address}
hostname(config-username)# no vpn-framed-ipv6-address
hostname(config-username)
```

다음 예는 이름이 anyuser인 사용자에 대해 2001::3000:1000:2000:1/64의 IP 주소 및 넷마스크를 설정하는 방법을 보여줍니다. 이 주소는 2001:0000:0000:0000의 앞에 붙은 값과 3000:1000:2000:1의 인터페이스 ID를 나타냅니다.

```
hostname(config)# username anyuser attributes
hostname(config-username)# vpn-framed-ipv6-address 2001::3000:1000:2000:1/64
hostname(config-username)
```

터널 프로토콜 지정

이 사용자가 사용할 수 있는 VPN 터널 유형(IPsec 또는 클라이언트리스 SSL VPN)을 지정합니다. 기본값은 기본 그룹 정책에서 가져오며 IPsec입니다. 실행 중인 구성에서 속성을 제거하려면 **no** 형식의 이 명령을 입력합니다.

```
hostname(config-username)# vpn-tunnel-protocol {webvpn | IPsec}
hostname(config-username)# no vpn-tunnel-protocol [webvpn | IPsec]
hostname(config-username)
```

이 명령에 대한 매개변수 값은 다음과 같습니다.

- **IPsec**—2개의 피어(원격 액세스 클라이언트 또는 다른 보안 게이트웨이) 사이에서 IPsec 터널을 협상합니다. 인증, 암호화, 캡슐화 및 키 관리를 제어하는 보안 연계를 생성합니다.
- **webvpn**—HTTPS 활성화 웹 브라우저를 통해 원격 사용자에게 클라이언트리스 SSL VPN 액세스를 제공하며 클라이언트가 필요하지 않습니다.

하나 이상의 터널링 모드를 구성하려면 다음 명령을 입력합니다. 사용자가 VPN 터널을 통해 연결하려면 하나 이상의 터널링 모드를 구성해야 합니다.

다음 예는 이름이 anyuser인 사용자에 대해 클라이언트리스 SSL VPN 및 IPsec 터널링 모드를 구성하는 방법을 보여줍니다.

```
hostname(config)# username anyuser attributes
hostname(config-username)# vpn-tunnel-protocol webvpn
hostname(config-username)# vpn-tunnel-protocol IPsec
hostname(config-username)
```

원격 사용자 액세스 제한

원격 사용자를 지정된 기존의 연결 프로파일을 통해서만 액세스하도록 제한하려면 **value** 키워드와 함께 **group-lock** 속성을 구성합니다. 그룹 잠금은 VPN 클라이언트에 구성된 그룹이 사용자가 할당된 연결 프로파일과 동일한지를 확인하여 사용자를 제한합니다. 동일하지 않으면 ASA에서 사용자의 연결을 차단합니다. 그룹 잠금을 구성하지 않은 경우 ASA는 할당된 그룹에 상관없이 사용자를 인증합니다.

실행 중인 구성에서 **group-lock** 속성을 제거하려면 **no** 형식의 이 명령을 입력합니다. 이 옵션을 사용하면 그룹 정책에서 값을 상속받을 수 있습니다. 그룹 잠금을 비활성화하고 기본 또는 지정된 그룹 정책에서 그룹 잠금 값을 상속받지 않도록 하려면 **none** 키워드와 함께 **group-lock** 명령을 입력합니다.

```
hostname(config-username)# group-lock {value tunnel-grp-name | none}
hostname(config-username)# no group-lock
hostname(config-username)
```

다음 예는 이름이 anyuser인 사용자에 대해 그룹 잠금을 설정하는 방법을 보여줍니다.

```
hostname(config)# username anyuser attributes
hostname(config-username)# group-lock value tunnel-group-name
hostname(config-username)
```

소프트웨어 클라이언트 사용자에 대한 비밀번호 저장 활성화

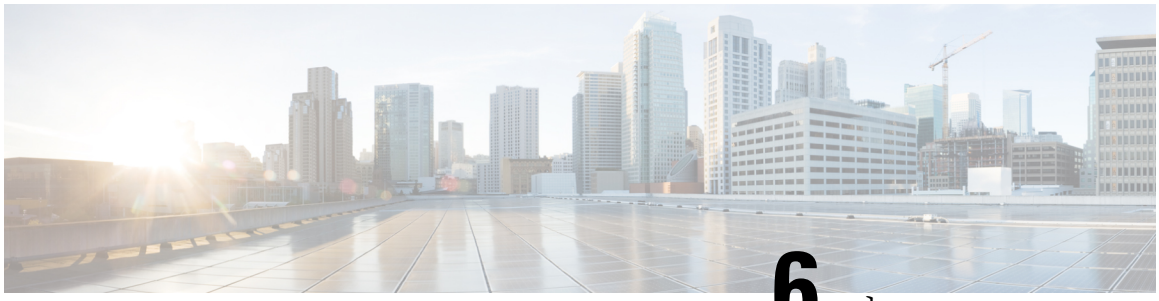
클라이언트 시스템에서 사용자가 자신의 로그인 비밀번호를 저장할지 여부를 지정합니다. 비밀번호 저장은 기본적으로 비활성화되어 있습니다. 안전한 사이트라고 간주되는 시스템에만 비밀번호 저장을 활성화합니다. 비밀번호 저장을 비활성화하려면 **disable** 키워드와 함께 **password-storage** 명령을 입력합니다. 실행 중인 구성에서 password-storage 속성을 제거하려면 이 명령의 **no** 형식을 입력합니다. 이렇게 하면 그룹 정책에서 password-storage에 대한 값을 상속받을 수 있습니다.

```
hostname(config-username)# password-storage {enable | disable}
hostname(config-username)# no password-storage
hostname(config-username)
```

이 명령은 하드웨어 클라이언트를 위한 인터랙티브 하드웨어 클라이언트 인증 또는 개별 사용자 인증과 관련이 없습니다.

다음 예는 이름이 anyuser인 사용자에 대해 비밀번호 저장을 활성화하는 방법을 보여줍니다.

```
hostname(config)# username anyuser attributes
hostname(config-username)# password-storage enable
hostname(config-username)
```



6 장

VPN용 IP 주소

IP 주소 할당 정책 구성

ASA에서는 다음 방법 중 하나 이상을 사용하여 IP 주소를 원격 액세스 클라이언트에 할당할 수 있습니다. 둘 이상의 주소 할당 방법을 구성한 경우에는 ASA에서 IP 주소를 찾을 때까지 각 옵션을 검색합니다. 기본적으로 모든 방법이 활성화되어 있습니다.

- aaa외부 인증, 권한 부여 및 계정 관리 서버에서 사용자 단위로 주소를 검색합니다. IP 주소가 구성된 인증 서버를 사용하는 경우 이 방법을 사용하는 것이 좋습니다. IPv4 및 IPv6 할당 정책에 이 방법을 사용할 수 있습니다.
- dhcpDHCP 서버에서 IP 주소를 가져옵니다. DHCP를 사용하려면 DHCP 서버를 구성해야 합니다. DHCP 서버에서 사용할 수 있는 IP 주소 범위도 정의해야 합니다. IPv4 할당 정책에 이 방법을 사용할 수 있습니다.
- **local** 내부적으로 구성된 주소 풀은 주소 풀 할당을 구성하는 가장 간편한 방법입니다. local을 선택하는 경우 **ip-local-pool** 명령을 사용하여 사용할 IP 주소 범위도 정의해야 합니다. IPv4 및 IPv6 할당 정책에 이 방법을 사용할 수 있습니다.
  - Allow the reuse of an IP address so many minutes after it is released(해제되고 몇 분이 경과한 후 IP 주소 재사용 허용) — IP 주소가 주소 풀로 반환된 이후에 해당 IP 주소의 재사용을 지연시킵니다. 지연을 추가하면 IP 주소가 신속하게 재할당될 경우 방화벽에서 발생할 수 있는 문제를 방지하는 데 도움이 됩니다. 기본적으로 ASA에서는 지연을 적용하지 않습니다. 이 구성 요소는 IPv4 할당 정책에 사용할 수 있습니다.

다음 방법 중 하나를 사용하여 원격 액세스 클라이언트에 IP 주소를 할당할 방법을 지정할 수 있습니다.

IPv4 주소 할당 구성

프로시저

VPN 연결에 IPv4 주소를 할당할 때 ASA에서 사용할 주소 할당 방법을 활성화합니다. AAA 서버, DHCP 서버 또는 로컬 주소 풀에서 IP 주소를 가져올 수 있습니다. 기본적으로 모든 방법이 활성화되어 있습니다.

vpn-addr-assign {**aaa** | **dhcp** | **local** [**reuse-delay** *minutes*]}

예제:

예를 들어, IP 주소가 해제된 후 0분에서 480분 동안 해당 IP 주소의 재사용을 구성할 수 있습니다.

```
hostname(config)#vpn-addr-assign aaa
hostname(config)#vpn-addr-assign local reuse-delay 180
```

이 예에서는 주소 할당 방법을 비활성화하기 위해 no 형식의 명령을 사용합니다.

```
hostname(config)# no vpn-addr-assign dhcp
```

IPv6 주소 할당 구성

프로시저

VPN 연결에 IPv6 주소를 할당할 때 ASA에서 사용할 주소 할당 방법을 활성화합니다. AAA 서버 또는 로컬 주소 풀에서 IP 주소를 가져올 수 있습니다. 기본적으로 두 가지 방법 모두 활성화되어 있습니다.

ipv6-vpn-addr-assign {**aaa** | local}

예제:

```
hostname(config)# ipv6-vpn-addr-assign aaa
```

이 예에서는 주소 할당 방법을 비활성화하기 위해 no 형식의 명령을 사용합니다.

```
hostname(config)# no ipv6-vpn-addr-assign local
```

주소 할당 방법 보기

프로시저

다음 방법 중 하나를 사용하여 ASA에 구성된 주소 할당 방법을 볼 수 있습니다.

- IPv4 주소 할당 보기

  구성된 주소 할당 방법을 보여줍니다. 구성된 주소 방법은 aaa, dhcp 또는 local일 수 있습니다.

  ```
  show running-config all vpn-addr-assign
  vpn-addr-assign aaa
  vpn-addr-assign dhcp
  vpn-addr-assign local
  ```

- IPv6 주소 할당 보기

  구성된 주소 할당 방법을 보여줍니다. 구성된 주소 방법은 aaa 또는 local일 수 있습니다.

  ```
  show running-config all ipv6-vpn-addr-assign
  ipv6-vpn-addr-assign aaa
  ipv6-vpn-addr-assign local reuse-delay 0
  ```

로컬 **IP** 주소 풀 구성

VPN 원격 액세스 터널에 사용할 IPv4 주소 풀을 구성하려면 전역 구성 모드에서 **ip local pool** 명령을 입력합니다. 주소 풀을 삭제하려면 **no** 형식의 이 명령을 입력합니다.

VPN 원격 액세스 터널에 사용할 IPv6 주소 풀을 구성하려면 전역 구성 모드에서 **ipv6 local pool** 명령을 입력합니다. 주소 풀을 삭제하려면 **no** 형식의 이 명령을 입력합니다.

ASA에서는 연결 프로파일 또는 그룹 정책을 기반으로 주소 풀을 사용하여 연결합니다. 풀을 지정하는 순서는 중요합니다. 연결 프로파일 또는 그룹 정책에 대해 둘 이상의 주소 풀을 구성한 경우 ASA에서는 ASA에 추가된 순서대로 주소 풀을 사용합니다.

로컬이 아닌 서브넷에서 주소를 할당할 경우 이러한 네트워크에 대한 경로를 보다 쉽게 추가할 수 있도록 서브넷 경계에 속하는 풀을 추가하는 것이 좋습니다.

로컬 **IPv4** 주소 풀 구성

프로시저

단계 **1** IP 주소 풀을 주소 할당 방법으로 구성합니다. **local** 인수와 함께 **vpn-addr-assign** 명령을 입력합니다.

예제:

```
hostname(config)# vpn-addr-assign local
```

단계 **2** 주소 풀을 구성합니다. 이 명령은 풀 이름과 IPv4 주소 및 서브넷 마스크 범위를 지정합니다.

ip local pool*poolname first_address-last_address***mask***mask*

예제**:**

이 예에서는 *firstpool*이라는 이름의 IP 주소 풀을 구성합니다. 시작 주소는 10.20.30.40이고 끝 주소는 10.20.30.50입니다. 네트워크 마스크는 255.255.255.0입니다.

```
hostname(config)# ip local pool firstpool 10.20.30.40-10.20.30.50 mask 255.255.255.0
```

이 예에서는 **firstpool**이라는 이름의 IP 주소 풀을 삭제합니다.

```
hostname(config)# no ip local pool firstpool
```

로컬 IPv6 주소 풀 구성

프로시저

단계 **1** IP 주소 풀을 주소 할당 방법으로 구성하고 **local** 인수와 함께 ipv6-**vpn-addr-assign** 명령을 입력합니다.

예제**:**

```
hostname(config)# ipv6-vpn-addr-assign local
```

단계 **2** 주소 풀을 구성합니다. 이 명령은 풀 이름을 지정하고, 시작 IPv6 주소, 접두사 길이(비트) 및 범위에서 사용할 주소 수를 식별합니다.

ipv6 local pool *pool_name starting_address prefix_length number_of_addresses*

예제**:**

이 예에서는 *ipv6pool*이라는 IP 주소 풀을 구성합니다. 시작 주소는 2001:DB8::1이고, 접두사 길이는 32비트이며, 풀에서 사용할 주소 수는 100개입니다.

```
hostname(config)# ipv6 local pool ipv6pool 2001:DB8::1/32 100
```

이 예에서는 *ipv6pool*이라는 이름의 IP 주소 풀을 삭제합니다.

```
hostname(config)# no ipv6 local pool ipv6pool
```

AAA 주소 지정 구성

AAA 서버를 사용하여 VPN 원격 액세스 클라이언트에 대한 주소를 할당하려면 먼저 AAA 서버 또는 서버 그룹을 구성해야 합니다. 명령 참조에서 **aaa-server protocol** 명령을 참조해 주십시오.

또한 사용자는 RADIUS 인증에 대해 구성된 연결 프로파일과 일치해야 합니다.

다음 예에서는 이름이 firstgroup인 터널 그룹에 대해 RAD2라는 AAA 서버 그룹을 정의하는 방법을 보여줍니다. 여기에는 이전에 터널 그룹의 이름을 지정하고 터널 그룹 유형을 정의한 경우에는 필요 없는 단계가 하나 더 포함되어 있습니다. 이 단계는 이러한 값을 설정할 때까지 후속 tunnel-group 명령에 액세스할 수 없음을 알려 주기 위해 다음 예에 나와 있습니다.

이러한 예에서 생성한 구성에 대한 개요는 다음과 같습니다.

```
hostname(config)# vpn-addr-assign aaa
hostname(config)# tunnel-group firstgroup type ipsec-ra
hostname(config)# tunnel-group firstgroup general-attributes
hostname(config)# authentication-server-group RAD2
```

IP 주소 지정에 대해 AAA를 구성하려면 다음 단계를 수행하십시오.

프로시저

단계 **1** AAA를 주소 할당 방법으로 구성하려면 **aaa** 인수와 함께 **vpn-addr-assign** 명령을 입력합니다.

```
hostname(config)# vpn-addr-assign aaa
hostname(config)#
```

단계 **2** firstgroup이라는 터널 그룹을 원격 액세스 또는 LAN-to-LAN 터널 그룹으로 설정하려면 **type** 키워드와 함께 **tunnel-group** 명령을 입력합니다. 다음 예에서는 원격 액세스 터널 그룹을 구성합니다.

```
hostname(config)# tunnel-group firstgroup type ipsec-ra
hostname(config)#
```

단계 **3** firstgroup이라는 터널 그룹에 대한 AAA 서버 그룹을 정의할 수 있는 general-attributes 구성 모드를 시작하려면 **general-attributes** 인수와 함께 **tunnel-group** 명령을 입력합니다.

```
hostname(config)# tunnel-group firstgroup general-attributes
hostname(config-general)#
```

단계 **4** 인증에 사용할 AAA 서버 그룹을 지정하려면 **authentication-server-group** 명령을 입력합니다.

```
hostname(config-general)# authentication-server-group RAD2
hostname(config-general)#
```

다음에 수행할 작업

이 명령에는 위의 예에 포함된 것보다 더 많은 인수가 있습니다. 자세한 내용은 명령행 참조를 참조해 주십시오.

DHCP 주소 지정 구성

DHCP를 사용하여 VPN 클라이언트에 대한 주소를 할당하려면 먼저 DHCP 서버와 이 서버에서 사용할 수 있는 IP 주소 범위를 구성해야 합니다. 그런 다음 연결 프로파일을 기반으로 DHCP 서버를 정의합니다. 선택적으로 연결 프로파일 또는 사용자 이름과 연결된 그룹 정책에서 DHCP 네트워크 범위를 정의할 수도 있습니다. 이 네트워크 범위는 DHCP 서버에 사용할 IP 주소 풀을 식별하는 IP 네트워크 번호 또는 IP 주소입니다.

다음 예에서는 IP 주소 172.33.44.19에서 이름이 **firstgroup**인 연결 프로파일에 대한 DHCP 서버를 정의합니다. 또한 **remotegroup**이라는 그룹 정책에 대한 DHCP 네트워크 범위 192.86.0.0을 정의합니다. (remotegroup이라는 그룹 정책은 firstgroup이라는 연결 프로파일과 연결됩니다.) 네트워크 범위를 정의하지 않으면 DHCP 서버에서 구성된 주소 풀 순으로 IP 주소를 할당합니다. 할당되지 않은 주소를 식별할 때까지 풀을 검색합니다.

다음 구성에는 이전에 연결 프로파일 유형의 이름을 지정하고 이를 원격 액세스로 정의했으며, 그룹 정책의 이름을 지정하고 이를 내부 또는 외부로 식별한 경우에는 필요 없는 단계가 추가로 포함되어 있습니다. 이 단계는 이러한 값을 설정할 때까지 후속 tunnel-group 및 group-policy 명령에 액세스할 수 없음을 알려 주기 위해 다음 예에 나와 있습니다.

지침 및 제한 사항

클라이언트 주소를 할당할 DHCP 서버를 식별하기 위해 IPv4 주소만 사용할 수 있습니다.

DHCP 주소 지정 구성

프로시저

단계 **1** IP 주소 풀을 주소 할당 방법으로 구성합니다.

vpn-addr-assign dhcp

단계 **2** *firstgroup*이라는 연결 프로파일을 원격 액세스 연결 프로파일로 설정합니다.

tunnel-group *firstgroup* **type remote-access**

단계 **3** DHCP 서버를 구성할 수 있도록 연결 프로파일에 대한 general-attributes 구성 모드를 시작합니다.

tunnel-group *firstgroup* **general-attributes**

단계 **4** IPv4 주소로 DHCP 서버를 정의합니다. IPv6 주소로는 DHCP 서버를 정의할 수 없습니다. 하나의 연결 프로파일에 대해 DHCP 서버 주소를 두 개 이상 지정할 수 있습니다. dhcp-server 명령을 입력합니

다. 이 명령을 사용하면 ASA에서 VPN 클라이언트에 대한 IP 주소를 가져오려고 할 때 지정된 DHCP 서버로 추가 옵션을 보내도록 구성할 수 있습니다.

dhcp-server *IPv4_address_of_DHCP_server*

예제:

위의 예에서는 IP 주소 172.33.44.19에서 DHCP 서버를 구성합니다.

```
hostname(config-general)# dhcp-server 172.33.44.19
hostname(config-general)#
```

단계 **5** tunnel-group 모드를 종료합니다.

```
 hostname(config-general)# exit
hostname(config)#
```

단계 **6** *remotegroup*이라는 내부 그룹 정책을 생성합니다.

```
hostname(config)# group-policy remotegroup internal
```

예제:

위의 예에서는 remotegroup 그룹 정책에 대한 그룹 정책 특성 구성 모드를 시작합니다.

```
 hostname(config)# group-policy remotegroup attributes
hostname(config-group-policy)#
```

단계 **7** (선택 사항) DHCP 서버에서 사용할 IP 주소의 서브네트워크를 구성할 수 있는 그룹 정책 속성 구성 모드를 시작합니다. **attributes** 키워드와 함께 **group-policy** 명령을 입력합니다.

예제:

```
hostname(config)# group-policy remotegroup attributes
```

단계 **8** (선택 사항) DHCP 서버에서 *remotegroup*이라는 그룹 정책의 사용자에게 주소를 할당하는 데 사용해야 하는 IP 주소 범위를 지정하려면 **dhcp-network-scope** 명령을 입력합니다.

위의 예에서는 네트워크 범위 192.86.0.0을 구성합니다.

```
 hostname(config-group-policy)# dhcp-network-scope 192.86.0.0
hostname(config-group-policy)#
```

참고 dhcp-network-scope는 라우팅 가능한 IP 주소여야 하며, DHCP 풀의 서브넷이 아니어야 합니다. DHCP 서버는 이 IP 주소가 속한 서브넷을 확인하고 해당 풀에서 IP 주소를 할당합니다. 어떤 IP 주소든 dhcp-network-scope로 사용할 수 있지만 네트워크에 정적 경로를 추가해야 할 수 있습니다.

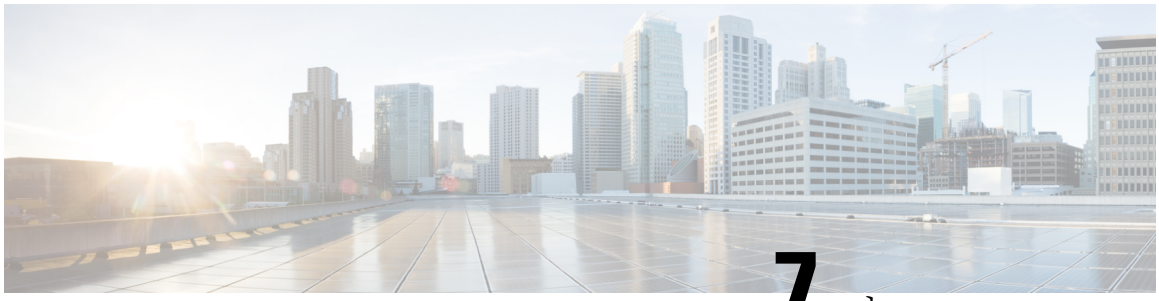
예

이러한 예에서 생성한 구성에 대한 요약은 다음과 같습니다.

```
hostname(config)# vpn-addr-assign dhcp
hostname(config)# tunnel-group firstgroup type remote-access
hostname(config)# tunnel-group firstgroup general-attributes
hostname(config-general)# dhcp-server 172.33.44.19
hostname(config-general)# exit
hostname(config)# group-policy remotegroup internal
hostname(config)# group-policy remotegroup attributes
hostname(config-group-policy)# dhcp-network-scope 192.86.0.0
```

다음에 수행할 작업

dhcp-server 명령은 Cisco Security Appliance 명령 참조 가이드에서 참조해 주십시오.



7 장

원격 액세스 IPsec VPN

원격 액세스 IPsec VPN 정보

원격 액세스 VPN을 통해 사용자는 TCP/IP 네트워크를 통해 안전하게 중앙 사이트에 연결할 수 있습니다. IKE라고도 하는 인터넷 보안 연계 및 키 관리 프로토콜은 원격 PC 및 ASA의 IPsec 클라이언트가 IPsec 보안 연계를 구축하는 방법에 동의할 수 있도록 해주는 협상 프로토콜입니다. 각 ISAKMP 협상은 1단계와 2단계라는 두 개의 섹션으로 나누어집니다.

1단계에서는 최신 ISAKMP 협상 메시지를 보호하는 첫 번째 터널을 생성합니다. 2단계에서는 보안 연결을 통해 이동하는 데이터를 보호하는 터널을 생성합니다.

ISAKMP 협상 조건을 설정하려면 ISAKMP 정책을 생성합니다. 여기에는 다음과 같은 항목이 포함됩니다.

- 피어의 ID를 확인할 인증 방법
- 데이터 및 개인정보를 보호할 암호화 방법
- 보낸 사람의 ID를 확인하고 메시지가 전송 중에 수정되지 않았는지 확인할 HMAC(Hashed Message Authentication Codes: 해시된 메시지 인증 코드) 방법
- 암호 키 크기를 설정할 Diffie-Hellman 그룹
- ASA에서 암호 키를 교체하지 않고 계속 사용할 수 있는 기간에 대한 시간 제한

변형 집합은 암호화 방법과 인증 방법을 통합합니다. ISAKMP와의 IPsec 보안 연계 협상 동안 피어는 특정 데이터 흐름을 보호하기 위해 특정 변형 집합을 사용하는 데 동의합니다. 변형 집합은 양쪽 피어에 대해 모두 동일해야 합니다.

변형 집합은 연계된 암호화 맵 항목에 지정된 ACL에 대한 데이터 흐름을 보호합니다. ASA 구성에서 변형 집합을 생성한 다음 암호화 맵 또는 동적 암호화 맵 항목에서 최대 11개의 집합을 지정할 수 있습니다. 유효한 암호화 및 인증 방법을 나열하는 표가 포함된 자세한 개요 정보에 대해서는 IKEv1 변형 집합 또는 IKEv2 제안서 생성, 213 페이지의 내용을 참조하십시오.

ASA에서 내부 주소 풀을 생성하거나 ASA에 있는 로컬 사용자에게 전용 주소를 할당하여 IPv4 주소, IPv6 주소 또는 두 주소 모두를 AnyConnect 클라이언트에 할당하도록 ASA를 구성할 수 있습니다.

엔드포인트에는 주소의 두 가지 유형에 할당되는 운영 체제에서 구현되는 이중 스택 프로토콜이 있어야 합니다. 두 가지 시나리오에서 IPv6 주소 풀이 남아 있지 않지만 IPv4 주소를 사용할 수 있거나 IPv4 주소 풀이 남아 있지 않지만 IPv6 주소를 사용할 수 있는 경우, 연결이 유지됩니다. 단, 클라이언트가 알림을 받지 않으면 관리자는 ASA 로그에서 세부사항을 검토해야 합니다.

클라이언트에 대한 IPv6 주소 할당은 SSL 프로토콜에 지원됩니다. 하지만 IKEv2/IPsec 프로토콜에 대해서는 지원되지 않습니다.

Mobike 및 원격 액세스 VPN 정보

모바일 IKEv2(mobike)에서 ASA RA VPN을 확장하여 모바일 디바이스 로밍을 지원합니다. 이 지원은 디바이스가 현재 연결 지점에서 다른 위치로 이동할 때 모바일 디바이스의 IKE/IPSEC SA(Security Association)에 대한 엔드포인트 IP 주소가 삭제되지 않고 업데이트될 수 있음을 의미합니다.

Mobike는 버전 9.8(1)부터 ASA에서 기본적으로 사용 가능합니다. 이는 Mobike가 "항상 켜져 있음"을 의미합니다. 클라이언트에서 제안하고 ASA에서 수락하는 경우에만 각 SA에 대해 Mobike가 활성화됩니다. 이 협상은 IKE_AUTH exchange의 한 부분으로 발생합니다.

Mobike 지원이 활성화된 상태에서 SA를 설정하면 클라이언트에서 언제든지 해당 주소를 변경하고 새 주소를 나타내는 UPDATE_SA_ADDRESS 페이로드를 통한 정보 교환을 사용하여 ASA에 알릴 수 있습니다. ASA에서 이 메시지를 처리하고 새 클라이언트 IP 주소로 SA를 업데이트합니다.

참고 모든 현재 SA에 대해 Mobike가 활성화되어 있는지 확인하려면 `show crypto ikev2 sa detail` 명령을 사용할 수 있습니다.

현재 Mobike 구현은 다음을 지원합니다.

- IPv4 주소만
- NAT 매핑의 변경 사항
- 선택 사항인 반환 라우팅 가능성 확인을 통해 경로 연결 및 중단 탐지
- 액티브/스탠바이 장애 조치
- VPN 로드 밸런싱

RRC(반환 라우팅 가능성 확인)을 활성화하면 RRC 메시지가 모바일 클라이언트로 전송되어 SA를 업데이트하기 전에 새 IP 주소를 확인합니다.

3.1용 원격 액세스 IPsec VPN에 대한 라이센싱 요건

참고 No Payload Encryption 모델에서는 이 기능을 사용할 수 없습니다.

IKEv2를 사용하는 IPsec 원격 액세스 VPN에는 각각 사용 가능한 AnyConnect Plus 또는 Apex 라이센스가 필요합니다. AnyConnect 라이센스 구매 시 다음의 최대값을 참조하십시오. IKEv1을 사용하는 IPsec 원격 액세스 VPN과 IKEv1 또는 IKEv2를 사용하는 IPsec site-to-site VPN은 Base 라이센스와 함께 제공되는 기타 VPN 라이센스를 사용합니다. 모든 유형의 결합 VPN 세션의 최대 수는 이 표에 표시된 최대 세션 수를 초과할 수 없습니다.

모델	라이센스 요건
ASA 5506-X, 5506H-X, 5506W-X	• IKEv2를 사용하는 IPsec 원격 액세스 VPN: 세션 50개. • IKEv1을 사용하는 IPsec 원격 액세스 VPN 및 IKEv1 또는 IKEv2를 사용하는 IPsec Site-to-Site VPN: • Base 라이센스: 세션 10개. • Security Plus 라이센스: 세션 50개.
ASA 5508-X	세션 100개.
ASA 5512-X	세션 250개.
ASA 5515-X	세션 250개.
ASA 5516-X	세션 300개.
ASA 5525-X	세션 750개.
ASA 5545-X	세션 2500개.
ASA 5555-X	세션 5000개.
ASA 5585-X(SSP-10 포함)	세션 5000개.
ASA 5585-X(SSP-20, -40 및 -60 포함)	세션 10,000개.
ASASM	세션 10,000개.
ASAv5	세션 250개.

모델	라이센스 요건
ASAv10	세션 250개.
ASAv30	세션 750개.

IPsec VPN의 제한 사항

- 방화벽 모드 지침 - 라우팅된 방화벽 모드에서만 지원됩니다. 투명 모드는 지원되지 않습니다.
- 장애 조치 지침 IPsec-VPN 세션이 활성/대기 장애 조치 구성에서만 복제됩니다. 활성/대기 장애 조치 구성은 지원되지 않습니다.

원격 액세스 IPsec VPN 구성

이 섹션에서는 원격 액세스 VPN을 구성하는 방법에 대해 설명합니다.

인터페이스 구성

ASA에는 최소 두 개의 인터페이스(여기서는 외부 및 내부 인터페이스)가 있습니다. 일반적으로 외부 인터페이스는 공용 인터넷에 연결되며, 내부 인터페이스는 사설 네트워크에 연결되고 공용 액세스로부터 보호됩니다.

시작하려면 ASA에서 두 개의 인터페이스를 구성하고 활성화하십시오. 그런 다음 이름, IP 주소 및 서브넷 마스크를 할당합니다. 선택적으로 보안 어플라이언스에 보안 수준, 속도 및 이중 작업을 구성합니다.

프로시저

단계 **1** 전역 구성 모드에서 인터페이스 구성 모드를 시작합니다.

interface {*interface*}

예제**:**

```
hostname(config)# interface ethernet0
hostname(config-if)#
```

단계 **2** 인터페이스에 대해 IP 주소 및 서브넷 마스크를 설정합니다.

ip address *ip_address* [*mask*] [*standby ip_address*]

예제**:**

```
hostname(config)# interface ethernet0
hostname(config-if)# ip address 10.10.4.200 255.255.0.0
```

단계 3 인터페이스(최대 48자)의 이름을 지정합니다. 이름을 설정한 후에는 이 이름을 변경할 수 없습니다.

nameif *name*

예제:

```
hostname(config-if)# nameif outside
hostname(config-if)#
```

단계 4 인터페이스를 활성화합니다. 기본적으로 인터페이스는 비활성화되어 있습니다.

예제:

```
hostname(config-if)# no shutdown
hostname(config-if)#
```

ISAKMP 정책 구성 및 외부 인터페이스에서 ISAKMP 활성화

프로시저

단계 1 인증 방법 및 매개변수 집합을 IKEv1 협상 동안 사용하도록 지정합니다.

Priority는 IKE(Internet Key Exchange: 인터넷 키 교환국) 정책을 고유하게 식별하고 정책에 우선순위를 할당합니다. 1이 우선순위가 가장 높고 65,534가 우선순위가 가장 낮은 1부터 65,534까지의 정수를 사용합니다.

다음 단계에서는 우선순위를 1로 설정했습니다.

단계 2 IKE 정책 내에서 사용할 암호화 방법을 지정합니다.

crypto ikev1 policy *priority* **encryption** {**aes** | **aes-192** | **aes-256** | **des** | **3des**}

예제:

```
hostname(config)# crypto ikev1 policy 1 encryption 3des
hostname(config)#
```

단계 3 (HMAC 변형이라고도 함) IKE 정책에 대해 해시 알고리즘을 지정합니다.

crypto ikev1 policy *priority* **hash** {**md5** | **sha**}

예제:

```
hostname(config)# crypto ikev1 policy 1 hash sha
hostname(config)#
```

단계 4 IKE 정책에 대해 Diffie-Hellman 그룹 지정 - IPsec 클라이언트와 ASA가 공유 비밀 키를 설정하도록 허용하는 암호화 프로토콜입니다.

crypto ikev1 policy *priority* **group** {**1** | **2** | **5**}

예제:

```
hostname(config)# crypto ikev1 policy 1 group 2
hostname(config)#
```

단계 **5** 암호 키 수명 지정 — 각 보안 연계가 만료될 때까지의 시간(초)입니다.

crypto ikev1 policy *priority* **lifetime** {*seconds*}

유한 수명의 범위는 120-2147483647초입니다. 무한 수명은 0초를 사용합니다.

예제:

```
hostname(config)# crypto ikev1 policy 1 lifetime 43200
hostname(config)#
```

단계 **6** outside라는 이름의 인터페이스에서 ISAKMP를 활성화합니다.

crypto ikev1 enable *interface-name*

예제:

```
hostname(config)# crypto ikev1 enable outside
hostname(config)#
```

단계 **7** 구성에 변경 사항을 저장합니다.

write memory

주소 풀 구성

ASA에는 사용자에게 IP 주소를 할당하기 위한 방법이 필요합니다. 이 섹션에서는 주소 풀을 예로 사용합니다.

프로시저

클라이언트에 주소를 할당하는 ASA에서 IP 주소의 범위가 있는 주소 풀을 생성합니다.

ip local pool *poolname first-address-last-address* [**mask** *mask*]

주소 마스크는 선택 사항입니다. 그러나 기본 마스크를 사용하는 경우 VPN 클라이언트에 할당된 IP 주소가 비표준 네트워크에 속하고 데이터가 잘못 라우팅될 수 있는 경우, 마스크 값을 제공해야 합니다. 전형적인 예는 IP 로컬 풀이 10.10.10.0/255.255.255.0 주소를 포함하는 경우입니다(기본적으로 클래스 A 네트워크이기 때문). 이때 VPN 클라이언트에서 서로 다른 인터페이스에서 10 네트워크의 다른 서브넷에 액세스해야 하는 경우 라우팅 문제가 발생할 수 있습니다.

예제:

```
hostname(config)# ip local pool testpool 192.168.0.10-192.168.0.15
hostname(config)#
```

사용자 추가

프로시저

사용자, 비밀번호 및 권한 수준을 생성합니다.

username *name* {**nopassword** | **password** *password* [**mschap** | **encrypted** | **nt-encrypted**]} [**privilege** *priv_level*]

예제:

```
Hostname(config)# username testuser password 12345678
```

IKEv1 변형 집합 또는 IKEv2 제안서 생성

이 섹션에서는 암호화 방법과 인증 방법을 결합하는 변형 집합(IKEv1) 또는 제안서(IKEv2)를 구성하는 방법에 대해 보여줍니다.

다음 단계는 IKEv1 및 IKEv2 제안서를 모두 생성하는 방법을 보여줍니다.

프로시저

단계 **1** 데이터 무결성을 보장하기 위해 사용되는 IPsec IKEv1 암호화 및 해시 알고리즘을 지정하는 IKEv1 변형 집합을 구성합니다.

crypto ipsec ikev1 transform-set *transform-set-name encryption-method* [*authentication*]

encryption에 대해 다음 값 중 하나를 사용합니다.

- 128비트 키가 있는 AES를 사용하려면 esp-aes
- 192비트 키가 있는 AES를 사용하려면 esp-aes-192
- 256비트 키가 있는 AES를 사용하려면 esp-aes-256
- 56비트 DES-CBC를 사용하려면 esp-des
- Triple DES 알고리즘을 사용하려면 esp-3des
- 암호화를 사용하지 않으려면 esp-null

authentication에 다음 값 중 하나를 사용합니다.

- 해시 알고리즘으로 MD5/HMAC-128을 사용하려면 esp-md5-hmac
- 해시 알고리즘으로 SHA/HMAC-160을 사용하려면 esp-sha-hmac
- HMAC 인증을 사용하지 않으려면 esp-none

예제:

IKEv1 변형 집합 구성:

```
hostname(config)# crypto ipsec transform set FirstSet esp-3des esp-md5-hmac
hostname(config)#
```

단계 **2** IPsec IKEv2 프로토콜, 암호화 및 무결성 알고리즘을 사용하도록 지정하는 IKEv2 제안서 집합을 구성합니다.

esp는 ESP(Encapsulating Security Payload) IPsec 프로토콜(현재 IPsec에 대해 유일하게 지원되는 프로토콜)을 지정합니다.

crypto ipsec ikev2 ipsec-proposal *proposal_name*

protocol {**esp**} {**encryption** {**des** | **3des** | **aes** | **aes-192** | **aes-256** | **null**} | **integrity** {**md5** | **sha-1**}

encryption에 대해 다음 값 중 하나를 사용합니다.

- ESP에 대해 56비트 DES-CBC 암호화를 사용하려면 des
- ESP에 대해 Triple DES 암호화 알고리즘을 사용하려면 3des(기본값)
- ESP에 대해 128비트 키 암호화가 있는 AES를 사용하려면 aes
- ESP에 대해 192비트 키 암호화가 있는 AES를 사용하려면 aes-192
- ESP에 대해 256비트 키 암호화가 있는 AES를 사용하려면 aes-256
- ESP에 대해 암호화를 사용하지 않으려면 null

integrity에 대해 다음 값 중 하나를 사용합니다.

- md5는 ESP 무결성 보호를 위해 md5 알고리즘을 지정합니다.
- sha-1(기본값)은 ESP 무결성 보호를 위해 미국 FIPS(Federal Information Processing Standard: 연방 정부 정보 처리 표준)에 정의된 SHA(Secure Hash Algorithm)인 SHA-1을 지정합니다.

IKEv2 제안서 구성:

```
hostname(config)# crypto ipsec ikev2 ipsec-proposal secure_proposal
hostname(config-ipsec-proposal)# protocol esp encryption des integrity md5
```

터널 그룹 정의

터널 그룹은 터널 연결 정책의 모음입니다. 터널 그룹이 AAA 서버를 식별하도록 구성하고 연결 매개변수를 지정하며 기본 그룹 정책을 정의합니다. ASA는 터널 그룹을 내부에서 저장합니다.

ASA 시스템에는 기본 원격 액세스 터널 그룹인 DefaultRAGroup과 기본 LAN-to-LAN 터널 그룹인 DefaultL2Lgroup의 두 가지 기본 터널 그룹이 있습니다. 이 그룹을 변경할 수는 있지만 삭제할 수는 없습니다. ASA는 이 그룹을 사용하여 터널 협상 동안 식별한 특정 터널 그룹이 없는 경우 원격 액세스 및 LAN-to-LAN 터널 그룹을 위한 기본 터널 매개변수를 구성합니다.

프로시저

단계 **1** IPsec 원격 액세스 터널 그룹(연결 프로파일이라고도 함)을 생성합니다.

tunnel-group *name* **type** *type*

예제:

```
hostname(config)# tunnel-group testgroup type ipsec-ra
hostname(config)#
```

단계 **2** 인증 방법을 입력할 수 있는 터널 그룹 일반 특성 모드를 시작합니다.

tunnel-group *name* **general-attributes**

예제:

```
hostname(config)# tunnel-group testgroup general-attributes
hostname(config-tunnel-general)#
```

단계 **3** 터널 그룹에 대해 사용할 주소 풀을 지정합니다.

address-pool [*(인터페이스 이름)*] *address_pool1* [*... address_pool6*]

예제:

```
hostname(config-general)# address-pool testpool
```

단계 **4** IKEv1 연결에 대해 IPsec에 특정한 특성을 입력할 수 있는 터널 그룹 ipsec 특성 모드를 시작합니다.

tunnel-group *name* **ipsec-attributes**

예제:

```
hostname(config)# tunnel-group testgroup ipsec-attributes
hostname(config-tunnel-ipsec)#
```

단계 **5** (선택 사항) 사전 공유 키(IKEv1만 해당)를 구성합니다. 키는 1-128자의 영숫자 문자열일 수 있습니다.

Adaptive Security Appliance 및 클라이언트에 대한 키가 동일해야 합니다. 다른 크기의 사전 공유 키를 지닌 Cisco VPN 클라이언트가 연결을 시도하는 경우, 클라이언트는 피어 인증에 실패했음을 표시하는 오류 메시지를 기록합니다.

ikev1 pre-shared-key *key*

예제:

```
hostname(config-tunnel-ipsec)# pre-shared-key 44kkaol59636jnfx
```

동적 암호화 맵 생성

동적 암호화 맵은 일부 매개변수가 구성된 정책 템플릿을 정의합니다. 그 결과 ASA가 원격 액세스 클라이언트 등 알 수 없는 IP 주소가 있는 피어에서 연결을 수신할 수 있습니다.

동적 암호화 맵 항목은 연결에 대한 변형 집합을 식별합니다. 또한 역방향 라우팅을 활성화하여 ASA가 연결된 클라이언트에 대해 라우팅 정보를 확인하고 RIP 또는 OSPF를 통해 이를 알리도록 할 수 있습니다.

다음 작업을 수행하십시오.

프로시저

단계 **1** 동적 암호화 맵을 생성하고 이 맵에 대해 IKEv1 변형 집합 또는 IKEv2 제안서를 지정합니다.

- IKEv1의 경우 다음 명령을 사용합니다.

  crypto dynamic-map *dynamic-map-name seq-num* **set ikev1 transform-set** *transform-set-name*

- IKEv2의 경우 다음 명령을 사용합니다.

  crypto dynamic-map *dynamic-map-name seq-num* **set ikev2 ipsec-proposal** *proposal-name*

예제:

```
hostname(config)# crypto dynamic-map dyn1 1 set ikev1 transform-set FirstSet
hostname(config)#

hostname(config)# crypto dynamic-map dyn1 1 set ikev2 ipsec-proposal FirstSet
hostname(config)#
```

단계 **2** (선택 사항) 이 암호화 맵 항목에 기반하여 모든 연결에 대해 역방향 라우팅 삽입을 활성화합니다.

crypto dynamic-map *dynamic-map-name dynamic-seq-num* **set reverse-route**

예제:

```
hostname(config)# crypto dynamic-map dyn1 1 set reverse route
hostname(config)#
```

동적 암호화 맵에 사용할 암호화 맵 항목 생성

ASA가 IPsec 보안 연계의 매개변수를 설정하는 데 동적 암호화 맵을 사용하도록 암호화 맵 항목을 생성합니다.

이 명령에 대한 다음 예에서 암호화 맵의 이름은 mymap이며 시퀀스 번호는 1이고 동적 암호화 맵의 이름은 이전 섹션에서 생성한 dyn1입니다.

프로시저

단계 **1** 동적 암호화 맵에 사용할 암호화 맵 항목을 생성합니다.

crypto map *map-name seq-num* **ipsec-isakmp dynamic** *dynamic-map-name*

예제:

```
hostname(config)# crypto map mymap 1 ipsec-isakmp dynamic dyn1
```

단계 **2** 외부 인터페이스에 암호화 맵을 적용합니다.

crypto map *map-name* **interface** *interface-name*

예제:

```
hostname(config)# crypto map mymap interface outside
```

단계 **3** 구성에 변경 사항을 저장합니다.

write memory

다중 상황 모드에서 IPSec IKEv2 원격 액세스 VPN 구성

원격 액세스 IPsec VPN 구성에 대한 자세한 내용은 다음의 내용을 참조하십시오.

- 인터페이스 구성, 210 페이지
- 주소 풀 구성, 212 페이지
- 사용자 추가, 213 페이지
- IKEv1 변형 집합 또는 IKEv2 제안서 생성, 213 페이지
- 터널 그룹 정의, 214 페이지
- 동적 암호화 맵 생성, 216 페이지
- 동적 암호화 맵에 사용할 암호화 맵 항목 생성, 216 페이지

원격 액세스 IPsec VPN에 대한 구성 예

다음 예는 원격 액세스 IPsec/IKEv1 VPN을 구성하는 방법을 보여줍니다.

```
hostname(config)# crypto ikev1 policy 10
hostname(config-ikev1-policy)# authentication pre-share
hostname(config-ikev1-policy)# encryption aes-256
hostname(config-ikev1-policy)# hash sha
hostname(config-ikev1-policy)# group 2
hostname(config)# crypto ikev1 enable outside
hostname(config)# ip local pool POOL 192.168.0.10-192.168.0.15
hostname(config)# username testuser password 12345678
hostname(config)# crypto ipsec ikev1 transform set AES256-SHA
esp-aes-256 esp-sha-hmac
hostname(config)# tunnel-group RAVPN type remote-access
hostname(config)# tunnel-group RAVPN general-attributes
```

```
hostname(config-general)# address-pool POOL
hostname(config)# tunnel-group RAVPN ipsec-attributes
hostname(config-ipsec)# ikev1 pre-shared-key ravpnkey
hostname(config)# crypto dynamic-map DYNMAP 1 set ikev1
transform-set AES256-SHA
hostname(config)# crypto dynamic-map DYNMAP 1 set reverse-route
hostname(config)# crypto map CMAP 1 ipsec-isakmp dynamic DYNMAP
hostname(config)# crypto map CMAP interface outside
```

다음 예는 원격 액세스 IPsec/IKEv2 VPN을 구성하는 방법을 보여줍니다.

```
hostname(config)# crypto ikev2 policy 1
hostname(config-ikev2-policy)# group 2
hostname(config-ikev2-policy)# integrity sha512
hostname(config-ikev2-policy)# prf sha512
hostname(config)# crypto ikev2 enable outside
hostname(config)# ip local pool POOL 192.168.0.10-192.168.0.15
hostname(config)# username testuser password 12345678
hostname(config)# crypto ipsec ikev2 ipsec-proposal  AES256-SHA512
hostname(config-ipsec-proposal)# protocol esp encryption  aes-256
hostname(config-ipsec-proposal)# protocol esp integrity sha-512
hostname(config)# tunnel-group RAVPN type remote-access
hostname(config)# tunnel-group RAVPN general-attributes
hostname(config-general)# address-pool POOL
hostname(config)# tunnel-group RAVPN ipsec-attributes
hostname(config-tunnel-ipsec)# ikev2 local-authentication
pre-shared-key localravpnkey
hostname(config-tunnel-ipsec)# ikev2 remote-authentication
pre-shared-key remoteravpnkey
hostname(config)# crypto dynamic-map DYNMAP 1 set ikev2
ipsec-proposal AES256-SHA512
hostname(config)# crypto dynamic-map DYNMAP 1 set reverse-route
hostname(config)# crypto map CMAP 1 ipsec-isakmp dynamic DYNMAP
hostname(config)# crypto map CMAP interface outside
```

다중 상황 모드에서 표준 기반 IPSec IKEv2 원격 액세스 VPN 구성 예

다음 예는 다중 상황 모드에서 표준 기반 원격 액세스 IPsec/IKEv2 VPN용 ASA를 구성하는 방법을 보여줍니다. 이러한 예는 각각 시스템 컨텍스트 및 사용자 컨텍스트 구성에 대한 정보를 제공합니다.

시스템 컨텍스트 구성:

```
class default
  limit-resource All 0
  limit-resource Mac-addresses 65536
  limit-resource ASDM 5
  limit-resource SSH 5
  limit-resource Telnet 5
  limit-resource VPN AnyConnect 4.0%

hostname(config)#context CTX2
hostname(config-ctx)#member default   ===============> License allotment for contexts using
```

```
 class
hostname(config-ctx)#allocate-interface Ethernet1/1.200
hostname(config-ctx)#allocate-interface Ethernet1/3.100
hostname(config-ctx)#config-url disk0:/CTX2.cfg
```

사용자 컨텍스트 구성:

```
hostname/CTX2(config)#ip local pool CTX2-pool 1.1.2.1-1.1.2.250 mask 255.255.255.0
hostname/CTX2(config)#aaa-server ISE protocol radius
hostname/CTX2(config)#aaa-server ISE (inside) host 10.10.190.100
hostname/CTX2(config-aaa-server-host)#key *****
hostname/CTX2(config-aaa-server-host)#exit
hostname/CTX2(config)#


hostname/CTX2(config)#group-policy GroupPolicy_CTX2-IKEv2 internal
hostname/CTX2(config)#group-policy GroupPolicy_CTX2-IKEv2 attributes
hostname/CTX2(config-group-policy)#vpn-tunnel-protocol ikev2
hostname/CTX2(config-group-policy)#exit
hostname/CTX2(config)#


hostname/CTX2(config)#crypto dynamic-map SYSTEM_DEFAULT_CRYPTO_MAP 65535 set ikev2
ipsec-proposal AES256 AES192 AES 3DES DES
hostname/CTX2(config)#crypto map outside_map 65535 ipsec-isakmp dynamic
SYSTEM_DEFAULT_CRYPTO_MAP
hostname/CTX2(config)#crypto map outside_map interface outside
```

표준 기반 클라이언트에서 IPSec/IKEv2 원격 액세스 연결은 기본적으로 터널 그룹 "DefaultRAGroup"에 속합니다.

```
hostname/CTX2(config)#tunnel-group DefaultRAGroup type remote-access
hostname/CTX2(config)#tunnel-group DefaultRAGroup general-attributes
hostname/CTX2(config-tunnel-general)#default-group-policy GroupPolicy_CTX2-IKEv2
hostname/CTX2(config-tunnel-general)#address-pool CTX2-pool
hostname/CTX2(config-tunnel-general)#authentication-server-group ISE
hostname/CTX2(config-tunnel-general)#exit
hostname/CTX2(config)#

hostname/CTX2(config)#tunnel-group DefaultRAGroup ipsec-attributes
hostname/CTX2(config-tunnel-ipsec)#ikev2 remote-authentication eap query-identity
hostname/CTX2(config-tunnel-ipsec)#ikev2 local-authentication certificate ASDM_TrustPoint0
hostname/CTX2(config-tunnel-ipsec)#exit
hostname/CTX2(config)#

hostname/CTX2(config)#crypto ikev2 enable outside client-services port 443
hostname/CTX2(config)#crypto ikev2 remote-access trustpoint ASDM_TrustPoint0
```

다중 상황 모드에서 **AnyConnect IPSec IKEv2** 원격 액세스 **VPN** 구성 예

다음 예는 다중 상황 모드에서 AnyConnect 원격 액세스 IPsec/IKEv2 VPN용 ASA를 구성하는 방법을 보여줍니다. 이러한 예는 각각 시스템 컨텍스트 및 사용자 컨텍스트 구성에 대한 정보를 제공합니다.

시스템 컨텍스트 구성:

```
class default
    limit-resource All 0
    limit-resource Mac-addresses 65536
    limit-resource ASDM 5
    limit-resource SSH 5
    limit-resource Telnet 5
    limit-resource VPN AnyConnect 4.0%
```

```
hostname(config)#context CTX3
hostname(config-ctx)#member default   ===============> License allotment for contexts using
 class
hostname(config-ctx)#allocate-interface Ethernet1/1.200
hostname(config-ctx)#allocate-interface Ethernet1/3.100
hostname(config-ctx)#config-url disk0:/CTX3.cfg
```

각 컨텍스트의 가상 파일 시스템 생성 시 이미지 및 프로파일 같은 Cisco Anyconnect 파일이 포함될 수 있습니다.

```
hostname(config-ctx)#storage-url shared disk0:/shared disk0
```

사용자 컨텍스트 구성:

```
hostname/CTX3(config)#ip local pool ctx3-pool 1.1.3.1-1.1.3.250 mask 255.255.255.0
hostname/CTX3(config)#webvpn
hostname/CTX3(config-webvpn)#enable outside
hostname/CTX3(config-webvpn)# anyconnect image
disk0:/anyconnect-win-4.6.00010-webdeploy-k9.pkg 1
hostname/CTX3(config-webvpn)#anyconnect profiles IKEv2-ctx1 disk0:/ikev2-ctx1.xml
hostname/CTX3(config-webvpn)#anyconnect enable
hostname/CTX3(config-webvpn)#tunnel-group-list enable
```

```
hostname/CTX3(config)#username cisco password *****
hostname/CTX3(config)#ssl trust-point ASDM_TrustPoint0 outside
hostname/CTX3(config)#group-policy GroupPolicy_CTX3-IKEv2 internal
hostname/CTX3(config)#group-policy GroupPolicy_CTX3-IKEv2 attributes
```

```
hostname/CTX3(config-group-policy)#vpn-tunnel-protocol ikev2 ssl-client
hostname/CTX3(config-group-policy)#dns-server value 10.3.5.6
hostname/CTX3(config-group-policy)#wins-server none
hostname/CTX3(config-group-policy)#default-domain none
hostname/CTX3(config-group-policy)#webvpn
hostname/CTX3(config-group-webvpn)#anyconnect profiles value IKEv2-ctx1 type user
```

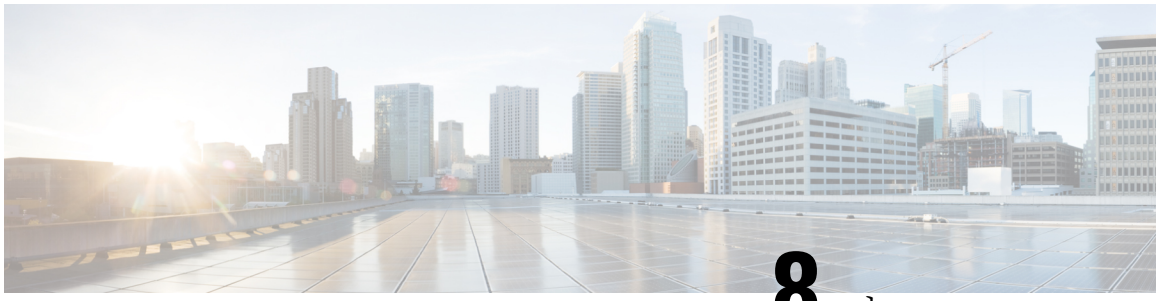
```
hostname/CTX3(config)#crypto ikev2 enable outside client-services port 443
hostname/CTX3(config)#crypto ikev2 remote-access trustpoint ASDM_TrustPoint0
hostname/CTX3(config)#crypto dynamic-map SYSTEM_DEFAULT_CRYPTO_MAP 65535 set ikev2
ipsec-proposal AES256 AES192 AES 3DES DES
hostname/CTX3(config)#crypto map outside_map 65535 ipsec-isakmp dynamic
SYSTEM_DEFAULT_CRYPTO_MAP
hostname/CTX3(config)#crypto map outside_map interface outside
```

```
hostname/CTX3(config)#tunnel-group CTX3-IKEv2 type remote-access
```

```
hostname/CTX3(config)#tunnel-group CTX3-IKEv2 general-attributes
hostname/CTX3(config-tunnel-general)#default-group-policy GroupPolicy_CTX3-IKEv2
hostname/CTX3(config-tunnel-general)#address-pool ctx3-pool
hostname/CTX3(config)#tunnel-group CTX3-IKEv2 webvpn-attributes
hostname/CTX3(config-tunnel-webvpn)#group-alias CTX3-IKEv2 enable
```

원격 액세스 VPN에 대한 기능 기록

기능 이름	릴리스	기능 정보
IPsec IKEv1 및 SSL용 원격 액세스 VPN	7.0	원격 액세스 VPN을 통해 사용자는 인터넷과 같은 TCP/IP 네트워크를 통해 안전하게 중앙 사이트에 연결할 수 있습니다.
IPsec IKEv2용 원격 액세스 VPN	8.4(1)	AnyConnect Secure Mobility Client에 대해 IPsec IKEv2 지원 추가됨
원격 액세스 VPN용 자동 Mobike 지원	9.8(1)	IPsec IKEv2 RA VPN에 대한 모바일 IKE(Mobike) 지원이 추가되었습니다. Mobike는 항상 켜져 있습니다. IKEv2 RA VPN 연결을 위한 Mobike 통신 중에 반환 라우팅 가능성 확인을 활성화하는 `ikev2 mobike-rrc` 명령이 추가되었습니다.
다중 상황 모드에서 IPSec IKEv2용 원격 액세스 VPN 구성	9.9(2)	Anyconnect 및 서드파티 표준 기반 IPSec IKEv2 VPN 클라이언트가 다중 상황 모드에서 작동하는 ASA에 대한 원격 액세스 VPN 세션을 설정할 수 있도록 ASA를 구성할 수 있습니다.



8 장

LAN-to-LAN IPsec VPN

LAN-to-LAN VPN은 다양한 위치에 있는 네트워크를 연결합니다.

Cisco 피어 및 모든 관련 표준을 준수하는 서드파티 피어와의 LAN-to-LAN IPsec 연결을 생성할 수 있습니다. 이러한 피어는 IPv4와 IPv6 주소를 사용하여 내부 주소와 외부 주소를 함께 포함할 수 있습니다 .

이 장에서는 LAN-to-LAN VPN 연결을 구축하는 방법에 대해 설명합니다.

구성 요약

이 섹션에서는 이 장에 설명된 LAN-to-LAN 구성 예에 대한 요약을 제공합니다. 다음 섹션에서는 단계별 지침을 제공합니다.

```
hostname(config)# interface ethernet0/0
hostname(config-if)# ip address 10.10.4.100 255.255.0.0
hostname(config-if)# nameif outside
hostname(config-if)# no shutdown
hostname(config)# crypto ikev1 policy 1
hostname(config-ikev1-policy)# authentication pre-share
hostname(config-ikev1-policy)# encryption 3des
hostname(config-ikev1-policy)# hash sha
hostname(config-ikev1-policy)# group 2
hostname(config-ikev1-policy)# lifetime 43200
hostname(config)# crypto ikev1 enable outside
hostname(config)# crypto ikev2 policy 1
hostname(config-ikev2-policy)# encryption 3des
```

```
hostname(config-ikev2-policy)# group 2
hostname(config-ikev12-policy)# prf sha
hostname(config-ikev2-policy)# lifetime 43200
hostname(config)# crypto ikev2 enable outside
hostname(config)# crypto ipsec ikev1 transform-set FirstSet esp-3des esp-md5-hmac
hostname(config)# crypto ipsec ikev2 ipsec-proposal secure
hostname(config-ipsec-proposal)# protocol esp encryption 3des aes des
hostname(config-ipsec-proposal)# protocol esp integrity sha-1
hostname(config)# access-list l2l_list extended permit ip 192.168.0.0 255.255.0.0 150.150.0.0
 255.255.0.0
hostname(config)# tunnel-group 10.10.4.108 type ipsec-l2l
hostname(config)# tunnel-group 10.10.4.108 ipsec-attributes
hostname(config-tunnel-ipsec)# ikev1 pre-shared-key 44kkaol59636jnfx
hostname(config)# crypto map abcmap 1 match address l2l_list
hostname(config)# crypto map abcmap 1 set peer 10.10.4.108
hostname(config)# crypto map abcmap 1 set ikev1 transform-set FirstSet
hostname(config)# crypto map abcmap 1 set ikev2 ipsec-proposal secure
hostname(config)# crypto map abcmap interface outside
hostname(config)# write memory
```

다중 상황 모드로 Site-to-Site VPN 구성

다중 모드로 Site-to-Site를 지원하려면 다음 단계를 수행하십시오. 이 단계를 수행하여 리소스 할당이 분할되는 방식을 확인할 수 있습니다.

프로시저

단계 **1** 다중 모드로 VPN을 구성하려면 리소스 클래스를 구성하고 VPN 라이센스를 허용되는 리소스의 일부로 선택합니다. "리소스 관리에 대한 클래스 구성"에서는 이 구성 단계를 제공합니다. 다음은 구성 예입니다.

```
class ctx1
 limit-resource VPN Burst Other 100
 limit-resource VPN Other 1000
```

단계 **2** 상황을 구성하고 VPN 라이센스를 허용하는 구성된 클래스의 멤버로 설정합니다. 다음은 구성 예입니다.

```
context context1
 member ctx1
 allocate-interface GigabitEthernet3/0.2
 allocate-interface GigabitEthernet3/1.2
 allocate-interface Management0/0
 config-url disk0:/sm_s2s_ik1_ip4_no_webvpn.txt
 join-failover-group 1
```

단계 **3** 연결 프로파일, 정책, 암호화 맵 등을 Site-to-Site VPN의 단일 상황 VPN 구성과 동일하게 구성합니다.

인터페이스 구성

ASA에는 최소 두 개의 인터페이스(여기서는 외부 및 내부 인터페이스)가 있습니다. 일반적으로 외부 인터페이스는 공용 인터넷에 연결되며, 내부 인터페이스는 사설 네트워크에 연결되고 공용 액세스로부터 보호됩니다.

시작하려면 ASA에서 두 개의 인터페이스를 구성하고 활성화하십시오. 그런 다음 이름, IP 주소 및 서브넷 마스크를 할당합니다. 선택적으로 보안 어플라이언스에 보안 수준, 속도 및 이중 작업을 구성합니다.

참고 ASA의 외부 인터페이스 주소(IPv4/IPv6 모두 해당)는 사설 측 어드레스 스페이스와 중복될 수 없습니다.

프로시저

단계 **1** 인터페이스 구성 모드를 시작하려면 전역 구성 모드에서 구성할 인터페이스의 기본 이름을 가진 **interface** 명령을 입력합니다. 다음 예에서 인터페이스는 ethernet0입니다.

```
hostname(config)# interface ethernet0/0
hostname(config-if)#
```

단계 **2** 인터페이스에 대한 IP 주소 및 서브넷 마스크를 설정하려면 **ip address** 명령을 입력합니다. 다음 예에서 IP 주소는 10.10.4.100이고 서브넷 마스크는 255.255.0.0입니다.

```
hostname(config-if)# ip address 10.10.4.100 255.255.0.0
hostname(config-if)#
```

단계 **3** 인터페이스 이름을 지정하려면 **nameif** 명령(최대 48자)을 입력합니다. 이름을 설정한 후에는 이 이름을 변경할 수 없습니다. 다음 예에서 ethernet0 인터페이스의 이름은 outside입니다.

```
hostname(config-if)# nameif outside
hostname(config-if)##
```

단계 **4** 인터페이스를 활성화하려면 **no** 버전의 **shutdown** 명령을 입력합니다. 기본적으로 인터페이스는 비활성화되어 있습니다.

```
hostname(config-if)# no shutdown
hostname(config-if)#
```

단계 **5** 변경 사항을 저장하려면 **write memory** 명령을 입력합니다.

```
hostname(config-if)# write memory
hostname(config-if)#
```

단계 6 두 번째 인터페이스를 구성하려면 동일한 절차를 수행합니다.

ISAKMP 정책 구성 및 외부 인터페이스에서 ISAKMP 활성화

ISAKMP는 2개의 호스트가 IPsec SA(security association: 보안 연계)를 구축하는 방법에 대해 합의할 수 있는 협상 프로토콜입니다. 이는 SA 특성의 형식에 대한 합의의 일반적인 프레임워크를 제공합니다. 여기에는 SA에 대한 피어와의 협상, SA 수정 또는 삭제가 포함됩니다. ISAKMP는 1단계와 2단계의 두 단계로 협상을 분리합니다. 1단계에서는 최신 ISAKMP 협상 메시지를 보호하는 첫 번째 터널을 생성합니다. 2단계에서는 데이터를 보호하는 터널을 생성합니다.

IKE는 ISAKMP를 통해 사용할 IPsec용 SA를 설정합니다. IKE는 피어를 인증하는 데 사용되는 암호화 키를 생성합니다.

ASA는 레거시 Cisco VPN 클라이언트에서의 연결을 위해 IKEv1을 지원하고 AnyConnect VPN 클라이언트를 위해 IKEv2를 지원합니다.

ISAKMP 협상 기간을 설정하려면 다음을 포함하는 IKE 정책을 생성하십시오.

- IKEv1 피어에 필요한 인증 유형 즉, 인증서를 사용하는 RSA 서명 또는 사전 공유 키(PSK)
- 데이터 및 개인정보를 보호할 암호화 방법
- 발신자의 ID를 확인하고 메시지가 전송 중에 변경되지 않았는지 확인하는 HMAC(Hashed Message Authentication Codes: 해시된 메시지 인증 코드) 방식
- encryption-key-determination 알고리즘의 수준을 결정하는 Diffie-Hellman 그룹. ASA는 이 알고리즘을 사용하여 암호화 및 해시 키를 파생합니다.
- IKEv2의 경우, IKEv2 터널 암호화에 필요한 키 요소 및 해싱 작업을 파생시키기 위해 알고리즘으로 사용되는 별도의 PRF(Pseudo Random Function: 의사 난수 함수)
- ASA가 교체 전 암호 키를 사용하는 시간 제한

IKEv1 정책의 경우 각 매개변수에 대해 하나의 값을 설정합니다. IKEv2의 경우 단일 정책에 여러 개의 암호화와 인증 유형 및 여러 개의 무결성 알고리즘을 구성할 수 있습니다. ASA는 설정을 가장 안전한 것부터 가장 안전하지 않은 것까지 나열하고 해당 순서를 사용하여 피어와 협상합니다. 이렇게 하면 IKEv1과 마찬가지로 허용되는 각 조합을 전송할 필요 없이 모든 허용되는 변형을 전달하기 위해 단일 제안서를 전송할 수 있습니다.

다음 섹션에서는 IKEv1 및 IKEv2 정책을 생성하고 인터페이스에서 활성화하기 위한 절차를 제시합니다.

- IKEv1 연결을 위한 ISAKMP 정책 구성, 227 페이지
- IKEv2 연결을 위한 ISAKMP 정책 구성, 228 페이지

IKEv1 연결을 위한 ISAKMP 정책 구성

IKEv1 연결을 위해 ISAKMP 정책을 구성하려면 **crypto ikev1 policy** 명령을 사용하여 IKEv1 매개변수를 구성할 수 있는 IKEv1 정책 구성 모드를 시작합니다.

프로시저

단계 **1** IPsec IKEv1 정책 구성 모드를 시작합니다. 예를 들면 다음과 같습니다.

```
hostname(config)# crypto ikev1 policy 1
hostname(config-ikev1-policy)#
```

단계 **2** 인증 방법을 설정합니다. 다음 예에서는 사전 공유 키를 구성합니다.

```
hostname(config-ikev1-policy)# authentication pre-share
hostname(config-ikev1-policy)#
```

단계 **3** 암호화 방법을 설정합니다. 다음 예에서는 3DES를 구성합니다.

```
hostname(config-ikev1-policy)# encryption 3des
hostname(config-ikev1-policy)#
```

단계 **4** HMAC 방법을 설정합니다. 다음 예에서는 SHA-1을 구성합니다.

```
hostname(config-ikev1-policy)# hash sha
hostname(config-ikev1-policy)#
```

단계 **5** Diffie-Hellman 그룹을 설정합니다. 다음 예에서는 그룹 2를 구성합니다.

```
hostname(config-ikev1-policy)# group 2
hostname(config-ikev1-policy)#
```

단계 **6** 암호 키 수명을 설정합니다. 다음 예에서는 43,200초(12시간)를 구성합니다.

```
hostname(config-ikev1-policy)# lifetime 43200
hostname(config-ikev1-policy)#
```

단계 **7** 단일 또는 다중 상황 모드로, 외부(outside)라는 이름의 인터페이스에서 IKEv1을 활성화합니다.

```
hostname(config)# crypto ikev1 enable outside
hostname(config)#
```

단계 **8** 변경 사항을 저장하려면 **write memory** 명령을 입력합니다.

```
hostname(config)# write memory
```

```
hostname(config)#
```

IKEv2 연결을 위한 ISAKMP 정책 구성

IKEv2 연결을 위해 ISAKMP 정책을 구성하려면 **crypto ikev2 policy** priority 명령을 사용하여 IKEv2 매개변수를 구성할 수 있는 IKEv2 정책 구성 모드를 시작합니다.

프로시저

단계 **1** IPsec IKEv2 정책 구성 모드를 시작합니다. 예를 들면 다음과 같습니다.

```
hostname(config)# crypto ikev2 policy 1
hostname(config-ikev2-policy)#
```

단계 **2** 암호화 방법을 설정합니다. 다음 예에서는 3DES를 구성합니다.

```
hostname(config-ikev2-policy)# encryption 3des
hostname(config-ikev2-policy)#
```

단계 **3** Diffie-Hellman 그룹을 설정합니다. 다음 예에서는 그룹 2를 구성합니다.

```
hostname(config-ikev2-policy)# group 2
hostname(config-ikev2-policy)#
```

단계 **4** IKEv2 터널 암호화에 필요한 키 요소 및 해싱 작업을 파생시키기 위해 알고리즘으로 사용되는 PRF(Pseudo Random Function: 의사 난수 함수)를 설정합니다. 다음 예에서는 SHA-1(HMAC 변형)을 구성합니다.

```
hostname(config-ikev12-policy)# prf sha
hostname(config-ikev2-policy)#
```

단계 **5** 암호 키 수명을 설정합니다. 다음 예에서는 43,200초(12시간)를 구성합니다.

```
hostname(config-ikev2-policy)# lifetime seconds 43200
hostname(config-ikev2-policy)#
```

단계 **6** 외부(outside)라는 이름의 인터페이스에서 IKEv2를 활성화합니다.

```
hostname(config)# crypto ikev2 enable outside
hostname(config)#
```

단계 **7** 변경 사항을 저장하려면 **write memory** 명령을 입력합니다.

```
hostname(config)# write memory
hostname(config)#
```

IKEv1 변형 집합 생성

IKEv1 변형 집합은 암호화 방법 및 인증 방법을 결합합니다. ISAKMP와의 IPsec 보안 연계 협상 동안 피어는 특정 데이터 흐름을 보호하기 위해 특정 변형 집합을 사용하는 데 동의합니다. 변형 집합은 양쪽 피어에 대해 모두 동일해야 합니다.

변형 집합은 연계된 암호화 맵 항목에 지정된 ACL에 대한 데이터 흐름을 보호합니다. ASA 구성에서 변형 집합을 생성한 다음 암호화 맵 또는 동적 암호화 맵 항목에서 최대 11개의 집합을 지정할 수 있습니다.

다음 표는 유효한 암호화 및 인증 방법을 나열합니다.

표 ***8:*** 유효한 암호화 및 인증 방법

유효한 암호화 방법	유효한 인증 방법
esp-des	esp-md5-hmac
esp-3des(기본값)	esp-sha-hmac(기본값)
esp-aes(128비트 암호화)	
esp-aes-192	
esp-aes-256	
esp-null	

터널 모드는 신뢰할 수 없는 네트워크(예: 공용 인터넷)를 통해 연결된 두 개의 ASA 간에 IPsec을 구현하는 일반적인 방식입니다. 터널 모드는 기본이며 구성할 필요가 없습니다.

변형 집합을 구성하려면 단일 또는 다중 상황 모드에서 다음 Site-to-Site 작업을 수행합니다.

프로시저

단계 **1** 전역 구성 모드에서 **crypto ipsec ikev1 transform-set** 명령을 입력합니다. 다음 예에서는 FirstSet 이름, esp-3des 암호화 및 esp-md5-hmac 인증으로 변형 집합을 구성합니다. 구문은 다음과 같습니다.

crypto ipsec ikev1 transform-set *transform-set-nameencryption-method authentication-method*

```
hostname(config)# crypto ipsec transform-set FirstSet esp-3des esp-md5-hmac
hostname(config)#
```

단계 **2** 변경 내용을 저장합니다.

```
hostname(config)# write memory
hostname(config)#
```

IKEv2 제안서 생성

IKEv2의 경우 단일 정책에 여러 개의 암호화와 인증 유형 및 여러 개의 무결성 알고리즘을 구성할 수 있습니다. ASA는 설정을 가장 안전한 것부터 가장 안전하지 않은 것까지 나열하고 해당 순서를 사용하여 피어와 협상합니다. 이렇게 하면 IKEv1과 마찬가지로 허용되는 각 조합을 전송할 필요 없이 모든 허용되는 변형을 전달하기 위해 단일 제안서를 전송할 수 있습니다.

다음 표는 유효한 IKEv2 암호화 및 인증 방법을 나열합니다.

표 ***9:*** 유효한 ***IKEv2*** 암호화 및 무결성 방법

유효한 암호화 방법	유효한 무결성 방법
des	sha(기본값)
3des(기본값)	md5
aes	
aes-192	
aes-256	

IKEv2 제안서를 구성하려면 단일 또는 다중 상황 모드에서 다음 작업을 수행합니다.

프로시저

단계 **1** 전역 구성 모드에서 **crypto ipsec ikev2 ipsec-proposal** 명령을 사용하여 제안서에 대해 다중 암호화 및 무결성 유형을 지정할 수 있는 ipsec 제안서 구성 모드를 시작합니다. 이 예에서 secure는 제안서의 이름입니다.

```
hostname(config)# crypto ipsec ikev2 ipsec-proposal secure
hostname(config-ipsec-proposal)#
```

단계 **2** 프로토콜 및 암호화 유형을 입력합니다. ESP는 지원되는 유일한 프로토콜입니다. 예를 들면 다음과 같습니다.

```
hostname(config-ipsec-proposal)# protocol esp encryption 3des aes des
hostname(config-ipsec-proposal)#
```

단계 **3** 무결성 유형을 입력합니다. 예를 들면 다음과 같습니다.

```
hostname(config-ipsec-proposal)# protocol esp integrity sha-1
hostname(config-ipsec-proposal)#
```

단계 **4** 변경 내용을 저장합니다.

ACL 구성

ASA는 액세스 제어 목록을 사용하여 네트워크 액세스를 제어합니다. 기본적으로 Adaptive Security Appliance는 모든 트래픽을 거부합니다. 트래픽을 허용하는 ACL을 구성해야 합니다. 자세한 내용은 일반 작업 구성 가이드에서 "액세스 제어 목록에 대한 정보"를 참조하십시오.

이 LAN-to-LAN VPN 제어 연결에 대해 구성한 ACL은 소스 및 변환된 대상 IP 주소를 기반으로 합니다. 연결의 양쪽 모두에서 상대방을 미러링하는 ACL을 구성해야 합니다.

VPN 트래픽에 대한 ACL은 변환된 주소를 사용합니다.

참고 VPN 필터로 ACL 구성에 대한 자세한 내용은 Specify a VLAN for Remote Access or Apply a Unified Access Control Rule to the Group Policy, 149 페이지를 참조하십시오.

프로시저

단계 **1** **access-list extended** 명령을 입력합니다. 다음 예에서는 192.168.0.0 네트워크의 IP 주소 트래픽이 150.150.0.0 네트워크로 이동하도록 허용하는 이름이 l2l_list인 ACL을 구성합니다. 구문은 **access-list** listname **extended permit ip** source-ipaddress source-netmask destination-ipaddress destination-netmask입니다.

```
hostname(config)# access-list l2l_list extended permit ip 192.168.0.0 255.255.0.0 150.150.0.0
 255.255.0.0
hostname(config)#
```

단계 **2** ACL을 미러링하는 연결의 다른 쪽에 있는 ASA에 대해 ACL을 구성합니다. 두 가지 다른 암호화 ACL에 정의되어 있고 동일한 암호화 맵에 연결된 서브넷을 오버랩하지 마십시오. 다음 예에서 피어에 대한 확인 상자는 hostname2입니다.

```
hostname2(config)# access-list l2l_list extended permit ip 150.150.0.0 255.255.0.0 192.168.0.0
 255.255.0.0
hostname(config)#
```

터널 그룹 정의

터널 그룹은 터널 연결 정책이 포함된 레코드 집합입니다. 터널 그룹이 AAA 서버를 식별하도록 구성하고 연결 매개변수를 지정하며 기본 그룹 정책을 정의합니다. ASA는 터널 그룹을 내부에서 저장합니다.

ASA에는 기본 IPsec 원격 액세스 터널 그룹인 DefaultRAGroup과 기본 IPsec LAN-to-LAN 터널 그룹인 DefaultL2Lgroup의 두 가지 기본 터널 그룹이 있습니다. 이 그룹을 수정할 수는 있지만 삭제할 수는 없습니다.

IKE 버전 1과 2 사이에는 그룹에서 허용하는 인증 방법 조건에 주요 차이점이 있습니다. IKEv1을 사용하면 두 개의 VPN 종단에서 한 가지 유형의 인증만 허용합니다(사전 공유 키 또는 인증서 중 하나). 그러나 IKEv2를 사용하면 별도의 로컬 및 원격 인증 CLI를 사용하여 비대칭 인증 방법을 구성(즉, 발신자용으로 사전 공유 키 인증을 구성하지만 응답자용으로는 인증서 인증을 구성)할 수 있습니다. 따라서 IKEv2에서 비대칭 인증이 있는 경우, 한쪽에서는 하나의 자격 증명으로 인증하고 다른 쪽에서는 다른 자격 증명을 사용합니다(사전 공유 키 또는 인증서 중 하나).

또한 환경에 적합한 하나 이상의 새 터널 그룹을 생성할 수 있습니다. ASA는 이 그룹을 사용하여 터널 협상 동안 식별한 특정 터널 그룹이 없는 경우 원격 액세스 및 LAN-to-LAN 터널 그룹을 위한 기본 터널 매개변수를 구성합니다.

기본 LAN-to-LAN 연결을 설정하려면 다음과 같이 터널 그룹에 대해 두 개의 특성을 설정해야 합니다.

- IPsec LAN-to-LAN에 연결 유형을 설정합니다.
- IP 주소에 대해 인증 방법을 구성합니다(즉, IKEv1 및 IKEv2에 대한 사전 공유 키).

프로시저

단계 **1** IPsec LAN-to-LAN에 연결 유형을 설정하려면 **tunnel-group** 명령을 입력합니다.

구문은 **tunnel-group** *name***type** *type*입니다. 이때 name은 터널 그룹에 할당한 이름이며 type은 터널 유형입니다. 터널 유형은 CLI에서 입력하는 경우 다음과 같습니다.

- **remote-access** (IPsec, SSL 및 클라이언트리스 SSL 원격 액세스)
- **ipsec-l2l** (IPsec LAN-to-LAN)

다음 예에서 터널 그룹의 이름은 LAN-to-LAN 피어인 10.10.4.108의 IP 주소입니다.

```
hostname(config)# tunnel-group 10.10.4.108 type ipsec-l2l
hostname(config)#
```

참고 IP 주소가 아닌 이름을 지닌 LAN-to-LAN 터널 그룹은 터널 인증 방법이 디지털 인증서 및/또는 적극적인 모드를 사용하도록 구성된 피어인 경우에만 사용할 수 있습니다.

1.

단계 **2** 사전 공유 키를 사용하도록 인증 방법을 설정하려면 ipsec 속성 모드를 시작한 다음 **ikev1pre-shared-key** 명령을 입력하여 사전 공유 키를 생성합니다. 이 LAN-to-LAN 연결을 위해 두 ASA 모두에서 동일한 사전 공유 키를 사용해야 합니다.

키는 1-128자의 영숫자 문자열입니다.

다음 예에서 IKEv1 사전 공유 키는 44kkaol59636jnfx입니다.

```
hostname(config)# tunnel-group 10.10.4.108 ipsec-attributes
hostname(config-tunnel-ipsec)# ikev1-pre-shared-key 44kkaol59636jnfx
```

단계 **3** 변경 내용을 저장합니다.

```
hostname(config)# write memory
hostname(config)#
```

터널이 작동 및 실행 중인지 확인하려면 **show vpn-sessiondb summary**, **show vpn-sessiondb detail l2l** 또는 **show crypto ipsec sa** 명령을 사용합니다.

암호화 맵 생성 및 인터페이스에 적용

암호화 맵 항목은 다음을 포함하는 IPsec 보안 연계의 다양한 요소를 통합합니다.

- ACL에 정의된 보호해야 할 트래픽 IPsec
- 피어 식별을 통한 IPsec 보호 트래픽의 전송 위치
- 이 트래픽에 적용하고 변형 집합이 지정하는 IPsec 보안
- 인터페이스에 암호화 맵을 적용하여 식별하는 IPsec 트래픽에 대한 로컬 주소

IPsec이 성공하려면 두 개의 피어 모두에 호환 가능한 구성이 있는 암호화 맵 항목이 있어야 합니다. 두 개의 암호화 맵 항목을 호환하려면 최소한 다음 기준을 충족해야 합니다.

- 암호화 맵 항목은 호환 가능한 암호화 ACL(예: 미러 이미지 ACL)을 포함해야 합니다. 응답 피어가 동적 암호화 맵을 사용하는 경우 ASA 암호화 ACL에 있는 항목은 피어의 암호화 ACL에서 "허용"되어야 합니다.
- 암호화 맵 항목은 각각 다른 피어(응답 피어가 동적 암호화 맵을 사용하지 않는 경우)를 식별해야 합니다.
- 암호화 맵 항목에는 최소 하나 이상의 공통된 변형 집합이 있어야 합니다.

지정된 인터페이스에 대해 두 개 이상의 암호화 맵 항목을 생성하는 경우 각 항목의 시퀀스 번호(seq-num)를 사용하여 seq-num이 낮을수록 높은 우선순위가 되도록 순서를 지정합니다. 암호화 맵이 설정된 인터페이스에서 ASA는 높은 우선순위의 맵 항목에 대한 트래픽을 먼저 평가합니다.

다음 조건 중 하나라도 해당하는 경우, 지정된 인터페이스에 대해 여러 암호화 맵 항목을 생성합니다.

- 여러 피어에서 여러 데이터 흐름을 처리합니다.
- 다른 IPsec 보안을 서로 다른 유형의 트래픽(동일하거나 별도의 피어)에 적용하려는 경우, 예를 들어 인증할 하나의 서브넷 집합 간의 트래픽과 인증 및 암호화할 또 다른 서브넷 집합 간의 트래픽을 필요로 하는 경우, 2개의 별도 ACL에서 서로 다른 유형의 트래픽을 정의하고 각 암호화 ACL에 대해 별도의 암호화 맵 항목을 생성합니다.

암호화 맵을 생성하고 전역 구성 모드에서 외부 인터페이스에 이 맵을 적용하려면, 단일 또는 다중 상황 모드에서 다음 단계를 수행하십시오.

프로시저

단계 **1** 암호화 맵 항목에 ACL을 할당하려면 **crypto map match address** 명령을 입력합니다.

구문은 **crypto map** map-name seq-num **match address** aclname입니다. 다음 예에서 맵 이름은 abcmap이며 시퀀스 번호는 1이고 ACL 이름은 **l2l_list**입니다.

```
hostname(config)# crypto map abcmap 1 match address l2l_list
hostname(config)#
```

단계 **2** IPsec 연결을 위해 피어를 식별하려면 **crypto map set peer** 명령을 입력합니다.

구문은 **crypto map** map-name seq-num **set peer** {ip_address1 | hostname1}[... ip_address10 | hostname10]입니다. 다음 예에서 피어 이름은 10.10.4.108입니다.

```
hostname(config)# crypto map abcmap 1 set peer 10.10.4.108
hostname(config)#
```

단계 **3** 암호화 맵 항목에 대해 IKEv1 변형 집합을 지정하려면 **crypto map ikev1 set transform-set** 명령을 입력합니다.

구문은 **crypto map** map-name seq-num **ikev1 set transform-set** transform-set-name입니다. 다음 예에서 변형 집합 이름은 FirstSet입니다.

```
hostname(config)# crypto map abcmap 1 set transform-set FirstSet
hostname(config)#
```

단계 **4** 암호화 맵 항목에 대해 IKEv2 제안서를 지정하려면 다음과 같이 crypto map ikev2 set ipsec-proposal 명령을 입력합니다.

구문은 **crypto map** map-name seq-num set**ikev2 ipsec-proposal proposal-name**입니다. 다음 예에서 제안서 이름은 secure입니다.

crypto map 명령을 사용하여 단일 맵 인덱스에 대해 여러 IPsec 제안서를 지정할 수 있습니다. 이 경우, 여러 제안서가 협상의 일부로 IKEv2 피어에 전송되며 제안서 순서는 암호화 맵 항목의 순서 지정 시 관리자가 결정합니다.

참고 결합 모드(AES-GCM/GMAC) 및 일반 모드(기타 모든 모드) 알고리즘이 IPsec 제안서에 존재하는 경우, 피어에 단일 제안서를 전송할 수 없습니다. 이 경우 최소 두 개 이상의 제안서(결합 모드 및 일반 모드 알고리즘용으로 각각 하나씩의 제안서)이 있어야 합니다.

```
hostname(config)# crypto map abcmap 1 set ikev2 ipsec-proposal secure
hostname(config)#
```

암호화 맵을 인터페이스에 적용

IPsec 트래픽이 이동하는 데 사용되는 각 인터페이스에 암호화 맵 설정을 적용해야 합니다. ASA는 모든 인터페이스에서 IPsec을 지원합니다. 인터페이스에 암호화 맵 집합을 적용하면 암호화 맵 집합에 대해 모든 인터페이스 트래픽을 평가하고 연결 또는 보안 연계 협상 동안 지정된 정책을 사용하도록 ASA에 지시합니다.

또한 인터페이스에 암호화 맵을 바인딩하면 보안 연계 데이터베이스, 보안 정책 데이터베이스 등의 실행 시간 데이터 구조가 초기화됩니다. 이후에 암호화 맵을 수정하는 경우 ASA는 실행 중인 구성에 변경 사항을 자동으로 적용합니다. 새 암호화 맵을 적용한 이후에 기존 연결을 끊고 연결을 재설정합니다.

외부 인터페이스에 구성된 암호화 맵을 적용하려면 다음 단계를 수행하십시오.

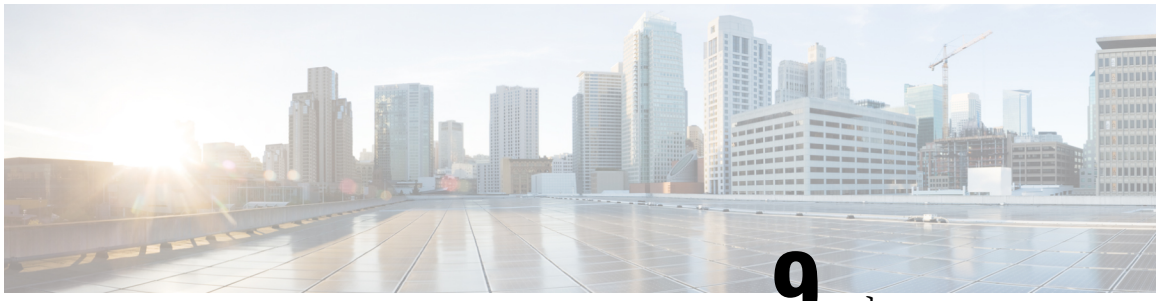
프로시저

단계 **1** **crypto map interface** 명령을 입력합니다. 구문은 **crypto map** map-name **interface** interface-name입니다.

```
hostname(config)# crypto map abcmap interface outside
hostname(config)#
```

단계 **2** 변경 내용을 저장합니다.

```
hostname(config)# write memory
hostname(config)#
```



9 장

AnyConnect VPN 클라이언트 연결

이 섹션에서는 AnyConnect VPN 클라이언트 연결을 구성하는 방법에 대해 설명합니다.

AnyConnect VPN 클라이언트 정보

Cisco AnyConnect Secure Mobility Client는 원격 사용자에게 보안 SSL 및 ASA에 대한 IPsec/IKEv2 연결을 제공합니다. 이전에 설치된 클라이언트가 없는 경우 원격 사용자는 SSL 또는 IPsec/IKEv2 VPN 연결을 허용하도록 구성된 인터페이스의 브라우저에 IP 주소를 입력합니다. ASA가 http:// 요청을 https://로 리디렉션하도록 구성하지 않은 경우, 사용자는 URL을 https://<*address*> 형식으로 입력해야 합니다.

URL을 입력하면 브라우저가 해당 인터페이스로 연결되고 로그인 화면이 표시됩니다. 사용자가 로그인 및 인증을 통과하면 ASA에서 사용자가 클라이언트를 요청하는 것으로 식별하고 원격 컴퓨터의 운영 체제에 맞는 클라이언트를 다운로드합니다. 다운로드 후 클라이언트가 자동으로 설치 및 구성되어 보안 SSL 또는 IPsec/IKEv2 연결을 설정한 다음 연결이 종료되면 구성에 따라 그대로 유지되거나 자동으로 제거됩니다.

클라이언트가 이전에 설치된 경우 사용자가 인증을 통과하면 ASA에서 클라이언트의 개정 내역을 확인하고 필요에 따라 클라이언트를 업그레이드합니다.

클라이언트가 ASA와 SSL VPN 연결을 협상하는 경우, TLS(Transport Layer Security: 전송 계층 보안)를 사용하여 연결하고 선택에 따라 DTLS(Datagram Transport Layer Security: 데이터그램 전송 계층 보안)를 사용하여 연결합니다. DTLS는 일부 SSL 연결에서 발생하는 레이턴시 및 대역폭 문제를 방지하고 패킷 지연에 민감한 실시간 애플리케이션의 성능을 높입니다.

AnyConnect 클라이언트는 ASA에서 다운로드할 수 있으며 시스템 관리자가 원격 PC에 수동으로 설치할 수도 있습니다. 클라이언트를 수동으로 설치하는 방법에 대한 자세한 내용은 해당 릴리스의 Cisco AnyConnect Secure Mobility 구성 가이드의 내용을 참조하십시오.

ASA는 연결을 설정하는 사용자의 그룹 정책 또는 사용자 속성에 기초하여 클라이언트를 다운로드합니다. 클라이언트를 자동으로 다운로드하도록 ASA를 구성하거나 클라이언트 다운로드 여부를 원격 사용자에게 묻는 확인 상자를 표시하도록 구성할 수도 있습니다. 후자의 경우, 사용자가 응답하지 않을 때 시간 제한 간격 이후에 클라이언트를 다운로드할지 또는 로그인 페이지를 표시할지 ASA에 구성할 수 있습니다.

AnyConnect의 요건

AnyConnect Secure Mobility Client를 실행하는 엔드포인트 컴퓨터의 요건에 대해서는 해당 릴리스의 Cisco AnyConnect Secure Mobility 릴리스 노트의 내용을 참조하십시오.

AnyConnect에 대한 지침 및 제한 사항

- ASA는 원격 HTTPS 인증서를 확인하지 않습니다.
- 단일 또는 다중 상황 모드에서 지원됩니다. 다중 상황 모드에서 원격 액세스 VPN을 사용하려면 AnyConnect Apex 라이선스가 필요합니다. ASA에서 AnyConnect Apex 라이선스를 인식하지 못하더라도, Apex 라이선스(예: 플랫폼 한도 내에서 라이선스가 허가된 AnyConnect Premium, AnyConnect for Mobile, for Cisco VPN Phone, 고급 엔드포인트 평가)의 라이선스 속성이 적용됩니다. 공유 라이선싱, AnyConnect Essentials, 장애 조치 라이선스 계약 및 자유 시간 기반 라이선스는 지원되지 않습니다.

AnyConnect의 라이선싱 요건

다음 표에서는 이 기능에 대한 라이센싱 요건을 보여줍니다.

참고 No Payload Encryption 모델에서는 이 기능을 사용할 수 없습니다.

VPN 라이센스에는 각각 사용 가능한 AnyConnect Plus 또는 Apex 라이센스가 필요합니다. AnyConnect 라이센스 구매 시 다음의 최대값을 참조해 주십시오. 모든 유형의 결합 VPN 세션의 최대 수는 이 표에 표시된 최대 세션 수를 초과할 수 없습니다.

모델	라이센스 요건
ASA 5506-X, 5506H-X, 5506W-X	세션 50개. 공유 라이센스는 지원되지 않습니다.
ASA 5508-X	세션 100개. 공유 라이센스는 지원되지 않습니다.

모델	라이센스 요건
ASA 5512-X	• 세션 250개. • 옵션 공유 라이센스: 참가자 또는 서버. 서버 라이센스의 경우 *500~50,000(500*씩 증가*)* 및 *50,000~545,000(1000*씩 증가*)*
ASA 5515-X	• 세션 250개. • 옵션 공유 라이센스: 참가자 또는 서버. 서버 라이센스의 경우 *500~50,000(500*씩 증가*)* 및 *50,000~545,000(1000*씩 증가*)*
ASA 5516-X	• 세션 300개. 공유 라이센스는 지원되지 않습니다.
ASA 5525-X	• 세션 750개. • 옵션 공유 라이센스: 참가자 또는 서버. 서버 라이센스의 경우 *500~50,000(500*씩 증가*)* 및 *50,000~545,000(1000*씩 증가*)*
ASA 5545-X	• 세션 2500개. • 옵션 공유 라이센스: 참가자 또는 서버. 서버 라이센스의 경우 *500~50,000(500*씩 증가*)* 및 *50,000~545,000(1000*씩 증가*)*
ASA 5555-X	• 세션 5000개. • 옵션 공유 라이센스: 참가자 또는 서버. 서버 라이센스의 경우 *500~50,000(500*씩 증가*)* 및 *50,000~545,000(1000*씩 증가*)*
ASA 5585-X(SSP-10 포함)	• 세션 5000개. • 옵션 공유 라이센스: 참가자 또는 서버. 서버 라이센스의 경우 *500~50,000(500*씩 증가*)* 및 *50,000~545,000(1000*씩 증가*)*
ASA 5585-X(SSP-20, -40 및 -60 포함)	• 세션 10,000개. • 옵션 공유 라이센스: 참가자 또는 서버. 서버 라이센스의 경우 *500~50,000(500*씩 증가*)* 및 *50,000~545,000(1000*씩 증가*)*

모델	라이센스 요건
ASASM	• 세션 10,000개. • 옵션 공유 라이센스: 참가자 또는 서버. 서버 라이센스의 경우 *500~50,000(500씩 증가)* 및 *50,000~545,000(1000씩 증가)*
ASAv5	세션 50개.
ASAv10	세션 250개.
ASAv30	세션 750개.

클라이언트리스 SSL VPN 세션을 시작한 후 포털에서 AnyConnect 클라이언트 세션을 시작한 경우, 총 1개의 세션이 사용됩니다. 그러나 처음에 AnyConnect 클라이언트를 시작(예: 독립형 클라이언트에서)한 후 클라이언트리스 SSL VPN 포털에 로그인할 경우 2개의 세션이 사용됩니다.

AnyConnect 연결 구성

이 섹션에서는 AnyConnect VPN 클라이언트 연결을 허용하도록 ASA를 구성하기 위한 사전 요구 사항, 제한 사항 및 세부 작업에 대해 설명합니다.

클라이언트 웹 배포를 위한 ASA 구성

이 섹션에서는 AnyConnect 클라이언트를 웹 배포하기 위해 ASA를 구성하는 단계에 대해 설명합니다.

시작하기 전에

TFTP 또는 다른 방법을 사용하여 ASA에 클라이언트 이미지 패키지를 복사하십시오.

프로시저

단계 **1** 플래시 파일을 AnyConnect 클라이언트 패키지 파일로 식별합니다.

ASA는 원격 PC에 다운로드하기 위해 캐시 메모리에 있는 파일을 펼칩니다. 여러 클라이언트가 있는 경우 순서 인수를 사용하여 클라이언트 이미지에 순서를 할당합니다.

ASA는 원격 PC의 운영 체제와 일치할 때까지 지정한 순서대로 각 클라이언트를 다운로드합니다. 따라서 가장 자주 사용하는 운영 체제에서 사용하는 이미지에 가장 작은 수를 할당합니다.

anyconnect image *filename order*

예제**:**

```
hostname(config-webvpn)# anyconnect image
```

```
anyconnect-win-2.3.0254-k9.pkg 1
hostname(config-webvpn)# anyconnect image
anyconnect-macosx-i386-2.3.0254-k9.pkg 2
hostname(config-webvpn)# anyconnect image
anyconnect-linux-2.3.0254-k9.pkg 3
```

참고 **anyconnect image** 명령을 사용하여 AnyConnect 이미지를 구성한 후에 **anyconnect enable** 명령을 발행해야 합니다. AnyConnect를 활성화하지 않은 경우, AnyConnect는 예상대로 작동하지 않으며 **show webvpn anyconnect**는 설치된 AnyConnect 패키지를 나열하는 대신 SSL VPN 클라이언트를 활성화되지 않은 것으로 간주합니다.

단계 **2** 클라이언트리스 또는 AnyConnect SSL 연결을 위한 인터페이스에서 SSL을 활성화합니다.

enable *interface*

예제**:**

```
hostname(config)# webvpn
hostname(config-webvpn)# enable outside
```

단계 **3** 이 명령을 발행하지 않은 경우 AnyConnect는 예상대로 작동하지 않으며 **show webvpn anyconnect** 명령은 설치된 AnyConnect 패키지를 나열하는 대신 "SSL VPN is not enabled(SSL VPN이 활성화되지 않았습니다.)"를 반환합니다.

anyconnect enable

단계 **4** (선택 사항) 주소 풀을 생성합니다. DHCP 및/또는 사용자 할당 주소 지정과 같은 다른 주소 지정 방법을 사용할 수 있습니다.

ip local pool *poolname startaddr-endaddr* **mask** *mask*

예제**:**

```
hostname(config)# ip local pool vpn_users 209.165.200.225-209.165.200.254
mask 255.255.255.224
```

단계 **5** 터널 그룹에 주소 풀을 할당합니다.

address-pool *poolname*

예제**:**

```
hostname(config)# tunnel-group telecommuters general-attributes
hostname(config-tunnel-general)# address-pool vpn_users
```

단계 **6** 터널 그룹에 기본 그룹 정책을 할당합니다.

default-group-policy *name*

```
hostname(config-tunnel-general)# default-group-policy sales
```

단계 **7** 클라이언트리스 포털 및 AnyConnect GUI 로그인 페이지에 터널 그룹 목록의 표시를 활성화합니다. 별칭 목록은 *group-alias name enable* 명령을 사용하여 정의됩니다.

group-alias *name* **enable**

예제:

```
hostname(config)# tunnel-group telecommuters webvpn-attributes
hostname(config-tunnel-webvpn)# group-alias sales_department enable
```

단계 **8** AnyConnect 클라이언트를 사용자 또는 그룹에 대해 허용되는 VPN 터널링 프로토콜로 지정합니다.

tunnel-group-list enable

예제:

```
hostname(config)# webvpn
hostname(config-webvpn)# tunnel-group-list enable
```

단계 **9** SSL을 사용자 또는 그룹에 대해 허용되는 VPN 터널링 프로토콜로 지정합니다. 추가 프로토콜을 지정할 수 있습니다. 자세한 내용은 명령 참조에서 vpn-tunnel-protocol 명령을 참조하십시오.

vpn-tunnel-protocol

예제:

```
hostname(config)# group-policy sales attributes
hostname(config-group-policy)# webvpn
hostname(config-group-webvpn)# vpn-tunnel-protocol
```

다음에 수행할 작업

그룹 정책에 사용자 할당에 대한 자세한 내용은 6장의 연결 프로파일, 그룹 정책 및 사용자 구성을 참조하십시오.

영구 클라이언트 설치 활성화

영구 클라이언트 설치를 활성화하면 클라이언트의 자동 제거 기능이 비활성화됩니다. 원격 사용자의 연결 시간을 줄일 수 있도록 후속 연결을 위해 원격 컴퓨터에 클라이언트가 설치된 상태로 있습니다.

특정 그룹 또는 사용자를 위해 영구 클라이언트 설치를 활성화하려면 다음과 같이 그룹 정책 또는 사용자 이름 webvpn 모드에서 anyconnect keep-installer 명령을 사용합니다.

기본값은 클라이언트의 영구 설치를 활성화하는 것입니다. 세션 마지막에 클라이언트는 원격 컴퓨터에 그대로 있습니다. 다음 예는 세션 마지막에 원격 컴퓨터에 있는 클라이언트를 제거하도록 기존 그룹 정책 *sales*를 구성합니다.

```
hostname(config)# group-policy sales attributes
hostname(config-group-policy)# webvpn
hostname(config-group-policy)# anyconnect keep-installer installed none
```

DTLS 구성

DTLS(Datagram Transport Layer Security: 데이터그램 전송 계층 보안)를 사용하면 SSL VPN 연결을 설정하는 AnyConnect 클라이언트가 동시에 2개의 터널(SSL 터널 및 DTLS 터널)을 사용할 수 있습니다.

DTLS를 사용하면 SSL 연결과 연계된 대기 시간 및 대역폭 문제를 방지하고 패킷 지연에 민감한 실시간 애플리케이션의 성능을 개선할 수 있습니다.

시작하기 전에

DTLS가 TLS 연결을 대체하려면 DPD(Dead Peer Detection: 데드 피어 감지)를 활성화해야 합니다. DPD를 활성화하지 않은 경우, DTLS 연결에 문제가 발생하고 TLS로 대체되는 대신 연결이 종료됩니다. DPD에 대한 자세한 내용은 데드 피어 감지 구성, 254 페이지를 참조하십시오.

프로시저

단계 **1** AnyConnect VPN 연결에 대한 DTLS 옵션을 지정합니다.

a) webvpn 모드의 인터페이스에서 SSL 및 DTLS를 활성화합니다.

기본적으로 DTLS는 SSL VPN 액세스가 인터페이스에서 활성화되어 있는 경우에 활성화됩니다.

```
hostname(config)# webvpn
hostname(config-webvpn)# enable outside
```

다음과 같이 webvpn 구성 모드에서 **enable** *interface* **tls-only** 명령을 사용하여 모든 AnyConnect 클라이언트 사용자에 대해 DTLS를 비활성화합니다.

DTLS를 비활성화하는 경우, SSL VPN 연결은 SSL VPN 터널에만 연결됩니다.

```
hostname(config)# webvpn
hostname(config-webvpn)# enable outside tls-only
```

b) **port** 및 **dtls port** 명령을 사용하여 SSL 및 DTLS의 포트를 구성합니다.

```
hostname(config)# webvpn
hostname(config-webvpn)# enable outside
hostname(config-webvpn)# port 555
hostname(config-webvpn)# dtls port 556
```

단계 **2** 특정 그룹 정책에 대한 DTLS 옵션을 지정합니다.

a) 다음과 같이 그룹 정책 webvpn 또는 사용자 이름 webvpn 구성 모드에서 **anyconnect ssl dtls** 명령을 사용하여 특정 그룹 또는 사용자에 대해 DTLS를 활성화합니다.

```
hostname(config)# group-policy sales attributes
hostname(config-group-policy)# webvpn
hostname(config-group-webvpn)# anyconnect ssl dtls enable
```

b) 원하는 경우, anyconnect dtls compression 명령을 사용하여 DTLS 압축을 활성화합니다.

```
hostname(config-group-webvpn)# anyconnect dtls compression lzs
```

원격 사용자 확인 상자 표시

프로시저

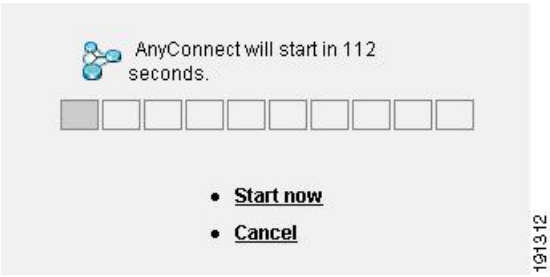
다음과 같이 그룹 정책 webvpn 또는 사용자 이름 webvpn 구성 모드에서 **anyconnect ask** 명령을 사용하여 클라이언트를 다운로드할지 묻는 확인 상자를 원격 SSL VPN 클라이언트 사용자에게 표시하도록 ASA를 활성화할 수 있습니다.

[**no**] **anyconnect ask** {**none** | **enable** [**default** {**webvpn** | } **timeout** *value*]}

- **anyconnect enable** 원격 사용자가 클라이언트를 다운로드하거나 클라이언트리스 포털 페이지로 이동하고 사용자 응답을 계속 기다릴지 묻는 확인 상자를 표시합니다.
- **anyconnect ask enable default** 클라이언트를 즉시 다운로드합니다.
- **anyconnect ask enable default webvpn** 즉시 포털 페이지로 이동합니다.
- **anyconnect ask enable default timeout** value는 원격 사용자가 클라이언트를 다운로드하거나 클라이언트리스 포털 페이지로 이동하고 클라이언트 다운로드와 같은 기본 작업을 수행하기 전에 *value*의 기간 동안 기다릴지 묻는 확인 상자를 표시합니다.
- **anyconnect ask enable default clientless timeout** value는 원격 사용자가 클라이언트를 다운로드하거나 클라이언트리스 포털 페이지로 이동하고, 클라이언트리스 포털 페이지 표시와 같은 기본 작업을 수행하기 전에 *value*의 기간 동안 기다릴지 묻는 확인 상자를 표시합니다.

아래 그림은 **default anyconnect timeout** *value* 또는 **default webvpn timeout** *value*가 구성된 경우 원격 사용자에게 표시되는 확인 상자를 보여줍니다.

그림 ***5:*** 원격 사용자에게 표시되는 ***SSL VPN*** 클라이언트 다운로드 프롬프트



예

다음 예는 사용자에게 클라이언트를 다운로드하거나 클라이언트리스 포털 페이지로 이동하고, 클라이언트를 다운로드하기 전에 응답을 *10*초 동안 기다릴지 묻는 확인 상자를 표시하도록 ASA를 구성합니다.

```
hostname(config-group-webvpn)# anyconnect ask enable default anyconnect timeout
 10
```

AnyConnect 클라이언트 프로파일 다운로드 활성화

VPN 기능이 있는 코어 클라이언트와 선택적 클라이언트 모듈에 대한 구성 설정을 포함하는 XML 파일인 AnyConnect 프로파일에서 Cisco AnyConnect Secure Mobility Client 기능을 활성화할 수 있습니다. ASA는 AnyConnect 설치 및 업데이트 시 프로파일을 구축합니다. 사용자는 프로파일을 관리하거나 수정할 수 없습니다.

ASDM 또는 ISE에서 실행하는 편리한 GUI 기반 구성 툴인 AnyConnect 프로파일 편집기를 사용하여 프로파일을 구성할 수 있습니다. Windows용 AnyConnect 소프트웨어 패키지에는 선택한 헤드엔드 디바이스에 AnyConnect 패키지를 로드하고 이 패키지를 AnyConnect 클라이언트 이미지로 지정할 때 활성화되는 편집기가 포함되어 있습니다.

또한 ASDM 또는 ISE와 통합된 프로파일 편집기 대신 사용할 수 있는 Windows용 프로파일 편집기의 독립 실행형 버전을 제공합니다. 클라이언트를 사전 배포하는 경우, 독립 실행형 프로파일 편집기를 사용하여 소프트웨어 관리 시스템을 사용하는 컴퓨터에 배포할 VPN 서비스 및 기타 모듈용으로 프로파일을 생성할 수 있습니다.

AnyConnect 클라이언트 및 해당 프로파일 편집기에 대한 자세한 내용은 해당 릴리스의 Cisco AnyConnect Secure Mobility 구성 가이드의 내용을 참조하십시오.

참고 AnyConnect 클라이언트 프로토콜은 SSL에 대해 기본값입니다. IPsec IKEv2를 활성화하려면 ASA에 IKEv2 설정을 구성하고 클라이언트 프로파일에서 기본 프로토콜로 IKEv2를 구성해야 합니다. IKEv2enabled 프로파일은 엔드포인트 컴퓨터에 배포해야 하며 그렇지 않은 경우, 클라이언트가 SSL을 사용하여 연결을 시도합니다.

프로시저

단계 **1** ASDM/ISE의 프로파일 편집기 또는 독립 실행형 프로파일 편집기를 사용하여 프로파일을 생성합니다.

단계 **2** 프로파일 파일을 tftp 또는 다른 방법을 사용하여 ASA에 있는 플래시 메모리에 로드합니다.

단계 **3** webvpn 구성 모드에서 **anyconnect profiles** 명령을 사용하여 파일을 캐시 메모리에 로드할 클라이언트 프로파일로 식별합니다.

예제:

다음 예에서는 sales_hosts.xml 및 engineering_hosts.xml 파일을 프로파일로 지정합니다.

```
asa1(config-webvpn)# anyconnect profiles sales
disk0:/sales_hosts.xml
asa1(config-webvpn)# anyconnect profiles engineering
disk0:/engineering_hosts.xml
```

이제 이 프로파일을 그룹 정책에 사용할 수 있습니다.

다음과 같이 **dir cache:stc/profiles** 명령을 사용하여 캐시 메모리에 로드된 프로파일을 볼 수 있습니다.

```
hostname(config-webvpn)# dir cache:/stc/profiles

Directory of cache:stc/profiles/

0      ----  774         11:54:41 Nov 22 2006  engineering.xml
0      ----  774         11:54:29 Nov 22 2006  sales.xml

2428928 bytes total (18219008 bytes free)
hostname(config-webvpn)#
```

단계 **4** 다음과 같이 **anyconnect profiles** 명령을 사용하여 그룹 정책 webvpn 구성 모드를 시작하고 그룹 정책에 대해 클라이언트 프로파일을 지정합니다.

예제**:**

사용 가능한 프로파일을 보려면 anyconnect profiles value 명령 뒤에 물음표(**?**)를 입력할 수 있습니다. 예를 들면 다음과 같습니다.

```
asa1(config-group-webvpn)# anyconnect profiles value ?

config-group-webvpn mode commands/options:
Available configured profile packages: engineering sales
```

다음 예에서 클라이언트 프로파일 유형이 *vpn*인 *sales* 프로파일을 사용하도록 그룹 정책을 구성합니다.

```
asa1(config-group-webvpn)# anyconnect profiles value sales type vpn
asa1(config-group-webvpn)#
```

AnyConnect 클라이언트 보류 업그레이드 활성화

Deferred Upgrade(보류 업그레이드)를 통해 AnyConnect 사용자는 클라이언트 업그레이드 다운로드를 지연시킬 수 있습니다. 클라이언트 업데이트를 사용할 수 있는 경우 AnyConnect에서 사용자에게 업데이트할지 또는 업그레이드를 보류할지 묻는 대화 상자가 열립니다. AnyConnect 프로파일 설정에서 AutoUpdate를 *Enabled(*활성화*)*로 설정하지 않으면 이 업그레이드 대화 상자가 표시되지 않습니다.

보류 업그레이드는 ASA에 사용자 지정 특성 유형 및 이름이 지정된 값을 추가한 다음 그룹 정책에서 이러한 특성을 참조 및 구성하여 활성화할 수 있습니다.

다음 사용자 지정 특성은 보류 업그레이드를 지원합니다.

표 ***10:*** 보류 업그레이드를 위한 사용자 지정 특성

사용자 지정 특성 유형	유효한 값	기본값	참고
DeferredUpdateAllowed	true false	false	값이 true이면 보류 업데이트가 활성화됩니다. 보류 업데이트가 비활성화된 경우(false) 아래 설정이 무시됩니다.

사용자 지정 특성 유형	유효한 값	기본값	참고
DeferredUpdateMinimumVersion	x.y.z	0.0.0	업데이트를 보류하기 위해 설치해야 하는 AnyConnect의 최소 버전입니다. 최소 버전 확인은 헤드엔드에서 활성화된 모든 모듈에 적용됩니다. 모든 활성화된 모듈(VPN 포함)이 설치되지 않았거나 최소 버전과 일치하지 않는 경우, 이 연결은 보류 업데이트에 적합하지 않습니다. 이 특성이 지정되지 않은 경우, 엔드포인트에 설치된 버전에 관계없이 보류 프롬프트가 표시되거나 자동으로 해제됩니다.
DeferredUpdateDismissTimeout	0-300 (초)	none(비활성화됨)	보류 업그레이드 프롬프트가 자동으로 해제될 때까지 표시되는 시간(초)입니다. 이 특성은 보류 업데이트 프롬프트가 표시될 예정인 경우에만 적용됩니다(최소 버전 특성이 먼저 평가됨). 이 특성을 설정하지 않은 경우, 자동 해제 기능이 비활성화되고 사용자가 응답할 때까지 대화상자가 표시됩니다(필요시). 이 특성을 0으로 설정하면 자동 보류 또는 업그레이드가 다음에 기초하여 강제로 적용됩니다. • DeferredUpdateMinimumVersion의 설치된 버전 및 값 • DeferredUpdateDismissResponse의 값
DeferredUpdateDismissResponse	defer update	update	DeferredUpdateDismissTimeout 발생 시 적용

프로시저

단계 **1** 다음과 같이 webvpn 구성 모드에서 **anyconnnect-custom-attr** 명령을 사용하여 맞춤형 속성 유형을 생성합니다.

[**no**] **anyconnect-custom-attr** *attr-type* [**description** *description*]

예제**:**

다음 예는 사용자 지정 특성 유형인 DeferredUpdateAllowed and DeferredUpdateDismissTimeout을 추가하는 방법을 보여줍니다.

```
hostame(config-webvpn)# anyconnect-custom-attr DeferredUpdateAllowed
description Indicates if the deferred update feature is enabled or not
hostame(config-webvpn)# anyconnect-custom-attr DeferredUpdateDismissTimeout
```

단계 **2** 다음과 같이 전역 구성 모드에서 **anyconnect-custom-data** 명령을 사용하여 맞춤형 속성에 대해 이름이 지정된 값을 추가합니다.

[**no**] **anyconnect-custom-data** *attr-type attr-name attr-value*

예제**:**

다음 예는 맞춤형 속성 유형인 DeferredUpdateDismissTimeout과 DeferredUpdateAllowed 활성화를 위해 이름이 지정된 값을 추가하는 방법을 보여줍니다.

```
hostname(config)# anyconnect-custom-data DeferredUpdateDismissTimeout
def-timeout 150
hostname(config)# anyconnect-custom-data DeferredUpdateAllowed
def-allowed true
```

단계 **3** 다음과 같이 **anyconnect-custom** 명령을 사용하여 그룹 정책에 맞춤형 속성의 이름이 지정된 값을 추가하거나 제거합니다.

- **anyconnect-custom** *attr-type* **value** *attr-name*
- **anyconnect-custom** *attr-type* **none**
- **no anyconnect-custom** *attr-type*

예제**:**

다음 예는 sales라는 이름의 그룹 정책에 대해 보류 업데이트를 활성화하고 시간 제한을 150초로 설정하는 방법을 보여줍니다.

```
hostname(config)# group-policy sales attributes
hostname(config-group-policy)# anyconnect-custom DeferredUpdateAllowed
value def-allowed
hostname(config-group-policy)# anyconnect-custom DeferredUpdateDismissTimeout
value def-timeout
```

DSCP 보존 활성화

다른 맞춤형 속성을 설정하면 DTLS 연결 전용으로 Windows 또는 OS X 플랫폼에서 DSCP(Differentiated Services Code Point)를 제어할 수 있습니다. DSCP 보존을 활성화하는 경우 디바이스가 레이턴시에 민감한 트래픽의 우선순위를 지정할 수 있습니다. 라우터는 이 우선순위가 설정되어 있는지를 고려하며 우선순위가 지정된 트래픽을 표시하여 아웃바운드 연결 품질을 개선합니다.

프로시저

단계 **1** 다음과 같이 webvpn 구성 모드에서 **anyconnect-custom-attr** 명령을 사용하여 맞춤형 속성 유형을 생성합니다.

[no] anyconnect-custom-attr DSCPPreservationAllowed description - DTLS 연결 전용으로 **Windows** 또는 **OS X** 플랫폼에서 **DSCP(Differentiated Services Code Point)** 제어하도록 설정

단계 **2** 다음과 같이 전역 구성 모드에서 **anyconnect-custom-data** 명령을 사용하여 사용자 지정 특성에 대해 이름이 지정된 값을 추가합니다.

[no] anyconnect-custom-data DSCPPreservationAllowed true

참고 AnyConnect는 기본적으로 DSCP 보존을 수행합니다(true). DSCP 보존을 비활성화하려면 헤드엔드에서 맞춤형 속성을 false로 설정하고 연결을 다시 시작합니다.

AnyConnect 클라이언트 추가 기능 활성화

다운로드 시간을 최소화하기 위해 클라이언트는 ASA 또는 ISE에서 필요한 코어 모듈의 다운로드만 요청합니다. AnyConnect 클라이언트에 대해 추가 기능을 사용할 수 있으므로 이 기능을 사용하려면 원격 클라이언트를 업데이트해야 합니다.

새로운 기능을 활성화하려면 다음과 같이 그룹 정책 webvpn 또는 사용자 이름 webvpn 구성 모드에서 **anyconnect modules** 명령을 사용하여 새로운 모듈 이름을 지정해야 합니다.

[**no**]**anyconnect modules** {**none** | **value** *string*}

문자열이 여러 개인 경우 쉼표로 구분하십시오.

로그온 전 시작 활성화

SBL(Start Before Logon: 로그온 전 시작)을 통해 Windows PC에 설치된 AnyConnect 클라이언트에 대해 로그인 스크립트, 비밀번호 캐싱, 드라이브 매핑 등을 사용할 수 있습니다. SBL을 위해서는 AnyConnect 클라이언트에 대해 GINA(Graphical Identification and Authentication: 그래픽 식별 및 인증)를 활성화하는 모듈을 다운로드하도록 ASA를 활성화해야 합니다. 다음 절차는 SBL을 활성화하는 방법을 보여줍니다.

프로시저

단계 **1** 그룹 정책 webvpn 또는 사용자 이름 webvpn 구성 모드에서 **anyconnect modules** *vpngina* 명령을 사용하여 특정 그룹 또는 사용자에게 VPN 연결을 위해 GINA 모듈을 다운로드하도록 ASA를 활성화합니다.

예제**:**

다음 예에서 사용자는 그룹 정책 *telecommuters*에 대해 그룹 정책 특성 모드를 시작하고 그룹 정책에 대해 webvpn 구성 모드를 시작하며 문자열 *vpngina*를 지정합니다.

```
hostname(config)# group-policy telecommuters attributes
hostname(config-group-policy)# webvpn
hostame(config-group-webvpn)#anyconnect modules value vpngina
```

단계 **2** 클라이언트 프로파일 파일(AnyConnectProfile.tmpl)의 사본을 검색합니다.

단계 **3** SBL이 활성화되도록 지정하려면 프로파일 파일을 수정합니다. 아래 예는 Windows용 프로파일 파일(AnyConnectProfile.tmpl)과 관련된 부분을 보여줍니다.

```
<Configuration>
    <ClientInitialization>
        <UseStartBeforeLogon>false</UseStartBeforeLogon>
    </ClientInitialization>
```

<UseStartBeforeLogon> 태그는 클라이언트에서 SBL 사용 여부를 결정합니다. SBL을 설정하려면 *false*를 *true*로 바꿉니다. 아래 예는 SBL이 설정되어 있는 상태의 태그를 보여줍니다.

```
<ClientInitialization>
        <UseStartBeforeLogon>true</UseStartBeforeLogon>
    </ClientInitialization>
```

단계 **4** webvpn 구성 모드에서 **profile** 명령을 사용하여 ASA에서 AnyConnectProfile.tmpl에 대한 변경 사항을 저장하고 그룹 또는 사용자에 대한 프로파일 파일을 업데이트합니다. 예를 들면 다음과 같습니다.

```
asa1(config-webvpn)#anyconnect profiles sales disk0:/sales_hosts.xml
```

AnyConnect 사용자 메시지의 언어 변환

ASA는 브라우저 기반 클라이언트리스 SSL VPN 연결을 시작하는 사용자에게 표시되는 포털 및 화면을 비롯해 Cisco AnyConnect VPN 클라이언트 사용자에게 표시되는 인터페이스에 대한 언어 변환 기능을 제공합니다.

이 섹션은 사용자 메시지를 변환하도록 ASA를 구성하는 방법에 대해 설명합니다.

언어 변환 이해

원격 사용자에게 표시되는 기능 영역 및 메시지는 변환 도메인으로 구성됩니다. Cisco AnyConnect VPN 클라이언트의 사용자 인터페이스에 표시되는 모든 메시지는 AnyConnect 도메인에 있습니다.

ASA에 대한 소프트웨어 이미지 패키지에는 AnyConnect 도메인에 대한 변환 테이블 템플릿이 포함되어 있습니다. 제공하는 URL에서 템플릿의 XML 파일을 생성하는 템플릿을 내보낼 수 있습니다. 이 파일의 메시지 필드는 비어 있습니다. 플래시 메모리에 있는 새로운 변환 테이블 개체를 생성하기 위해 이 메시지를 수정하고 템플릿을 가져올 수 있습니다.

또한 기존의 변환 테이블을 내보낼 수 있습니다. 생성한 XML 파일에 이전에 수정한 메시지가 표시됩니다. 동일한 언어 이름으로 이 XML 파일을 다시 가져오면 새 버전의 변환 테이블 개체가 생성되어 이전 메시지를 덮어씁니다. AnyConnect 도메인에 대한 변환 테이블 변경사항은 AnyConnect 클라이언트 사용자에게 바로 표시됩니다.

변환 테이블 생성

다음 절차는 AnyConnect 도메인에 대한 변환 테이블을 생성하는 방법을 설명합니다.

프로시저

단계 **1** 특권 EXEC 모드에서 **export webvpn translation-table** 명령을 사용하여 변환 테이블 템플릿을 컴퓨터에 내보냅니다.

다음 예에서 **show import webvpn translation-table** 명령은 사용 가능한 변환 테이블 템플릿과 테이블을 보여줍니다.

```
hostname# show import webvpn translation-table
Translation Tables' Templates:
customization
AnyConnect

PortForwarder
url-list
webvpn
Citrix-plugin
RPC-plugin
Telnet-SSH-plugin
VNC-plugin

Translation Tables:
```

그런 다음 사용자는 AnyConnect 변환 도메인에 대한 변환 테이블을 내보냅니다. 다음과 같이 생성된 XML 파일의 파일 이름은 *client*로 지정되고 빈 메시지 필드를 포함합니다.

```
hostname# export webvpn translation-table AnyConnect
template tftp://209.165.200.225/client
```

다음 예에서 사용자는 템플릿에서 이전에 가져온 *zh*라는 이름의 변환 테이블을 내보냅니다. zh는 Microsoft Internet Explorer에서 중국어의 약어입니다.

```
hostname# export webvpn translation-table customization
language zh tftp://209.165.200.225/chinese_client
```

단계 **2** 변환 테이블 XML 파일을 수정합니다. 다음 예는 AnyConnect 템플릿의 일부를 보여줍니다. 이 출력의 끝부분에는 클라이언트가 VPN 연결을 설정할 때 AnyConnect 클라이언트 GUI에 표시되는 *Connected* 메시지에 대한 메시지 ID 필드(msgid) 및 메시지 문자열 필드(msgstr)가 포함되어 있습니다. 전체 템플릿에는 다음과 같이 여러 쌍의 메시지 필드가 포함되어 있습니다.

```
# SOME DESCRIPTIVE TITLE.
# Copyright (C) YEAR THE PACKAGE'S COPYRIGHT HOLDER
# This file is distributed under the same license as the PACKAGE package.
# FIRST AUTHOR <EMAIL@ADDRESS>, YEAR.
#
#, fuzzy
msgid ""
msgstr ""
"Project-Id-Version: PACKAGE VERSION\n"
"Report-Msgid-Bugs-To: \n"
"POT-Creation-Date: 2006-11-01 16:39-0700\n"
"PO-Revision-Date: YEAR-MO-DA HO:MI+ZONE\n"
"Last-Translator: FULL NAME <EMAIL@ADDRESS>\n"
```

```
"Language-Team: LANGUAGE <LL@li.org>\n"
"MIME-Version: 1.0\n"
"Content-Type: text/plain; charset=CHARSET\n"
"Content-Transfer-Encoding: 8bit\n"

#: C:\cygwin\home\<user>\cvc\main\Api\AgentIfc.cpp:23
#: C:\cygwin\home\<user>\cvc\main\Api\check\AgentIfc.cpp:22
#: C:\cygwin\home\<user>\cvc\main\Api\save\AgentIfc.cpp:23
#: C:\cygwin\home\<user>\cvc\main\Api\save\AgentIfc.cpp~:20
#: C:\cygwin\home\<user>\cvc\main\Api\save\older\AgentIfc.cpp:22
msgid "Connected"
msgstr ""
```

msgid에는 기본 변환이 포함됩니다. msgid 다음에 오는 msgstr은 변환을 제공합니다. 변환을 생성하려면 msgstr 문자열의 따옴표 사이에 변환된 텍스트를 입력하십시오. 예를 들어 “Connected” 메시지를 스페인어로 변환하려면 따옴표 사이에 스페인어 텍스트를 삽입하십시오.

```
msgid "Connected"
msgstr "Conectado"
```

파일을 저장하십시오.

단계 **3** 특권 EXEC 모드에서 **import webvpn translation-table** 명령을 사용하여 변환 테이블을 가져옵니다. 새 변환 테이블의 이름은 브라우저와 호환되는 언어의 약어로 지정하십시오.

다음 예에서 XML 파일은 미국에서 사용되는 스페인어에 대해 Microsoft Internet Explorer에서 사용하는 약어인 *es-us*로 가져옵니다.

```
hostname# import webvpn translation-table AnyConnect
language es-us tftp://209.165.200.225/client
hostname# !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
hostname# show import webvpn translation-table
Translation Tables' Templates:
AnyConnect
PortForwarder

customization
keepout
url-list
webvpn
Citrix-plugin
RPC-plugin
Telnet-SSH-plugin
VNC-plugin

Translation Tables:
es-us AnyConnect
```

변환 테이블 제거

더 이상 변환 테이블이 필요하지 않은 경우에는 변환 테이블을 제거할 수 있습니다.

프로시저

단계 **1** 기존의 변환 테이블을 나열합니다.

다음 예에서 **show import webvpn translation-table** 명령은 사용 가능한 변환 테이블 템플릿과 테이블을 보여줍니다. 다양한 테이블을 프랑스어(fr), 일본어(ja), 러시아어(ru)로 사용할 수 있습니다.

```
hostname# show import webvpn translation-table
Translation Tables' Templates:
  AnyConnect
  PortForwarder
  banners
  csd
  customization
  url-list
  webvpn
Translation Tables:
  fr                    PortForwarder
  fr                    AnyConnect
  fr                    customization
  fr                    webvpn
  ja                    PortForwarder
  ja                    AnyConnect
  ja                    customization
  ja                    webvpn
  ru                    PortForwarder
  ru                    customization
  ru                    webvpn
```

단계 **2** 원치 않는 변환 테이블을 제거합니다.

revert webvpn translation-table *translationdomain* **language** *language*

여기서 *Translationdomain*은 위에 표시된 변환 테이블 목록의 오른쪽에 나열된 도메인이고, *language*는 2자로 된 언어 이름입니다.

각 테이블은 개별적으로 제거해야 합니다. 지정된 언어에 대한 모든 테이블을 하나의 명령으로 제거할 수는 없습니다.

예를 들어, AnyConnect의 프랑스어 변환 테이블을 제거하려는 경우 다음 명령을 사용합니다.

```
ciscoasa# revert webvpn translation-table anyconnect language fr
ciscoasa#
```

고급 **AnyConnect SSL** 기능 구성

다음 섹션은 AnyConnect SSL VPN 연결을 세부적으로 조정하는 고급 기능에 대해 설명합니다.

키 재설정 활성화

ASA 및 AnyConnect 클라이언트가 SSL VPN 연결에서 키 재설정을 수행하는 경우, 암호화 키 및 초기화 벡터를 재협상하므로 연결 보안이 강화됩니다.

특정 그룹 또는 사용자를 위한 SSL VPN 연결에서 키 재설정을 수행하도록 클라이언트를 활성화하려면 그룹 정책 또는 사용자 이름 webvpn 모드에서 **anyconnect ssl** rekey 명령을 사용합니다.

[no] anyconnect ssl rekey {**method** {**new-tunnel** | **none** | **ssl**} | **time** *minutes*}

- **method new-tunnel** 키 재설정 동안 클라이언트가 새 터널을 설정함을 지정합니다.
- **method ssl** 키 재설정 동안 클라이언트가 새 터널을 설정함을 지정합니다.
- **method none** rekey를 비활성화합니다.
- **time***minutes*는 세션 시작 또는 마지막 키 재설정부터 키 재설정이 발생할 때까지의 시간(분)을 1분에서 10080분(1주)의 범위에서 지정합니다.

참고 rekey 방식을 **ssl** 또는 **new-tunnel**로 구성하면 rekey 과정에서 SSL 재협상이 일어나지 않고 클라이언트가 새 터널을 설정합니다. **anyconnect ssl rekey** 명령 기록은 명령 참조를 참고하십시오.

다음 예에서 클라이언트는 기존 그룹 정책인 *sales*에 대해 세션이 다시 시작되고 30분 후에 키 재설정 동안 SSL과 재협상하도록 구성됩니다.

```
hostname(config)# group-policy sales attributes
hostname(config-group-policy)# webvpn
hostname(config-group-webvpn)# anyconnect ssl rekey method ssl
hostname(config-group-webvpn)# anyconnect ssl rekey time 30
```

데드 피어 감지 구성

DPD(Dead Peer Detection: 데드 피어 감지)를 통해 ASA(게이트웨이) 또는 클라이언트는 피어가 응답하지 않으며 연결이 실패했음을 신속하게 감지합니다. DPD(Dead Peer Detection: 데드 피어 감지)를 활성화하고 AnyConnect 클라이언트 또는 ASA 게이트웨이가 DPD를 수행하는 빈도를 설정하려면 다음을 수행합니다.

시작하기 전에

- 이 기능은 ASA 게이트웨이 및 AnyConnect SSL VPN 클라이언트 간의 연결에만 적용됩니다. 이 기능은 IPsec과 함께 작동하지 않습니다. DPD는 패딩을 허용하지 않는 표준 구현을 기반으로 하기 때문입니다. 클라이언트리스 SSL VPN은 지원되지 않습니다.
- DTLS를 활성화하면 DPD(Dead Peer Detection: 데드 피어 감지)도 활성화됩니다. DPD는 실패한 DTLS 연결을 활성화하여 TLS로 대체합니다. 그렇지 않으면 연결이 종료됩니다.
- ASA에서 DPD가 활성화되면 OMTU(Optimal MTU) 기능을 사용하여 클라이언트가 DTLS 패킷을 전달할 수 있는 최대 엔드포인트 MTU를 찾을 수 있습니다. 패딩된 DPD 패킷을 최대 MTU로 보내 OMTU를 구현하십시오. 헤드 엔드에서 올바른 페이로드 에코가 수신되면 해당 MTU 크기

가 수락됩니다. 그렇지 않을 경우 MTU 크기가 줄어들고, 프로토콜에 허용되는 최소 MTU 크기에 도달할 때까지 프로브가 다시 전송됩니다.

프로시저

단계 **1** 원하는 그룹 정책으로 이동합니다.

그룹 정책 또는 사용자 이름 webvpn 모드를 입력합니다.

```
hostname(config)# group-policy group-policy-name  attributes
hostname(config-group-policy)# webvpn
hostname(config-group-webvpn)#
```

아니면

```
hostname# username username attributes
hostname(config-username)# webvpn
hostname (config-username-webvpn #
```

단계 **2** 게이트웨이 측 탐지를 설정합니다.

[**no**] **anyconnect dpd-interval** {[**gateway** {*seconds* | **none**}] 명령을 사용합니다.

gateway는 ASA를 의미합니다. DPD를 활성화하고 ASA가 DPD 테스트를 수행하는 빈도를 30초(기본값)에서 3600초(1시간) 범위로 지정할 수 있습니다. 값을 300으로 지정하는 것이 좋습니다.

none을 지정하면 ASA가 수행하는 DPD 테스트가 비활성화됩니다. **no anyconnect dpd-interval** 을 사용하여 구성에서 이 명령을 제거합니다.

단계 **3** 클라이언트 측 탐지를 설정합니다.

[**no**] **anyconnect dpd-interval** {[**client** {*seconds* | **none**}]} 명령을 사용합니다.

client는 AnyConnect 클라이언트를 의미합니다. DPD를 활성화하고 클라이언트가 DPD 테스트를 수행하는 빈도를 30초(기본값)에서 3600초(1시간) 범위로 지정할 수 있습니다. 값을 300으로 지정하는 것이 좋습니다.

client none을 지정하면 클라이언트가 수행하는 DPD가 비활성화됩니다. **no anyconnect dpd-interval** 을 사용하여 구성에서 이 명령을 제거합니다.

예

다음 예는 기존 그룹 정책인 *sales*에 대해 ASA가 DPD를 수행하는 빈도를 30초로 구성하며 클라이언트가 DPD를 수행하는 빈도를 10초로 설정합니다.

```
hostname(config)# group-policy sales attributes
hostname(config-group-policy)# webvpn
hostname(config-group-webvpn)# anyconnect dpd-interval gateway 30
hostname(config-group-webvpn)# anyconnect dpd-interval client 10
```

킵얼라이브 활성화

킵얼라이브 메시지 빈도를 조정함으로써 디바이스에서 연결 유휴 가능 시간을 제한하는 경우에도 프록시, 방화벽 또는 NAT 디바이스를 통해 SSL VPN 연결이 열려 있도록 할 수 있습니다. 또한 이 빈도를 조정함으로써 원격 사용자가 소켓 기반 애플리케이션(예: Microsoft Outlook, Microsoft Internet Explorer)을 능동적으로 실행하고 있지 않을 때 클라이언트의 연결이 끊겼다가 다시 연결되는 현상을 방지할 수 있습니다.

킵얼라이브는 기본적으로 활성화되어 있습니다. 킵얼라이브를 비활성화할 경우 장애 조치 상황에서 SSL VPN 클라이언트 세션이 대기 디바이스에 전달되지 않습니다.

킵얼라이브 메시지 빈도를 설정하려면 다음과 같이 그룹 정책 webvpn 또는 사용자 이름 webvpn 구성 모드에서 **keepalive** 명령을 사용하거나, **no** 형식의 명령을 사용하여 구성에서 명령을 제거하고 값을 상속하도록 합니다.

[**no**] **anyconnect ssl keepalive** {**none** | *seconds*}

- **none** 클라이언트 킵얼라이브 메시지를 비활성화합니다.
- *seconds*는 킵얼라이브 메시지를 전송하도록 클라이언트를 활성화하고 메시지 빈도를 15초에서 600초 범위로 지정합니다.

다음 예에서 ASA는 클라이언트에서 기존 그룹 정책인 *sales*에 대해 300초(5분) 빈도로 킵얼라이브 메시지를 전송하도록 구성됩니다.

```
hostname(config)# group-policy sales attributes
hostname(config-group-policy)# webvpn
hostname(config-group-webvpn)# anyconnect ssl keepalive 300
```

압축 사용

압축은 낮은 대역폭 연결을 위해 전송 중인 패킷의 크기를 줄여 ASA와 클라이언트 간의 통신 성능을 향상시킵니다. 기본적으로 모든 SSL VPN 연결에 대한 압축은 ASA에서 특정 그룹 또는 사용자를 위해 전역 수준으로 활성화되어 있습니다.

참고 광대역 연결에서 압축을 구현하는 경우 손실이 적은 연결을 사용한다는 사실을 신중하게 고려해야 합니다. 이러한 이유로 광대역 연결에서는 압축이 기본적으로 활성화되어 있지 않습니다.

전역 구성 모드에서 **compression** 명령을 사용하여 압축을 전역으로 설정해야 하며 이후에 그룹 정책 및 사용자 이름 webvpn 모드에서 **anyconnect ssl compression** 명령을 사용하여 특정 그룹 또는 사용자에 대해 압축을 설정할 수 있습니다.

전역으로 압축 변경

전역 압축 설정을 변경하려면 전역 구성 모드에서 다음과 같은 anyconnect ssl **compression** 명령을 사용합니다. 구성에서 이 명령을 제거하려면 **no** 형식의 명령을 사용합니다.

다음 예에서 모든 SSL VPN 연결에 대해 압축이 전역으로 비활성화됩니다.

```
hostname(config)# no compression
```

그룹 및 사용자에 대한 압축 변경

특정 그룹 또는 사용자에 대한 압축을 변경하려면 다음과 같이 그룹 정책 및 사용자 이름 webvpn 모드에서 anyconnect ssl compression 명령을 사용합니다.

[**no**] **anyconnect ssl compression** {**deflate** | **none**}

기본적으로 그룹 및 사용자에 대해 SSL 압축이 *deflate*(활성화됨)로 설정됩니다.

구성에서 **anyconnect ssl compression** 명령을 제거하고 전역 설정에서 값을 상속받도록 하려면 **no** 형식의 다음 명령을 사용합니다.

다음은 group-policy sales에 대해 압축을 비활성화하는 예입니다.

```
hostname(config)# group-policy sales attributes
hostname(config-group-policy)# webvpn
hostname(config-group-webvpn)# no anyconnect ssl compression none
```

MTU 크기 조정

다음과 같이 그룹 정책 webvpn 또는 사용자 이름 webvpn 구성 모드에서 **anyconnect mtu** 명령을 사용하여 클라이언트가 설정한 SSL VPN 연결에 대해 MTU 크기(576바이트부터 1406바이트까지)를 조정할 수 있습니다.

[**no**] **anyconnect mtu** *size*

이 명령은 AnyConnect 클라이언트에만 영향을 줍니다. 레거시 Cisco SSL VPN 클라이언트는 다른 MTU 크기로 조정할 수 없습니다. 또한, SSL에 설정된 클라이언트 연결 및 DTLS를 통해 SSL에 설정된 클라이언트 연결도 이 명령의 영향을 받습니다.

기본 그룹 정책에서 이 명령에 대한 기본값은 **no anyconnect mtu**입니다. MTU 크기는 연결 시 사용하는 인터페이스의 MTU에 기초하여 IP/UDP/DTLS 오버헤드를 뺀 값으로 자동으로 조정됩니다.

ISE Posture AnyConnect 모듈을 실행하는 경우, 예를 들어 "보안 게이트웨이에서 전송된 MTU 구성이 너무 작습니다."라는 메시지를 받을 수 있습니다. **anyconnect mtu 1200**을 **anyconnect ssl df-bit-ignore disable**과 함께 입력하면 이러한 시스템 스캔 오류를 방지할 수 있습니다.

예

다음은 그룹 정책 telecommuters에 대해 MTU 크기를 1200바이트로 구성하는 예입니다.

```
hostname(config)# group-policy telecommuters attributes
hostname(config-group-policy)# webvpn
hostname(config-group-webvpn)# anyconnect mtu 1200
```

AnyConnect 클라이언트 이미지 업데이트

다음 절차를 통해 ASA에서 클라이언트 이미지를 업데이트할 수 있습니다.

프로시저

단계 1 특권 EXEC 모드에서 **copy** 명령을 사용하거나 다른 방법을 사용하여 ASA에 새 클라이언트 이미지를 복사합니다.

단계 2 새 클라이언트 이미지 파일에 이미 로드한 파일과 동일한 파일 이름이 있는 경우, 이 구성에서 **anyconnect image** 명령을 다시 입력합니다. 새 파일 이름이 다른 경우 [**no**]**anyconnect image**image 명령을 사용하여 기존 파일을 제거합니다. 그런 다음 **anyconnect image** 명령을 사용하여 이미지에 순서를 할당하고 ASA가 새 이미지를 로드하도록 합니다.

IPv6 VPN 액세스 활성화

IPv6 액세스를 구성하려면 명령행 인터페이스를 사용해야 합니다. ASA의 릴리스 9.0(x)은 SSL 및 IKEv2/IPsec 프로토콜을 사용하여 외부 인터페이스에 IPv6 VPN 연결 지원을 추가합니다.

SSL VPN 연결 활성화의 일부로 **ipv6 enable** 명령을 사용하여 IPv6 액세스를 활성화합니다. 다음은 외부 인터페이스에서 IPv6를 활성화하는 IPv6 연결에 대한 예입니다.

```
hostname(config)# interface GigabitEthernet0/0
hostname(config-if)# ipv6 enable
```

IPV6 SSL VPN을 활성화하려면 다음과 같이 일반적인 작업을 수행하십시오.

1. 외부 인터페이스에서 IPv6를 활성화합니다.
2. 내부 인터페이스에서 IPv6 및 IPv6 주소를 활성화합니다.
3. 클라이언트가 할당한 IP 주소에 대해 IPv6 주소 로컬 풀을 구성합니다.
4. IPv6 터널 기본 게이트웨이를 구성합니다.

프로시저

단계 1 다음과 같이 인터페이스를 구성합니다.

```
interface GigabitEthernet0/0
 nameif outside
 security-level 0
 ip address 192.168.0.1 255.255.255.0
 ipv6 enable      ; Needed for IPv6.
!
interface GigabitEthernet0/1
 nameif inside
 security-level 100
 ip address 10.10.0.1 255.255.0.0
 ipv6 address 2001:DB8::1/32        ; Needed for IPv6.
 ipv6 enable      ; Needed for IPv6.
```

단계 2 다음과 같이 'ipv6 local pool'(IPv6 주소 할당에 사용됨)을 구성합니다.

```
ipv6 local pool ipv6pool 2001:DB8:1:1::5/32 100     ; Use your IPv6 prefix here
```

참고 ASA에서 내부 주소 풀을 생성하거나 ASA에 있는 로컬 사용자에게 전용 주소를 할당하여 IPv4 주소, IPv6 주소 또는 두 주소 모두를 AnyConnect 클라이언트에 할당하도록 ASA를 구성할 수 있습니다.

단계 **3** 다음과 같이 터널 그룹 정책(또는 그룹 정책)에 ipv6 주소 풀을 추가합니다.

```
tunnel-group YourTunGrp1 general-attributes  ipv6-address-pool ipv6pool
```

참고 IPv4 주소 풀도 이 위치에 구성해야 합니다('address-pool' 명령 사용).

단계 **4** 다음과 같이 IPv6 터널 기본 게이트웨이를 구성합니다.

```
ipv6 route inside ::/0 X:X:X:X::X tunneled
```

AnyConnect 연결 모니터링

활성 세션에 대한 정보를 보려면 **show vpn-sessiondb** 명령을 사용하십시오.

명령어	목적
show vpn-sessiondb	활성 세션에 대한 정보를 표시합니다.
vpn-sessiondb logoff	VPN 세션에서 로그오프합니다.
show vpn-sessiondb anyconnect	OSPFv3 세션 정보를 표시하도록 VPN 세션 요약을 개선합니다.
show vpn-sessiondb ratio encryption	Suite B 알고리즘(AES-GCM-128, AES-GCM-192, AES-GCM-256, AES-GMAC-128 등)을 위한 터널 수 및 백분율을 표시합니다.

예

Inactivity 필드에 AnyConnect 세션의 연결이 끊어진 이후 경과한 시간이 표시됩니다. 세션이 활성 상태인 경우, 이 필드에 00:00m:00s가 나타납니다.

```
hostname# show vpn-sessiondb

Session Type: SSL VPN Client

Username     : lee
Index        : 1                     IP Addr      : 209.165.200.232
Protocol     : SSL VPN Client        Encryption   : 3DES
Hashing      : SHA1                  Auth Mode    : userPassword
TCP Dst Port : 443                   TCP Src Port : 54230
```

```
Bytes Tx     : 20178                  Bytes Rx     : 8662
Pkts Tx      : 27                     Pkts Rx      : 19
Client Ver   : Cisco STC 1.1.0.117
Client Type  : Internet Explorer
Group        : DfltGrpPolicy
Login Time   : 14:32:03 UTC Wed Mar 20 2007
Duration     : 0h:00m:04s
Inactivity    : 0h:00m:04s
Filter Name  :

hostname# vpn-sessiondb logoff
INFO: Number of sessions of type "" logged off : 1

hostname# vpn-sessiondb logoff name tester
Do you want to logoff the VPN session(s)? [confirm]
INFO: Number of sessions with name "tester" logged off : 1
```

AnyConnect VPN 세션 로그오프

모든 VPN 세션에서 로그오프하려면 전역 구성 모드에서 **vpn-sessiondb logoff** 명령을 사용합니다.

다음은 모든 VPN 세션에서 로그오프하는 예입니다.

```
hostname# vpn-sessiondb logoff
INFO: Number of sessions of type “” logged off : 1
```

이름 인수 또는 인덱스 인수 중 하나를 사용하여 개별 세션을 로그오프할 수 있습니다.

vpn-sessiondb logoff name *name*
vpn-sessiondb logoff index *index*

최장 시간 동안 비활성 상태인 세션은 유휴로 표시되고 자동으로 로그오프되므로 라이센스 용량에 도달하지 않고 새 사용자가 로그인할 수 있습니다. 세션이 나중에 재개되면 비활성 목록에서 제거됩니다.

show vpn-sessiondb anyconnect 명령의 출력에서 사용자 이름과 인덱스 번호(클라이언트 이미지의 순서에 따라 설정) 모두를 찾을 수 있습니다. 다음은 사용자 이름이 *lee*이고 인덱스 번호가 *1*인 예를 보여줍니다.

```
hostname# show vpn-sessiondb anyconnect

Session Type: AnyConnect

Username     : lee                    Index        : 1
Assigned IP  : 192.168.246.1           Public IP    : 10.139.1.2
Protocol     : AnyConnect-Parent SSL-Tunnel DTLS-Tunnel
License      : AnyConnect Premium
Encryption   : RC4 AES128             Hashing      : SHA1
Bytes Tx     : 11079                  Bytes Rx     : 4942
Group Policy : EngPolicy            Tunnel Group : EngGroup
Login Time   : 15:25:13 EST Fri Jan 28 2011
Duration     : 0h:00m:15s
Inactivity   : 0h:00m:00s
NAC Result   : Unknown
VLAN Mapping : N/A                   VLAN         : none
```

다음은 **vpn-session-db logoff** 명령의 **name** 옵션을 사용하여 세션을 종료하는 예입니다.

```
hostname# vpn-sessiondb logoff name lee
Do you want to logoff the VPN session(s)? [confirm]
INFO: Number of sessions with name “lee” logged off : 1

hostname#
```

AnyConnect 연결의 기능 기록

다음 표에는 이 기능에 대한 릴리스 기록이 나와 있습니다.

표 ***11: AnyConnect*** 연결의 기능 기록

기능 이름	릴리스	기능 정보
AnyConnect 연결	7.2(1)	다음 명령은 새로 도입되었거나 수정되었습니다. authentication eap-proxy, authentication ms-chap-v1, authentication ms-chap-v2, authentication pap, l2tp tunnel hello, vpn-tunnel-protocol l2tp-ipsec
IPsec IKEv2	8.4(1)	IKEv2가 AnyConnect 및 LAN-to-LAN에 대한 IPsec IKEv2 연결을 지원하도록 추가되었습니다.

10 장

AnyConnect HostScan

AnyConnect Posture 모듈은 호스트에 설치된 운영 체제, 악성코드 차단 및 방화벽 소프트웨어를 식별하는 기능을 AnyConnect Secure Mobility Client에 제공합니다. HostScan 애플리케이션은 이 정보를 수집합니다. 상태 진단의 경우 HostScan을 호스트에서 설치해야 합니다.

HostScan에 대한 사전 요구 사항

Posture 모듈이 있는 AnyConnect Secure Mobility Client는 다음과 같은 최소 ASA 구성 요소가 필요합니다.

- ASA 8.4
- ASDM 6.4

이러한 AnyConnect 기능을 사용하려면 Posture 모듈을 설치해야 합니다.

- SCEP 인증
- AnyConnect Telemetry 모듈

Posture 모듈은 다음 플랫폼 중 하나에 설치할 수 있습니다.

- Windows 7, 8, 8.1, 10, 10 RS1, RS2, & RS3 x86(32비트) 및 x64(64비트)
- macOS 10.11, 10.12 및 10.13

- Linux Red Hat 6, 7 및 Ubuntu 14.04(LTS), 16.04(LTS)(64비트 전용)

Host Scan에 대한 라이센싱

다음은 Posture 모듈에 대한 AnyConnect 라이센싱 요건입니다.

- 기본 HostScan에 대한 AnyConnect Apex
- AnyConnect Plus는 교정에 필요합니다.

HostScan 패키징

HostScan 패키지를 ASA에 독립 실행형 패키지로 로드할 수 있습니다(**hostscan-**버전**.pkg**). 이 파일에는 HostScan 소프트웨어뿐만 아니라 HostScan 라이브러리 및 지원 차트가 포함되어 있습니다.

HostScan 설치 또는 업그레이드

HostScan 패키지를 설치 또는 업그레이드하고 ASA에 대한 명령행 인터페이스를 사용하여 이 패키지를 활성화하려면 다음 절차를 수행하십시오.

시작하기 전에

참고 HostScan 버전 4.3.x 이전 버전에서 HostScan 4.6.x 이상으로 업그레이드를 시도 중인 경우, 모든 기존 AV/AS/FW DAP 정책 및 이전에 설정한 LUA 스크립트가 HostScan 4.6.x 이상과 호환되지 않는다는 사실 때문에 오류 메시지를 받게 됩니다.

구성에 맞게 수행해야 하는 일회성 마이그레이션 절차가 있습니다. 이 절차는 이 구성을 저장하기 전에 HostScan 4.4.x와 호환되도록 구성을 마이그레이션하도록 이 대화 상자를 그대로 둡니다. 자세한 내용을 보려면 이 절차를 중단하고 AnyConnect HostScan 4.3.x를 4.6.x로 마이그레이션하는 가이드를 참조하십시오. 간략하게 설명하자면, 마이그레이션은 호환되지 않는 AV/AS/FW 속성을 검토하고 수동으로 삭제한 다음 LUA 스크립트를 검토하고 재작성하기 위해 ASDM DAP 정책 페이지로 이동하는 작업과 관련이 있습니다.

- ASA에 로그온하고 전역 구성 모드를 시작합니다. 전역 구성 모드에서 ASA에 다음 확인 상자가 표시됩니다. hostname(config)#
- hostscan_version-k9.pkg 파일을 ASA에 업로드합니다.

프로시저

단계 **1** webvpn 구성 모드를 시작합니다.

예제:

```
hostname(config)# webvpn
```

단계 **2** HostScan 이미지로 지정하려는 패키지에 경로를 지정합니다. 독립 실행형 HostScan 패키지 또는 AnyConnect Secure Mobility Client 패키지를 HostScan 패키지로 지정할 수 있습니다.

hostscan image *path*

예제:

```
ASAName(webvpn)#hostscan image disk0:/ hostscan-3.6.0-k9.pkg
```

단계 **3** 이전 단계에서 지정한 HostScan 이미지를 활성화합니다.

예제:

```
ASAName(webvpn)#hostscan enable
```

단계 **4** 실행 중인 구성을 플래시에 저장합니다. 플래시 메모리에 새 구성을 성공적으로 저장한 이후에 [OK] 메시지를 받습니다.

예제:

```
hostname(webvpn)# write memory
```

단계 **5**

HostScan 활성화 또는 비활성화

이 명령은 ASA의 명령행 인터페이스를 사용하여 설치된 HostScan 이미지를 활성화 또는 비활성화합니다.

시작하기 전에

ASA에 로그온하고 전역 구성 모드를 시작합니다. 전역 구성 모드에서 ASA에 다음 확인 상자가 표시됩니다. hostname(config)#

프로시저

단계 **1** webvpn 구성 모드를 시작합니다.

예제:

webvpn

단계 **2** ASA에서 제거하지 않은 경우 독립형 HostScan 이미지를 활성화합니다.

hostscan enable

단계 **3** 모든 설치된 HostScan 패키지에 대한 HostScan을 비활성화합니다.

참고 활성화된 HostScan 이미지를 제거하기 전에, 이 명령을 사용하여 먼저 HostScan을 비활성화해야 합니다.

no hostscan enable

ASA에 활성화되어 있는 HostScan 버전 보기

ASA의 명령행 인터페이스를 사용하여 활성화된 HostScan 버전을 판단하려면 다음 절차를 수행하십시오.

시작하기 전에

ASA에 로그온하고 특권 EXEC 모드를 시작합니다. 특권 EXEC 모드에서는 ASA가 다음 확인 상자를 표시합니다. hostname#

프로시저

ASA에 활성화되어 있는 HostScan 버전을 보여줍니다.

show webvpn hostscan

HostScan 제거

HostScan 패키지를 제거하면 ASDM 인터페이스에 있는 보기에서 제거되며 HostScan이 활성화된 경우에도 ASA가 이를 배포하는 것이 방지됩니다. HostScan을 제거해도 플래시 드라이브에서 HostScan 패키지는 삭제되지 않습니다.

시작하기 전에

ASA에 로그온하고 전역 구성 모드를 시작합니다. 전역 구성 모드에서 ASA에 다음 확인 상자가 표시됩니다. hostname(config)#

프로시저

단계 1 webvpn 구성 모드를 시작합니다.

webvpn

단계 2 제거할 HostScan 이미지를 비활성화합니다.

no hostscanenable

단계 3 제거할 HostScan 이미지의 경로를 지정합니다. 독립형 HostScan 패키지는 HostScan 패키지로 지정될 수 있습니다.

no hostscan image *path*

예제:

```
hostname(webvpn)#no hostscan image disk0:/hostscan-3.6.0-k9.pkg
```

단계 4 실행 중인 구성을 플래시에 저장합니다. 플래시 메모리에 새 구성을 성공적으로 저장한 이후에 [OK] 메시지를 받습니다.

write memory

그룹 정책에 AnyConnect 기능 모듈 할당

이 절차에서는 AnyConnect 기능 모듈을 그룹 정책과 연계합니다. VPN 사용자가 ASA에 연결하는 경우 ASA는 엔드포인트 컴퓨터에 이 AnyConnect 기능 모듈을 다운로드하여 설치합니다.

시작하기 전에

ASA에 로그온하고 전역 구성 모드를 시작합니다. 전역 구성 모드에서 ASA에 다음 확인 상자가 표시됩니다. hostname(config)#

프로시저

단계 1 네트워크 클라이언트 액세스를 위해 내부 그룹 정책을 추가합니다.

group-policy *name* **internal**

예제:

```
hostname(config)# group-policy PostureModuleGroup internal
```

단계 2 새 그룹 정책을 수정합니다. 명령을 입력한 다음 그룹 정책 구성 모드에 대해 확인 상자 hostname(config-group-policy)#를 받습니다.

group-policy *name* **attributes**

예제:

```
hostname(config)# group-policy PostureModuleGroup attributes
```

단계 **3** 그룹 정책 webvpn 구성 모드를 시작합니다. 명령을 입력하면 ASA가 다음 확인 상자를 반환합니다. hostname(config-group-webvpn)#

webvpn

단계 **4** 그룹의 모든 사용자에 대해 AnyConnect 기능 모듈을 다운로드하도록 그룹 정책을 구성합니다.

anyconnect modules value *AnyConnect Module Name*

anyconnect 모듈 명령 값은 다음 값 중 하나 이상을 포함할 수 있습니다. 두 개 이상의 모듈을 지정하는 경우 값을 쉼표로 구분합니다.

값	**AnyConnect** 모듈 이름
dart	AnyConnect DART(Diagnostics and Reporting Tool)
vpngina	AnyConnect SBL(Start Before Logon)
websecurity	AnyConnect Web Security Module
telemetry	AnyConnect Telemetry 모듈
posture	AnyConnect Posture 모듈
nam	Cisco AnyConnect Network Access Manager
none	그룹 정책에서 모든 AnyConnect 모듈을 제거하기 위해 자체에서 사용됩니다.

예제:

```
hostname(config-group-webvpn)# anyconnect modules value websecurity,telemetry,posture
```

모듈 중 하나를 제거하려면 유지하려는 모듈 값만 지정하는 명령을 다시 전송합니다. 예를 들어 다음 명령은 WebSecurity 모듈을 제거합니다.

```
hostname(config-group-webvpn)# anyconnect modules value telemetry,posture
```

단계 **5** 실행 중인 구성을 플래시에 저장합니다.

플래시 메모리에 새 구성을 성공적으로 저장한 이후에 [OK] 메시지를 받으며 ASA는 다음 확인 상자를 반환합니다. hostname(config-group-webvpn)#

write memory

HostScan 관련 문서

HostScan이 엔드포인트 컴퓨터에서 상태 크리덴셜을 수집하면 동적 액세스 정책 구성 및 이 정보를 활용하기 위한 LUA 표현식 사용과 같은 주제를 이해해야 합니다.

이 주제에 대해서는 다음 문서에서 자세히 다룹니다.

- Cisco Secure Desktop 구성 가이드
- Cisco Adaptive Security Device Manager 구성 가이드

HostScan이 AnyConnect 클라이언트에서 작동하는 방식에 대한 자세한 내용은 Cisco *AnyConnect Secure Mobility Client* 관리자 설명서를 참조하십시오.

11 장

용이한 VPN

이 장에서는 ASA를 Easy VPN 서버로 구성하는 방법 및 FirePOWER- 5506-X, 5506W-X, 5506H-X 및 5508-X 모델을 사용하는 Cisco ASA을 Easy VPN Remote 하드웨어 클라이언트로 구성하는 방법을 설명합니다.

Easy VPN 정보

Cisco Ezvpn은 원격 사무실 및 모바일 근무자용 VPN의 구성 및 구축을 크게 간소화합니다. Cisco Easy VPN은 사이트 대 사이트 및 원격 액세스 VPN에 유연성, 확장성 및 사용 편의성을 제공합니다. Cisco Unity 클라이언트 프로토콜을 구현하여 관리자가 Easy VPN 서버에서 대부분의 VPN 매개변수를 정의할 수 있으므로 Easy VPN Remote 구성이 간편해집니다.

FirePOWER 모델 5506-X, 5506W-X, 5506H-X, 5508-X를 Cisco ASA는 VPN 터널을 Easy VPN 서버로 시작하는 하드웨어 클라이언트로 Easy VPN Remote를 사용하도록 지원합니다. Easy VPN 서버는 다른 ASA(모든 모델) 또는 Cisco IOS 기반 라우터가 될 수 있습니다. ASA는 동시에 Easy VPN Remote와 Easy VPN 서버로 작동할 수 없습니다.

참고 Cisco ASA 5506-X, 5506W-X, 5506H-X, 5508-X 모델은 L2 스위칭이 아니라 L3 스위칭을 지원합니다. 내부 네트워크의 여러 호스트 또는 디바이스에서 Easy VPN Remote를 사용하는 경우 외부 스위치를 사용하십시오. ASA의 내부 네트워크에 단일 호스트가 있는 경우에는 스위치가 필요하지 않습니다.

다음 섹션에서는 Easy VPN 옵션과 설정에 대해 설명합니다. ASA를 Easy VPN Remote 하드웨어 클라이언트로 구성하려면

Easy VPN 인터페이스

시스템 시작 시 Easy VPN 외부 및 내부 인터페이스가 보안 레벨에 따라 결정됩니다. 최저 보안 레벨의 물리적 인터페이스는 Easy VPN 서버에 대한 외부 연결에 사용됩니다. 최고 보안 레벨의 물리적 또

는 가상 인터페이스는 보안 리소스에 대한 내부 연결에 사용됩니다. Easy VPN에서 동일한 최고 보안 레벨의 인터페이스가 둘 이상 있음을 확인하면 Easy VPN이 비활성화됩니다.

원하는 경우 **vpnclient secure interface** 명령을 사용하여 내부 보안 인터페이스와 물리적 또는 가상 인터페이스 간에 서로 변경할 수 있습니다. 자동으로 선택된 기본 물리적 인터페이스에서는 외부 인터페이스를 변경할 수 없습니다.

예를 들어, ASA5506 플랫폼의 공장 구성은 최고 보안 레벨 인터페이스가 100으로 설정된 BVI(해당 멤버 인터페이스도 100 레벨에 있음)와, 보안 레벨이 0인 외부 인터페이스가 있습니다. 기본적으로 Easy VPN은 이러한 인터페이스를 선택합니다.

시작할 때 가상 인터페이스(브리지 가상 인터페이스 또는 BVI)를 선택하거나 관리자가 내부 보안 인터페이스로 가상 인터페이스를 할당하는 경우 다음이 적용됩니다.

- 모든 BVI 멤버 인터페이스는 자체 보안 레벨에 관계없이 내부 보안 인터페이스로 간주됩니다.
- ACL 및 NAT 규칙을 모든 멤버 인터페이스에 추가해야 합니다. AAA 규칙은 BVI 인터페이스에만 추가됩니다.

Easy VPN 연결

Easy VPN은 IPsec IKEv1 터널을 사용합니다. Easy VPN Remote 하드웨어 클라이언트의 구성은 Easy VPN 서버 헤드엔드의 VPN 구성과 호환되어야 합니다. 보조 서버를 사용하는 경우 해당 구성이 기본 서버와 동일해야 합니다.

ASA Easy VPN Remote는 기본 Easy VPN 서버의 IP 주소를 구성하며, 필요한 경우 최대 10개의 보조(백업) 서버도 구성합니다. 이러한 서버를 구성하려면 전역 구성 모드에서 **vpnclient server** 명령을 사용합니다. 기본 서버에 대한 터널을 설정할 수 없는 경우, 클라이언트가 첫 번째 보조 VPN 서버에 연결하려고 시도한 다음, 8초 간격으로 VPN 서버 목록의 순서대로 시도합니다. 첫 번째 보조 서버에 대한 터널 설정에 실패하고, 이 시간 동안 기본 서버가 온라인 상태가 되는 경우, 클라이언트는 계속해서 두 번째 보조 VPN 서버에 대한 터널을 설정합니다.

기본적으로 Easy VPN 하드웨어 클라이언트 및 서버는 UDP(사용자 데이터그램 프로토콜) 패킷에서 IPsec을 캡슐화합니다. 특정 방화벽 규칙 또는 NAT 및 PAT 디바이스가 있는 일부 환경에서는 UDP를 금지합니다. 이러한 환경에서 표준 ESP(Encapsulating Security Protocol, Protocol 50) 또는 IKE(인터넷 키 교환국, UDP 500)를 사용하려면 TCP 패킷 내에서 IPsec을 캡슐화하여 보안 터널링을 활성화하도록 클라이언트 및 서버를 구성해야 합니다. **vpnclient ipsec-over-tcp** 명령을 사용하여 클라이언트와 서버를 구성합니다. 그러나 UDP를 허용하는 환경에서 IPsec over TCP를 구성하면 불필요한 오버헤드가 추가됩니다.

Easy VPN 터널 그룹

터널을 설정할 때 Easy VPN Remote에서 연결에 사용할 Easy VPN 서버에 구성된 터널 그룹을 지정합니다. Easy VPN 서버는 Easy VPN Remote 하드웨어 클라이언트로 그룹 정책 또는 사용자 속성을 푸시하여 터널 동작을 결정합니다. 특정 속성을 변경하려면 기본 또는 보조 Easy VPN 서버로 구성된 ASA에서 해당 속성을 수정해야 합니다.

Easy VPN Remote 클라이언트는 이름 및 사전 공유 키를 구성하는 **vpnclient vpngroup** 명령을 사용하여 그룹 정책을 지정하거나, **vpnclient trustpoint** 명령을 사용하여 사전 구성된 트러스트 포인트를 식별합니다.

작업의 **Easy VPN** 모드

이 모드는 엔터프라이즈 네트워크에서 터널을 통해 Easy VPN Remote 뒤에 있는 호스트에 액세스할 수 있는지 여부를 결정합니다.

- 클라이언트 모드(PAT(포트 주소 변환) 모드라고도 함)는 Easy VPN Remote 프라이빗 네트워크의 모든 디바이스를 엔터프라이즈 네트워크에 있는 디바이스와 격리합니다. Easy VPN Remote는 내부 호스트의 모든 VPN 트래픽에 대해 PAT(포트 주소 변환)를 수행합니다. Easy VPN Remote의 비공개 부분에 있는 네트워크와 주소는 숨겨져 있기 때문에 직접 액세스할 수 없습니다. Easy VPN 클라이언트 내부 인터페이스 또는 내부 호스트에 대해서는 IP 주소 관리가 필요하지 않습니다.
- 네트워크 확장 모드(NEM)는 내부 인터페이스 및 모든 내부 호스트가 터널을 통해 엔터프라이즈 네트워크 전체에서 라우팅 가능하도록 설정합니다. 내부 네트워크에 있는 호스트는 고정 IP 주소로 미리 구성되어 있는 액세스 가능한 서브넷(정적으로 또는 DHCP를 통해)에서 IP 주소를 얻습니다. PAT는 NEM에서 VPN 트래픽에 적용되지 않습니다. 이 모드에서는 내부 네트워크의 각 호스트에 대한 VPN 구성 또는 터널이 필요하지 않으며 Easy VPN Remote는 모든 호스트에 대해 터널링을 제공합니다.

Easy VPN 서버는 기본적으로 클라이언트 모드입니다. NEM 모드를 구성하려면 그룹 정책 구성 모드에서 **nem enable** 명령을 사용합니다. Easy VPN Remote에는 기본 모드가 없기 때문에 터널을 설정하려면 먼저 작동 모드 중 하나를 지정해야 합니다. Easy VPN Remote에서 PAT 또는 NEM을 구성하려면 **vpnclient mode** 명령을 사용합니다.

참고 NEM 모드에 대해 구성된 Easy VPN Remote ASA는 자동 터널 시작을 지원합니다. 자동 시작 시에는 터널을 설정하는 데 사용된 크리덴셜 구성 및 스토리지가 필요합니다. 보안 유닛 인증이 활성화된 경우, 자동 터널 시작이 비활성화됩니다.

여러 인터페이스가 구성된 네트워크 확장 모드에서 Easy VPN Remote는 가장 높은 보안 수준의 인터페이스에서 로컬로 암호화된 트래픽에 대한 터널만 구축합니다.

Easy VPN 사용자 인증

ASA Easy VPN Remote는 **vpnclient username** 명령을 사용하여 자동 로그인을 위해 사용자 이름 및 비밀번호를 저장할 수 있습니다..

추가 보안을 위해 Easy VPN 서버에는 다음 항목이 필요할 수 있습니다.

- 보안 유닛 인증(SUA) - 사용자에게 수동으로 인증하도록 요청하면서 구성된 사용자 이름 및 비밀번호를 무시합니다. 기본적으로 SUA가 비활성화되며 **secure-unit-authentication enable** 명령을 사용하여 Easy VPN 서버에서 SUA를 활성화합니다.
- 개별 사용자 인증(IUA) - 사용자가 Easy VPN Remote 뒤에서 엔터프라이즈 VPN 네트워크에 대한 액세스를 수신하기 전에 인증하도록 요청합니다. 기본적으로 IUA가 비활성화되며 **user-authentication enable** 명령을 사용하여 Easy VPN 서버에서 IUA를 활성화합니다.

  IUA를 사용할 경우, Cisco IP Phone 또는 프린터와 같은 특정 디바이스는 하드웨어 클라이언트 뒤에서 개별 사용자 인증을 우회해야 합니다. 이렇게 구성하려면 **ip-phone-bypass** 명령을 사용

하여 Easy VPN 서버에서 IP 전화기 우회를 지정하고 MAC 주소 면제 시 Easy VPN Remote에서 **mac-exempt** 명령을 사용합니다.

또한, Easy VPN 서버는 Easy VPN Server에서 **user-authentication-idle-timeout** 명령을 사용하여 Easy VPN 서버가 클라이언트의 액세스를 종료한 후에 유휴 시간 제한 기간을 설정하거나 제거할 수 있습니다.

Cisco Easy VPN 서버는 HTTP 트래픽을 차단하고 사용자 이름 및 비밀번호가 구성되지 않았거나 SUA가 비활성화되었거나 IUA가 활성화된 경우 사용자를 로그인 페이지로 리디렉션합니다. HTTP 리디렉션은 자동이며 Easy VPN 서버에서 구성할 필요가 없습니다.

Remote Management(원격 관리**)**

ASA는 Easy VPN Remote 하드웨어 클라이언트가 추가 IPsec 암호화를 사용하거나 사용하지 않고 SSH 또는 HTTPS를 사용하는 관리 액세스를 지원할 때 작동합니다.

기본적으로 관리 터널은 SSH 내부의 IPsec 암호화 또는 HTTPS 암호화를 사용합니다. **vpnclient management clear** 명령을 사용하여 VPN 터널 외부에서 관리 액세스를 허용하는 IPsec 암호화 Layer를 지울 수 있습니다. 터널 관리를 지우면 IPsec 암호화 레벨만 제거되며 SSH 또는 HTTPS와 같이 연결에 존재하는 다른 암호화에는 영향을 주지 않습니다.

추가 보안을 위해 Easy VPN Remote는 전역 구성 모드에서 **vpnclient management tunnel** 명령을 사용하여 IPsec 암호화를 요청하고 특정 호스트 또는 회사측의 네트워크에 대한 관리 액세스를 제한할 수 있습니다.

기본 원격 관리 작업으로 돌아가려면 **no vpnclient management**를 사용합니다.

참고 NAT 디바이스가 ASA Easy VPN Remote와 인터넷 사이에서 작동하는 경우 ASA Easy VPN Remote에서 관리 터널을 구성하지 마십시오. 해당 구성에서 **vpnclient management clear**명령을 사용하여 원격 관리를 지웁니다.

구성에 관계없이 DHCP 요청(갱신 메시지 포함)은 IPsec 터널을 통해 흐를 수 없습니다. vpnclient 관리 터널에서도 DHCP 트래픽은 금지됩니다.

Easy VPN Remote 구성

시작하기 전에

Easy VPN Remote를 구성하려면 다음 정보를 수집합니다.

- 기본 Easy VPN 서버 및 보조 서버(사용 가능한 경우)의 주소.
- 주소 지정 모드인 클라이언트 또는 NEM, Easy VPN Remote는 작동해야 합니다.
- Easy VPN 서버 그룹 정책 이름 및 비밀번호(사전 공유 키) 또는 원하는 그룹 정책을 선택 및 인증하는 사전 구성된 트러스트 포인트.

- VPN 터널을 사용하도록 권한이 부여된 Easy VPN 서버에 구성된 사용자.
- BVI 인터페이스가 원격 관리 인터페이스용으로 사용되고 있는 경우, 해당 인터페이스에서 **management-access**를 구성해야 합니다.

프로시저

단계 **1** Easy VPN 서버 주소를 구성합니다.

vpnclient server *ip-primary* [*ip-secondary-1... ip-secondary-n*]

- *ip-primary-address* - 기본 Easy VPN 서버의 IP 주소 또는 DNS 이름입니다.
- *ip-secondary-n*(선택 사항) - 최대 10개의 Easy VPN 백업 서버에 대한 IP 주소 또는 DNS 이름 목록입니다. 공백을 사용하여 목록의 항목을 구분합니다.

예제**:**

```
asa(config)#vpnclient server 10.10.10.15 10.10.10.30 192.168.10.10
```

단계 **2** (선택 사항) 자동으로 선택한 기본값이 바람직하지 않은 경우 내부 보안 인터페이스를 재지정합니다.

시작할 때, 최고 보안 레벨의 물리적 인터페이스 또는 BVI는 보안 리소스에 대한 내부 연결에 사용됩니다. 다른 인터페이스를 선택하려면 **vpnclient secure interface** *interface-name* 명령을 사용합니다. 물리적 또는 가상 인터페이스를 할당할 수 있습니다.

단계 **3** 작업 모드를 지정합니다.

vpnclient mode {**client-mode** | **network-extension-mode**}

- **client-mode**- PAT(포트 주소 변환) 모드를 사용하여 클라이언트를 기준으로 엔터프라이즈 네트워크에서 내부 호스트의 주소를 격리합니다.
- **network-extension-mode**- 엔터프라이즈 네트워크에서 내부 호스트의 주소에 액세스할 수 있습니다.

예제**:**

```
asa(config)#vpnclient mode network-extension-mode
```

단계 **4** (선택 사항) 필요한 경우 Easy VPN 하드웨어 클라이언트에서 TCP 캡슐화된 IPsec을 사용하도록 구성합니다.

vpnclient ipsec-over-tcp [**port** *tcp_port*]

포트를 지정하지 않으면 Easy VPN 하드웨어 클라이언트에서 포트 10000을 사용합니다.

TCP 캡슐화된 IPsec을 사용하기 위해 Easy VPN Remote를 구성하는 경우 **crypto ipsec df-bit clear-df outside** 명령을 입력하여 캡슐화된 헤더에서 DF(Don't Fragment) 비트를 지웁니다. DF 비트는 패킷을 프래그먼트할 수 있는지 여부를 결정하는 IP 헤더 내의 비트입니다. 이 명령을 사용하면 Easy VPN 하드웨어 클라이언트가 MTU 크기보다 큰 패킷을 전송할 수 있습니다.

예제:

Easy VPN 하드웨어 클라이언트에서 포트 10501을 사용하여 TCP 캡슐화된 IPsec을 사용하도록 구성하고 외부 인터페이스를 통해 대용량 패킷을 전송할 수 있도록 합니다.

```
hostname(config)# vpnclient ipsec-over-tcp port 10501
hostname(config)# crypto ipsec df-bit clear-df outside
```

단계 **5** 다음 방법 중 하나를 사용하여 Easy VPN 서버에 구성된 터널 그룹을 식별합니다.

- Easy VPN 서버 그룹 정책 이름 및 비밀번호(사전 공유 키)를 지정합니다.

  vpnclient vpngroup *group_name* **password** *preshared_key*

  - *group_name*- Easy VPN 서버에 구성된 VPN 터널 그룹의 이름입니다. 연결을 설정하기 전에 서버에서 이 터널 그룹을 구성해야 합니다.
  - *preshared_key*- Easy VPN 서버에서 인증에 사용되는 IKE 사전 공유 키입니다.

  예를 들어, TestGroup1이라는 VPN 터널 그룹과 my_key123이라는 IKE 사전 공유 키를 식별하려면 다음 명령을 입력합니다.

  ```
  hostname(config)# vpnclient vpngroup TestGroup1 password my_key123
  hostname(config)#
  ```

- 사전 구성된 트러스트 포인트를 지정하여 그룹 정책을 선택하고 인증합니다.

  vpnclient trustpoint *trustpoint_name* [**chain**]

  - *trustpoint_name*- 인증에 사용할 RSA 인증서를 식별하는 트러스트 포인트 이름을 지정합니다.
  - **chain**(선택 사항)-- 전체 인증서 체인을 전송합니다.

  예를 들어, central이라는 ID 인증서를 지정하고 전체 인증서 체인을 전송하려면 다음 명령을 입력합니다.

  ```
  hostname(config)# crypto ca trustpoint central
  hostname(config)# vpnclient trustpoint central chain
  hostname(config)#
  ```

단계 **6** 그룹 정책에 NEM 및 스플릿 터널링이 구성된 경우 자동 연결할 VPN 터널을 구성합니다.

vpnclient nem-st-autoconnect

단계 **7** (선택 사항) Easy VPN 서버의 그룹 정책에 IAU(개별 사용자 인증) 및 IP 전화기 우회가 구성되어 있으면, Cisco IP phone, 무선 액세스 포인트 및 프린터 같은 디바이스는 인증할 수 없으므로 인증에서 제외됩니다.

vpnclient mac-exempt *mac_addr_1 mac_mask_1* [*mac_addr_2 mac_mask_2...mac_addr_n mac_mask_n*]

- 주소 목록은 15개를 초과할 수 없습니다.
- *mac_addr*- 개별 사용자 인증을 우회할 디바이스의 MAC 주소(점으로 구분된 16진수 표기법)입니다.
- *mac_mask*-해당 MAC 주소에 대한 네트워크 마스크입니다.

MAC 마스크가 ffff.ff00.0000이면 동일한 제조업체에서 만든 모든 디바이스와 매치합니다. MAC 마스크가 ffff.ffff.ffff이면 단일 디바이스와 매치합니다.

MAC 마스크 ffff.ff00.0000을 사용하여 동일한 제조업체의 모든 디바이스를 지정하는 경우 특정 MAC 주소의 처음 6자만 필요합니다.

예제:

Cisco IP Phone은 제조업체 ID가 00036b이므로 다음 명령은 Cisco IP Phone을 포함하여 향후에 추가할 수 있는 모든 Cisco IP Phone을 제외합니다.

```
hostname(config)# vpnclient mac-exempt 0003.6b00.0000 ffff.ff00.0000
hostname(config)#
```

참고 표시된 대로 Easy VPN 서버 그룹 정책에 개별 사용자 인증 및 IP 전화기 우회를 구성해야 합니다.

```
hostname(config-group-policy)#user-authentication enable
hostname(config-group-policy)#ip-phone-bypass enable
```

단계 **8** 자동 Xauth 사용자 로그인 크리덴셜을 구성합니다.

vpnclient username *username* **password** *password*

단계 **9** (선택 사항) Easy VPN Remote의 원격 관리를 구성합니다.

기본적으로 관리 터널은 SSH 내부의 IPsec 암호화 또는 HTTPS 암호화를 사용합니다. IPsec 암호화를 제거하거나 이 암호화를 유지하고 특정 호스트만 ASA를 관리하도록 하려면 다음 명령 중 하나를 사용합니다.

- **vpnclient management clear**

  VPN 터널 외부에서 관리 액세스를 허용하는 IPsec 암호화 Layer를 지웁니다.

- **vpnclient management tunnel ip_addr_1 ip_mask_1** [*ip_addr_2 ip_mask_2...ip_addr_n ip_mask_n*]

예제:

IPsec 터널의 생성을 자동화하여 IP 주소가 192.168.10.10인 호스트에 관리 액세스를 제공하려면 다음 명령을 입력합니다.

```
hostname(config)# vpnclient management tunnel 192.198.10.10 255.255.255.0
```

참고 NAT 디바이스가 ASA Easy VPN Remote와 인터넷 사이에서 작동하는 경우 ASA Easy VPN Remote에서 관리 터널을 구성하지 마십시오. 해당 구성에서 **vpnclient management clear**명령을 사용하여 원격 관리를 지웁니다.

단계 **10** ASA에서 Easy VPN 하드웨어 클라이언트를 활성화합니다.

vpnclient enable

Easy VPN Remote을 활성화하기 전에 서버 주소, 모드 및 터널 그룹 사양을 구성해야 합니다.

단계 **11** (선택 사항) 구성할 때 이 정보가 필요한 경우 수동으로 Easy VPN 터널을 연결합니다.

vpnclient connect

Easy VPN 서버 구성

시작하기 전에

모든 보조 Easy VPN 서버가 기본 Easy VPN 서버와 동일한 옵션 및 설정으로 구성되어 있는지 확인합니다.

프로시저

단계 **1** IPsec IKEv1을 지원하도록 Easy VPN 서버를 구성합니다. 연결 프로파일, 그룹 정책 및 사용자, 97 페이지의 내용을 참조하십시오.

단계 **2** 특정 Easy VPN 서버 속성을 설정합니다. VPN 하드웨어 클라이언트에 대한 속성 구성, 168 페이지의 내용을 참조하십시오.

Easy VPN에 대한 기능 기록

기능 이름	릴리스	기능 정보
ASA 5506-X, 5506W-X, 5506H-X 및 5508-X의 Cisco Easy VPN 클라이언트	9.5(1)	이 릴리스는 ASA 5506-X 시리즈 및 ASA 5508-X용 Cisco Easy VPN을 지원합니다. ASA는 VPN 헤드엔드에 연결할 때 VPN 하드웨어 클라이언트 역할을 합니다. Easy VPN 포트의 ASA 뒤에 있는 모든 디바이스(컴퓨터, 프린터 등)는 VPN을 통해 통신할 수 있습니다. 이러한 디바이스는 VPN 클라이언트를 개별적으로 실행할 필요가 없습니다. 참고로 하나의 ASA 인터페이스만 Easy VPN 포트 역할을 수행할 수 있습니다. 여러 디바이스를 해당 포트에 연결하려면 포트에 Layer 2 스위치를 배치한 다음 디바이스를 스위치에 연결해야 합니다. 다음 명령을 도입했습니다. **vpnclient enable, vpnclient server, vpnclient mode, vpnclient username, vpnclient ipsec-over-tcp, vpnclient management, vpnclient vpngroup, vpnclient trustpoint, vpnclient nem-st-autoconnect, vpnclient mac-exempt**

기능 이름	릴리스	기능 정보
BVI 지원에 대한 Easy VPN 개선 사항	9.9(2)	Easy VPN은 내부 보안 인터페이스로 브리지 가상 인터페이스를 지원하도록 기능이 개선되었으며 관리자는 이제 새로운 **vpnclient secure interface** [*interface-name*] 명령을 사용하여 내부 보안 인터페이스를 직접 구성할 수 있습니다. 물리적 인터페이스 또는 브리지 가상 인터페이스는 내부 보안 인터페이스로 할당될 수 있습니다. 관리자가 이렇게 설정하지 않은 경우, Easy VPN은 이전과 같이 보안 레벨을 사용하여 독립적인 물리적 인터페이스 또는 BVI인지 여부에 관계없이 내부 보안 인터페이스를 선택합니다. 또한 관리 액세스가 BVI에서 활성화된 경우 관리 서비스(**telnet**, **http**, **ssh** 등)를 이제 BVI에서 구성할 수 있습니다. 신규 또는 수정된 명령: **vpnclient secure interface** [*interface-name*], **https**, **telnet**, **ssh**, **management-access**

12 장

Virtual Tunnel Interface

이 장에서는 VTI 터널을 구성하는 방법에 대해 설명합니다.

Virtual Tunnel Interface 정보

ASA는 VTI(Virtual Tunnel Interface)라는 논리적 인터페이스를 지원합니다. 정책 기반 VPN 대신, 구성된 Virtual Tunnel Interface와 피어 간에 VPN 터널을 생성할 수 있습니다. 이것은 각 터널 끝에 IPsec 프로파일이 연결된 라우팅 기반 VPN을 지원합니다. 그러면 동적 또는 정적 경로를 사용할 수 있습니다. VTI에서 이그레스(Egress)되는 트래픽은 암호화되어 피어로 전송되고, 연결된 SA가 VTI로 인그레스(Ingress)되는 트래픽의 암호를 해독합니다.

VTI를 사용하면 정적 암호화 맵 액세스 목록을 구성하고 이를 인터페이스에 매핑하기 위한 요구 사항이 없어집니다. 더 이상 모든 원격 서브넷을 추적하고 암호화 맵 액세스 목록에 포함하지 않아도 됩니다. 구축이 더 간편해지고, 동적 라우팅 프로토콜과 라우팅 기반 VPN을 지원하는 정적 VTI가 있어 가상 프라이빗 클라우드의 많은 요구 사항도 충족합니다.

Virtual Tunnel Interface에 대한 지침

IPv6

- IPv6은 지원되지 않습니다.

일반 구성 지침

- 터널 인터페이스를 사용하여 트래픽에 대한 동적 또는 정적 경로를 사용할 수 있습니다.
- 기본 물리적 인터페이스에 따라 VTI에 대한 MTU가 자동으로 설정됩니다.
- 네트워크 주소 변환을 적용해야 할 경우, IKE 및 ESP 패킷이 UDP 헤더에서 캡슐화됩니다.

- IKE 및 IPsec 보안 연계는 터널에서 데이터 트래픽에 관계없이 지속적으로 다시 입력됩니다. 이렇게 하면 VTI 터널은 항상 작동합니다.
- 터널 그룹 이름은 피어가 IKEv1 id로 전송하는 항목과 일치해야 합니다.
- 터널 그룹 이름은 피어가 IKEv1 또는 IKEv2 id로 전송하는 항목과 일치해야 합니다.
- LAN-to-LAN 터널 그룹에서 IKEv1의 경우, 터널 인증 방법이 디지털 인증서 및/또는 적극적인 모드를 사용하도록 구성된 피어인 경우, IP 주소가 아닌 이름을 사용할 수 있습니다.
- VTI 및 암호화 맵 구성은 동일한 물리적 인터페이스에서 공존할 수 있으며 암호화 맵에 구성된 피어 주소를 제공하며 VTI에 대한 터널 대상은 서로 다릅니다.
- 기본적으로 VTI를 통과하는 모든 트래픽이 암호화됩니다.
- VTI 인터페이스에 대한 보안 레벨 구성이 없습니다.
- 액세스 목록은 VTI를 통과하는 트래픽을 제어하기 위해 VTI 인터페이스에 적용될 수 있습니다.
- VTI에서는 BGP만 지원됩니다.

상황 모드

단일 모드에서만 지원됩니다.

방화벽 모드

라우팅 모드에서만 지원됩니다.

VTI 터널 생성

VTI 터널을 구성하려면 IPsec 제안서(변형 집합)를 생성합니다. IPsec 제안서를 참조하는 IPsec 프로파일을 생성한 후 IPsec 프로파일을 사용하여 VTI 인터페이스를 생성해야 합니다. 동일한 IPsec 제안서 및 IPsec 프로파일 매개변수로 원격 피어를 구성합니다. 모든 터널 매개변수가 구성되면 SA 협상이 시작됩니다.

참고 두 VPN VTI 도메인의 일부인 ASA의 경우 물리적 인터페이스에 BGP 인접성이 있습니다.

인터페이스 상태 검사로 인해 상태 변경이 트리거되면 BGP 인접성이 새 활성 피어로 다시 설정될 때까지 물리적 인터페이스의 라우팅이 삭제됩니다. 논리적 VTI 인터페이스에는 이 동작이 적용되지 않습니다.

프로시저

단계 **1** IPsec 제안서(변형 집합)를 추가합니다.

단계 **2** IPsec 프로필을 추가합니다.

단계 3 VTI 터널을 추가합니다.

IPsec 제안서(변형 집합) 추가

변형 집합은 VTI 터널에서의 보안 트래픽에 필요합니다. IPsec 프로파일의 일부로 사용되었으며 VPN에서 트래픽을 보호하는 보안 프로토콜 및 알고리즘 집합입니다.

시작하기 전에

- VTI와 연결된 IKEv1 세션을 인증하기 위해 사전 공유 키 또는 인증서 중 하나를 사용할 수 있습니다. VTI에 사용되는 터널 그룹에서 사전 공유 키를 구성해야 합니다.
- IKEv1을 사용하는 인증서 기반 인증의 경우, 이니시에이터에서 사용할 트러스트 포인트를 지정해야 합니다. 응답자의 경우 터널 그룹 명령에서 트러스트 포인트를 구성해야 합니다.
- VTI와 연결된 IKE 세션을 인증하기 위해 사전 공유 키 또는 인증서 중 하나를 사용할 수 있습니다. IKEv2의 경우 비대칭 인증 방법 및 키를 사용할 수 있습니다. IKEv1 및 IKEv2의 경우, VTI에 사용되는 터널 그룹에서 사전 공유 키를 구성해야 합니다.
- IKEv1을 사용하는 인증서 기반 인증의 경우, 이니시에이터에서 사용할 신뢰 지점을 지정해야 합니다. 응답자의 경우, 터널 그룹 명령에서 트러스트 포인트를 구성해야 합니다. IKEv2의 경우 이니시에이터 및 응답자 모두에 대한 터널 그룹 명령에서 인증에 사용할 트러스트 포인트를 구성해야 합니다.

프로시저

보안 연결을 설정하려면 IKEv1 변형 집합 또는 IKEv2 IPsec 제안서를 추가합니다.

IKEv1 변형 집합 추가:

crypto ipsec ikev1 transform-set {*transform-set-name* | *encryption* | *authentication*}

예제:

```
ciscoasa(config)#crypto ipsec ikev1 transform-set SET1 esp-aes esp-sha-hmac
```

*Encryption*은 IPsec 데이터 흐름을 보호하는 암호화 방식의 종류를 지정합니다.

- esp-aes — 128비트 키의 AES를 사용합니다.
- esp-aes-192 — 192비트 키의 AES를 사용합니다.
- esp-aes-256 — 256비트 키의 AES를 사용합니다.
- esp-des — 56비트 DES-CBC를 사용합니다.
- esp-3des — 삼중 DES 알고리즘을 사용합니다.
- esp-null — 암호화하지 않습니다.

*Authentication*은 IPsec 데이터 흐름을 보호하는 암호화 방식의 종류를 지정합니다.

- esp-md5-hmac — MD5/HMAC-128을 해시 알고리즘으로 사용합니다.
- esp-sha-hmac — SHA/HMAC-160을 해시 알고리즘으로 사용합니다.
- esp-none — HMAC 인증을 사용하지 않습니다.

IKEv2 IPsec 제안서를 추가합니다.

참고 IOS 플랫폼의 경우, 구성 교환 옵션을 비활성화하려면 IKEv2 프로파일 구성 모드에서 **no config-exchange request** 명령을 사용합니다. 자세한 내용은 http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/security/a1/sec-a1-cr-book/sec-cr-c2.html#wp3456426280를 참조하십시오.

- IPsec 제안서의 이름을 지정합니다.

  crypto ipsec ikev2 ipsec-proposal *IPSec proposal name*

예제:

```
ciscoasa(config)#crypto ipsec ikev2 ipsec-proposal SET1
```

- crypto IPsec ikev2 ipsec-proposal 구성 모드에서 보안 매개변수를 지정합니다.

  protocol esp {encryption {des | 3des | aes | aes-192 | aes-256 | aes-gcm | aes-gcm-192 | aes-gcm-256 | aes-gmac | aes-gmac-192 | aes-gmac-256 | null} | integrity {md5 | sha-1 | sha-256 | sha-384 | sha-512 | null}

예제:

```
ciscoasa(config-ipsec-proposal)#protocol esp encryption 3des aes des
```

IPsec 프로필 추가

IPsec 프로파일에는 프로파일이 참조하는 IPsec 제안서 또는 변형 집합에 필수 보안 프로토콜 및 알고리즘이 포함되어 있습니다. 이러한 점은 두 개의 사이트 대 사이트 VTI VPN 피어 간에 논리적 보안 통신 경로를 보장합니다.

프로시저

단계 **1** 프로파일 이름을 설정합니다.

crypto ipsec profile *name*

예제:

```
ciscoasa(config)#crypto ipsec profile PROFILE1
```

단계 **2** IKEv1 또는 IKEv2 제안서를 설정합니다. IKEv1 변형 집합 또는 IKEv2 IPsec 제안서를 선택할 수 있습니다.

a) IKEv1 변형 집합을 설정합니다.

- IKEv1 제안서를 설정하려면 crypto ipsec profile command 하위 모드에서 다음 명령을 입력합니다.

  set ikev1 transform set *set_name*

  이 예에서 SET1은 이전에 생성한 IKEv1 제안서 집합입니다.

  ```
  ciscoasa(config-ipsec-profile)#set ikev1 transform-set SET1
  ```

b) IKEv2 제안서를 설정합니다.

- IKEv2 제안서를 설정하려면 crypto ipsec profile command 하위 모드에서 다음 명령을 입력합니다.

  set ikev2 ipsec-proposal*IPsec_proposal_name*

  이 예에서 SET1은 이전에 생성한 IKEv2 IPsec 제안서입니다.

  ```
  ciscoasa(config-ipsec-profile)#set ikev2 ipsec-proposal SET1
  ```

단계 **3** (선택 사항) 보안 연결의 지속 기간을 지정합니다.

set security-association lifetime { **seconds** *number* | **kilobytes** {*number* | **unlimited**}}

예제**:**

```
ciscoasa(config-ipsec-profile)#set security-association lifetime
seconds 120 kilobytes 10000
```

단계 **4** (선택 사항) 응답자로 작동하려면 VTI 터널의 종료를 구성합니다.

responder-only

- 응답자로만 수행하도록 VTI 터널의 한 쪽 끝을 구성할 수 있습니다. 응답자 전용 끝은 터널 또는 키 재생성을 시작하지 않습니다.
- IKEv2를 사용 중인 이니시에이터 종료에서 IPsec 프로파일의 수명 값보다 큰 보안 연계 수명 기간을 설정합니다. 이 작업은 이니시에이터 종료를 통해 키 재생성을 성공적으로 수행하고 터널이 계속 작동하도록 보장하기 위해 수행됩니다.
- 이니시에이터 종료에서 키 재생성 구성을 알 수 없는 경우, 응답자 전용 모드를 제거하여 SA 설정 양방향으로 설정하거나 만료를 방지하기 위해 응답자 전용 종료에서 무한 IPsec 수명 값을 구성합니다.

단계 **5** (선택 사항) PFS 그룹을 지정합니다. PFS(Perfect Forward Secrecy)는 암호화된 각 교환에 대해 고유 세션 키를 생성합니다. 이 고유한 세션 키는 후속 암호 해독에서 교환을 보호합니다. PFS를 구성하려면 PFS 세션 키를 생성할 때 사용할 Diffie-hellman 키 파생 알고리즘을 선택해야 합니다. 키 파생 알고리즘은 IPsec 보안 연계(SA) 키를 생성합니다. 각 그룹의 크기 모듈러스는 서로 다릅니다. 대형 모듈러스는 보안성은 더 높지만, 처리 시간이 더 오래 걸립니다. Diffie-hellman 그룹은 두 피어 모두에서 일치하는 항목을 지녀야 합니다.

set pfs {**group1** | **group2** | **group5**}

예제**:**

```
ciscoasa(config-ipsec-profile)#set pfs group2
```

단계 **6** (선택 사항) VTI 터널 연결을 시작하는 동안 사용할 인증서를 정의하는 트러스트 포인트를 지정합니다.

set trustpoint *name*

예제:

```
ciscoasa(config-ipsec-profile)#set trustpoint TPVTI
```

VTI 인터페이스 추가

새 VTI 인터페이스를 생성하고 VTI 터널을 설정하려면 다음 단계를 수행합니다.

참고 활성 터널의 라우터를 사용할 수 없는 경우 터널을 유지하기 위해 IP SLA를 구현합니다. http://www.cisco.com/go/asa-config의 ASA 일반 작업 구성 가이드에서 정적 경로 추적 구성을 참조하십시오.

프로시저

단계 **1** 새 터널 인터페이스를 생성합니다.

interface tunnel *tunnel_interface_number*

예제:

```
ciscoasa(config)#interface tunnel 100
```

0~100 범위에서 터널 ID를 지정합니다. 최대 100개의 VTI 인터페이스가 지원됩니다.

참고 다른 디바이스에서 ASA 5506 디바이스로 구성을 마이그레이션하는 경우, 1~100의 터널 ID 범위를 사용합니다. 이 작업은 ASA 5506 디바이스에서 사용 가능한 1~100의 터널 범위의 호환성을 확인합니다.

단계 **2** VTI 인터페이스의 이름을 입력합니다.

interface tunnel 명령 하위 모드에서 다음 명령을 입력합니다.

nameif *interface name*

예제:

```
ciscoasa(config-if)#nameif vti
```

단계 **3** VTI 인터페이스의 IP 주소를 입력합니다.

ip address *IP addressmask*

예제:

```
ciscoasa(config-if)#ip address 192.168.1.10 255.255.255.254
```

단계 **4** 터널 소스 인터페이스를 지정합니다.

tunnel source interface *interface name*

예제:

```
ciscoasa(config-if)#tunnel source interface outside
```

단계 **5** 터널 대상 IP 주소를 지정합니다.

tunnel destination *IP address*

예제:

```
ciscoasa(config-if)#tunnel destination 10.1.1.1
```

단계 **6** 터널 모드 IPsec IPv4로 터널을 구성합니다.

tunnel mode ipsec *ipv4*

예제:

```
ciscoasa(config-if)#tunnel mode ipsec ipv4
```

단계 **7** IPsec 프로파일을 터널에 할당합니다.

tunnel protection ipsec *IPsec profile*

예제:

```
ciscoasa(config-if)#tunnel protection ipsec Profile1
```

이 새 VTI는 IPsec 사이트 대 사이트 VPN을 생성할 때 사용할 수 있습니다.

13 장

VPN을 위한 외부 AAA 서버 구성

외부 AAA 서버 정보

ASA에 대해 AAA(인증, 권한 부여, 계정 관리)를 지원하기 위해 외부 LDAP, RADIUS 또는 TACACS+ 서버를 사용하도록 이 ASA를 구성할 수 있습니다. 외부 AAA 서버는 구성된 권한 및 특성을 적용합니다. 외부 서버를 사용하도록 ASA를 구성하려면 먼저 올바른 ASA 권한 부여 속성을 사용하여 외부 AAA 서버를 구성해야 하며 이러한 속성의 하위 집합에서 특정한 권한을 개별 사용자에게 할당해야 합니다.

권한 부여 특성의 정책 시행 이해

ASA는 다양한 방법으로 VPN 연결에 사용자 권한 부여 속성(사용자 권한 또는 허가라고도 함)을 적용할 수 있습니다. 다음 조합을 통해 사용자 속성을 얻을 수 있도록 ASA를 구성할 수 있습니다.

- ASA의 DAP(Dynamic Access Policy: 동적 액세스 정책)
- 외부 RADIUS 또는 LDAP 인증 및/또는 권한 부여 서버
- ASA의 그룹 정책

ASA에서 모든 소스의 속성을 수신하면 속성이 평가 및 병합되어 사용자 정책에 적용됩니다. 특성 간에 충돌이 있을 경우 DAP 특성이 우선적으로 적용됩니다.

ASA에서는 다음 순서로 속성을 적용합니다.

1. ASA의 DAP 속성 — 8.0(2) 버전에서 도입된 이러한 속성은 다른 모든 속성보다 우선적으로 적용됩니다. DAP에서 책갈피 또는 URL 목록을 설정하면 그룹 정책에서 설정한 책갈피 또는 URL 목록이 해당 설정으로 재정의됩니다.

2. AAA 서버의 사용자 특성 — 사용자 인증 및/또는 권한 부여가 성공적으로 수행되면 서버에서 이러한 특성을 반환합니다. ASA에서 로컬 AAA 데이터베이스의 개별 사용자에 대해 설정되는 속성과 혼동하지 마십시오(ASDM의 사용자 어카운트).
3. ASA에 구성된 그룹 정책 — RADIUS 서버에서 사용자에 대해 RADIUS CLASS 속성 IETF-Class-25(OU=*group-policy*) 값을 반환하면 에서는 해당 사용자를 이름이 같은 그룹 정책에 배치하고 서버에서 반환하지 않은 그룹 정책의 모든 속성을 적용합니다.

   LDAP 서버의 경우 세션에 대한 그룹 정책을 설정하는 데 모든 특성 이름을 사용할 수 있습니다. ASA에 구성하는 LDAP 속성 맵은 LDAP 속성을 Cisco 속성 IETF-Radius-Class에 매핑합니다.
4. 연결 프로파일을 통해 할당된 그룹 정책(CLI에서는 터널 그룹이라고 함) — 연결 프로파일에는 연결을 위한 예비 설정이 있으며 인증 전에 사용자에게 적용되는 기본 그룹 정책을 포함합니다. ASA에 대한 모든 사용자 연결은 이 그룹에 소속되며 DAP, 서버에서 반환한 사용자 속성 또는 사용자에 할당된 그룹 정책에 없는 모든 속성을 제공합니다.
5. ASA에서 할당한 기본 그룹 정책(DfltGrpPolicy) — 시스템 기본 속성에서는 DAP, 사용자 속성, 그룹 정책 또는 연결 프로필에 없는 모든 값을 제공합니다.

외부 AAA 서버 사용 지침

ASA는 숫자 ID가 아니라 속성 이름을 기반으로 LDAP 속성을 적용합니다. RADIUS 특성은 이름이 아니라 숫자 ID를 통해 적용됩니다.

ASDM 7.0 버전의 경우 LDAP 특성에 cVPN3000 접두사가 포함됩니다. ASDM 7.1 이상 버전의 경우 이 접두사가 제거되었습니다.

LDAP 특성은 Radius 특성의 하위 집합으로, Radius 장에서 설명합니다.

다중 인증서 인증 구성

이제 AnyConnect SSL 및 IKEv2 클라이언트 프로토콜을 사용하여 세션당 여러 인증서를 검증할 수 있습니다. 여러 인증서 인증을 위해 프로토콜 교환을 정의하고 두 가지 세션 유형에 활용하기 위해 Aggregate Authentication 프로토콜이 확장되었습니다. 예를 들어 머신 인증서의 발급자 이름이 특정한 CA와 일치하는지 확인할 수 있으므로 해당 디바이스는 회사에서 발급한 디바이스입니다.

다중 인증서 옵션은 인증서를 통해 머신과 사용자 모두의 인증서 인증을 허용합니다. 이 옵션을 사용하지 않으면 하나 또는 다른 대상에 대한 인증서 인증만 수행할 수 있으며 두 가지 모두에 대한 인증서 인증은 수행할 수 없습니다.

사전 채우기 사용자 이름 필드에서는 인증서의 필드를 구문 분석할 수 있으며 AAA 및 인증서 인증 연결에서 후속 AAA 인증에 사용할 수 있습니다. 기본 및 보조 사전 채우기에 사용할 사용자 이름은 항상 클라이언트에서 수신한 첫 번째 인증서에서 검색됩니다.

다중 인증서 인증을 사용하면 두 개의 인증서가 인증됩니다. 즉, 클라이언트에서 수신한 첫 번째 인증서는 사전 채우기 인증서이며 username-from-certificate은 구문 분석한 기본 및 보조 사용자 이름 인

증서입니다. 그런 다음 어떤 인증서를 첫 번째로 전송하고 두 번째로 전송할지 선택하기 위해 클라이언트에 대해 규칙을 구성할 수 있습니다.

기존 인증 webvpn 속성은 다중 인증서 인증에 대한 옵션을 포함하도록 수정됩니다.

```
tunnel-group <name> webvpn-attributes
authentication {[aaa] [certificate | multiple-certificate] | saml}
```

다중 인증서 인증을 사용하면 연결 시도를 인증하는 데 사용된 인증서의 필드를 기반으로 정책 의사 결정을 수행할 수 있습니다. 다중 인증서 인증 중에 클라이언트에서 수신한 사용자 및 머신 인증서는 인증서 필드를 기반으로 정책을 구성할 수 있도록 DAP에 로드됩니다. DAP(Dynamic Access Policies)를 사용하여 다중 인증서 인증을 추가하여 연결 시도를 허용하거나 허용하지 않도록 규칙을 설정하려면 DAP에서 해당 릴리스의 ASA VPN ASDM 구성 가이드에 여러 인증서 인증 추가를 참조하십시오.

VPN용 LDAP 권한 부여 구성

VPN 액세스를 위한 LDAP 인증이 성공하면 ASA에서 LDAP 서버를 조회하여 LDAP 속성을 반환합니다. 이러한 특성은 일반적으로 VPN 세션에 적용되는 권한 부여 데이터를 포함하고 있습니다.

인증 메커니즘과 독립된 별도의 LDAP 디렉토리 서버에서 권한을 부여해야 할 수도 있습니다. 예를 들어 인증에 SDI 또는 인증서 서버를 사용할 경우 권한 부여 정보가 다시 전달되지 않습니다. 이러한 사용자 권한 부여의 경우 인증에 성공한 후 LDAP 디렉토리를 조회하면 인증 및 권한 부여를 두 단계로 완료할 수 있습니다.

LDAP을 사용하여 VPN 사용자 권한 인증을 설정하려면 다음 단계를 수행합니다.

프로시저

단계 **1** AAA 서버 그룹을 생성합니다.

aaa-server *server_group* **protocol** {**kerberos** | **ldap** | **nt** | **radius** | **sdi** | **tacacs+**}

예제:

```
hostname(config)# aaa-server servergroup1 protocol ldap
hostname(config-aaa-server-group)
```

단계 **2** 이름이 remotegrp인 IPsec 원격 액세스 터널 그룹을 생성합니다.

tunnel-group *groupname*

예제:

```
hostname(config)# tunnel-group remotegrp
```

단계 **3** 서버 그룹과 터널 그룹을 연결합니다.

tunnel-group *groupname* **general-attributes**

예제:

```
hostname(config)# tunnel-group remotegrp general-attributes
```

단계 **4** 권한을 부여하기 위해 새 터널 그룹을 이전에 생성한 AAA 서버 그룹에 할당합니다.
authorization-server-group *group-tag*

예제:

```
hostname(config-general)# authorization-server-group ldap_dir_1
```

예

다음의 예는 LDAP을 통해 사용자 권한 부여를 활성화하는 명령을 보여줍니다. 그런 다음 RAVPN이라는 IPsec 원격 액세스 터널 그룹을 만들고, 권한 부여를 위해 앞서 만든 LDAP AAA 서버 그룹에 새 터널 그룹을 지정합니다.

```
hostname(config)# tunnel-group RAVPN type remote-access
hostname(config)# tunnel-group RAVPN general-attributes
hostname(config-general)# authorization-server-group (inside) LDAP
hostname(config-general)#
```

이 구성 작업을 완료했으면 다음 명령을 사용하여 디렉터리 비밀번호, 디렉터리 검색의 시작점, 디렉터리 검색의 범위와 같은 추가 LDAP 권한 부여 매개변수를 구성할 수 있습니다.

```
hostname(config)# aaa-server LDAP protocol ldap
hostname(config-aaa-server-group)# aaa-server LDAP (inside) host 10.0.2.128
hostname(config-aaa-server-host)# ldap-base-dn DC=AD,DC=LAB,DC=COM
hostname(config-aaa-server-host)# ldap-group-base-dn DC=AD,DC=LAB,DC=COM
hostname(config-aaa-server-host)# ldap-scope subtree
hostname(config-aaa-server-host)# ldap-login-dn AD\cisco
hostname(config-aaa-server-host)# ldap-login-password cisco123
hostname(config-aaa-server-host)# ldap-over-ssl enable
hostname(config-aaa-server-host)# server-type microsoft
```

Active Directory/LDAP VPN 원격 액세스 권한 부여의 예

이 섹션에서는 Microsoft Active Directory 서버를 사용하여 ASA에 인증 및 권한 부여를 구성하는 절차의 예를 보여 줍니다. 여기에는 다음과 같은 항목이 포함됩니다.

- 로그온 시간 및 시간 규칙 적용, 300 페이지

Cisco.com에서 제공하는 기타 구성 예에는 다음 테크노트(TechNote)가 포함되어 있습니다.

- ASA/PIX: LDAP 구성을 통해 VPN 클라이언트를 VPN 그룹 정책에 매핑하는 예
- PIX/ASA 8.0: LDAP 인증을 사용하여 로그인에서 그룹 정책을 할당하는 예

사용자 기반 특성의 정책 시행

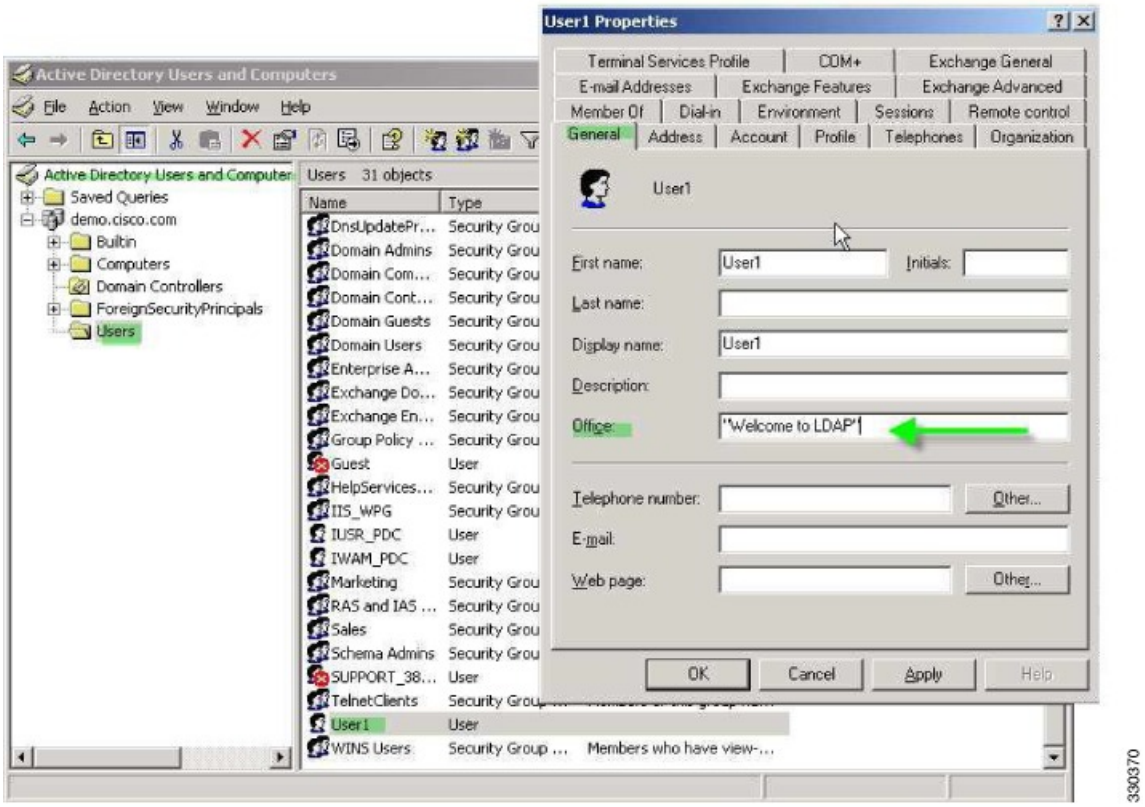
이 예에서는 모든 표준 LDAP 특성을 잘 알려진 VSA(Vendor-Specific Attribute)에 매핑할 수 있으며, 하나 또는 여러 LDAP 특성을 하나 또는 여러 Cisco LDAP 특성에 매핑할 수 있는 방법을 보여주는 간단한 배너를 사용자에게 표시합니다. 이 예는 IPsec VPN 클라이언트, AnyConnect SSL VPN 클라이언트 또는 클라이언트리스 SSL VPN을 포함한 모든 연결 유형에 적용됩니다.

AD LDAP 서버에 구성되어 있는 사용자에게 간단한 배너를 적용하려면 General(일반) 탭의 Office(사무실) 필드를 사용하여 배너 텍스트를 입력합니다. 이 필드는 physicalDeliveryOfficeName이라는 특성을 사용합니다. ASA에서 physicalDeliveryOfficeName을 Cisco 속성 Banner1에 매핑하는 속성 맵을 생성합니다.

인증되는 동안 ASA는 서버에서 physicalDeliveryOfficeName 값을 검색하여 해당 값을 Cisco 속성 Banner1에 매핑하고 사용자에게 배너를 표시합니다.

프로시저

단계 **1** 사용자 이름을 마우스 오른쪽 버튼으로 클릭하고 Properties(속성) 대화 상자를 연 다음 **General(일반)** 탭의 Office(사무실) 필드에 배너 텍스트를 입력합니다. Office(사무실) 필드에서는 AD/LDAP 특성인 physicalDeliveryOfficeName을 사용합니다.



단계 **2** ASA에서 LDAP 속성 맵을 생성합니다.

맵 배너를 생성하고 AD/LDAP 특성 physicalDeliveryOfficeName을 Cisco 특성 Banner1에 매핑합니다.

```
hostname(config)# ldap attribute-map Banner
hostname(config-ldap-attribute-map)# map-name physicalDeliveryOfficeName Banner1
```

단계 **3** LDAP 특성 맵을 AAA 서버에 연결합니다.

호스트 10.1.1.2에 대한 aaa 서버 호스트 구성 모드를 AAA 서버 그룹 MS_LDAP에 입력하고 이전에 생성한 특성 맵 배너를 연계합니다.

```
hostname(config)# aaa-server MS_LDAP host 10.1.1.2
hostname(config-aaa-server-host)# ldap-attribute-map Banner
```

단계 **4** 배너 실행을 테스트합니다.

특정 그룹 정책에 LDAP 사용자 배치

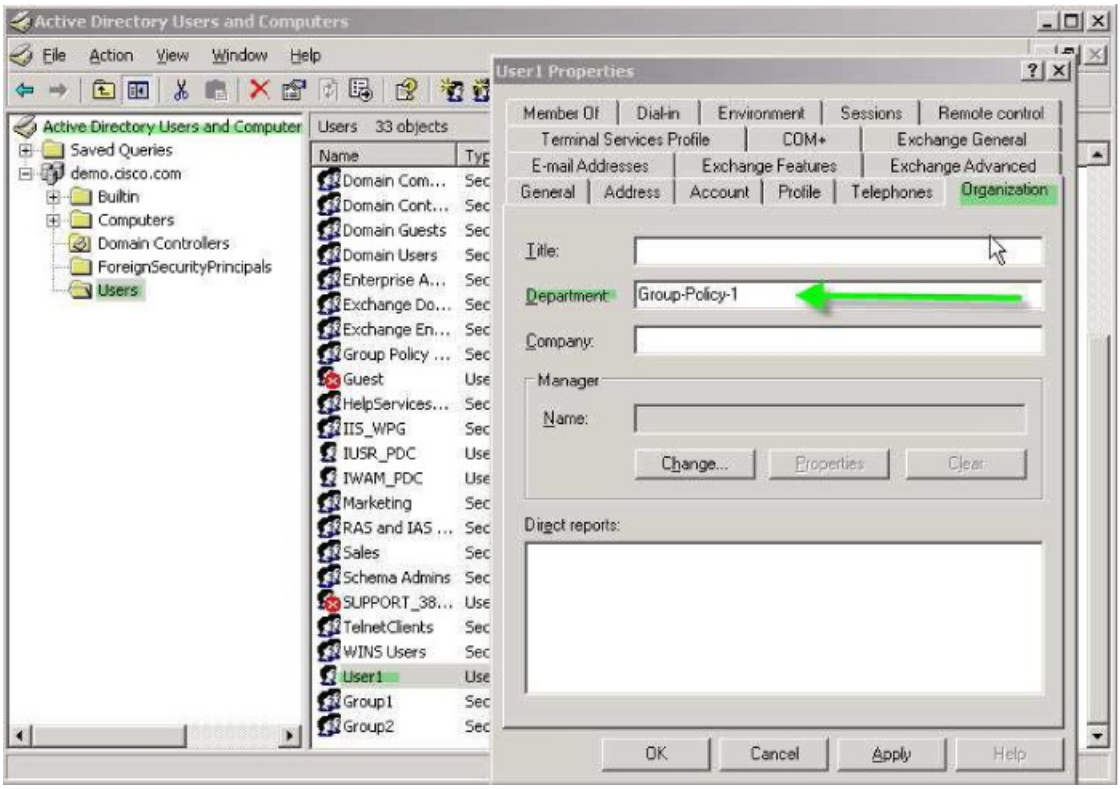
이 예는 IPsec VPN 클라이언트, AnyConnect SSL VPN 클라이언트 또는 클라이언트리스 SSL VPN을 포함한 모든 연결 유형에 적용됩니다. 이 예에서는 클라이언트리스 SSL VPN 연결을 통해 User1을 연결합니다.

특정 그룹 정책에 LDAP 사용자를 배치하려면 Organization(조직) 탭의 Department(부서) 필드를 사용하여 그룹 정책 이름을 입력합니다. 그런 다음 특성 맵을 생성하고, Department를 Cisco 특성 IETF RADIUS CLASS에 매핑합니다.

인증되는 동안 ASA는 서버에서 Department 값을 검색하여 해당 값을 IETF-Radius-Class에 매핑하고 User1을 그룹 정책에 배치합니다.

프로시저

단계 **1** 사용자 이름을 마우스 오른쪽 버튼으로 클릭하고 Properties(속성) 대화 상자를 연 다음 **Organization(**조직**)** 탭의 Department(부서) 필드에 **Group-Policy-1**을 입력합니다.



단계 **2** LDAP 구성에 대한 특성 맵을 정의합니다.

AD 특성 Department를 Cisco 특성 IETF-Radius-Class에 매핑합니다.

```
hostname(config)# ldap attribute-map group_policy
hostname(config-ldap-attribute-map)# map-name Department IETF-Radius-Class
```

단계 **3** LDAP 특성 맵을 AAA 서버에 연결합니다.

호스트 10.1.1.2에 대한 aaa 서버 호스트 구성 모드를 AAA 서버 그룹 MS_LDAP에 입력하고 이전에 생성한 특성 맵 그룹 정책을 연결합니다.

```
hostname(config)# aaa-server MS_LDAP host 10.1.1.2
hostname(config-aaa-server-host)# ldap-attribute-map group_policy
```

단계 **4** 서버에서 Department(부서) 필드에 입력한 대로 그룹 정책, *Group-policy-1*을 추가하고 ASA에서 사용자에게 할당할 필수 정책 속성을 구성합니다.

```
hostname(config)# group-policy Group-policy-1 external server-group LDAP_demo
hostname(config-aaa-server-group)#
```

단계 **5** 사용자가 하는 것처럼 VPN 연결을 설정하고 세션이 Group-Policy1(및 기본 그룹 정책의 적용 가능한 모든 기타 특성)에서 특성을 상속받는지 확인합니다.

단계 **6** 특권 EXEC 모드에서 **debug ldap 255** 명령을 활성화하여 ASA와 서버 간 통신을 모니터링합니다. 다음은 이 명령의 샘플 출력이며, 핵심 메시지가 표시되도록 수정되었습니다.

```
[29] Authentication successful for user1 to 10.1.1.2
[29] Retrieving user attributes from server 10.1.1.2
[29] Retrieved Attributes:
[29] department: value = Group-Policy-1
[29] mapped to IETF-Radius-Class: value = Group-Policy-1
```

AnyConnect 터널에 고정 IP 주소 할당 적용

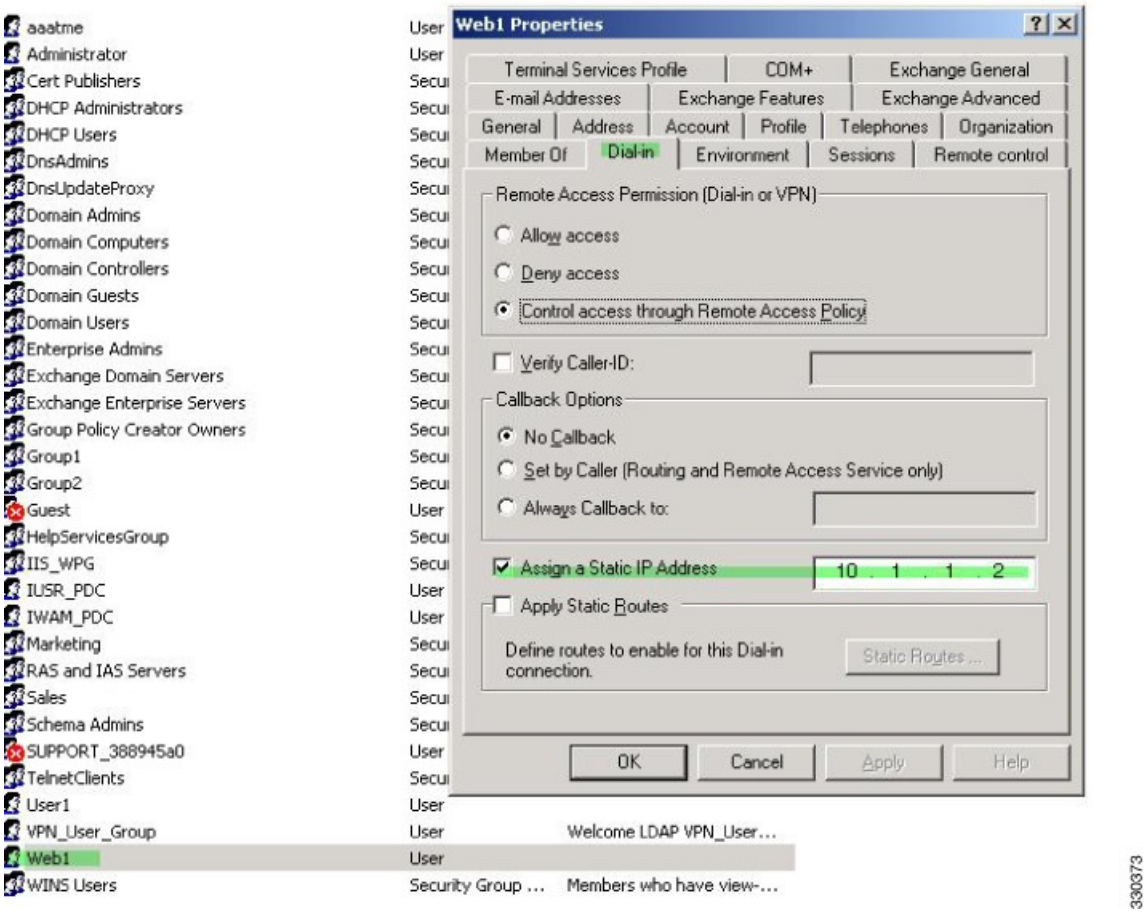
이 예는 IPsec 클라이언트 및 SSL VPN 클라이언트 등 전체 터널 클라이언트에 적용됩니다.

고정 AnyConnect의 고정 IP 할당을 적용하려면 AnyConnect 클라이언트 사용자 Web1이 고정 IP 주소를 수신하도록 구성하고 이 주소를 AD LDAP 서버에 있는 Dialin(다이얼인) 탭의 Assign Static IP Address(고정 IP 주소 할당) 필드에 입력합니다. 이 필드는 msRADIUSFramedIPAddress 특성을 사용합니다. 이 특성을 Cisco 특성인 IETF-Radius-Framed-IP-Address에 매핑하는 특성 맵을 생성합니다.

인증되는 동안 ASA는 서버에서 msRADIUSFramedIPAddress 값을 검색하여 해당 값을 Cisco 속성 IETF-Radius-Framed-IP-Address에 매핑하고 User1에게 고정 주소를 제공합니다.

프로시저

단계 **1** 사용자 이름을 마우스 오른쪽 버튼으로 클릭하고 Properties(속성) 대화 상자를 연 다음 **Dial-in(**다이얼인**)** 탭에서 **Assign Static IP Address(**고정 **IP** 주소 할당**)** 확인란을 선택하고 IP 주소 10.1.1.2를 입력합니다.



단계 **2** 표시된 LDAP 구성에 대한 특성 맵을 생성합니다.

다음과 같이 Static Address(고정 주소) 필드에서 사용하는 AD 특성 msRADIUSFramedIPAddress를 Cisco 특성 IETF-Radius-Framed-IP-Address에 매핑합니다.

```
hostname(config)# ldap attribute-map static_address
hostname(config-ldap-attribute-map)# map-name msRADIUSFramedIPAddress
IETF-Radius-Framed-IP-Address
```

단계 **3** LDAP 특성 맵을 AAA 서버에 연결합니다.

호스트 10.1.1.2에 대한 aaa 서버 호스트 구성 모드를 AAA 서버 그룹 MS_LDAP에 입력하고 이전에 생성한 특성 맵 static_address를 연계합니다.

```
hostname(config)# aaa-server MS_LDAP host 10.1.1.2
hostname(config-aaa-server-host)# ldap-attribute-map static_address
```

단계 **4** 구성의 이 부분을 살펴보고 AAA를 지정하도록 **vpn-address-assignment** 명령이 구성되었는지 확인합니다.

```
hostname(config)# show run all vpn-addr-assign
vpn-addr-assign aaa   << Make sure this is configured >>
no vpn-addr-assign dhcp
vpn-addr-assign local
hostname(config)#
```

단계 **5** AnyConnect 클라이언트를 사용하여 ASA와 연결을 설정합니다. 사용자가 서버에 구성되어 ASA에 매핑된 IP 주소를 수신하는지 확인합니다.

단계 **6** **show vpn-sessiondb svc** 명령을 사용하여 세션 세부사항을 보고 주소가 할당되었는지 확인합니다.

```
hostname# show vpn-sessiondb svc

Session Type: SVC
Username     : web1                   Index        : 31
Assigned IP  : 10.1.1.2              Public IP    : 10.86.181.70
Protocol     : Clientless SSL-Tunnel DTLS-Tunnel
Encryption   : RC4 AES128             Hashing      : SHA1
Bytes Tx     : 304140                 Bytes Rx     : 470506
Group Policy : VPN_User_Group         Tunnel Group : Group1_TunnelGroup
Login Time   : 11:13:05 UTC Tue Aug 28 2007
Duration     : 0h:01m:48s
NAC Result   : Unknown
VLAN Mapping : N/A                    VLAN         : none
```

다이얼인 액세스 허용 또는 액세스 거부 적용

이 예에서는 사용자가 허용한 터널링 프로토콜을 지정하는 LDAP 특성 맵을 생성합니다. Dialin(다이얼인) 탭의 Allow access(액세스 허용) 및 Deny access(액세스 거부) 설정을 Cisco 특성 Tunneling-Protocol에 매핑합니다. 이 특성은 다음 비트맵 값을 지원합니다.

값	터널링 프로토콜
1	PPTP
2	L2TP
4	IPsec(IKEv1)
8	L2TP/IPsec
16	클라이언트리스 SSL
32	SSL 클라이언트 — AnyConnect 또는 SSL VPN 클라이언트
64	IPsec(IKEv2)

[1] (1) IPsec과 L2TP over IPsec은 동시에 지원되지 않습니다. 따라서 값 4와 8은 동시에 사용할 수 없습니다.

[2] (2) 참고 1을 참조하십시오.

이 특성을 사용하여 프로토콜에 대해 액세스 허용(TRUE) 또는 액세스 거부(FALSE) 조건을 생성하고 사용자 액세스가 허용되는 방법을 적용합니다.

다이얼인 액세스 허용 또는 액세스 거부의 또 다른 예는 테크노트 ASA/PIX: LDAP 구성을 통해 VPN 클라이언트를 VPN 그룹 정책에 매핑 예를 참조해 주십시오.

프로시저

단계 **1** 사용자 이름을 마우스 오른쪽 버튼으로 클릭하고 Properties(속성) 대화 상자를 연 다음 **Dial-in(**다이얼인**)** 탭에서 Allow Access(액세스 허용) 라디오 버튼을 클릭합니다.

참고 Control access through the Remote Access Policy(원격 액세스 정책을 통해 액세스 제어) 옵션을 선택할 경우 서버에서 값이 반환되지 않으며, 적용되는 권한은 ASA의 내부 그룹 정책 설정을 기반으로 합니다.

단계 **2** IPsec과 AnyConnect 연결을 모두 허용하는 특성 맵을 생성하십시오. 단, 클라이언트리스 SSL 연결은 거부해야 합니다.

a) 맵 tunneling_protocols를 생성합니다.

```
hostname(config)# ldap attribute-map tunneling_protocols
```

b) Allow Access(액세스 허용) 설정에서 사용하는 AD 특성 msNPAllowDialin을 Cisco 특성 Tunneling-Protocols에 매핑합니다.

```
hostname(config-ldap-attribute-map)# map-name msNPAllowDialin Tunneling-Protocols
```

c) 맵 값을 추가합니다.

```
hostname(config-ldap-attribute-map)# map-value msNPAllowDialin FALSE 48
hostname(config-ldap-attribute-map)# map-value msNPAllowDialin TRUE 4
```

단계 **3** LDAP 특성 맵을 AAA 서버에 연결합니다.

a) 호스트 10.1.1.2에 대한 aaa 서버 호스트 구성 모드를 AAA 서버 그룹 MS_LDAP에 입력합니다.

```
hostname(config)# aaa-server MS_LDAP host 10.1.1.2
```

b) 사용자가 생성한 특성 맵 tunneling_protocols를 연계합니다.

```
hostname(config-aaa-server-host)# ldap-attribute-map tunneling_protocols
```

단계 **4** 특성 맵이 구성된 대로 작동하는지 확인합니다.

클라이언트리스 SSL을 사용하여 연결을 시도합니다. 사용자에게는 무단 연결 메커니즘 때문에 연결에 실패했다는 알림이 제공됩니다. IPsec은 특성 맵에 따라 허용되는 터널링 프로토콜이므로 IPsec 클라이언트가 연결됩니다.

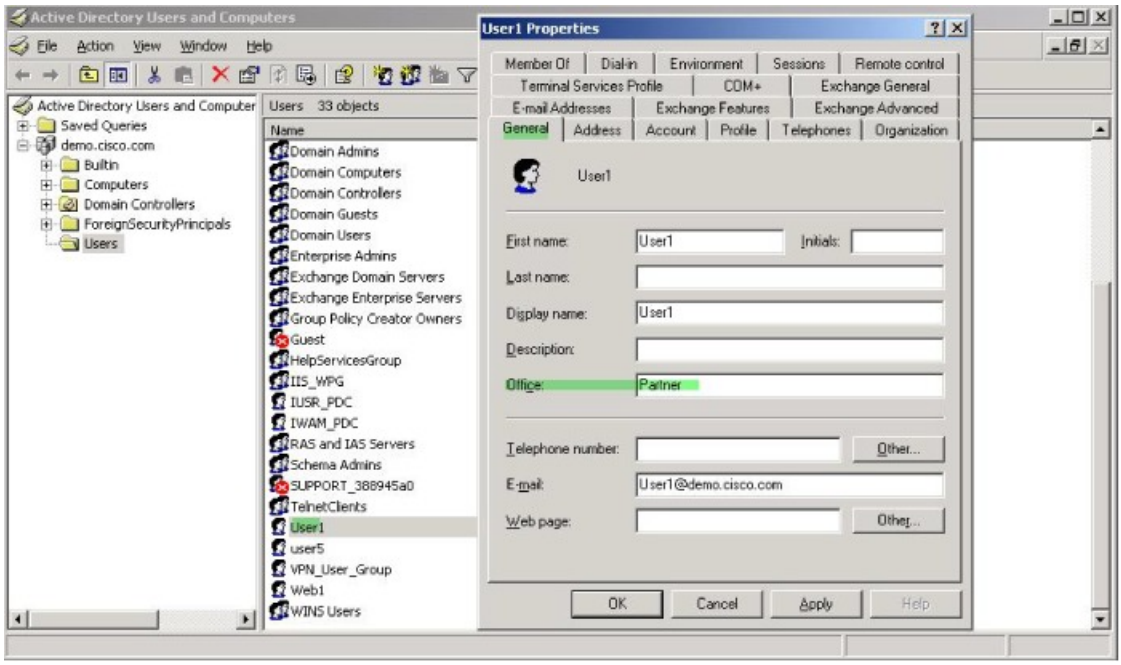
로그온 시간 및 시간 규칙 적용

다음 예에서는 비즈니스 파트너 같은 클라이언트리스 SSL 사용자가 네트워크에 액세스할 수 있도록 시간을 구성하고 적용하는 방법을 보여 줍니다.

AD 서버에서 Office(사무실) 필드를 사용하여 파트너 이름을 입력합니다. 이 필드에서는 physicalDeliveryOfficeName 특성을 사용합니다. 그런 다음 ASA에서 속성 맵을 생성하여 해당 속성을 Cisco 속성 Access-Hours에 매핑합니다. 인증되는 동안 ASA는 physicalDeliveryOfficeName 값을 검색하여 Access-Hours에 매핑합니다.

프로시저

단계 **1** 사용자를 선택하고 **Properties(**속성**)**를 마우스 오른쪽 버튼으로 클릭하고 **General(**일반**)** 탭을 엽니다.



단계 **2** 특성 맵을 생성합니다.

특성 맵 access_hours를 생성하여 Office 필드에서 사용하는 AD 특성 physicalDeliveryOfficeName을 Cisco 특성 Access-Hours에 매핑합니다.

```
hostname(config)# ldap attribute-map access_hours
hostname(config-ldap-attribute-map)# map-name physicalDeliveryOfficeName Access-Hours
```

단계 **3** LDAP 특성 맵을 AAA 서버에 연결합니다.

호스트 10.1.1.2에 대한 aaa 서버 호스트 구성 모드를 AAA 서버 그룹 MS_LDAP에 입력하고 생성한 특성 맵 access_hours를 연계합니다.

```
hostname(config)# aaa-server MS_LDAP host 10.1.1.2
hostname(config-aaa-server-host)# ldap-attribute-map access_hours
```

단계 **4** 서버에서 허용되는 각 값의 시간 범위를 구성합니다.

파트너 액세스 시간을 월~금요일 오전 9시부터 오후 5시로 구성합니다.

```
hostname(config)# time-range Partner
hostname(config-time-range)# periodic weekdays 09:00 to 17:00
```

II 부

클라이언트리스 SSL VPN

14 장

클라이언트리스 SSL VPN 개요

클라이언트리스 SSL VPN 소개

클라이언트리스 SSL VPN을 통해 엔드 유저는 SSL 지원 웹 브라우저를 사용하여 어디에서나 기업 네트워크에 있는 리소스에 안전하게 액세스할 수 있습니다. 사용자는 먼저 클라이언트리스 SSL VPN 게이트웨이를 통해 인증된 다음 미리 구성된 네트워크 리소스에 액세스합니다.

참고 클라이언트리스 SSL VPN이 활성화된 경우 보안 상황(방화벽 다중 모드라고도 함) 및 활성/활성 상태 저장 장애 조치는 지원되지 않습니다.

클라이언트리스 SSL VPN은 소프트웨어 또는 하드웨어 클라이언트를 요청하지 않고 웹 브라우저를 사용하여 ASA에 대해 안전한 원격 액세스 VPN 터널을 생성합니다. 또한 HTTP를 통해 인터넷에 연결할 수 있는 거의 모든 디바이스의 광범위한 웹 리소스, 웹 지원 애플리케이션 및 레거시 애플리케이션 모두에 안전하고 쉽게 액세스할 수 있도록 지원합니다. 그 기능은 다음과 같습니다.

- 내부 웹 사이트
- 웹 지원 애플리케이션
- NT/Active Directory 파일 공유
- Microsoft Outlook Web Access Exchange Server 2000, 2003, 2007 및 2013
- Exchange Server 2010, 8.4(2) 이상에 대한 Microsoft Web App
- Application Access(다른 TCP 기반 애플리케이션에 대한 스마트 터널 또는 포트 전달 액세스)

클라이언트리스 SSL VPN에서는 SSL/TLS1(Secure Sockets Layer 프로토콜과 그 후속 프로토콜 및 전송 계층 보안)을 사용하여 원격 사용자와 내부 서버로 구성한 지원되는 특정 내부 리소스 간의 보안

연결을 제공합니다. ASA는 프록시가 필요한 연결을 인식하고 HTTP 서버는 사용자를 인증하기 위해 인증 하위 시스템과 상호 작용합니다.

네트워크 관리자는 그룹을 기준으로 하여 클라이언트리스 SSL VPN 세션 사용자별로 리소스에 대한 액세스를 제공합니다. 사용자는 내부 네트워크의 리소스에 직접 액세스할 수 없습니다.

클라이언트리스 SSL VPN에 대한 사전 요구 사항

ASA의 클라이언트리스 SSL VPN에서 지원하는 플랫폼 및 브라우저에 대해서는 지원되는 VPN 플랫폼, Cisco ASA 5500 Series의 내용을 참조하십시오.

클라이언트리스 SSL VPN에 대한 지침 및 제한 사항

- ActiveX 페이지에서 ActiveX Relay를 활성화하거나 연계된 그룹 정책에 **activex-relay**를 입력해야 합니다. 이 명령을 입력하거나 스마트 터널 목록을 정책에 할당하고 엔드포인트에 있는 브라우저 프록시 예외 목록에서 프록시를 지정하는 경우, 사용자는 "shutdown.webvpn.relay." 항목을 해당 목록에 추가해야 합니다.
- ASA는 Windows 7, Vista, Internet Explorer 8-10, Mac OS X 또는 Linux의 Windows 공유(CIFS) 웹 폴더에 대해 클라이언트리스 액세스를 지원하지 않습니다.
- DoD 공통 액세스 카드 및 스마트 카드를 포함하는 인증서 인증은 Safari 키체인에서만 작동합니다.
- 클라이언트리스 연결에 대해 신뢰할 수 있는 인증서를 설치한 경우에도 클라이언트는 신뢰할 수 없는 인증서 경고를 볼 수 있습니다.
- ASA는 클라이언트리스 SSL VPN 연결에 대해 DSA 또는 RSA 인증서를 지원하지 않습니다. RSA 인증서는 지원됩니다.
- 일부 도메인 기반 보안 제품에는 ASA에서 시작되는 이러한 요청 이외의 요구 사항이 있습니다.
- Modular Policy Framework의 구성 제어 검사 및 기타 검사 기능은 지원되지 않습니다.
- 그룹 정책의 **vpn-filter** 명령은 클라이언트 기반 액세스용이므로 지원되지 않습니다. 그룹 정책에서 클라이언트리스 SSL VPN 모드의 **Filter**는 클라이언트리스 기반 액세스 전용입니다.
- NAT와 PAT는 클라이언트에 적용되지 않습니다.
- ASA는 **police** 또는 **priority-queue** 같은 QoS rate-limiting 명령을 사용하도록 지원하지 않습니다.
- ASA는 연결 제한 사용을 지원하지 않으며 정적 또는 Modular Policy Framework **set connection** 명령을 통해 확인할 수 있습니다.
- 클라이언트리스 SSL VPN의 일부 구성 요소에는 JRE(Java Runtime Environment)가 필요합니다. Mac OS X v10.7 이상에서는 Java가 기본적으로 설치되지 않습니다. Mac OS X에 Java를 설치하는 방법에 대한 자세한 내용은 http://java.com/en/download/faq/java_mac.xml을 참조하십시오.

- 클라이언트리스 VPN 세션이 시작되면 RADIUS 어카운팅 시작 메시징이 생성됩니다. 주소가 클라이언트리스 VPN 세션에 할당되지 않으므로 시작 메시지에는 Framed IP 주소가 포함되지 않습니다. 클라이언트리스 포털 페이지에서 Layer3 VPN 연결을 후속 작업으로 시작한 후에 주소가 할당되고 중간 업데이트 어카운팅 메시지로 RADIUS 서버에 보고됩니다. weblaunch 기능을 사용하여 Layer3 VPN 터널을 설정할 때 유사한 RADIUS 동작을 예측할 수 있습니다. 이 경우 어카운팅 시작 메시지는 사용자가 인증된 이후에 Layer3 터널이 설정되기 전에 Framed IP 주소 없이 전송됩니다. 이 시작 메시지 뒤에는 Layer3 터널이 설정된 후에 중간 업데이트 메시지가 나타납니다.

클라이언트리스 포털에 대해 여러 그룹 정책을 구성한 경우 로그온 페이지의 드롭다운 목록에 표시됩니다. 목록에 있는 첫 번째 그룹 정책에 인증서가 필요한 경우 사용자에게 일치하는 인증서가 있어야 합니다. 일부 그룹 정책에서 인증서를 사용하지 않는 경우, 인증서 없는 정책을 먼저 표시하도록 목록을 구성해야 합니다. 또는 이름이 “0-Select-a-group.”인 더미 그룹 정책을 생성할 수도 있습니다.

팁 알파벳순으로 또는 이름 앞에 숫자를 붙여 그룹 정책의 이름을 지정하여 먼저 표시할 정책을 제어할 수 있습니다(예: 1-AAA, 2-Certificate).

클라이언트리스 SSL VPN에 대한 라이센싱

AnyConnect Secure Mobility Client를 사용하려면 AnyConnect Plus 및 Apex 라이선스를 구매해야 합니다. 필요한 라이선스는 사용하려는 AnyConnect VPN 클라이언트와 Secure Mobility 기능 및 지원하려는 세션 수에 따라 다릅니다. 이러한 사용자 기반 라이선스에는 일반적인 BYOD 트렌드에 맞추기 위한 지원 및 소프트웨어 업데이트에 대한 액세스가 포함됩니다.

AnyConnect 4.4 라이선스는 ASA(및 ISR, CSR, ASR) 뿐만 아니라 ISE(Identity Services Engine), CWS(Cloud Web Security) 및 WSA(Web Security Appliance)와 같은 기타 비 VPN 헤드엔드와 함께 사용됩니다. 헤드엔드와 관계없이 일관된 모델이 사용되므로 헤드엔드 마이그레이션이 발생하더라도 아무런 영향을 미치지 않습니다.

AnyConnect용 라이선싱 모델에 대한 모든 설명은 http://www.cisco.com/c/dam/en/us/products/collateral/security/anyconnect-og.pdf의 내용을 참조하십시오.

15 장

기본 클라이언트리스 SSL VPN 구성

각 URL 재작성

기본적으로 ASA는 모든 웹 리소스(예: HTTPS, CIFS, RDP 및 플러그인)에 대해 모든 포털 트래픽을 허용합니다. 클라이언트리스 SSL VPN은 ASA에만 유효한 리소스에 각 URL을 재작성합니다. 사용자는 이 URL을 사용하여 요청한 웹사이트에 연결되어 있는지 확인할 수 없습니다. 사용자가 피싱 웹사이트에 연결되는 위험한 상황에 처하지 않도록 클라이언트리스 액세스에 대해 구성된 정책(그룹 정책, 동적 액세스 정책 또는 두 가지 모두)에 웹 ACL을 할당하여 포털의 트래픽 흐름을 제어해야 합니다. 액세스 가능한 URL에 대한 사용자의 혼란을 방지하기 위해 이러한 정책에서 URL 입력을 해제할 것을 권장합니다.

그림 ***6:*** 사용자가 입력하는 ***URL*** 예

그림 7: 보안 어플라이언스가 재작성하고 브라우저 창에 표시되는 동일한 *URL*

포털 페이지에서 URL 입력 해제

사용자가 브라우저 기반 연결을 설정할 때 포털 페이지가 열립니다.

시작하기 전에

클라이언트리스 SSL VPN 액세스를 필요로 하는 모든 사용자에 대해 그룹 정책을 구성하고 해당 그룹 정책에 대해서만 클라이언트리스 SSL VPN을 활성화합니다.

프로시저

단계 **1** group policy 클라이언트리스 SSL VPN 구성 모드로 전환합니다.

webvpn

단계 **2** 사용자의 HTTP/HTTPS URL 입력 가능 여부를 제어합니다.

url-entry

단계 **3** (선택 사항) URL 입력을 해제합니다.

url-entry disable

신뢰할 수 있는 인증서 풀

ASA는 신뢰할 수 있는 인증서를 신뢰 풀로 그룹화합니다. 신뢰 풀은 알려진 여러 CA 인증서를 나타내는 트러스트 포인트의 특별한 사례로 간주할 수 있습니다. ASA에는 웹 브라우저와 함께 제공되는 인증서 번들과 유사한 인증서의 기본 번들이 포함되어 있습니다. 관리자가 crypto ca import default 명령을 실행하여 활성화할 때까지 이 기본 번들은 비활성 상태로 있습니다.

웹 브라우저에서 HTTPS 프로토콜을 사용하여 원격 서버에 연결하는 경우, 서버는 자체 식별을 위해 CA에서 서명한 디지털 인증서를 제공합니다. 웹 브라우저에는 서버 인증서의 유효성을 확인하는 데 사용되는 CA 인증서의 컬렉션이 포함되어 있습니다.

클라이언트리스 SSL VPN을 통해 원격 SSL 활성화 서버에 연결할 경우, 원격 서버를 신뢰할 수 있는지, 올바른 원격 서버에 연결 중인지를 아는 것이 중요합니다. ASA 9.0은 클라이언트리스 SSL VPN에 대해 신뢰할 수 있는 CA(Certificate Authority: 인증 기관) 인증서 목록을 대상으로 SSL 서버 인증서 확인을 지원하기 시작했습니다.

Configuration(구성**)** > **Remote Access VPN(**원격 액세스 **VPN)** > **Certificate Management(**인증서 관리**)** > **Trusted Certificate Pool(**신뢰할 수 있는 인증서 풀**)**에서 https 사이트에 대한 SSL 연결을 위해 인증서 확인을 활성화할 수 있습니다. 신뢰할 수 있는 인증서 풀에서 인증서를 관리할 수도 있습니다.

참고 ASA 신뢰 풀은 Cisco IOS 신뢰 풀과 유사하지만 동일하지는 않습니다.

신뢰 풀 인증서의 자동 가져오기 구성

스마트 라이선싱은 Smart Call Home 인프라를 사용합니다. ASA가 Smart Call Home 백그라운드에서 익명 보고를 구성하면 ASA에서 자동으로 Call Home 서버 인증서를 발급한 CA 인증서를 포함하는 트러스트 포인트를 생성합니다. ASA는 이제 인증서 계층 구조 변경 사항을 조정하기 위해 고객이 참여할 필요 없이 서버 인증서 변경 사항의 계층 구조를 발급하는 경우, 인증서 유효성 검사를 지원합니다. CA 서버의 자체 서명된 인증서가 변경되는 경우 해당 Smart Call Home이 활성 상태로 남아 있을 수 있도록 신뢰 풀 번들의 업데이트를 주기적으로 자동화할 수 있습니다. 다중 상황 구축에서는 이 기능이 지원되지 않습니다.

신뢰 풀 인증서 번들의 자동 가져오기를 수행하려면 ASA에서 번들을 다운로드하고 가져오기 위해 사용하는 URL을 지정해야 합니다. 기본 Cisco URL을 사용하며 기본 시간이 22시간인 기본 간격으로 매일 가져오기를 수행하려면 다음 명령을 사용하십시오.

```
ciscoasa(config-ca-trustpool)# auto-import-url Default
```

다음 명령을 사용하여 맞춤형 URL로 자동 가져오기를 활성화할 수도 있습니다.

```
ciscoasa(config-ca-trustpool)# auto-import url http://www.thawte.com
```

피크 시간 또는 다른 편리한 시간 동안 다운로드하도록 설정하는 유연한 기능을 활용하려면 맞춤형 시간에 가져오기를 활성화하는 다음 명령을 입력하십시오.

```
ciscoasa(config-ca-trustpool)# auto-import time 23:23:23
```

맞춤형 URL 및 맞춤형 시간에 자동 가져오기를 설정하려면 다음 명령이 필요합니다.

```
ciscoasa(config-ca-trustpool)# auto-import time 23:23:23 url http://www.thawte.com
```

신뢰 풀 정책의 상태 표시

신뢰 풀 정책의 현재 상태를 확인하려면 다음 명령을 사용하십시오.

```
show crypto ca trustpool policy
```

이 명령은 다음과 같은 정보를 반환합니다.

```
0 trustpool certificates installed
Trustpool auto renewal statistics:
 State: Not in progress
 Last import result: Not attempted N/A
 Current Jitter: 0

Trustpool auto import statistics:
 Last import result: N/A
 Next schedule import at 22:00:00 Tues Jul 21 2015

Trustpool Policy
```

```
 Trustpool revocation checking is disabled.
 CRL cache time: 60 seconds
 CRL next update field: required and enforced
 Auto import of trustpool is enabled
 Automatic import URL: http://www.cisco.com/security/pki/trs/ios_core.p7b
 Download time: 22:00:00

Policy Overrides:
 None configured
```

CA 신뢰 풀 지우기

신뢰 풀 정책을 기본 상태로 재설정하려면 다음 명령을 사용하십시오.

```
clear configure crypto ca trustpool
```

트러스트 포인트 인증서 자동 가져오기가 기본적으로 해제되어 있으므로 이 명령을 사용하면 이 기능이 비활성화됩니다.

신뢰할 수 있는 인증서 풀의 정책 수정

프로시저

단계 **1** Revocation Check(해지 확인) - 풀에서 인증서 해지를 확인할지 여부를 구성한 다음, CLR을 사용할지 아니면 OCSP를 사용할지, 그리고 해지 확인에 실패할 경우 인증서를 무효화할지 여부를 선택합니다.

단계 **2** Certificate Matching Rules(인증서 일치 규칙) - 해지 또는 만료 확인에서 면제할 인증서 맵을 선택합니다. 인증서 맵은 인증서를 AnyConnect 또는 클라이언트리스 SSL 연결 프로파일(터널 그룹이라고도 함)에 연결합니다.

단계 **3** CRL 옵션 - 1~1440분(1140분은 24시간) 사이에서 CRL 캐시를 새로 고치는 빈도를 결정합니다.

단계 **4** 자동 가져오기 - Cisco는 신뢰할 수 있는 CA의 "기본" 목록을 정기적으로 업데이트합니다. Enable Automatic Import(자동 가져오기 활성화)를 선택하고 기본 설정을 유지하는 경우, ASA는 24시간 마다 Cisco 사이트에서 신뢰할 수 있는 CA의 업데이트된 목록을 확인합니다. 목록이 변경된 경우, ASA는 새로운 신뢰할 수 있는 기본 CA 목록을 다운로드하고 가져옵니다.

플러그인에 대한 브라우저 액세스 구성

브라우저 플러그인은 웹 브라우저가 브라우저 창 내에서 클라이언트를 서버에 연결하는 등의 전용 기능을 수행하기 위해 호출하는 별도의 프로그램입니다. ASA를 사용하면 클라이언트리스 SSL VPN 세션에서 원격 브라우저로 다운로드할 플러그인을 가져올 수 있습니다. Cisco에서는 재배포하는 플러그인을 테스트하며, 경우에 따라 재배포할 수 없는 플러그인의 연결성을 테스트합니다. 그러나 현재 스트리밍 미디어를 지원하는 플러그인 가져오기는 권장하지 않습니다.

ASA는 플래시 디바이스에 플러그인을 설치할 때 다음 작업을 수행합니다.

- (Cisco 배포 플러그인만 해당) URL에 지정되어 있는 jar 파일의 압축을 풉니다.

- 파일을 ASA 파일 시스템에 작성합니다.
- ASDM에서 URL 특성 옆에 있는 드롭다운 목록을 채웁니다.
- 이후의 모든 클라이언트리스 SSL VPN 세션에 대해 플러그인을 활성화하고 포털 페이지의 Address(주소) 필드 옆에 있는 드롭다운 목록에 기본 메뉴 옵션 및 옵션을 추가합니다.

다음 페이지에는 다음 섹션에 설명된 플러그인을 추가할 경우 포털 페이지의 기본 메뉴 및 주소 필드에 대한 변경 사항이 나와 있습니다.

표 ***12:*** 클라이언트리스 ***SSL VPN*** 포털 페이지에 있는 플러그인의 효과

플러그인	포털 페이지에 추가된 기본 메뉴 옵션	포털 페이지에 추가된 주소 필드 옵션
ica	Citrix MetaFrame 서비스	ica://
rdp	Terminal Servers	rdp://
rdp2*	Terminal Servers Vista	rdp2://
ssh,telnet	SSH(Secure Shell)	ssh://
	텔넷 서비스(v1 및 v2 지원)	telnet://
vnc	가상 네트워크 컴퓨팅 서비스	vnc://

* 권장 플러그인이 아닙니다.

클라이언트리스 SSL VPN 세션에 있는 사용자가 포털 페이지에서 관련 메뉴 옵션을 클릭하면 포털 페이지에는 인터페이스에 대한 창과 도움말 창이 표시됩니다. 사용자가 드롭다운 목록에 표시된 프로토콜을 선택하고 주소 필드에서 URL을 입력하여 연결을 설정할 수 있습니다.

플러그인은 SSO(Single Sign-On: 단일 로그인)를 지원합니다.

플러그인의 사전 요구 사항

- 클라이언트리스 SSL VPN은 플러그인에 대한 원격 액세스를 제공하도록 ASA에서 활성화되어 있어야 합니다.
- 플러그인에 대한 SSO 지원을 구성하려면 플러그인을 설치하고 책갈피 항목을 추가하여 서버에 대한 링크를 표시하고 책갈피를 추가할 때 SSO 지원을 지정하십시오.
- 원격 사용에 필요한 최소 액세스 권한은 게스트 권한 모드에 속합니다.
- 플러그인을 사용하려면 ActiveX 또는 Oracle JRE(Java Runtime Environment)가 필요합니다. 버전 요건에 대해서는 지원되는 VPN 플랫폼, Cisco ASA 5500 Series 호환성 매트릭스를 참조하십시오.

플러그인의 제한 사항

참고 원격 데스크톱 프로토콜 플러그인은 세션 브로커를 통한 로드 밸런싱을 지원하지 않습니다. 프로토콜에서 세션 브로커의 리디렉션을 처리하는 방식으로 인해 연결이 실패합니다. 세션 브로커를 사용하지 않는 경우 플러그인이 작동합니다.

- 플러그인은 SSO(Single Sign-On: 단일 로그인)를 지원합니다. 플러그인은 입력된 동일한 자격 증명을 사용하여 클라이언트리스 SSL VPN 세션을 엽니다. 플러그인은 매크로 대체를 지원하지 않으므로 내부 도메인 비밀번호와 같은 다른 필드나 RADIUS 또는 LDAP 서버의 특성에서 SSO를 수행하는 옵션을 제공하지 않습니다.
- 상태 저장 장애 조치는 플러그인을 사용하여 설정된 세션을 그대로 유지하지 않습니다. 사용자는 장애 조치 후 다시 연결해야 합니다.
- 상태 저장 장애 조치 대신 상태 비저장 장애 조치를 사용하는 경우에는 클라이언트리스 기능(예: 책갈피, 사용자 지정 및 동적 액세스 정책 등)이 장애 조치 ASA 쌍 간에 동기화되지 않습니다. 장애 조치 시 이러한 기능이 작동하지 않습니다.

플러그인 설치 전 보안 어플라이언스 준비

시작하기 전에

클라이언트리스 SSL VPN이 ASA 인터페이스에서 활성화되어 있는지 확인합니다.

IP 주소를 SSL 인증서의 CN(Common Name: 공통 이름)으로 지정하지 마십시오. 원격 사용자는 FQDN을 사용하여 ASA와의 통신을 시도합니다. 원격 PC에서 DNS 또는 System32\drivers\etc\hosts 파일의 항목을 사용하여 FQDN을 확인할 수 있어야 합니다.

프로시저

단계 **1** 클라이언트리스 SSL VPN이 ASA에서 활성화되어 있는지를 표시합니다.

show running-config

단계 **2** ASA 인터페이스에 SSL 인증서를 설치하고 원격 사용자 연결을 위해 FQDN(Fully Qualified Domain Name)을 제공합니다.

Cisco에서 재배포하는 플러그인 설치

Cisco에서는 클라이언트리스 SSL VPN 세션에서 웹 브라우저용 플러그인으로 액세스되는 다음의 오픈 소스 Java 기반 구성 요소를 재배포합니다.

시작하기 전에

클라이언트리스 SSL VPN이 ASA의 인터페이스에서 활성화되어 있는지 확인합니다. 이 작업을 수행하려면 **show running-config** 명령을 입력합니다.

표 ***13: Cisco***에서 재배포하는 플러그인

프로토콜	설명	재배포되는 플러그인의 소스*
RDP	Windows Vista 및 Windows 2003 R2에서 호스팅되는 Microsoft 터미널 서비스에 액세스합니다. 원격 데스크톱 ActiveX 컨트롤을 지원합니다. RDP와 RDP2를 모두 지원하는 이 플러그인을 사용하는 것을 권장합니다. 5.1 이하 버전의 RDP 및 RDP2 프로토콜만 지원됩니다. 5.2 이상 버전은 지원되지 않습니다.	http://properjavardp.sourceforge.net/
RDP2	Windows Vista 및 Windows 2003 R2에서 호스팅되는 Microsoft 터미널 서비스에 액세스합니다. 원격 데스크톱 ActiveX 컨트롤을 지원합니다. 이 레거시 플러그인은 RDP2만 지원합니다. 이 플러그인을 사용하지 않는 것을 권장합니다. 대신 위의 RDP 플러그인을 사용하십시오.	
SSH	SSH(Secure Shell) 텔넷 플러그인을 사용하여 원격 사용자는 원격 컴퓨터에 대해 SSH(Secure Shell)(v1 또는 v2) 또는 텔넷 연결을 설정할 수 있습니다. 키보드 인터랙티브 인증은 JavaSSH에서 지원되지 않으므로 다른 인증 메커니즘 구현 시 사용되는 SSH 플러그인을 사용하여 지원할 수 없습니다.	http://javassh.org/

프로토콜	설명	재배포되는 플러그인의 소스*
VNC	가상 네트워크 컴퓨팅 플러그인을 통해 원격 사용자는 모니터, 키보드 및 마우스를 사용하여 원격 데스크톱 공유(VNC 서버 또는 서비스라고도 함)가 켜져 있는 컴퓨터를 확인하고 제어할 수 있습니다. 이 버전에서는 텍스트의 기본 색상이 변경되었으며 업데이트된 프랑스어 및 일본어 도움말 파일이 포함되어 있습니다.	http://www.tightvnc.com/

* 구축 구성 및 제한 사항에 대한 자세한 내용은 플러그인 설명서를 참조해 주십시오.

해당 플러그인은 Cisco Adaptive Security Appliance 소프트웨어 다운로드 사이트에서 다운로드할 수 있습니다.

참고 ASA는 구성에서 **import webvpn plug-in protocol** 명령을 유지하지 않습니다. 대신 `csco-config/97/plugin` 디렉토리의 내용을 자동으로 로드합니다. 보조 ASA는 기본 ASA에서 플러그인을 가져옵니다.

프로시저

단계 **1** ASA의 플래시 디바이스에 플러그인을 설치합니다.

import webvpn plug-in protocol [**rdp** | **rdp2** | [**ssh** | **telnet**] | **vnc**] *URL*

참고 이 명령을 SSH와 텔넷에 대해 각각 한 번씩 입력하지 마십시오. **ssh,telnet** 을 입력할 때 공백을 삽입하지 마십시오. 이렇게 하면 SSH(Secure Shell) 및 텔넷 서비스 둘 다에 대한 플러그인 액세스가 제공됩니다.

예제:

다음 예에서는 URL이 플러그인 .jar 파일에 대한 원격 경로인 플러그인에 TFTP 또는 FTP 서버의 호스트 이름 또는 주소 및 경로를 입력하는 것을 보여줍니다.

```
hostname# import webvpn plug-in protocol ssh,telnet
tftp://local_tftp_server/plugins/ssh-plugin.jar
Accessing
tftp://local_tftp_server/plugins/ssh-plugin.jar...!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Writing file disk0:/csco_config/97/plugin/ssh...
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
238510 bytes copied in 3.650 secs (79503 bytes/sec)
```

단계 **2** (선택 사항) 플러그인에 대한 클라이언트리스 SSL VPN 지원을 해제 및 제거하고 ASA의 플래시 드라이브에서도 제거합니다.

revert webvpn plug-in protocol *protocol*

예제:

```
hostname# revert webvpn plug-in protocol rdp
```

Citrix XenApp Server에 대한 액세스 제공

서드파티 플러그인에 대한 클라이언트리스 SSL VPN 브라우저 액세스를 제공하는 방법의 한 가지 예로, 이 섹션에서는 Citrix XenApp Server Client에 대해 클라이언트리스 SSL VPN 지원을 추가하는 방법을 설명합니다.

Citrix 플러그인이 ASA에 설치되어 있는 경우 클라이언트리스 SSL VPN 사용자는 ASA에 대한 연결을 사용하여 Citrix XenApp 서비스에 액세스할 수 있습니다.

상태 저장 장애 조치 시 Citrix 플러그인을 사용하여 설정된 세션이 그대로 유지되지 않습니다. Citrix 사용자는 장애 조치 후에 재인증해야 합니다.

Citrix 플러그인 생성 및 설치

시작하기 전에

플러그인 설치 전에 보안 애플리케이션을 준비하십시오.

Citrix "보안 게이트웨이"를 사용하지 않는 모드에서 작동하도록 Citrix Web Interface 소프트웨어를 구성해야 합니다. 그렇지 않으면 Citrix 클라이언트에서 Citrix XenApp Server에 연결할 수 없습니다.

프로시저

단계 **1** Cisco 소프트웨어 다운로드 웹사이트에서 ica-plugin.zip 파일을 다운로드합니다.

이 파일에는 Cisco에서 Citrix 플러그인에 사용하도록 사용자 지정한 파일이 포함되어 있습니다.

단계 **2** Citrix 사이트에서 Citrix Java 클라이언트를 다운로드합니다.

Citrix 웹사이트의 다운로드 영역에서 Citrix Receiver(Citrix 리시버) 및 Receiver for Other Platforms(다른 플랫폼용 리시버)를 선택하고 Find(찾기)를 클릭합니다. Receiver for Java(Java용 리시버) 하이퍼링크를 클릭하고 압축 파일을 다운로드합니다.

단계 **3** 압축 파일에서 다음 파일의 압축을 푼 다음 ica-plugin.zip 파일에 추가합니다.

- JICA-configN.jar
- JICAEngN.jar

단계 **4** Citrix Java 클라이언트에 포함된 EULA에서 웹 서버에 있는 클라이언트를 구축할 수 있는 권한을 부여하는지 확인합니다.

단계 **5** ASDM을 사용하거나 특권 EXEC 모드에서 다음 CLI 명령을 입력하여 플러그인을 설치합니다.

import webvpn plug-in protocol ica URL

URL은 ica-plugin.zip 파일의 호스트 이름 또는 IP 주소 및 경로입니다.

참고 Citrix 세션에 대한 SSO 지원을 제공하려면 책갈피를 추가해야 합니다. 간편한 보기를 위해 책갈피에서 이 URL 매개변수를 사용하는 것을 권장합니다. 예를 들어 다음과 같습니다.

ica://10.56.1.114/?DesiredColor=4&DesiredHRes=1024&DesiredVRes=768

단계 **6** SSL VPN 클라이언트리스 세션을 설정하고 책갈피를 클릭하거나 Citrix 서버에 대해 URL을 입력합니다.

필요 시 Java용 클라이언트 관리자 설명서를 사용합니다.

보안 어플라이언스에 설치된 플러그인 보기

프로시저

단계 **1** 클라이언트리스 SSL VPN의 사용자가 사용할 수 있는 Java 기반 클라이언트 애플리케이션을 나열합니다.

예제:

```
hostname# show import webvpn plug
ssh
rdp
vnc
ica
```

단계 **2** 플러그인의 해시 및 날짜를 포함합니다.

예제:

```
hostname show import webvpn plug detail
post GXN2BIGGOAOkBMibDQsMu2GWZ3Q= Tues, 29 Apr 2008 19:57:03 GMT
rdp fHeyReIOUwDCgAL9HdTs PnjdBoo= Tues, 15 Sep 2009 23:23:56 GMT
```

포트 전달 구성

포트 전달을 사용하여 사용자는 클라이언트리스 SSL VPN 연결을 통해 TCP 기반 애플리케이션에 액세스할 수 있습니다. 해당하는 애플리케이션은 다음과 같습니다.

- Lotus Notes
- Microsoft Outlook

- Microsoft Outlook Express
- Perforce
- Sametime
- 보안 FTP(FTP over SSH)
- SSH
- 텔넷
- Windows 터미널 서비스
- XDDTS

다른 TCP 기반 애플리케이션도 작동될 수 있지만 이를 대상으로 테스트를 실시하지 않았습니다. UDP를 사용하는 프로토콜은 작동하지 않습니다.

포트 전달은 클라이언트리스 SSL VPN 연결을 통해 TCP 기반 애플리케이션을 지원하는 레거시 기술입니다. 이미 이 기술을 지원하는 구성을 완료했으므로 포트 전달을 사용하도록 선택할 수 있습니다.

포트 전달에 대한 대안으로 다음 사항을 고려하십시오.

- 스마트 터널 액세스는 사용자에게 다음과 같은 이점을 제공합니다.
  - 스마트 터널은 플러그인보다 우수한 성능을 제공합니다.
  - 포트 전달과 달리 스마트 터널을 사용할 경우 로컬 애플리케이션을 로컬 포트에 연결할 필요가 없으므로 사용자 환경이 간소화됩니다.
  - 또한 포트 전달과 달리 스마트 터널은 사용자의 관리자 권한이 필요하지 않습니다.
- 포트 전달 및 스마트 터널 액세스와 달리 플러그인은 원격 컴퓨터에 클라이언트 애플리케이션을 설치할 필요가 없습니다.

ASA에서 포트 전달을 구성할 경우 애플리케이션에서 사용할 포트를 지정하십시오. 스마트 터널 액세스를 구성할 경우 실행 파일의 이름 또는 경로를 지정하십시오.

포트 전달을 위한 사전 요구 사항

- 포트 전달(애플리케이션 액세스) 및 디지털 인증서를 지원하려면 Oracle JRE(Java Runtime Environment) 1.5.x 이상이 원격 컴퓨터에 설치되어 있어야 합니다.
- 브라우저 기반 Mac OS X 10.5.3 Safari 사용자는 ASA의 URL에서 사용할 클라이언트 인증서를 식별해야 하며 Safari에서 URL을 해석하는 방법으로 인해 한 번은 후행 슬래시를 사용하고 한 번은 후행 슬래시를 사용하지 않습니다. 예:
  - https://example.com/
  - https://example.com

  자세한 내용은 Safari, Mac OS X 10.5.3: 클라이언트 인증서 인증의 변경사항을 참조하십시오.

- 포트 전달 또는 스마트 터널을 사용하는 Microsoft Windows Vista 이상 사용자는 신뢰할 수 있는 사이트 영역에 ASA의 URL을 추가해야 합니다. 신뢰할 수 있는 사이트 영역에 액세스하려면 Internet Explorer를 시작한 다음 **Tools(**도구**) > Internet Options(**인터넷 옵션**) > Security(**보안**)** 탭을 선택합니다. 또한 Vista 이상 사용자는 스마트 터널 액세스를 보다 쉽게 사용할 수 있도록 보호 모드를 해제할 수 있습니다. 단, 컴퓨터가 공격에 더욱 취약해지므로 이 방법은 권장되지 않습니다.

포트 전달의 제한 사항

- 포트 전달은 정적 TCP 포트를 사용하는 TCP 애플리케이션만 지원합니다. 동적 포트 또는 여러 TCP 포트를 사용하는 애플리케이션은 지원되지 않습니다. 예를 들어 포트 22를 사용하는 보안 FTP는 클라이언트리스 SSL VPN 포트 전달을 통해 작동하지만 포트 20 및 21을 사용하는 표준 FTP는 작동하지 않습니다.
- 포트 전달은 UDP를 사용하는 프로토콜을 지원하지 않습니다.
- 포트 전달은 MAPI(Microsoft Outlook Exchange) 프록시를 지원하지 않습니다. 그러나 Microsoft Outlook Exchange Server와 함께 Microsoft Office Outlook에 대한 스마트 터널 지원을 구성할 수 있습니다.
- 상태 저장 장애 조치에서는 애플리케이션 액세스(포트 전달 또는 스마트 터널 액세스)를 사용하여 설정된 세션을 그대로 유지하지 않습니다. 사용자는 장애 조치 후 다시 연결해야 합니다.
- 포트 전달은 개인용 정보 단말기에 대한 연결을 지원하지 않습니다.
- 포트 전달을 사용하려면 Java 애플릿을 다운로드하고 로컬 클라이언트를 구성해야 합니다. 이를 위해서는 로컬 시스템에 대한 관리자 권한이 필요하므로 사용자가 공용 원격 시스템에서 연결한 경우 애플리케이션을 사용하지 못할 수도 있습니다.

  Java 애플릿은 엔드 유저 HTML 인터페이스의 고유한 창에 표시됩니다. 여기에는 사용자가 사용할 수 있는 전달된 포트 목록의 내용뿐만 아니라 활성 상태의 포트와 전송 및 수신한 트래픽 용량(바이트)도 표시됩니다.

- 포트 전달 애플릿은 로컬 IP 주소 127.0.0.1을 사용하고 ASA에서 클라이언트리스 SSL VPN 연결을 통해 이를 업데이트할 수 없는 경우 로컬 포트와 원격 포트를 동일하게 표시합니다. 따라서 ASA는 로컬 프록시 ID에 대해 새 IP 주소인 127.0.0.2, 127.0.0.3 등을 생성합니다. 호스트 파일을 수정하고 다른 루프백을 사용할 수 있으므로 원격 포트는 애플릿에서 로컬 포트로 사용됩니다. 연결하려면 포트를 지정하지 않고 호스트 이름을 통해 텔넷을 사용할 수 있습니다. 정확한 로컬 IP 주소는 로컬 호스트 파일에서 사용할 수 있습니다.

포트 전달을 위한 **DNS** 구성

포트 전달은 확인 및 연결을 위해 원격 서버의 도메인 이름 또는 IP 주소를 ASA에 전달합니다. 즉 포트 전달 애플릿은 애플리케이션의 요청을 수락하여 ASA에 전달합니다. ASA에서는 포트 전달 애플릿을 대신해 적절한 DNS 쿼리를 생성하고 연결을 설정합니다. 포트 전달 애플릿은 ASA에 대해 DNS 쿼리만 생성합니다. 포트 전달 애플릿은 포트 전달 애플리케이션에서 DNS 쿼리를 시도할 때 쿼리가

루프백 주소로 리디렉션되도록 호스트 파일을 업데이트합니다. 다음과 같이 포트 전달 애플릿의 DNS 요청을 수락하도록 ASA를 구성합니다.

프로시저

단계 **1** dns server-group 모드로 들어가 이름이 example.com인 DNS 서버 그룹을 구성합니다.

예제**:**

```
hostname(config)# dns server-group example.com
```

단계 **2** 도메인 이름을 지정합니다. 기본 도메인 이름 설정은 DefaultDNS입니다.

예제**:**

```
hostname(config-dns-server-group)# domain-name example.com
```

단계 **3** 도메인 이름을 IP 주소로 확인합니다.

예제**:**

```
hostname(config-dns-server-group)# name-server 192.168.10.10
```

단계 **4** 클라이언트리스 SSL VPN 구성 모드로 전환합니다.

webvpn

단계 **5** tunnel-group 클라이언트리스 SSL VPN 구성 모드로 전환합니다.

tunnel-group webvpn

단계 **6** 터널 그룹에서 사용할 도메인 이름을 지정합니다. 기본적으로 보안 어플라이언스는 기본 클라이언트리스 SSL VPN 그룹을 클라이언트리스 연결에 대한 기본 터널 그룹으로 할당합니다. ASA에서 이 터널 그룹을 사용하여 클라이언트리스 연결에 설정을 할당하는 경우 이 지침을 따릅니다. 그렇지 않은 경우에는 클라이언트리스 연결용으로 구성된 각 터널에 대해 다음 단계를 수행합니다.

예제**:**

```
asa2(config-dns-server-group)# exit
asa2(config)# tunnel-group DefaultWEBVPNGroup webvpn-attributes
asa2(config-tunnel-webvpn)# dns-group example.com
```

애플리케이션을 포트 전달에 맞게 설정

각 ASA의 클라이언트리스 SSL VPN 구성에서는 포트 전달 목록을 지원하며 각 해당 목록은 애플리케이션에서 액세스를 제공하는 데 사용되는 로컬 및 원격 포트를 지정합니다. 각 그룹 정책 또는 사용자 이름은 하나의 포트 전달 목록만 지원하므로 지원되는 각 애플리케이션 집합을 목록으로 그룹화해야 합니다.

프로시저

단계 **1** ASA 구성에 이미 설정되어 있는 포트 전달 목록 항목을 표시합니다.

show run webvpn port-forward

단계 **2** 클라이언트리스 SSL VPN 구성 모드로 전환합니다.

webvpn

다음 섹션에 설명된 대로 포트 전달 목록의 구성에 따라 그룹 정책 또는 사용자 이름에 목록을 할당합니다.

포트 전달 목록 할당

클라이언트리스 SSL VPN 연결을 통해 액세스하기 위해 사용자 또는 그룹 정책과 연계할 TCP 애플리케이션의 이름이 지정된 목록을 추가하거나 수정할 수 있습니다. 각 그룹 정책 및 사용자 이름에 대해 다음 중 하나를 수행하도록 클라이언트리스 SSL VPN을 구성할 수 있습니다.

참고 이러한 옵션은 각 그룹 정책 및 사용자 이름에 대해 상호 배타적입니다. 한 가지만 사용하십시오.

- 사용자 로그인 시 포트 전달 액세스를 자동으로 시작합니다.

시작하기 전에

port-forward enable *list name* 명령을 시작하기 전에 사용자는 클라이언트리스 SSL VPN 포털 페이지에서 **Application Access** > **Start Applications**를 사용하여 수동으로 포트 전달을 시작해야 합니다.

이러한 명령은 각 그룹 정책 및 사용자 이름에 사용할 수 있습니다. 각 그룹 정책 및 사용자 이름 구성에서는 이러한 명령을 한 번에 하나씩만 지원하므로 한 가지 명령을 입력하면 ASA에서 해당 그룹 정책 또는 사용자 이름의 구성에 있는 기존 명령을 새 명령으로 교체하거나 마지막 명령인 경우 정책 그룹 또는 사용자 이름 구성에서 **port-forward** 명령을 제거합니다.

프로시저

단계 **1** 사용자 로그인 시 포트 전달을 자동으로 시작합니다.

port-forward auto-start <*list name*>

단계 **2** 사용자 로그인 시 포트 전달을 활성화하거나 방지합니다.

port-forward enable <*list name*>

port-forward disable

단계 **3** (선택 사항) 그룹 정책 또는 사용자 이름 구성에서 **port-forward** 명령을 제거한 다음 기본 그룹 정책에서 [**no**] **port-forward** 명령을 상속받습니다. **no port-forward** 명령 뒤에 오는 키워드는 선택 사항이지만 이름이 지정된 **port-forward** 명령의 제거를 제한합니다.

no port-forward [**auto-start** <*list name*> | **enable** <*list name*> | **disable**]

포트 전달 자동화

사용자 로그인 시 포트 전달을 자동으로 시작하려면 다음 명령을 입력합니다.

프로시저

단계 **1** 클라이언트리스 SSL VPN 구성 모드로 전환합니다.

webvpn

단계 **2** group-policy 또는 username 클라이언트리스 SSL VPN 구성 모드로 전환합니다.

group-policy webvpn 또는 **username webvpn**

단계 **3** 사용자 로그인 시 포트 전달을 자동으로 시작합니다.

port-forward auto-start *list_name*

*list_name*은 ASA 클라이언트리스 SSL VPN 구성에 이미 있는 포트 전달 목록의 이름을 지정합니다. 그룹 정책 또는 사용자 이름에 둘 이상의 포트 전달 목록을 할당할 수 없습니다.

예제**:**

다음 예에서는 이름이 apps1인 포트 전달 목록을 그룹 정책에 할당합니다.

```
hostname(config-group-policy)# webvpn
hostname(config-group-webvpn)# port-forward auto-start apps1
```

단계 **4** ASA 구성에 있는 포트 전달 목록 항목을 표시합니다.

show run webvpn port-forward

단계 **5** (선택 사항) 그룹 정책 또는 사용자 이름에서 port-forward 명령을 제거하고 기본값으로 되돌립니다.

no port-forward

포트 전달 활성화 및 해제

기본적으로 포트 전달은 해제되어 있습니다.

프로시저

단계 **1** 포트 전달을 활성화합니다.

port-forward auto-start *list_name*을 입력한 경우 포트 전달을 수동으로 시작할 필요가 없습니다. 여기서 *list_name*은 ASA 클라이언트리스 SSL VPN 구성에 이미 있는 포트 전달 목록의 이름입니다. 그룹 정책 또는 사용자 이름에 둘 이상의 포트 전달 목록을 할당할 수 없습니다.

port-forward [**enable** l<*list name*> | **disable**]

예제**:**

다음 예에서는 이름이 apps1인 포트 전달 목록을 그룹 정책에 할당합니다.

```
hostname(config-group-policy)# webvpn
hostname(config-group-webvpn)# port-forward enable apps1
```

단계 **2** 포트 전달 목록 항목을 표시합니다.

show running-config port-forward

단계 **3** (선택 사항) 그룹 정책 또는 사용자 이름에서 port-forward 명령을 제거하고 기본값으로 되돌립니다.

no port-forward

단계 **4** (선택 사항) 포트 전달을 해제합니다.

port-forward disable

파일 액세스 구성

클라이언트리스 SSL VPN은 원격 사용자에게 ASA에서 실행 중인 프록시 CIFS 및/또는 FTP 클라이언트와 인터페이스로 접속할 수 있는 HTTPS 포털 페이지를 제공합니다. 클라이언트리스 SSL VPN은 사용자가 인증 요건을 충족하고 파일 속성에서 액세스를 제한하지 않는 경우에 한해, CIFS 또는 FTP를 사용하여 사용자에게 네트워크의 파일에 대한 네트워크 액세스를 제공합니다. CIFS 및 FTP 클라이언트는 파악하기 쉬우며 클라이언트리스 SSL VPN에서 제공하는 포털 페이지는 파일 시스템에 대한 직접 액세스 표시를 제공합니다.

사용자가 파일 목록을 요청하면 클라이언트리스 SSL VPN은 마스터 브라우저로 지정된 서버에 해당 목록이 포함된 서버의 IP 주소를 쿼리합니다. ASA에서 목록을 가져와 포털 페이지의 원격 사용자에게 제공합니다.

클라이언트리스 SSL VPN을 통해 사용자는 사용자 인증 요건 및 파일 속성에 따라 다음 CIFS 및 FTP 기능을 호출할 수 있습니다.

- 도메인 및 작업 그룹, 도메인 또는 작업 그룹 내의 서버, 서버 내의 공유 및 공유 또는 디렉토리 내의 파일을 탐색하고 나열합니다.
- 디렉토리를 생성합니다.

- 파일 다운로드, 업로드, 이름 바꾸기, 이동 및 삭제를 수행합니다.

ASA에서는 원격 사용자가 포털 페이지 또는 클라이언트리스 SSL VPN 세션 동안 표시되는 툴바의 메뉴에서 **Browse Networks(**네트워크 찾아보기**)**를 클릭한 경우 일반적으로 ASA와 동일한 네트워크에 있거나 해당 네트워크에서 연결할 수 있는 마스터 브라우저, WINS 서버 또는 DNS 서버를 사용하여 네트워크에 서버 목록을 쿼리합니다.

마스터 브라우저 또는 DNS 서버는 ASA의 CIFS/FTP 클라이언트에 클라이언트리스 SSL VPN에서 원격 사용자에게 제공하는 네트워크에 있는 리소스 목록을 제공합니다.

참고 파일 액세스를 구성하기 전에 서버에 사용자가 액세스할 수 있는 공유 폴더를 구성해야 합니다.

CIFS 파일 액세스 요건 및 제한 사항

`\\server\share\subfolder\personal` 폴더에 액세스하려면 사용자에게 share 폴더 자체를 포함한 모든 상위 폴더에 대한 읽기 이상의 권한이 있어야 합니다.

Download(다운로드) 또는 Upload(업로드)를 사용하여 CIFS 디렉토리와 로컬 데스크톱 간에 파일을 복사하여 붙여 넣을 수 있습니다. Copy(복사) 및 Paste(붙여넣기) 버튼은 원격-원격 작업용이며 로컬-원격 또는 원격-로컬 작업에는 사용되지 않습니다.

웹 폴더에서 파일을 끌어서 워크스테이션에 있는 폴더에 가져가면 임시 파일로 표시되는 항목을 확인할 수 있습니다. 보기를 업데이트하고 전송된 파일을 표시하려면 워크스테이션에서 폴더를 새로 고칩니다.

CIFS 찾아보기 서버 기능은 더블바이트 문자 공유 이름(길이가 13자를 초과하는 공유 이름)을 지원하지 않습니다. 이는 표시되는 폴더 목록에만 적용되며 폴더에 대한 사용자 액세스에는 영향을 주지 않습니다. 차선책으로 더블바이트 공유 이름을 사용하는 CIFS 폴더에 대한 책갈피를 미리 구성하거나 사용자가 cifs://server/<long-folder-name> 형식으로 폴더의 URL 또는 책갈피를 입력할 수 있습니다. 예를 들면 다음과 같습니다.

```
cifs://server/Do you remember?
cifs://server/Do%20you%20remember%3F
```

파일 액세스 지원 추가

참고 이 절차에서는 마스터 브라우저 및 WINS 서버를 지정하는 방법에 대해 설명합니다. 한 가지 대안으로 ASDM을 사용하여 파일 공유에 대한 액세스를 제공하는 URL 목록 및 항목을 구성할 수 있습니다.

ASDM에서 공유를 추가하는 경우 마스터 브라우저나 WINS 서버가 필요하지 않습니다. 그러나 이 경우 Browse Networks(네트워크 찾아보기) 링크가 지원되지 않습니다. nbns-server 명령을 입력할 때 호스트 이름 또는 IP 주소를 사용하여 ServerA를 참조할 수 있습니다. 호스트 이름을 사용하는 경우 ASA에서 DNS 서버를 IP 주소로 확인해야 합니다.

프로시저

단계 **1** 클라이언트리스 SSL VPN 구성 모드로 전환합니다.

webvpn

단계 **2** tunnel-group 클라이언트리스 SSL VPN 구성 모드로 전환합니다.

tunnel-group webvpn

단계 **3** 각 NBNS(NetBIOS Name Server: NetBIOS 이름 서버)에 대한 네트워크 또는 도메인을 찾습니다.

nbns-server {*IPaddress* | *hostname*} [**master**] [**timeout** *timeout*] [**retry** *retries*]

- **master** 마스터 브라우저로 지정된 컴퓨터입니다. 마스터 브라우저는 컴퓨터 및 공유 리소스 목록을 유지 관리합니다. 명령의 마스터 부분을 입력하지 않고 이 명령을 통해 식별하는 모든 NBNS 서버는 WINS(Windows Internet Naming Server: Windows 인터넷 명명 서버)여야 합니다. 먼저 마스터 브라우저를 지정한 다음 WINS 서버를 지정합니다. 하나의 연결 프로파일에 대해 마스터 브라우저를 포함하여 최대 3개의 서버를 지정할 수 있습니다.
- *timeout*은 동일한 서버(서버가 하나뿐인 경우) 또는 다른 서버(서버가 둘 이상인 경우)로 쿼리를 다시 전송하기 전에 ASA에서 대기하는 시간(초)입니다. 기본 시간 제한은 2초이며 범위는 1초에서 30초입니다.
- *retries*는 NBNS 서버에 대한 쿼리를 재시도하는 횟수입니다. ASA는 이 횟수까지 서버 목록 전체를 재사용한 후 오류 메시지를 전송합니다. 기본값은 2이며 범위는 1부터 10까지입니다.

예제:

```
hostname(config-tunnel-webvpn)# nbns-server 192.168.1.20 master
hostname(config-tunnel-webvpn)# nbns-server 192.168.1.41
hostname(config-tunnel-webvpn)# nbns-server 192.168.1.47
```

단계 **4** 연결 프로파일 구성에 이미 있는 NBNS 서버를 표시합니다.

show tunnel-group webvpn-attributes

단계 **5** (선택 사항) 원격 사용자에게 제공되는 클라이언트리스 SSL VPN 포털 페이지에서 인코딩할 문자 집합을 지정합니다. 기본적으로 원격 브라우저에 설정된 인코딩 유형에 따라 클라이언트리스 SSL VPN 포털 페이지에 대한 문자 집합이 결정되므로 브라우저에서 적절한 인코딩을 사용하는 데 필요한 경우에만 문자 인코딩을 설정해야 합니다.

character-encoding *charset*

*charset*은 최대 40자로 구성된 문자열이며 http://www.iana.org/assignments/character-sets에서 확인한 유효한 문자 집합 중 하나와 동일합니다. 이 페이지에 나열된 문자 집합의 이름 또는 별칭을 사용할 수 있습니다. 이를테면 iso-8859-1, shift_jis, ibm850입니다.

참고 문자 인코딩 값과 파일 인코딩 값은 브라우저에서 사용하는 글꼴 패밀리를 제외하지 않습니다. 따라서 일본어 Shift_JIS 문자 인코딩을 사용하는 경우 다음 예에 표시된 대로 webvpn 맞춤화 명령 모드에서 **page style** 명령을 통해 이러한 값의 설정을 보완하여 글꼴 패밀리를 교체하거나 webvpn 맞춤화 명령 모드에서 **no page style** 명령을 입력하여 글꼴 패밀리를 제거해야 합니다.

예제**:**

다음 예에서는 일본어 Shift_JIS 문자를 지원하도록 문자 인코딩 특성을 설정하고 글꼴 패밀리를 제거하며 기본 배경색을 유지합니다.

```
hostname(config)# webvpn
hostname(config-webvpn)# character-encoding shift_jis
hostname(config-webvpn)# customization DfltCustomization
hostname(config-webvpn-custom)# page style background-color:white
```

단계 **6** (선택 사항) 특정 CIFS 서버의 클라이언트리스 SSL VPN 포털 페이지에 대한 인코딩을 지정합니다. 이를 통해 다른 문자 인코딩이 필요한 CIFS 서버에 다른 파일 인코딩 값을 사용할 수 있습니다.

file-encoding {*server-name* | *server-ip-address*} *charset*

예제**:**

다음 예에서는 IBM860(일명 "CP860") 문자를 지원하기 위해 CIFS 서버 10.86.5.174의 파일 인코딩 특성을 설정합니다.

```
hostname(config-webvpn)# file-encoding 10.86.5.174 cp860
```

SharePoint 액세스를 위한 시계 정확도 확인

ASA의 클라이언트리스 SSL VPN 서버는 쿠키를 사용하여 엔드포인트의 Microsoft Word와 같은 애플리케이션과 상호 작용합니다. ASA의 시간이 잘못된 경우 SharePoint 서버에 있는 문서에 액세스하면 ASA에서 설정한 쿠키 만료 시간으로 인해 Word가 제대로 작동하지 않을 수 있습니다. 오동작을 방지하려면 ASA 시계를 올바르게 설정해야 합니다. NTP 서버와 시간을 동적으로 동기화하도록 ASA를 구성하는 것을 권장합니다. 자세한 내용은 일반 작업 구성 가이드의 날짜 및 시간 설정 섹션을 참조하십시오.

VDI(Virtual Desktop Infrastructure)

ASA는 Citrix 및 VMware VDI 서버에 대한 연결을 지원합니다.

- Citrix의 경우 ASA를 사용하여 클라이언트리스 포털을 통해 사용자가 실행 중인 Citrix Receiver에 액세스할 수 있습니다.
- VMware는 (스마트 터널) 애플리케이션으로 구성됩니다.

다른 서버 애플리케이션과 마찬가지로 클라이언트리스 포털의 책갈피를 통해 VDI 서버에 액세스할 수도 있습니다.

VDI 제한 사항

- 인증서 또는 스마트 카드를 사용한 인증은 해당 형식의 인증에서 ASA를 통과하는 것을 허용하지 않기 때문에 자동 로그온이 지원되지 않습니다.

- XenApp 및 XenDesktop 서버에 XML 서비스를 설치 및 구성해야 합니다.
- 클라이언트 인증서 확인, 이중 인증, 내부 비밀번호 및 CSD(자격 증명 모음을 비롯해 모든 CSD)는 독립 실행형 모바일 클라이언트를 사용하는 경우 지원되지 않습니다.

Citrix 모바일 지원

Citrix Receiver를 실행하는 모바일 사용자는 다음 방법으로 Citrix 서버에 연결할 수 있습니다.

- AnyConnect를 통해 ASA에 연결한 다음 Citrix 서버에 연결합니다.
- AnyConnect 클라이언트를 사용하지 않고 ASA를 통해 Citrix 서버에 연결합니다. 로그온 자격 증명에는 다음이 포함될 수 있습니다.
  - Citrix 로그온 화면의 연결 프로파일 별칭(터널 그룹 별칭이라고도 함). VDI 서버에는 각각의 권한 부여 및 연결 설정이 다른 여러 그룹 정책이 있을 수 있습니다.
  - RSA 서버가 구성된 경우 RSA SecureID 토큰 값. RSA는 무효한 항목을 비롯해 초기 또는 만료된 PIN에 대한 새 PIN 입력에 대해 다음 토큰을 지원합니다.

Citrix용으로 지원되는 모바일 디바이스

- iPad — Citrix Receiver 4.x 이상 버전
- iPhone/iTouch — Citrix Receiver 4.x 이상 버전
- Android 2.x/3.x/4.0/4.1 전화기 — Citrix Receiver 2.x 이상 버전
- Android 4.0 전화기 — Citrix Receiver 2.x 이상 버전

Citrix 제한 사항

인증서 제한 사항

- 인증서/스마트카드 인증은 자동 로그온 방법으로 지원되지 않습니다.
- 클라이언트 인증서 확인 및 CSD는 지원되지 않습니다.
- 인증서의 Md5 서명은 iOS의 문제(http://support.citrix.com/article/CTX132798)에 해당하는 보안 문제로 인해 작동하지 않습니다.
- SHA2 서명은 Citrix 웹사이트(http://www.citrix.com/)에 설명된 대로 Windows 외에는 지원되지 않습니다.
- 키 크기가 1024보다 큰 경우 지원되지 않습니다.

기타 제한 사항

- HTTP 리디렉션은 지원되지 않으며 Citrix Receiver 애플리케이션은 리디렉션 시 작동하지 않습니다.
- XenApp 및 XenDesktop 서버에 XML 서비스를 설치 및 구성해야 합니다.

Citrix Mobile Receiver 사용자 로그온 정보

Citrix 서버에 연결하는 모바일 사용자의 로그온은 ASA에서 Citrix 서버를 VDI 서버 또는 VDI 프록시 서버로 구성했는지에 따라 다릅니다.

Citrix 서버가 VDI 서버로 구성된 경우 다음을 수행하십시오.

1. AnyConnect Secure Mobility Client를 사용하여 VPN 자격 증명으로 ASA에 연결합니다.
2. Citrix Mobile Receiver를 사용하여 Citrix 서버 자격 증명으로 Citrix 서버에 연결합니다(단일 로그온이 구성된 경우에는 Citrix 자격 증명이 필요하지 않음).

ASA가 VDI 프록시 서버로 구성된 경우 다음을 수행하십시오.

1. Citrix Mobile Receiver를 사용하여 VPN 및 Citrix 서버 모두에 대해 자격 증명 입력으로 ASA에 연결합니다. 첫 번째 연결이 올바르게 구성된 경우 후속 연결에서는 VPN 자격 증명만 제공하면 됩니다.

Citrix 서버의 프록시로 ASA 구성

Citrix 서버의 프록시 역할을 하도록 ASA를 구성하여 ASA 연결이 사용자에게 Citrix 서버 연결처럼 표시되도록 할 수 있습니다. ASDM에서 VDI 프록시를 활성화한 경우 AnyConnect 클라이언트가 필요하지 않습니다. 엔드 유저가 Citrix에 연결되는 방식을 보여주는 상위 수준의 단계는 다음과 같습니다.

프로시저

단계 **1** 모바일 사용자가 Citrix Receiver를 열고 ASA의 URL에 연결합니다.

단계 **2** 사용자가 Citrix 로그온 화면에서 XenApp 서버 및 VPN 자격 증명을 제공합니다.

단계 **3** 이후에는 Citrix 서버에 연결할 때마다 VPN 자격 증명만 입력하면 됩니다.

ASA를 XenApp 및 XenDesktop의 프록시로 사용하는 경우에는 Citrix 액세스 게이트웨이에 대한 요건이 필요하지 않습니다. XenApp 서버 정보가 ASA에 로깅되고 ASDM에 표시됩니다.

Citrix 서버의 주소 및 로그온 자격 증명을 구성하고 해당 VDI 서버를 그룹 정책 또는 사용자 이름에 할당합니다. 사용자 이름과 그룹 정책을 둘 다 구성한 경우에는 사용자 이름 설정이 그룹 정책 설정을 재정의합니다.

다음에 수행할 작업

http://www.youtube.com/watch?v=JMM2RzppaG8 - 이 비디오에서는 ASA를 Citrix 프록시로 사용할 경우의 이점에 대해 설명합니다.

그룹 정책에 **VDI** 서버 할당

다음과 같은 방법으로 VDI 서버를 구성하고 그룹 정책에 할당합니다.

- VDI Access(VDI 액세스) 창에서 VDI 서버를 추가하고 이 서버에 그룹 정책을 할당합니다.
- 그룹 정책에 VDI 서버를 추가합니다.

사용자 이름과 그룹 정책을 둘 다 구성한 경우에는 사용자 이름 설정이 그룹 정책보다 우선적으로 적용됩니다. 다음을 입력합니다.

```
configure terminal
 group-policy DfltGrpPolicy attributes
  webvpn
   vdi type <citrix> url <url> domain <domain> username <username> password
   <password>
configure terminal
 username <username> attributes
  webvpn
   vdi type <citrix> url <url> domain <domain> username <username> password
   <password>]
```

구문 옵션은 다음과 같이 정의됩니다.

- type — VDI의 유형입니다. Citrix Receiver 유형의 경우 이 값은 *citrix*입니다.
- url — http 또는 https, 호스트 이름, 포트 번호 및 XML 서비스의 경로를 포함하는 XenApp 또는 XenDesktop 서버의 전체 URL입니다.
- Username — 가상화 인프라 서버에 로그인하는 데 필요한 사용자 이름입니다. 이 값은 클라이언트리스 매크로일 수 있습니다.
- Password — 가상화 인프라 서버에 로그인하는 데 필요한 비밀번호입니다. 이 값은 클라이언트리스 매크로일 수 있습니다.
- domain — 가상화 인프라 서버에 로그인하는 데 필요한 도메인입니다. 이 값은 클라이언트리스 매크로일 수 있습니다.

SSL을 사용하여 내부 서버에 액세스

프로시저

단계 **1** group policy 클라이언트리스 SSL VPN 구성 모드로 전환합니다.

webvpn

단계 **2** URL 입력을 해제합니다.

url-entry disable

클라이언트리스 SSL VPN에서는 SSL과 후속 기술인 TLS1을 사용하여 원격 사용자와 내부 서버에서 지원되는 특정 내부 리소스 간의 보안 연결을 제공합니다.

클라이언트리스 **SSL VPN** 및 **ASDM** 포트 구성

8.0(2) 버전부터 ASA에서는 외부 인터페이스의 포트 443에서 클라이언트리스 SSL VPN 세션과 ASDM 관리 세션을 동시에 지원합니다. 이러한 애플리케이션을 다른 인터페이스에서 구성할 수 있습니다.

프로시저

단계 **1** 클라이언트리스 SSL VPN 구성 모드로 전환합니다.

webvpn

단계 **2** 클라이언트리스 SSL VPN에 대한 SSL 수신 대기 포트를 변경합니다.

port *port_number*

예제**:**

이 예에서는 외부 인터페이스의 포트 444에서 클라이언트리스 SSL VPN을 활성화합니다. 이 구성에서 클라이언트리스 SSL VPN 세션을 시작하는 원격 사용자는 브라우저에 https://<outside_ip>:444를 입력합니다.

```
hostname(config)# http server enable
hostname(config)# http 192.168.3.0 255.255.255.0 outside
hostname(config)# webvpn
hostname(config-webvpn)# port 444
hostname(config-webvpn)# enable outside
```

단계 **3** (특권 모드) ASDM에 대한 수신 대기 포트를 변경합니다.

http server enable

예제**:**

이 예에서는 HTTPS ASDM 세션에서 외부 인터페이스의 포트 444를 사용하도록 지정합니다. 클라이언트리스 SSL VPN 또한 외부 인터페이스에서 활성화되고 기본 포트(443)를 사용합니다. 이 구성에서 원격 사용자는 https://<outside_ip>:444를 입력하여 ASDM 세션을 시작합니다.

```
hostname(config)# http server enable
hostname(config)# http 192.168.3.0 255.255.255.0 outside
```

```
hostname(config)# webvpn
hostname(config-webvpn)# enable outside
```

클라이언트리스 SSL VPN 세션에 HTTPS 사용

HTTPS 구성 외에 HSTS(HTTP Strict-Transport-Security) 활성화, 웹 보안 정책 메커니즘은 프로토콜 다운그레이드 공격 및 쿠키 가로채기로부터 웹사이트를 보호하는 데 도움이 됩니다. HSTS는 다음과 같은 지시문을 전송하여 지정된 시간 제한이 만료될 때까지 웹 서버에 안전하게 연결할 HTTPS 웹사이트에 UA/브라우저를 리디렉션합니다.

```
Strict-Transport-Security: max-age="31536000"; preload;
```

여기서 각 항목은 다음을 나타냅니다.

- 최대 기간 - 구성 가능한 항목으로, 웹 서버가 HSTS 호스트로 간주되어야 하고 HTTPS만 사용하여 안전하게 액세스되어야 하는 시간(초 단위)을 지정합니다. 기본값은 18주(10,886,400초)입니다. 범위는 8~365일(0-31,536,000 > 초)입니다.
- 사전 로드 - 브라우저에 UA/브라우저에서 이미 등록되어 있는 도메인 목록을 로드하라고 알려주며 이제는 HSTS 호스트로 처리되어야 합니다. 사전 로드된 목록의 구현은 UA/브라우저에 종속되며 각 UA/브라우저는 다른 지시문이 어떻게 가능한지에 대한 추가 제한 사항을 지정할 수 있습니다. 예를 들어, Chrome의 사전 로드 목록은 HSTS의 최대 기간을 최소 18주(10,886,400초)가 되도록 지정합니다.

프로시저

단계 **1** 클라이언트리스 SSL VPN 구성 모드로 전환합니다.

webvpn을 입력합니다.

단계 **2** 외부 인터페이스에서 클라이언트리스 SSL VPN 세션을 활성화합니다.

enable *interface-name*을 입력합니다.

단계 **3** HSTS를 활성화합니다.

hsts enable을 입력합니다.

HSTS를 비활성화하려면 이 명령의 no 형식 즉, **no hsts enable**을 사용합니다.

단계 **4** HSTS가 계속해서 적용되는 시간(초 단위)을 구성합니다.

hsts max-age *max-age-in-seconds*를 입력합니다.

이 값의 범위는 <0-31536000>초입니다. 기본값은 10,886,400(18주)입니다. 이 제한에 도달하면 HSTS가 더 이상 적용되지 않습니다.

예

```
hostname(config)# webvpn
hostname(config-webvpn)# enable outside

hostname(config-webvpn)# hsts enable
hostname(config-webvpn)# hsts max-age 31536000
```

다음에 수행할 작업

현재 구성을 보려면 **show running-config webvpn** [*hsts*]를 사용합니다.

현재 구성을 지우려면 **clear configure webvpn**를 사용합니다.

프록시 서버에 대한 지원 구성

ASA에서는 HTTPS 연결을 종료하고 HTTP 및 HTTPS 요청을 프록시 서버에 전달할 수 있습니다. 이 서버는 사용자와 공용 또는 사설 네트워크 간의 중개자 역할을 합니다. 조직에서 제어하는 프록시 서버를 통해 네트워크에 액세스하도록 하면 추가 필터링을 통해 보안 네트워크 액세스 및 관리 제어를 유지할 수 있습니다.

HTTP 및 HTTPS 프록시 서비스에 대한 지원을 구성할 때 사전 설정한 자격 증명을 할당하여 기본 인증에 대한 각 요청과 함께 전송할 수 있습니다. 또한 HTTP 및 HTTPS 요청에서 제외할 URL을 지정할 수 있습니다.

시작하기 전에

HTTP 프록시 서버에서 다운로드할 PAC(Proxy Autoconfiguration) 파일을 지정할 수 있지만 PAC 파일을 지정할 때는 프록시 인증을 사용할 수 없습니다.

프로시저

단계 **1** 클라이언트리스 SSL VPN 구성 모드로 전환합니다.

webvpn

단계 **2** 외부 프록시 서버를 사용하여 HTTP 및 HTTPS 요청을 처리하도록 ASA를 구성합니다.

http-proxy and https-proxy

참고 Proxy NTLM 인증은 **http-proxy**에서 지원되지 않습니다. 인증 없는 프록시와 기본 인증의 프록시만 지원됩니다.

단계 **3** HTTP 프록시를 구성합니다.

http-proxy *host* [*port*] [**exclude** *url*] [**username** *username* {**password** *password*}]

단계 **4** HTTPS 프록시를 구성합니다.

https-proxy *host* [*port*] [**exclude** *url*] [**username** *username* {**password** *password*}]

단계 **5** PAC 파일 URL을 설정합니다.

http-proxy pac *url*

단계 **6** (선택 사항) 프록시 서버로 전송할 수 있는 URL에서 URL을 제외합니다.

exclude

단계 **7** 외부 프록시 서버의 호스트 이름 또는 IP 주소를 제공합니다.

호스트

단계 **8** 각 URL에 대한 프록시를 식별하는 JavaScript 기능을 사용하여 ASA에 프록시 자동 구성 파일을 다운로드합니다.

pac

단계 **9** (선택 사항) (사용자 이름을 지정할 경우에만 사용 가능) 기본적인 프록시 인증을 제공하기 위해 각 프록시 요청에 비밀번호를 추가합니다.

password

단계 **10** 각 HTTP 또는 HTTPS 요청을 통해 프록시 서버로 비밀번호를 전송합니다.

password

단계 **11** (선택 사항) 프록시 서버에서 사용하는 포트 번호를 제공합니다. 기본 HTTP 포트는 80입니다. 기본 HTTPS 포트는 443입니다. 대체 값을 지정하지 않은 경우 ASA에서 이러한 포트를 사용합니다. 범위는 1부터 65535까지입니다.

port

단계 **12** **exclude**를 입력한 경우 프록시 서버에 전송할 수 있는 URL에서 제외할 URL 또는 쉼표로 구분된 여러 URL 목록을 입력합니다. 이 문자열은 길이 제한이 없지만, 전체 명령이 512자를 초과해서는 안 됩니다. 리터럴 URL을 지정하거나 다음 와일드카드를 사용할 수 있습니다.

- ***** 슬래시(/) 및 마침표(.)를 포함하여 모든 문자열과 일치합니다. 이 와일드카드는 영숫자 문자열과 함께 사용해야 합니다.
- **?** 슬래시 및 마침표를 포함하여 모든 단일 문자와 일치합니다.
- [x-y]는 x~y 범위에 속한 임의의 단일 문자와 일치합니다. 여기서 x는 ANSI 문자 세트의 한 문자, y 역시 이 세트의 또 다른 문자를 나타냅니다.
- [**!**x-y]는 이 범위에 속하지 않는 단일 문자와 일치합니다.

단계 **13** **http-proxy pac**를 입력한 경우 **http://**를 사용하고 프록시 자동 구성 파일의 URL을 입력합니다. (**http://** 부분을 생략하면 CLI에서 이 명령을 무시합니다.)

단계 **14** (선택 사항) 기본 프록시 인증을 위해 각 HTTP 프록시 요청을 사용자 이름과 함께 사용합니다. **http-proxy***host* 명령만 이 키워드를 지원합니다.

username

단계 **15** 각 HTTP 또는 HTTPS 요청을 통해 프록시 서버로 사용자 이름을 전송합니다.

username

단계 **16** 기본 포트를 사용하여 IP 주소가 209.165. 201.1인 HTTP 프록시 서버에서 각 HTTP 요청을 통해 사용자 이름 및 비밀번호를 전송하도록 구성하는 방법을 보여줍니다.

예제:

```
hostname(config-webvpn)# http-proxy 209.165.201.1 user jsmith password
mysecretdonttell
```

단계 **17** ASA가 HTTP 요청에서 특정 URL www.example.com을 수신할 때 이를 프록시 서버로 전달하는 대신 해당 요청을 확인하는 경우를 제외하고 동일한 명령을 보여줍니다.

예제:

```
hostname(config-webvpn)# http-proxy 209.165.201.1 exclude www.example.com
username jsmith password mysecretdonttell
```

단계 **18** 브라우저에 프록시 자동 구성 파일을 제공하도록 URL을 지정하는 방법을 보여줍니다.

예제:

```
hostname(config-webvpn)# http-proxy pac http://www.example.com/pac
```

ASA 클라이언트리스 SSL VPN 구성에서는 **http-proxy**와 **https-proxy** 명령을 각각 하나씩만 지원합니다. 예를 들어 실행 중인 구성에 **http-proxy** 명령의 인스턴스 하나가 이미 있는 경우, 다른 명령을 입력하면 CLI에서 이전 인스턴스를 덮어씁니다.

참고 Proxy NTLM 인증은 **http-proxy**에서 지원되지 않습니다. 인증 없는 프록시 및 기본 인증만 지원됩니다.

SSL/TLS 암호화 프로토콜 구성

포트 전달에는 Oracle JRE(Java Runtime Environment)가 필요합니다. 포트 전달은 클라이언트리스 SSL VPN 사용자가 일부 SSL 버전을 사용하여 연결하는 경우 작동하지 않습니다. 지원되는 JRE 버전에 대해서는 지원되는 VPN 플랫폼, Cisco ASA 5500 Series의 내용을 참조하십시오.

디지털 인증서를 사용하여 인증

SSL에서는 인증에 디지털 인증서를 사용합니다. ASA가 부팅 시 자체 서명된 SSL 서버 인증서를 생성하거나 사용자가 PKI 상황에서 발급된 SSL 인증서를 ASA에 설치할 수 있습니다. HTTPS의 경우 이 인증서를 클라이언트에 설치해야 합니다.

디지털 인증서 인증의 제한 사항

MS Outlook, MS Outlook Express 및 Eudora와 같은 이메일 클라이언트에는 인증서 저장소에 액세스하는 기능이 없습니다.

디지털 인증서를 사용하는 인증 및 권한 부여에 대한 자세한 내용은 일반 작업 구성 가이드에서 인증서 및 사용자 로그인 자격 증명 사용 섹션을 참조하십시오.

클라이언트-서버 플러그인에 대한 브라우저 액세스 구성

클라이언트-서버 플러그인 표에는 ASA에서 클라이언트리스 SSL VPN 세션의 브라우저에 사용하도록 제공하는 플러그인이 표시됩니다.

플러그인을 추가, 변경 또는 제거하려면 다음 중 하나를 수행하십시오.

- 플러그인을 추가하려면 **Import(**가져오기**)**를 클릭합니다. Import Plug-ins(플러그인 가져오기) 대화 상자가 열립니다.
- 플러그인을 제거하려면 해당 플러그인을 선택하고 **Delete(**삭제**)**를 클릭합니다.

브라우저 플러그인 설치 정보

브라우저 플러그인은 웹 브라우저가 브라우저 창 내에서 클라이언트를 서버에 연결하는 등의 전용 기능을 수행하기 위해 호출하는 별도의 프로그램입니다. ASA를 사용하면 클라이언트리스 SSL VPN 세션에서 원격 브라우저로 다운로드할 플러그인을 가져올 수 있습니다. Cisco에서는 재배포하는 플러그인을 테스트하며, 경우에 따라 재배포할 수 없는 플러그인의 연결성을 테스트합니다. 그러나 현재 스트리밍 미디어를 지원하는 플러그인 가져오기는 권장하지 않습니다.

ASA는 플래시 디바이스에 플러그인을 설치할 때 다음 작업을 수행합니다.

- (Cisco 배포 플러그인만 해당) URL에 지정되어 있는 jar 파일의 압축을 풉니다.
- ASA 파일 시스템의 csco-config/97/plugin 디렉터리에 파일을 씁니다.
- ASDM에서 URL 특성 옆에 있는 드롭다운 목록을 채웁니다.
- 이후의 모든 클라이언트리스 SSL VPN 세션에 대해 플러그인을 활성화하고 포털 페이지의 Address(주소) 필드 옆에 있는 드롭다운 목록에 기본 메뉴 옵션 및 옵션을 추가합니다.

다음 표에는 다음 섹션에 설명된 플러그인을 추가할 경우 포털 페이지의 기본 메뉴 및 주소 필드에 대한 변경 사항이 나와 있습니다.

표 ***14:*** 클라이언트리스 ***SSL VPN*** 포털 페이지에 있는 플러그인의 효과

플러그인	포털 페이지에 추가된 기본 메뉴 옵션	포털 페이지에 추가된 주소 필드 옵션
ica	Citrix 클라이언트	citrix://
rdp	Terminal Servers	rdp://
rdp2	Terminal Servers Vista	rdp2://

플러그인	포털 페이지에 추가된 기본 메뉴 옵션	포털 페이지에 추가된 주소 필드 옵션
ssh,telnet	SSH	ssh://
	텔넷	telnet://
vnc	VNC Client	vnc://

참고 보조 ASA는 기본 ASA에서 플러그인을 가져옵니다.

클라이언트리스 SSL VPN 세션에 있는 사용자가 포털 페이지에서 관련 메뉴 옵션을 클릭하면 포털 페이지에는 인터페이스에 대한 창과 도움말 창이 표시됩니다. 사용자가 드롭다운 목록에 표시된 프로토콜을 선택하고 주소 필드에서 URL을 입력하여 연결을 설정할 수 있습니다.

참고 일부 Java 플러그인은 대상 서비스의 세션이 설정되지 않은 경우에도 연결됨 또는 온라인 상태를 보고할 수 있습니다. 오픈 소스 플러그인은 상태를 보고하지만 ASA는 보고하지 않습니다.

브라우저 플러그인 설치 요건

- 보안 어플라이언스가 프록시 서버를 사용하도록 클라이언트리스 세션을 구성한 경우 플러그인이 작동하지 않습니다.

  참고 원격 데스크톱 프로토콜 플러그인은 세션 브로커를 통한 로드 밸런싱을 지원하지 않습니다. 프로토콜에서 세션 브로커의 리디렉션을 처리하는 방식으로 인해 연결이 실패합니다. 세션 브로커를 사용하지 않는 경우 플러그인이 작동합니다.

- 플러그인은 SSO(Single Sign-On: 단일 로그인)를 지원합니다. 플러그인은 입력된 동일한 자격 증명을 사용하여 클라이언트리스 SSL VPN 세션을 엽니다. 플러그인은 매크로 대체를 지원하지 않으므로 내부 도메인 비밀번호와 같은 다른 필드나 RADIUS 또는 LDAP 서버의 특성에서 SSO를 수행하는 옵션을 제공하지 않습니다.
- 플러그인에 대한 SSO 지원을 구성하려면 플러그인을 설치하고 책갈피 항목을 추가하여 서버에 대한 링크를 표시하고 책갈피를 추가할 때 SSO 지원을 지정하십시오.
- 원격 사용에 필요한 최소 액세스 권한은 게스트 권한 모드에 속합니다.

브라우저 플러그인 설치 요건

- GNU GPL(General Public License: 일반 공중 사용 허가서)에 따라 Cisco에서는 플러그인을 변경하지 않고 재배포합니다. GPL에 따라 Cisco에서는 해당 플러그인을 직접 개선할 수 없습니다.

- 클라이언트리스 SSL VPN은 플러그인에 대한 원격 액세스를 제공하도록 ASA에서 활성화되어 있어야 합니다.
- 상태 저장 장애 조치는 플러그인을 사용하여 설정된 세션을 그대로 유지하지 않습니다. 사용자는 장애 조치 후 다시 연결해야 합니다.
- 플러그인을 사용하려면 ActiveX 또는 Oracle JRE(Java Runtime Environment)가 브라우저에서 활성화되어 있어야 합니다. 64비트 브라우저용 RDP 플러그인의 ActiveX 버전은 없습니다.

RDP 플러그인 설정

RDP 플러그인을 설치하고 사용하려면 새 환경 변수를 추가해야 합니다.

프로시저

단계 **1** **My Computer(**내 컴퓨터**)**를 마우스 오른쪽 버튼으로 클릭하여 시스템 속성에 액세스한 후 **Advanced(**고급**)** 탭을 선택합니다.

단계 **2** Advanced(고급) 탭에서 환경 변수 버튼을 선택합니다.

단계 **3** 새 사용자 변수 대화 상자에서 RF_DEBUG 변수를 입력합니다.

단계 **4** 사용자 변수 섹션에서 새 환경 변수를 확인합니다.

단계 **5** 클라이언트 컴퓨터에서 8.3 이전의 버전 클라이언트리스 SSL VPN을 사용하는 경우에는 기존 Cisco Portforwarder Control을 제거해야 합니다. C:/WINDOWS/Downloaded Program Files 디렉토리로 이동하여 Portforwarder Control을 마우스 오른쪽 버튼으로 클릭하고 **Remove(**제거**)**를 선택합니다.

단계 **6** Internet Explorer 브라우저 캐시를 모두 지웁니다.

단계 **7** 클라이언트리스 SSL VPN 세션을 시작하고 RDP ActiveX 플러그인을 통해 RDP 세션을 설정합니다.

이제 Windows 애플리케이션 이벤트 뷰어에서 이벤트를 관찰할 수 있습니다.

플러그인 설치 전 보안 어플라이언스 준비

프로시저

단계 **1** 클라이언트리스 SSL VPN이 ASA 인터페이스에서 활성화되어 있는지 확인합니다.

단계 **2** 원격 사용자가 FQDN(Fully Qualified Domain Name: 정규화된 도메인 이름)을 사용하여 연결하는 ASA 인터페이스에 SSL 인증서를 설치합니다.

참고 IP 주소를 SSL 인증서의 CN(Common Name: 공통 이름)으로 지정하지 마십시오. 원격 사용자는 FQDN을 사용하여 ASA와의 통신을 시도합니다. 원격 PC에서 DNS 또는 System32\drivers\etc\hosts 파일의 항목을 사용하여 FQDN을 확인할 수 있어야 합니다.

새 **HTML** 파일을 사용하도록 **ASA** 구성

프로시저

단계 **1** 파일 및 이미지를 웹 콘텐츠로서 가져옵니다.

import webvpn webcontent *<file> <url>*

예제**:**

```
hostname# import webvpn webcontent /+CSCOU+/login.inc tftp://209.165.200.225/login.inc
!!!!* Web resource `+CSCOU+/login.inc' was successfully initialized
hostname#
```

단계 **2** 사용자 지정 템플릿을 내보냅니다.

export webvpn customization *<file> <URL>*

예제**:**

```
hostname# export webvpn customization template tftp://209.165.200.225/sales_vpn_login
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
%INFO: Customization object 'Template' was exported to tftp://10.21.50.120/sales
_vpn_login
```

단계 **3** 활성화하려면 파일에서 전체 사용자 지정 모드 태그를 변경합니다.

예제**:**

이 예는 ASA 메모리에 저장된 로그인 파일의 URL을 제공합니다.

```
<full-customization>
          <mode>enable</mode>
          <url>/+CSCOU+/login.inc</url>
      </full-customization>
```

단계 **4** 파일을 새 사용자 지정 개체로 가져옵니다.

예제**:**

```
hostname# import webvpn customization sales_vpn_login tftp://10.21.50.120/sales_vpn_login$
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
%INFO: customization object 'sales_vpn_login' was successfully imported
```

단계 **5** 연결 프로파일(터널 그룹)에 사용자 지정 개체를 적용합니다.

예제**:**

```
hostname(config)# tunnel-group Sales webvpn-attributes
hostname(config-tunnel-webvpn)#customization sales_vpn_login
```

16 장

고급 클라이언트리스 SSL VPN 구성

Microsoft Kerberos 제한 위임 솔루션

많은 조직에서는 현재 ASA SSO 기능이 제공할 수 있는 것보다 더 많은 인증 방법을 사용하여 클라이언트리스 VPN 사용자를 인증하고 조직의 인증 크리덴셜을 웹 기반 리소스로 원활하게 확장하고자 합니다. 스마트 카드 및 OTP(One-time Password: 일회용 비밀번호)를 사용하여 원격 액세스 사용자를 인증하려는 수요가 증가하는 상황에서, SSO 기능은 인증이 필요할 때 정적 사용자 이름 및 비밀번호와 같이 기본적인 사용자 자격 증명만을 클라이언트리스 웹 기반 리소스에 전달하기 때문에 이러한 수요를 충족시키기에 충분하지 않습니다.

예를 들어 인증서 또는 OTP 기반 인증 방법에는 모두 ASA가 웹 기반 리소스에 대해 SSO 액세스를 원활하게 수행하는 데 필요한 기본적인 사용자 이름 및 비밀번호가 포함되지 않습니다. 인증서를 사용하여 인증할 경우, 사용자 이름과 비밀번호는 ASA가 웹 기반 리소스로 확장하는 데 필요하지 않으므로 SSO에 대해 지원되지 않는 인증 방법입니다. 반면에 OTP는 정적 사용자 이름을 포함하지만 비밀번호가 동적이므로 VPN 세션 전체에서 이후에 변경됩니다. 일반적으로 웹 기반 리소스는 정적 사용자 이름 및 비밀번호를 수락하도록 구성되므로 OTP는 SSO에 대해 지원되지 않는 인증 방법이 됩니다.

Microsoft의 KCD(Kerberos Constrained Delegation: Kerberos 제한 위임)는 ASA 소프트웨어 릴리스 8.4에서 소개된 새로운 기능으로, 사설 네트워크의 Kerberos 보호 웹 애플리케이션에 대해 액세스를 제공합니다. 이러한 이점 덕분에 인증서 및 OTP 기반 인증 방법을 웹 애플리케이션으로 원활하게 확장할 수 있습니다. 따라서 SSO 및 KCD가 개별적으로 작동되는 경우에도 많은 조직에서는 이제 ASA에서 지원하는 모든 인증 방법을 사용하여 클라이언트리스 VPN 사용자를 인증하고 인증 크리덴셜을 웹 애플리케이션으로 원활하게 확장할 수 있습니다.

KCD 작동 방식

Kerberos는 신뢰할 수 있는 서드파티를 사용하여 네트워크에서 엔터티의 디지털 ID를 확인합니다. 이러한 엔터티(예: 호스트에서 실행 중인 사용자, 호스트 컴퓨터 및 서비스)는 보안 주체라고 하며 동일한 도메인에 있어야 합니다. 비밀 키 대신 Kerberos는 티켓을 사용하여 서버에 대해 클라이언트를 인증합니다. 티켓은 비밀 키에서 파생되며 클라이언트 ID, 암호화된 세션 키, 플래그로 구성됩니다. 각 티켓은 키 배포 센터에서 발행되며 수명이 설정되어 있습니다.

Kerberos 보안 시스템은 데이터를 암호화하여 엔터티(사용자, 컴퓨터 또는 애플리케이션)를 인증하고 네트워크 전송을 보호하기 위해 사용되는 네트워크 인증 프로토콜이므로 정보의 대상이 되는 디바이스만 암호 해독할 수 있습니다. 클라이언트리스 SSL VPN 사용자에게 Kerberos로 보호되는 모든 웹 서비스에 대한 SSO 액세스를 제공하기 위해 KCD를 구성할 수 있습니다. 이러한 웹 서비스 또는 애플리케이션의 예로는 OWA(Outlook Web Access: Outlook 웹 액세스), Sharepoint 및 IIS(Internet Information Server: 인터넷 정보 서버)가 있습니다.

Kerberos 프로토콜에 대해 프로토콜 전환 및 제한 위임이라는 두 가지 확장 기능이 구현되었습니다. 이러한 확장을 통해 클라이언트리스 SSL VPN 원격 액세스 사용자가 사설 네트워크에 있는 Kerberos 인증 애플리케이션에 액세스할 수 있습니다.

프로토콜 전환은 사용자 인증 수준에서 다양한 인증 메커니즘을 지원하고 후속 애플리케이션 계층에서 보안 기능(예: 상호 인증 및 제한 위임)을 위해 Kerberos 프로토콜로 전환함으로써 향상된 유연성 및 보안을 제공합니다. 제한 위임은 애플리케이션 서비스가 사용자 대신 역할을 수행할 수 있는 한계를 정하여 도메인 관리자가 애플리케이션 신뢰 경계를 지정하고 이를 적용할 수 있는 방법을 제공합니다. 이러한 유연성 덕분에 신뢰할 수 없는 서비스로 인해 손상될 가능성이 줄어들어 애플리케이션 보안 설계가 개선됩니다.

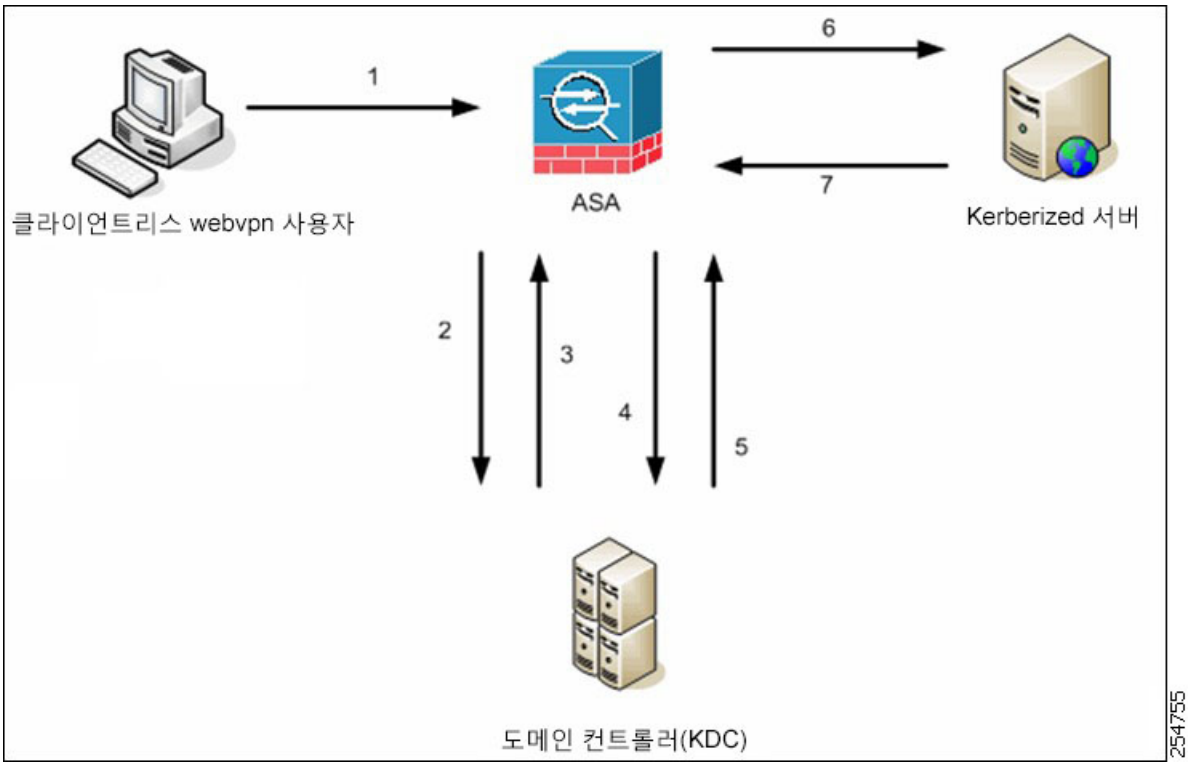
제한 위임에 대한 자세한 내용은 IETF 웹 사이트(http://www.ietf.org)에서 RFC 1510을 참조하십시오.

KCD를 통한 인증 흐름

다음 그림은 클라이언트리스 포털을 통해 위임에 대해 신뢰할 수 있는 리소스에 액세스할 때 사용자가 직간접적으로 경험하는 패킷 및 프로세스 흐름을 표시한 것입니다. 이 프로세스는 다음 작업이 완료된 상태라고 가정합니다.

- ASA에 KCD가 구성되어 있음
- Windows Active Directory에 가입하고 위임을 위해 서비스를 신뢰할 수 있는지 확인
- Windows Active Directory 도메인의 요소로 ASA 위임

그림 8: KCD 프로세스



참고 클라이언트리스 사용자 세션은 사용자용으로 구성된 인증 메커니즘을 사용하여 ASA에서 인증됩니다. (스마트 카드 크리덴셜의 경우 ASA는 Windows Active Directory에 대한 디지털 인증서에서 userPrincipalName을 사용하여 LDAP 권한 부여를 수행합니다.

1. 인증이 성공한 후에 사용자는 ASA 클라이언트리스 포털 페이지에 로그인합니다. 사용자는 포털 페이지에 URL을 입력하거나 책갈피를 클릭하여 웹 서비스에 액세스합니다. 웹 서비스에 인증이 필요한 경우 서버는 크리덴셜을 위해 ASA에 챌린지하고 서버에서 지원되는 인증 방법 목록을 전송합니다.

참고 클라이언트리스 SSL VPN에 대한 KCD는 모든 인증 방법(RADIUS, RSA/SDI, LDAP, 디지털 인증서 등)에 지원됩니다. AAA 지원 표 (http://www.cisco.com/en/US/docs/security/asa/asa84/configuration/guide/access_aaa.html#wp1069492)를 참조하십시오.

2. 챌린지의 HTTP 헤더에 기반하여 ASA는 서버에 Kerberos 인증이 필요한지 판단합니다. (이는 SPNEGO 메커니즘의 일부입니다.) 백엔드 서버에 연결하는 데 Kerberos 인증이 필요한 경우, ASA는 키 배포 센터의 사용자 대신 자체적으로 서비스 티켓을 요청합니다.

3. 키 배포 센터는 요청한 티켓을 ASA에 반환합니다. 이 티켓이 ASA에 전달되는 경우에도 사용자의 권한 부여 데이터가 포함되어 있습니다. ASA는 사용자가 액세스하려는 특정 서비스에 대해 KDC의 서비스 티켓을 요청합니다.

참고 1~3단계는 프로토콜 전환을 구성합니다. 이 단계를 수행한 후 비 Kerberos 인증 프로토콜을 사용하여 ASA를 인증하는 모든 사용자는 Kerberos를 사용하여 키 배포 센터를 분명하게 인증해야 합니다.

4. ASA는 사용자가 액세스하려는 특정 서비스에 대해 키 배포 센터의 서비스 티켓을 요청합니다.
5. 키 배포 센터는 특정 서비스에 대한 서비스 티켓을 ASA에 반환합니다.
6. ASA는 서비스 티켓을 사용하여 웹 서비스에 대한 액세스를 요청합니다.
7. 웹 서버는 Kerberos 서비스 티켓을 인증하고 서비스에 대한 액세스 권한을 부여합니다. 인증이 실패할 경우 적절한 오류 메시지가 표시되고 확인을 요구합니다. Kerberos 인증이 실패할 경우에 예상되는 동작은 기본 인증으로 돌아가는 것입니다.

교차 영역 인증을 위한 **ASA** 구성

교차 영역 인증을 위해 ASA를 구성하려면 다음 명령을 사용해야 합니다.

프로시저

단계 **1** Active Directory 도메인에 가입합니다. 10.1.1.10 도메인 컨트롤러(인터페이스 내부에서 연결 가능).

ntp *hostname*

예제**:**

```
hostname(config)# configure terminal
#Create an alias for the Domain Controller

hostname(config)# name 10.1.1.10 DC
#Configure the Name server
```

단계 **2** 조회를 수행합니다.

dns domain-lookup

dns server-group

예제**:**

이 예에서는 사용자 이름으로 dcuser, 비밀번호로 dcuser123!을 사용하여 private.net의 도메인 이름과 도메인 컨트롤러의 서비스 어카운트를 보여줍니다.

```
hostname(config)# ntp server DC
#Enable a DNS lookup by configuring the DNS server and Domain name
hostname(config)# dns domain-lookup inside
```

```
hostname(config)# dns server-group DefaultDNS
hostname(config-dns-server-group)# name-server DC
hostname(config-dns-server-group)# domain-name private.net

#Configure the AAA server group with Server and Realm

hostname(config)# aaa-server KerberosGroup protocol Kerberos
hostname(config-asa-server-group)# aaa-server KerberosGroup (inside) host DC
hostname(config-asa-server-group)# Kerberos-realm PRIVATE.NET

#Configure the Domain Join

hostname(config)# webvpn
hostname(config-webvpn)# kcd-server KerberosGroup username dcuser password dcuser123!
hostname(config)#
```

KCD 구성

ASA가 Windows Active Directory 도메인에 가입하고 성공 또는 실패 상태로 돌아가려면 다음 단계를 수행하십시오.

프로시저

단계 **1** 클라이언트리스 SSL VPN 구성 모드로 전환합니다.

webvpn

단계 **2** KCD를 구성합니다.

kcd-server

단계 **3** 도메인 컨트롤러 이름 및 영역을 지정합니다. AAA 서버 그룹은 Kerberos 유형이어야 합니다.

kcd-server aaa-server-group

예제**:**

```
ASA(config)# aaa-server KG protocol kerberos
ASA(config)# aaa-server KG (inside) host DC
ASA(config-aaa-server-host)# kerberos-realm test.edu
ASA(webvpn-config)# kcd-server KG username user1 password abc123
ASA(webvpn-config)# no kcd-server
```

단계 **4** (선택 사항) ASA에 대해 지정된 동작을 제거합니다.

no kcd-server

단계 **5** (선택 사항) 내부 상태로 재설정합니다.

kcd-server reset

단계 **6** KCD 서버가 있는지 확인하고 도메인 가입 프로세스를 시작합니다. Active Directory 사용자 이름과 비밀번호는 EXEC 모드에서만 사용되며 구성에 저장되지 않습니다.

참고 최초 가입 시 관리자 권한이 필요합니다. 도메인 컨트롤러에서 서비스 수준 권한이 있는 사용자는 액세스하지 못합니다.

kcd domain-join username <*user*> **password** <*pass*>

user — 특정 관리자가 아니라 Windows 도메인 컨트롤러에 디바이스를 추가하는 서비스 수준 권한이 있는 사용자에 해당합니다.

pass - 특정 비밀번호가 아니라 Windows 도메인 컨트롤러에서 디바이스를 추가할 서비스 수준 비밀번호 권한이 있는 사용자에 해당합니다.

단계 **7** KCD 서버 명령에 유효한 도메인 가입 상태가 있는지 확인한 후 도메인 나가기를 시작합니다.

kcd domain-leave

KCD 상태 정보 표시

프로시저

	명령 또는 동작	목적
단계 **1**	9.5.2 릴리스에서 다음 명령은 ADI를 통해 도메인 구성원 자격을 요청합니다. 최소한 해당하는 경우 도메인 가입 상태(가입됨 또는 가입되지 않음) 및 실패 사유(알 수 없음, 서버에 연결할 수 없음 또는 유효하지 않은 권한)를 반환합니다. 예제: `ASA#show webvpn kcd` `KCD-Server Name : DC` `User : user1` `Password : ****` `KCD State : Joined` `Failure Reason : Unknown`	**show webvpn kcd**

KCD 디버그

9.5.2 버전 이전의 사례에서와 같이 ADI가 syslog를 방출하는 수준을 제어하는 대신 KCD 특정 디버그 메시지에 대한 출력을 제어하려면 다음 명령을 사용합니다.

debug webvpn kcd

캐시된 **Kerberos** 티켓 표시

ASA에 캐시된 모든 Kerberos 티켓을 표시하려면 다음 명령을 입력합니다.

show aaa kerberos[**username** *user* | **host** *ip* | **hostname**]

예

```
ASA# show aaa kerberos

Default Principal     Valid Starting       Expires     Service Principal
asa@example.COM     06/29/10 18:33:00      06/30/10 18:33:00
krbtgt/example.COM@example.COM
kcduser@example.COM     06/29/10 17:33:00      06/30/10 17:33:00
asa$/example.COM@example.COM
kcduser@example.COM     06/29/10 17:33:00      06/30/10 17:33:00
http/owa.example.com@example.COM

ASA# show aaa kerberos username kcduser

Default Principal     Valid Starting      Expires     Service Principal
kcduser@example.COM     06/29/10 17:33:00      06/30/10 17:33:00
asa$/example.COM@example.COM
kcduser@example.COM     06/29/10 17:33:00      06/30/10 17:33:00
http/owa.example.com@example.COM

ASA# show aaa kerberos host owa.example.com

Default Principal     Valid Starting      Expires     Service Principal
kcduser@example.COM     06/29/10      06/30/10 17:33:00
```

캐시된 **Kerberos** 티켓 지우기

ASA의 모든 Kerberos 티켓 정보를 지우려면 다음 명령을 입력합니다.

clear aaa kerberos [**username** *user* | **host** *ip* | *hostname*]

- user - 특정 사용자의 Kerberos 티켓을 지우는 데 사용됨
- hostname - 특정 호스트의 Kerberos 티켓을 지우는 데 사용됨

Microsoft Kerberos 요건

kcd-server 명령이 작동하려면 ASA가 소스 도메인(ASA가 있는 도메인)과 대상 또는 리소스 도메인(웹 서비스가 있는 도메인) 간의 신뢰 관계를 설정해야 합니다. 고유 형식을 사용하는 ASA는 소스에서 대상 도메인으로 인증 경로를 교차시키고 원격 액세스 사용자를 대신하여 서비스에 액세스하는 데 필요한 티켓을 획득합니다.

이러한 인증서 경로 교차를 교차 영역 인증이라고 합니다. 교차 영역 인증의 각 단계에서 ASA는 특정 도메인에 있는 자격 증명 및 후속 도메인과의 신뢰 관계에 의존합니다.

애플리케이션 프로파일 사용자 지정 프레임워크 구성

클라이언트리스 SSL VPN에는 APCF(Application Profile Customization Framework:애플리케이션 프로필 맞춤화 프레임워크) 옵션이 포함되어 있어 ASA가 비표준 애플리케이션 및 웹 리소스를 처리하여 클라이언트리스 SSL VPN 연결에 정확하게 표시할 수 있습니다. APCF 프로파일에는 특정 애플리케이션을 언제(이전, 이후), 어디서(헤더, 본문, 요청, 응답), 무엇(데이터)에 대해 변형할지를 지정하는 스크립트가 포함되어 있습니다. 이 스크립트는 XML로 작성되며 sed(스트림 편집기) 구문을 사용하여 문자열/텍스트를 변형합니다.

ASA에서 동시에 여러 APCF 프로필을 구성하고 실행할 수 있습니다. APCF 프로파일 스크립트 내에서 여러 APCF 규칙을 적용할 수 있습니다. ASA는 가장 오래된 규칙을 구성 기록에 기초하여 먼저 처리하고 다음으로 가장 오래된 규칙을 처리합니다.

APCF 프로필을 ASA 플래시 메모리나 HTTP, HTTPS 또는 TFTP 서버에 저장할 수 있습니다.

반드시 Cisco 직원의 도움을 받아서 APCF 프로파일을 구성할 것을 권장합니다.

APCF 패킷 관리

프로시저

단계 **1** 클라이언트리스 SSL VPN 구성 모드로 전환합니다.

webvpn

단계 **2** ASA에 로드할 APCF 프로파일을 식별 및 검색합니다.

apcf

예제**:**

이 예에서는 플래시 메모리에 있는 apcf1.xml이라는 이름의 APCF 프로파일을 활성화 하는 방법과 myserver라는 HTTPS 서버에 있고, 포트 1440을 사용하고, 경로가 /apcf인 apcf2.xml이라는 이름의 APCF 프로파일을 활성화하는 방법을 보여 줍니다.

```
hostname(config)# webvpn
hostname(config-webvpn)# apcf flash:/apcf/apcf1.xml

hostname(config)# webvpn
hostname(config-webvpn)# apcf https://myserver:1440/apcf/apcf2.xml
```

APCF 구문

APCF 프로파일은 다음 표에 있는 XML 태그와 함께 XML 형식 및 sed 스크립트 구문을 사용합니다.

APCF용 지침

APCF 프로파일을 잘못 사용하면 성능이 저하되고 원하지 않는 콘텐츠가 렌더링될 수 있습니다. 대부분의 경우 Cisco Engineering에서 특정한 애플리케이션 렌더링 문제를 해결하도록 APCF 프로파일을 제공합니다.

표 ***15: APCF XML*** 태그

태그	사용 환경
<APCF>...</APCF>	모든 APCF XML 파일을 여는 필수 루트 요소입니다.
<version>1.0</version>	APCF 구현 버전을 지정하는 필수 태그입니다. 현재 고유한 버전은 1.0입니다.
<application>...</application>	XML 설명의 본문을 래핑하는 필수 태그입니다.
<id> text </id>	이 특정 APCF 기능에 대해 설명하는 필수 태그입니다.
<apcf-entities>...</apcf-entities>	단일 또는 다중 APCF 엔터티를 래핑하는 필수 태그입니다.
<js-object>…</js-object> <html-object>…</html-object> <process-request-header>...</process-request-header> <process-response-header>...</process-response-header> <preprocess-response-body>...</preprocess-response-body> <postprocess-response-body>...</postprocess-response-body>	이 태그 중 하나는 APCF 처리가 발생해야 하는 콘텐츠 또는 단계의 유형을 지정합니다.

태그	사용 환경
<conditions>… </conditions>	처리를 위해 기준을 지정하는 프로세스 이전/이후 태그의 하위 요소입니다. 예: • http-버전(예: 1.1, 1.0, 0.9) • http-메서드(get, put, post, webdav) • http-스키마(“http/”, “https/” 및 기타) • server-regexp("a".."z" | "A".."Z" | "0".."9" | ".-_*[]?"를 포함하는 정규식) • server-fnmatch("a".."z" | "A".."Z" | "0".."9" | ".-_*[]?+()\{},"를 포함하는 정규식) • user-agent-regexp • user-agent-fnmatch • request-uri-regexp • request-uri-fnmatch • 두 개 이상의 조건 태그가 있는 경우 ASA는 모든 태그에 대해 논리적 AND를 수행합니다.
<action> … </action>	지정된 조건에 해당하는 콘텐츠에서 수행할 작업을 하나 이상 래핑합니다. 다음 태그를 사용하여 이러한 작업을 정의할 수 있습니다(아래에 표시). • <do> • <sed-script> • <rewrite-header> • <add-header> • <delete-header>

태그	사용 환경
<do>…</do>	다음 작업 중 하나를 정의하는 데 사용되는 작업 태그의 하위 요소: • <no-rewrite/> — 원격 서버에서 수신한 콘텐츠를 바꾸지 마십시오. • <no-toolbar/> — 툴바를 삽입하지 마십시오. • <no-gzip/> — 콘텐츠를 압축하지 마십시오. • <force-cache/> — 원래 캐싱 지침을 준수하십시오. • <force-no-cache/> — 개체를 캐시 불가능 상태로 설정하십시오. • < downgrade-http-version-on-backend> — 원격 서버에 요청을 전송할 때 HTTP/1.0을 사용합니다.
<sed-script> TEXT </sed-script>	텍스트 기반 개체의 콘텐츠를 변경하는 데 사용되는 작업 태그의 하위 요소입니다. 이 텍스트는 유효한 Sed 스크립트여야 합니다. <sed-script>는 이전에 정의한 <conditions> 태그에 적용됩니다.
<rewrite-header></rewrite-header>	작업 태그의 하위 요소입니다. 아래에 표시된 하위 요소인 태그에 지정된 HTTP 헤더의 값을 <header> 변경합니다.
<add-header></add-header>	아래에 표시된 하위 요소인 태그에 지정된 새 HTTP 헤더를 추가하는 데 사용되는 작업 태그의 <header> 하위 요소입니다.
<delete-header></delete-header>	아래에 표시된 하위 요소인 태그에서 지정된 HTTP 헤더를 삭제하는 데 사용되는 작업 태그의 <header> 하위 요소입니다.
<header></header>	재작성, 추가 또는 삭제할 이름 HTTP 헤더를 지정합니다. 예를 들어 다음 태그는 이름이 Connection인 HTTP 헤더의 값을 변경합니다. `<rewrite-header>` `<header>Connection</header>` `<value>close</value>` `</rewrite-header>`

APCF 구성 예

```
<APCF>
<version>1.0</version>
<application>
  <id>Do not compress content from example.com</id>
  <apcf-entities>
      <process-request-header>
         <conditions>
           <server-fnmatch>*.example.com</server-fnmatch>
         </conditions>
           <action>
             <do><no-gzip/></do>
           </action>
      </process-request-header>
  </apcf-entities>
</application>
</APCF>

<APCF>
<version>1.0</version>
<application>
 <id>Change MIME type for all .xyz objects</id>
 <apcf-entities>
      <process-response-header>
        <conditions>
            <request-uri-fnmatch>*.xyz</request-uri-fnmatch>
        </conditions>
         <action>
           <rewrite-header>
                <header>Content-Type</header>
                <value>text/html</value>
           </rewrite-header>
         </action>
      </process-response-header>
 </apcf-entities>
</application>
</APCF>
```

인코딩

문자 인코딩은 "문자 코딩" 및 "문자 집합"이라고도 하며 데이터를 표현하기 위한 원시 데이터(예: 0 및 1)와 문자의 쌍입니다. 언어는 사용할 문자 인코딩 방법을 결정합니다. 일부 언어에서는 단일 방법을 사용하지만 나머지는 그렇지 않습니다. 일반적으로 지리적 지역에 따라 브라우저가 사용하는 기본 인코딩 방법이 결정되지만 원격 사용자가 이 방법을 변경할 수 있습니다. 브라우저는 페이지에서 지정된 인코딩을 탐지할 수 있으며 이에 따라 문서를 렌더링합니다.

인코딩 특성을 사용하여 포털 페이지에서 사용되는 문자 인코딩 방법의 값을 지정하여 사용자가 브라우저를 사용하는 지역과 브라우저에 수행한 변경사항에 관계 없이 브라우저에서 이 값을 적절하게 렌더링하도록 할 수 있습니다.

기본적으로 ASA는 공통 인터넷 파일 시스템 서버의 페이지에 "전역 인코딩 유형"을 적용합니다. "전역 인코딩 유형" 특성에 따라 전역으로 그리고, 표에 표시된 파일 인코딩 예외에 따라 개별적으로 CIFS 서버를 해당하는 문자 인코딩에 매핑하면, 파일 이름, 디렉토리 경로 및 페이지를 적절하게 렌더링하는 것이 문제인 경우 CIFS 페이지를 정확하게 처리하여 표시할 수 있습니다.

문자 인코딩 확인 또는 지정

인코딩을 통해 클라이언트리스 SSL VPN 포털 페이지에 대해 문자 인코딩을 보거나 지정할 수 있습니다.

프로시저

단계 **1** 전역 인코딩 유형은 표에 나열된 CIFS 서버의 문자열 인코딩을 제외하고 모든 클라이언트리스 SSL VPN 포털 페이지가 상속 받을 문자열 인코딩을 결정합니다. 문자열을 입력하거나 다음과 같이 가장 일반적인 값을 포함하는 드롭다운 목록에서 옵션 중 하나를 선택할 수 있습니다.

- big5
- gb2312
- ibm-850
- iso-8859-1
- shift_jis

  참고 일본어 Shift_jis 문자 인코딩을 사용 중인 경우 연결된 Select Page Font(페이지 글꼴 선택) 창의 Font Family(글꼴 패밀리) 영역에서 **Do Not Specify(**지정 안 함**)**를 클릭하여 글꼴 패밀리를 제거합니다.

- unicode
- windows-1252
- 없음

  참고 없음을 클릭하거나 클라이언트리스 SSL VPN 세션에 있는 브라우저가 지원하지 않는 값을 지정한 경우 고유한 기본 인코딩을 사용합니다.

최대 40개의 문자로 구성된 문자열을 입력할 수 있으며 이는 http://www.iana.org/assignments/character-sets에서 확인한 유효한 문자 집합 중 하나와 동일합니다. 이 페이지에 나열된 문자 집합의 이름 또는 별칭을 사용할 수 있습니다. 이 문자열은 대/소문자를 구분하지 않습니다. 명령어 인터프리터는 ASA 구성을 저장할 때 대문자를 소문자로 변환합니다.

단계 **2** 인코딩 요건이 "전역 인코딩 유형" 특성 설정과 다른 CIFS 서버의 이름 또는 IP 주소를 입력합니다. ASA는 이름을 서버와 일치시킬 때는 대/소문자를 무시하지만 지정한 대/소문자는 그대로 유지합니다.

단계 **3** CIFS 서버가 클라이언트리스 SSL VPN 포털 페이지에 제공해야 하는 문자 인코딩을 선택합니다. 문자열을 입력하거나 다음과 같이 가장 일반적인 값만 포함하는 드롭다운 목록에서 다음 중 하나를 선택할 수 있습니다.

- big5
- gb2312

- ibm-850
- iso-8859-1
- shift_jis

  참고 일본어 Shift_jis 문자 인코딩을 사용 중인 경우 연결된 Select Page Font(페이지 글꼴 선택) 창의 Font Family(글꼴 패밀리) 영역에서 **Do Not Specify(**지정 안 함**)**를 클릭하여 글꼴 패밀리를 제거합니다.

- unicode
- windows-1252
- 없음

없음을 클릭하거나 클라이언트리스 SSL VPN 세션에 있는 브라우저가 지원하지 않는 값을 지정한 경우 고유한 기본 인코딩을 사용합니다.

최대 40개의 문자로 구성된 문자열을 입력할 수 있으며 이는 http://www.iana.org/assignments/character-sets에서 확인한 유효한 문자 집합 중 하나와 동일합니다. 이 페이지에 나열된 문자 집합의 이름 또는 별칭을 사용할 수 있습니다. 이 문자열은 대/소문자를 구분하지 않습니다. 명령어 인터프리터는 ASA 구성을 저장할 때 대문자를 소문자로 변환합니다.

클라이언트리스 SSL VPN을 통한 이메일 사용

웹 이메일 구성: MS Outlook Web App

ASA는 Exchange Server 2010에 대해 Microsoft Outlook Web App을 지원하고 Exchange Server 2007, 2003 및 2000에 대해 Microsoft Outlook Web Access를 지원합니다.

프로시저

단계 **1** 이메일 서비스 URL을 주소 필드에 입력하거나 클라이언트리스 SSL VPN 세션에서 연결된 책갈피를 클릭합니다.

단계 **2** 확인 상자가 표시되면 도메인\사용자 이름 형식으로 이메일 서버 사용자 이름을 입력합니다.

단계 **3** 이메일 비밀번호를 입력합니다.

17 장

정책 그룹

리소스 액세스를 위한 클라이언트리스 SSL VPN 정책 생성 및 적용

내부 서버에서 리소스에 대한 액세스를 제어하는 클라이언트리스 SSL VPN에 대한 정책을 생성하고 적용하려면 그룹 정책을 할당해야 합니다.

그룹 정책에 사용자를 할당하면 여러 사용자에게 정책을 적용할 수 있어 구성이 단순화됩니다. ASA의 내부 인증 서버 또는 외부 RADIUS 또는 LDAP 서버를 사용하여 그룹 정책에 사용자를 할당할 수 있습니다. 그룹 정책이 있는 구성을 단순화하는 방법에 대한 자세한 설명은 4장, “연결 프로파일, 그룹 정책 및 사용자”를 참조하십시오.

클라이언트리스 SSL VPN에 대한 연결 프로파일 특성

다음 표는 클라이언트리스 SSL VPN에 특정한 연결 프로파일 특성의 목록을 제공합니다. 이 특성 외에 모든 VPN 연결에 공통적인 일반 연결 프로파일 특성을 구성하십시오. 연결 프로파일 구성에 대한 단계별 정보는 4장, “연결 프로파일, 그룹 정책 및 사용자”를 참조하십시오.

참고 이전 릴리스에서 “연결 프로파일”은 “터널 그룹”이라고 했습니다. tunnel-group 명령을 사용하여 연결 프로파일을 구성하십시오. 이 장에서는 이 용어를 교대로 자주 사용합니다.

표 16: 클라이언트리스 SSL VPN에 대한 연결 프로파일 특성

명령	기능
authentication	인증 방법을 설정합니다.
customization	적용하기 위해 이전에 정의한 사용자 지정 이름을 식별합니다.
exit	tunnel-group 클라이언트리스 SSL VPN 특성 구성 모드를 종료합니다.
nbns-server	CIFS 이름 확인에 사용할 NetBIOS 이름 서비스 서버(nbns-server)의 이름을 식별합니다.
group-alias	서버에서 연결 프로파일을 나타낼 수 있는 대체 이름을 지정합니다.
group-url	하나 이상의 그룹 URL을 식별합니다. 이 특성이 있는 URL을 설정하는 경우, 사용자가 해당 URL을 사용하여 액세스할 때 이 그룹이 사용자에게 자동으로 선택됩니다.
dns-group	DNS 서버 이름, 도메인 이름, 이름 서버, 재시도 횟수 및 시간 제한 값을 지정하는 DNS 서버 그룹을 식별합니다.
help	터널 그룹 구성 명령에 대한 도움말을 제공합니다.
hic-fail-group-policy	Cisco Secure Desktop Manager를 사용하여 그룹 기반 정책 특성을 "실패 그룹 정책 사용" 또는 "기준이 일치하는 경우 성공 그룹 정책 사용"으로 설정하는 경우, VPN 기능 정책을 지정합니다.
no	특성 값 쌍을 제거합니다.
override-svc-download	원격 사용자를 대상으로 AnyConnect VPN 클라이언트를 다운로드하도록 구성된 그룹 정책 또는 사용자 이름 특성의 다운로드를 재정의합니다.
pre-fill-username	이 터널 그룹에서 username-to-certificate 바인딩을 구성합니다.
proxy-auth	이 터널 그룹을 특정 프록시 인증 터널 그룹으로 식별합니다.
radius-reject-message	인증이 거부될 경우 로그인 화면에서 RADIUS 거부 메시지 표시를 활성화합니다.
secondary-pre-fill-username	이 터널 그룹에서 보조 username-to-certificate 바인딩을 구성합니다.
without-csd	터널 그룹에 대해 CSD를 해제합니다.

클라이언트리스 SSL VPN에 대한 그룹 정책 및 사용자 특성

다음 표는 클라이언트리스 SSL VPN에 대한 그룹 정책 및 사용자 속성의 목록을 제공합니다. 그룹 정책 및 사용자 속성 구성에 대한 단계별 지침은 클라이언트리스 SSL VPN 세션에 대한 그룹 정책 속성

구성, 358 페이지 또는 특정 사용자에 대한 클라이언트리스 SSL VPN 액세스 구성, 366 페이지의 내용을 참조하십시오.

명령	기능
activex-relay	클라이언트리스 SSL VPN 세션을 설정한 사용자는 브라우저를 사용하여 Microsoft Office 애플리케이션을 실행할 수 있습니다. 이 애플리케이션은 이 세션을 사용하여 ActiveX를 다운로드 및 업로드합니다. ActiveX Relay는 클라이언트리스 SSL VPN 세션이 종료될 때까지 그대로 실행됩니다.
auto-sign-on	클라이언트리스 SSL VPN 연결을 위해 사용자가 사용자 이름과 비밀번호 자격 증명을 한 번만 입력해야 하는 자동 로그온에 대해 값을 설정합니다.
customization	그룹 정책 또는 사용자에게 사용자 지정 개체를 할당합니다.
deny-message	클라이언트리스 SSL VPN에 성공적으로 로그인하지만 VPN 권한이 없는 원격 사용자에게 제공되는 메시지를 지정합니다.
file-browsing	파일 서버 및 공유를 위해 CIFS 파일 브라우징을 활성화합니다. 브라우징에는 NBNS(마스터 브라우저 또는 WINS)가 필요합니다.
file-entry	사용자가 액세스할 파일 서버 이름을 입력할 수 있습니다.
filter	webtype 액세스 목록의 이름을 설정합니다.
hidden-shares	CIFS 파일에 대해 숨겨진 공유의 가시성을 제어합니다.
homepage	로그인 시 표시되는 웹 페이지의 URL을 설정합니다.
html-content-filter	콘텐츠 및 개체를 이 그룹 정책에 대한 HTML에서 필터링하도록 구성합니다.
http-comp	압축을 구성합니다.
http-proxy	외부 프록시 서버를 사용하여 HTTP 요청을 처리하도록 ASA를 구성합니다. 참고 Proxy NTLM 인증은 **http-proxy**에서 지원되지 않습니다. 인증 없는 프록시와 기본 인증의 프록시만 지원됩니다.
keep-alive-ignore	세션 타이머 업데이트를 무시하도록 최대 개체 크기를 설정합니다.
port-forward	전달할 클라이언트리스 SSL VPN TCP 포트 목록을 적용합니다. 사용자 인터페이스에 이 목록에 있는 애플리케이션이 표시됩니다.
post-max-size	게시할 최대 개체 크기를 설정합니다.
smart-tunnel	스마트 터널을 사용하도록 프로그램 및 일부 스마트 터널 매개변수 목록을 구성합니다.
storage-objects	세션 간에 저장된 데이터의 저장소 개체를 구성합니다.
svc	SSL VPN 클라이언트 특성을 구성합니다.

명령	기능
unix-auth-gid	UNIX 그룹 ID를 설정합니다.
unix-auth-uid	UNIX 사용자 ID를 설정합니다.
url-entry	사용자의 HTTP/HTTPS URL 입력 가능 여부를 제어합니다.
url-list	클라이언트리스 SSL VPN 포털 페이지에서 엔드 유저 액세스를 위해 표시하는 서버 및 URL 목록을 적용합니다.
user-storage	세션 간에 사용자 데이터를 저장할 위치를 구성합니다.

클라이언트리스 **SSL VPN** 세션에 대한 그룹 정책 속성 구성

클라이언트리스 SSL VPN을 통해 사용자는 웹 브라우저를 사용하는 ASA에 보안, 원격 액세스 VPN 터널을 설정할 수 있습니다. 소프트웨어 또는 하드웨어 클라이언트가 필요하지 않습니다. 클라이언트리스 SSL VPN은 HTTPS 인터넷 사이트에 연결할 수 있는 거의 모든 컴퓨터의 광범위한 웹 리소스 및 웹 활성화 애플리케이션에 쉽게 액세스할 수 있도록 지원합니다. 클라이언트리스 SSL VPN은 SSL과 후속 작업, TLS1을 사용하여 중앙 사이트에서 구성한 특정 지원 내부 리소스와 원격 사용자 간에 보안 연결을 제공합니다. ASA는 프록시가 필요한 연결을 인식하고 HTTP 서버는 사용자를 인증하기 위해 인증 하위 시스템과 상호 작용합니다. 클라이언트리스 SSL VPN은 기본적으로 비활성화되어 있습니다.

특정한 내부 그룹 정책에 대한 클라이언트리스 SSL VPN 구성을 사용자 지정할 수 있습니다.

참고 전역 구성 모드에서 시작한 webvpn 모드를 사용하여 클라이언트리스 SSL VPN 세션에 대한 전역 설정을 구성할 수 있습니다. 이 섹션에서 설명한 webvpn 모드는 그룹 정책 구성 모드에서 시작되며 이를 통해 클라이언트리스 SSL VPN 세션에 특정하게 그룹 정책의 구성을 사용자 지정할 수 있습니다.

그룹 정책 webvpn 구성 모드에서 다음 매개변수(각 후속 섹션에 설명됨)를 상속받거나 사용자 지정할지 여부를 지정할 수 있습니다.

- customizations
- html-content-filter
- homepage
- filter
- url-list
- port-forward
- port-forward-name
- auto-signon

- deny message
- AnyConnect Secure Mobility Client
- keep-alive ignore
- HTTP compression

많은 경우 webvpn 특성을 클라이언트리스 SSL VPN의 일부로 정의한 다음 그룹 정책 webvpn 특성을 구성할 때 이 정의를 특정 그룹에 적용하십시오. 그룹 정책 구성 모드에서 **webvpn** 명령을 사용하여 그룹 정책 그룹 정책 webvpn 구성 모드를 시작합니다. 그룹 정책에 대한 Webvpn 명령은 클라이언트리스 SSL VPN 세션을 통한 파일, URL 및 TCP 애플리케이션에 대한 액세스를 정의합니다. 또한 필터링할 ACL 및 트래픽 유형을 식별합니다. 클라이언트리스 SSL VPN은 기본적으로 비활성화되어 있습니다.

그룹 정책 webvpn 구성 모드에서 입력한 모든 명령을 제거하려면 이 명령의 **no** 형식을 입력합니다. 이 webvpn 명령은 이 명령을 구성한 사용자 이름 또는 그룹 정책에 적용됩니다.

webvpn

no webvpn

다음 예는 이름이 FirstGroup인 그룹 정책에 대해 그룹 정책 webvpn 구성 모드를 시작하는 방법을 보여줍니다.

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# webvpn
hostname(config-group-webvpn)#
```

거부 메시지 지정

다음과 같이 그룹 정책 webvpn 구성 모드에서 **deny-message** 명령을 입력하여 클라이언트리스 SSL VPN 세션에 성공적으로 로그인하지만 VPN 권한이 없는 원격 사용자에게 제공되는 메시지를 지정할 수 있습니다.

```
hostname(config-group-webvpn)# deny-message value "message"
hostname(config-group-webvpn)# no deny-message value "message"
hostname(config-group-webvpn)# deny-message none
```

no deny-message value 명령은 원격 사용자가 메시지를 수신하지 않도록 메시지 문자열을 제거합니다.

no deny-message none 명령은 연결 프로파일 정책 구성에서 특성을 제거합니다. 이 정책은 특성 값을 상속받습니다.

메시지는 최대 491자의 영숫자 문자로, 특수 문자, 공백, 구두점을 포함하나 인용 따옴표는 수에 포함하지 않습니다. 텍스트는 로그인 시 원격 사용자의 브라우저에 나타납니다. **deny-message value** 명령에 문자열을 입력하는 경우 명령이 래핑되더라도 계속 입력하십시오.

기본 거부 메시지는 다음과 같습니다. “로그인에 성공했지만 특정 기준이 충족되지 않았거나 일부 특정한 그룹 정책으로 인해 VPN 기능을 사용할 권한이 없습니다. 자세한 내용은 IT 관리자에게 문의하십시오.”

다음 예에서 첫 번째 명령은 이름이 group2인 내부 그룹을 생성합니다. 후속 명령은 이 정책과 연계된 webvpn 거부 메시지를 포함하여 특성을 수정합니다.

```
hostname(config)# group-policy group2 internal
hostname(config)# group-policy group2 attributes
hostname(config-group)# webvpn
hostname(config-group-webvpn)# deny-message value "Your login credentials are OK. However,
 you have not been granted rights to use the VPN features. Contact your administrator for
more information."
hostname(config-group-webvpn)
```

클라이언트리스 SSL VPN 세션에 대한 그룹 정책 필터 속성 구성

webvpn 모드에서 **html-content-filter** 명령을 사용하여 이 그룹 정책에 대한 클라이언트리스 SSL VPN 세션에서 Java, ActiveX, 이미지, 스크립트 및 쿠키를 필터링할지 지정합니다. HTML 필터링은 기본적으로 비활성화되어 있습니다.

콘텐츠 필터를 제거하려면 **no** 형식의 이 명령을 입력합니다. **none** 키워드와 함께 **html-content-filter** 명령을 발행하여 생성한 null 값을 포함하여 모든 콘텐츠 필터를 제거하려면 인수 없이 **no** 형식의 이 명령을 입력합니다. **no** 옵션을 사용하면 다른 그룹 정책에서 값을 상속받을 수 있습니다. html 콘텐츠 필터 상속을 방지하려면 **none** 키워드와 함께 **html-content-filter** 명령을 입력합니다.

명령을 한 번 더 사용하면 이전 설정이 재정의됩니다.

```
hostname(config-group-webvpn)# html-content-filter {java | images | scripts |
cookies | none}

hostname(config-group-webvpn)# no html-content-filter [java | images | scripts |
 cookies | none]
```

아래 표는 이 명령에서 사용되는 키워드의 의미를 설명합니다.

표 ***17:*** 필터 명령 키워드

키워드	의미
cookies	이미지에서 쿠키를 제거하여 제한된 광고 필터링 및 개인정보 보호를 제공합니다.
images	이미지 참조를 제거합니다(<IMG> 태그 제거).
java	Java 및 ActiveX 참조를 제거합니다(<EMBED>, <APPLET> 및 <OBJECT> 태그 제거).
none	필터가 없음을 나타냅니다. null 값을 설정하므로 필터링을 허용하지 않습니다. 필터 값 상속을 방지합니다.
scripts	스크립팅 참조를 제거합니다(제거 <SCRIPT> tags).

다음 예는 이름이 FirstGroup인 그룹 정책에 대해 JAVA, ActiveX, 쿠키 및 이미지 필터링을 설정하는 방법을 보여줍니다.

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# webvpn
hostname(config-group-webvpn)# html-content-filter java cookies images
hostname(config-group-webvpn)#
```

사용자 홈 페이지 지정

그룹 정책 webvpn 구성 모드에서 **homepage** 명령을 사용하여 이 그룹의 사용자가 로그인할 때 표시되는 웹 페이지에 대해 URL을 지정합니다. 기본 홈 페이지는 없습니다.

homepage none 명령을 발행하여 생성한 null 값을 포함하는 구성된 홈 페이지를 제거하려면 **no** 형식의 이 명령을 입력합니다. **no** 옵션을 사용하면 다른 그룹 정책에서 값을 상속받을 수 있습니다. 홈 페이지 상속을 방지하려면 **homepage none** 명령을 입력합니다.

none 키워드는 클라이언트리스 SSL VPN 세션에 대해 홈 페이지가 없음을 나타냅니다. 이 키워드는 null 값을 설정하므로 홈 페이지를 허용하지 않고 홈 페이지 상속을 방지합니다.

url-string 변수는 **value** 키워드 다음에 오며 홈 페이지의 URL을 제공합니다. 문자열은 http:// 또는 https://로 시작해야 합니다.

```
hostname(config-group-webvpn)# homepage {value url-string | none}
hostname(config-group-webvpn)# no homepage
hostname(config-group-webvpn)#
```

자동 로그온 구성

auto-signon 명령은 클라이언트리스 SSL VPN 세션의 사용자를 위한 SSO(Single Sign-On) 방법입니다. 이 명령은 로그인 자격 증명(사용자 이름 및 비밀번호)을 NTLM 인증, 기본 인증 또는 두 가지 모두를 사용하는 인증을 위해 내부 서버에 전달합니다. 여러 auto-signon 명령을 입력할 수 있으며, 이는 입력 순서에 따라 처리됩니다. 즉 먼저 입력된 명령이 우선합니다.

auto-signon 기능은 webvpn 구성, webvpn 그룹 구성 또는 webvpn 사용자 이름 구성 모드의 세 가지 모드로 사용할 수 있습니다. 일반적인 우선순위 동작은 사용자 이름이 그룹을 교체하고, 그룹이 전역을 교체하는 경우 적용됩니다. 선택한 모드는 인증의 적절한 범위에 따라 다릅니다.

특정 사용자를 위한 auto-signon을 특정 서버에 대해 비활성화하려면 IP 블록 또는 URI의 원래 사양에 대해 **no** 형식의 명령을 사용합니다. 모든 서버에 대한 인증을 비활성화하려면 인수 없이 **no** 형식을 사용합니다. **no** 옵션을 사용하면 그룹 정책에서 값을 상속받을 수 있습니다.

그룹 정책 webvpn 구성 모드에서 입력한 다음의 예는 기본 인증을 사용하여 이름이 anyuser인 사용자를 위해 auto-signon을 10.1.1.0에서 10.1.1.255 범위의 IP 주소 서버에 구성합니다.

다음 예에서 명령은 기본 인증 또는 NTLM 인증을 사용하여 클라이언트리스 SSL VPN 세션의 사용자를 위한 auto-signon을 URI 마스크 https://*.example.com/*를 사용하여 정의한 서버에 구성합니다.

```
hostname(config)# group-policy ExamplePolicy attributes
hostname(config-group-policy)# webvpn
hostname(config-group-webvpn)# auto-signon allow uri https://*.example.com/*
```

```
auth-type all
hostname(config-group-webvpn)#
```

다음 예에서 명령은 기본 인증 또는 NTLM 인증을 사용하여 클라이언트리스 SSL VPN 세션의 사용자를 위한 auto-signon을 서브넷 마스크 255.255.255.0을 사용하며 IP 주소가 10.1.1.0인 서버에 구성합니다.

```
hostname(config)# group-policy ExamplePolicy attributes
hostname(config-group-policy)# webvpn
hostname(config-group-webvpn)# auto-signon allow ip 10.1.1.0 255.255.255.0
auth-type all
hostname(config-group-webvpn)#
```

클라이언트리스 SSL VPN 세션에 대한 ACL 지정

webvpn 모드에서 **filter** 명령을 사용하여 이 그룹 정책에 대한 클라이언트리스 SSL VPN 세션에 사용할 ACL 이름 또는 사용자 이름을 지정합니다. 클라이언트리스 SSL VPN ACL은 이를 지정하기 위해 **filter** 명령을 입력할 때까지 적용되지 않습니다.

filter none 명령을 발행하여 생성한 null 값을 포함하는 ACL을 제거하려면 **no** 형식의 이 명령을 입력합니다. **no** 옵션을 사용하면 다른 그룹 정책에서 값을 상속받을 수 있습니다. 필터 값 상속을 방지하려면 **filter value none** 명령을 입력합니다.

클라이언트리스 SSL VPN 세션에 대한 ACL은 이를 지정하기 위해 **filter** 명령을 입력할 때까지 적용되지 않습니다.

이 그룹 정책에 대한 다양한 유형의 트래픽을 허용하거나 거부하도록 ACL을 구성합니다. 그런 다음 **filter** 명령을 입력하여 클라이언트리스 SSL VPN 트래픽에 대한 ACL을 적용합니다.

```
hostname(config-group-webvpn)# filter {value ACLname | none}
hostname(config-group-webvpn)# no filter
```

none 키워드는 **webvpntype** ACL이 없음을 나타냅니다. 이 키워드는 null 값을 설정하므로 ACL을 허용하지 않고 다른 그룹 정책에서의 ACL 상속을 방지합니다.

value 키워드 다음에 오는 *ACLname* 문자열은 이전에 구성한 ACL의 이름을 제공합니다.

참고 클라이언트리스 SSL VPN 세션은 **vpn-filter** 명령에 정의된 ACL을 사용하지 않습니다.

다음 예는 이름이 FirstGroup인 그룹 정책에 대해 acl_in이라는 ACL을 호출하는 필터를 설정하는 방법을 보여줍니다.

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# webvpn
hostname(config-group-webvpn)# filter acl_in
hostname(config-group-webvpn)#
```

URL 목록 적용

그룹 정책에 대한 클라이언트리스 SSL VPN 홈 페이지에 나타나는 URL 목록을 지정할 수 있습니다. 먼저 전역 구성 모드에서 **url-list** 명령을 입력하여 하나 이상의 이름이 지정된 목록을 생성해야 합니다. 특정 그룹 정책에 대한 목록에 있는 URL에 액세스를 허용하면서 특정 그룹 정책에 클라이언트리스 SSL VPN 세션에 대한 서버 및 URL 목록을 적용하려면 그룹 정책 webvpn 구성 모드에서 **url-list** 명령을 사용하여 생성한 목록의 이름을 사용합니다. 기본 URL 목록은 없습니다.

url-list none 명령**,** 을 사용하여 생성한 null 값을 포함하는 목록을 제거하려면 **no** 형식의 이 명령을 사용합니다. **no** 옵션을 사용하면 다른 그룹 정책에서 값을 상속받을 수 있습니다. URL 목록 상속을 방지하려면 **url-list none** 명령을 사용합니다. 명령을 한 번 더 사용하면 이전 설정이 재정의됩니다.

```
hostname(config-group-webvpn)# url-list {value name | none} [index]
hostname(config-group-webvpn)# no url-list
```

아래 표는 **url-list** 명령 매개변수 및 의미를 보여줍니다.

표 ***18: url-list*** 명령 키워드 및 변수

매개변수	의미
index	홈 페이지에서의 표시 우선순위를 나타냅니다.
none	url 목록에 대해 null 값을 설정합니다. 기본 또는 지정된 그룹 정책에서 목록을 상속받는 것을 방지합니다.
value name	이전에 구성된 url 목록의 이름을 지정합니다. 이러한 목록을 구성하려면 전역 구성 모드에서 **url-list** 명령을 사용합니다.

다음 예는 이름이 FirstGroup인 그룹 정책에 대해 FirstGroupURL이라는 URL 목록을 설정하고 이 목록이 홈 페이지에 표시되는 첫 번째 URL 목록이 되도록 지정합니다.

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# webvpn
hostname(config-group-webvpn)# url-list value FirstGroupURLs 1
hostname(config-group-webvpn)#
```

그룹 정책에 대한 **ActiveX Relay** 활성화

ActiveX Relay를 통해 클라이언트리스 SSL VPN 세션을 설정한 사용자는 브라우저를 사용하여 Microsoft Office 애플리케이션을 시작할 수 있습니다. 이 애플리케이션은 이 세션을 사용하여 Microsoft Office 문서를 다운로드 및 업로드합니다. ActiveX Relay는 클라이언트리스 SSL VPN 세션이 종료될 때까지 그대로 실행됩니다.

클라이언트리스 SSL VPN 세션에서 ActiveX 컨트롤을 활성화하거나 비활성화하려면 그룹 정책 webvpn 구성 모드에서 다음 명령을 입력합니다.

activex-relay {**enable** | **disable**}

기본 그룹 정책에서 **activex-relay** 명령을 상속받으려면 다음 명령을 입력합니다.

no activex-relay

다음 명령은 지정된 그룹 정책과 연계된 클라이언트리스 SSL VPN 세션에서 ActiveX 컨트롤을 활성화합니다.

```
hostname(config-group-policy)# webvpn
hostname(config-group-webvpn)# activex-relay enable
hostname(config-group-webvpn)
```

그룹 정책에 대한 클라이언트리스 SSL VPN 세션에서 애플리케이션 액세스 활성화

이 그룹 정책에 대한 애플리케이션 액세스를 활성화하려면 그룹 정책 webvpn 구성 모드에서 **port-forward** 명령을 입력합니다. 포트 전달은 기본적으로 비활성화되어 있습니다.

애플리케이션 액세스를 활성화하기 위해 그룹 정책 webvpn 구성 모드에서 **port-forward** 명령을 입력하려면 먼저 사용자가 클라이언트리스 SSL VPN 세션에서 사용할 수 있는 애플리케이션 목록을 정의해야 합니다. 이 목록을 정의하려면 전역 구성 모드에서 **port-forward** 명령을 입력합니다.

port-forward none 명령을 발행하여 생성한 null 값을 포함하여 그룹 정책 구성에서 포트 전달 속성을 제거하려면 이 명령의 **no** 형식을 입력합니다. **no** 옵션을 사용하면 다른 그룹 정책에서 목록을 상속받을 수 있습니다. 포트 전달 목록의 상속을 방지하려면 **none** 키워드와 함께 **port-forward** 명령을 입력합니다. **none** 키워드는 필터링이 없음을 나타냅니다. 이 키워드는 null 값을 설정하므로 필터링을 허용하지 않고 필터링 값 상속을 방지합니다.

명령의 구문은 다음과 같습니다.

```
hostname(config-group-webvpn)# port-forward {value listname | none}
hostname(config-group-webvpn)# no port-forward
```

value 키워드 다음에 오는 *listname* 문자열은 클라이언트리스 SSL VPN 세션의 사용자가 액세스할 수 있는 애플리케이션 목록을 식별합니다. 이 목록을 정의하려면 webvpn 구성 모드에서 port-forward 명령을 입력합니다.

명령을 한 번 더 사용하면 이전 설정이 재정의됩니다.

다음 예는 이름이 FirstGroup인 내부 그룹 정책에 대해 ports1이라는 포트 전달 목록을 설정하는 방법을 보여줍니다.

```
hostname(config)# group-policy FirstGroup internal attributes
hostname(config-group-policy)# webvpn
hostname(config-group-webvpn)# port-forward value ports1
hostname(config-group-webvpn)#
```

포트 전달 표시 이름 구성

그룹 정책 webvpn 구성 모드에서 **port-forward-name**명령을 사용하여 특정 사용자 또는 그룹 정책에 대해 엔드 유저로의 TCP 포트 전달을 식별하는 표시 이름을 구성합니다. **port-forward-name none** 명령**,** 을 사용하여 생성한 null 값을 포함하는 표시 이름을 삭제하려면 **no** 형식의 명령을 입력합니다. **no**

옵션은 기본 이름인 애플리케이션 액세스를 복원합니다. 표시 이름을 방지하려면 **port-forward none** 명령을 입력합니다. 명령의 구문은 다음과 같습니다.

```
hostname(config-group-webvpn)# port-forward-name {value name | none}
hostname(config-group-webvpn)# no port-forward-name
```

다음 예는 이름이 FirstGroup인 내부 그룹 정책에 대해 이름, 원격 액세스 TCP 애플리케이션을 설정하는 방법을 보여줍니다.

```
hostname(config)# group-policy FirstGroup internal attributes
hostname(config-group-policy)# webvpn
hostname(config-group-webvpn)# port-forward-name value Remote Access TCP
Applications
hostname(config-group-webvpn)#
```

세션 타이머 업데이트를 무시하도록 최대 개체 크기 구성

네트워크 디바이스는 네트워크 디바이스 간에 가상 회로가 계속 활성 상태인지 확인하기 위해 짧은 킵얼라이브 메시지를 교환합니다. 이 메시지의 길이는 서로 다를 수 있습니다. **keep-alive-ignore** 명령을 사용하면 세션 타이머를 업데이트할 때 지정된 크기보다 작거나 같은 모든 메시지를 트래픽이 아니라 킵얼라이브 메시지로 간주하도록 ASA에 알려줄 수 있습니다. 범위는 0부터 900KB까지입니다. 기본값은 4KB입니다.

트랜잭션당 HTTP/HTTPS 트래픽의 상한을 지정하고 이를 무시하려면 다음과 같이 그룹 정책 속성 webvpn 구성 모드에서 **keep-alive-ignore** 명령을 사용합니다.

```
hostname(config-group-webvpn)# keep-alive-ignore size
hostname(config-group-webvpn)#
```

no 형식의 다음 명령은 구성에서 이 사양을 제거합니다.

```
hostname(config-group-webvpn)# no keep-alive-ignore
hostname(config-group-webvpn)#
```

다음은 무시하려는 개체의 최대 크기를 5KB로 설정하는 예입니다.

```
hostname(config-group-webvpn)# keep-alive-ignore 5
hostname(config-group-webvpn)#
```

HTTP 압축 지정

그룹 정책 webvpn 모드에서 http-comp 명령을 입력하여 특정 그룹 또는 사용자에 대해 클라이언트리스 SSL VPN 세션을 통한 http 데이터 압축을 활성화합니다.

```
hostname(config-group-webvpn)# http-comp {gzip | none}
hostname(config-group-webvpn)#
```

구성에서 명령을 제거하고 값을 상속받도록 하려면 **no** 형식의 다음 명령을 사용합니다.

```
hostname(config-group-webvpn)# no http-comp {gzip | none}
hostname(config-group-webvpn)#
```

이 명령의 구문은 다음과 같습니다.

- **gzip**—그룹 또는 사용자에 대해 압축을 활성화하도록 지정합니다. 이는 기본값입니다.
- **none**—그룹 또는 사용자에 대해 압축을 비활성화하도록 지정합니다.

클라이언트리스 SSL VPN 세션의 경우, 전역 구성 모드에서 구성한 **compression** 명령이 그룹 정책 및 사용자 이름 webvpn 모드에서 구성한 **http-comp** 명령을 재정의합니다.

다음은 group-policy sales에 대해 압축을 비활성화하는 예입니다.

```
hostname(config)# group-policy sales attributes
hostname(config-group-policy)# webvpn
hostname(config-group-webvpn)# http-comp none
hostname(config-group-webvpn)#
```

특정 사용자에 대한 클라이언트리스 **SSL VPN** 액세스 구성

다음 섹션에서는 클라이언트리스 SSL VPN 세션의 특정 사용자에 대해 구성을 사용자 지정하는 방법에 대해 설명합니다. 사용자 이름 구성 모드에서 **webvpn** 명령을 사용하여 사용자 이름 webvpn 구성 모드를 시작합니다. 클라이언트리스 SSL VPN을 통해 사용자는 웹 브라우저를 사용하는 ASA에 보안, 원격 액세스 VPN 터널을 설정할 수 있습니다. 소프트웨어 또는 하드웨어 클라이언트가 필요하지 않습니다. 클라이언트리스 SSL VPN은 HTTPS 인터넷 사이트에 연결할 수 있는 거의 모든 컴퓨터의 광범위한 웹 리소스 및 웹 활성화 애플리케이션에 쉽게 액세스할 수 있도록 지원합니다. 클라이언트리스 SSL VPN은 SSL과 후속 작업, TLS1을 사용하여 중앙 사이트에서 구성한 특정 지원 내부 리소스와 원격 사용자 간에 보안 연결을 제공합니다. ASA는 프록시가 필요한 연결을 인식하고 HTTP 서버는 사용자를 인증하기 위해 인증 하위 시스템과 상호 작용합니다.

사용자 이름 webvpn 구성 모드 명령은 클라이언트리스 SSL VPN 세션을 통한 파일, URL 및 TCP 애플리케이션에 대한 액세스를 정의합니다. 또한 필터링할 ACL 및 트래픽 유형을 식별합니다. 클라이언트리스 SSL VPN은 기본적으로 비활성화되어 있습니다. 이 **webvpn** 명령은 이 명령을 구성한 사용자 이름에만 적용됩니다. 현재 사용자 이름 webvpn 구성 모드에 있음을 나타내도록 다음과 같이 확인 상자가 변경되었음을 유의하십시오.

```
hostname(config-username)# webvpn
hostname(config-username-webvpn)#
```

사용자 이름 webvpn 구성 모드에서 입력한 모든 명령을 제거하려면 **no** 형식의 다음 명령을 사용합니다.

```
hostname(config-username)# no webvpn
hostname(config-username)#
```

이메일 프록시를 사용하도록 클라이언트리스 SSL VPN을 구성할 필요가 없습니다.

참고 전역 구성 모드에서 시작한 webvpn 모드를 사용하여 클라이언트리스 SSL VPN 세션에 대한 전역 설정을 구성할 수 있습니다. 이 섹션에서 설명한 사용자 이름 webvpn 구성 모드는 사용자 이름 모드에서 시작되며 이를 통해 클라이언트리스 SSL VPN 세션에 해당하는 특정 사용자의 구성을 사용자 지정할 수 있습니다.

사용자 이름 webvpn 구성 모드에서 다음 매개변수(각 후속 단계에 설명됨)를 사용자 지정할 수 있습니다.

- customizations
- deny message
- html-content-filter
- homepage
- filter
- url-list
- port-forward
- port-forward-name
- auto-signon
- AnyConnect Secure Mobility Client
- keep-alive ignore
- HTTP compression

다음 예는 사용자 이름 anyuser 특성에 대해 사용자 이름 webvpn 구성 모드를 시작하는 방법을 보여줍니다.

```
hostname(config)# username anyuser attributes
hostname(config-username)# webvpn
hostname(config-username-webvpn)#
```

HTML에서 필터링할 콘텐츠/개체 지정

이 사용자를 위한 클라이언트리스 SSL VPN 세션에 대해 Java, ActiveX, 이미지, 스크립트 및 쿠키를 필터링하려면 사용자 이름 webvpn 구성 모드에서 **html-content-filter** 명령을 입력합니다. 콘텐츠 필터를 제거하려면 **no** 형식의 이 명령을 입력합니다. **html-content-filter none** 명령을 발행하여 생성한 null 값을 포함하여 모든 콘텐츠 필터를 제거하려면 인수 없이 **no** 형식의 이 명령을 입력합니다. **no** 옵션을 사용하면 그룹 정책에서 값을 상속받을 수 있습니다. HTML 콘텐츠 필터 상속을 방지하려면 키워드와 함께 **html-content-filter none** 명령을 입력합니다. HTML 필터링은 기본적으로 비활성화되어 있습니다.

명령을 한 번 더 사용하면 이전 설정이 재정의됩니다.

```
hostname(config-username-webvpn)# html-content-filter {java | images | scripts |
 cookies | none}

hostname(config-username-webvpn)# no html-content-filter [java | images | scripts
 | cookies | none]
```

이 명령에서 사용되는 키워드는 다음과 같습니다.

- **cookies**—이미지에서 쿠키를 제거하여 제한된 광고 필터링 및 개인정보 보호를 제공합니다.
- **images**—이미지 참조를 제거합니다(<IMG> 태그 제거).
- **java**—Java 및 ActiveX 참조를 제거합니다(<EMBED>, <APPLET> 및 <OBJECT> 태그 제거).
- **none**—필터가 없음을 나타냅니다. null 값을 설정하므로 필터링을 허용하지 않습니다. 필터 값 상속을 방지합니다.
- **scripts**- 스크립팅 참조를 제거합니다(다음을 제거: <SCRIPT> tags).

다음 예는 이름이 anyuser인 사용자에 대해 JAVA, ActiveX, 쿠키 및 이미지 필터링을 설정하는 방법을 보여줍니다.

```
hostname(config)# username anyuser attributes
hostname(config-username)# webvpn
hostname(config-username-webvpn)# html-content-filter java cookies images
hostname(config-username-webvpn)#
```

사용자 홈 페이지 지정

이 사용자가 클라이언트리스 SSL VPN 세션에 로그인할 때 표시되는 웹 페이지에 대해 URL을 지정하려면 사용자 이름 webvpn 구성 모드에서 **homepage** 명령을 입력합니다. **homepage none** 명령을 발행하여 생성한 null 값을 포함하는 구성된 홈 페이지를 제거하려면 **no** 형식의 이 명령을 입력합니다. **no** 옵션을 사용하면 그룹 정책에서 값을 상속받을 수 있습니다. 홈 페이지 상속을 방지하려면 **homepage none** 명령을 입력합니다.

none 키워드는 클라이언트리스 SSL VPN 홈 페이지가 없음을 나타냅니다. 이 키워드는 null 값을 설정하므로 홈 페이지를 허용하지 않고 홈 페이지 상속을 방지합니다.

url-string 변수는 **value** 키워드 다음에 오며 홈 페이지의 URL을 제공합니다. 문자열은 http:// 또는 https://로 시작해야 합니다.

기본 홈 페이지는 없습니다.

```
hostname(config-username-webvpn)# homepage {value url-string | none}
hostname(config-username-webvpn)# no homepage
hostname(config-username-webvpn)#
```

다음 예는 이름이 anyuser인 사용자에 대해 홈 페이지로 www.example.com을 지정하는 방법을 보여줍니다.

```
hostname(config)# username anyuser attributes
```

```
hostname(config-username)# webvpn
hostname(config-username-webvpn)# homepage value www.example.com
hostname(config-username-webvpn)#
```

거부 메시지 지정

다음과 같이 사용자 이름 webvpn 구성 모드에서 **deny-message** 명령을 입력하여, 클라이언트리스 SSL VPN 세션에 성공적으로 로그인하지만 VPN 권한이 없는 원격 사용자에게 제공되는 메시지를 지정할 수 있습니다.

```
hostname(config-username-webvpn)# deny-message value "message"
hostname(config-username-webvpn)# no deny-message value "message"
hostname(config-username-webvpn)# deny-message none
```

no deny-message value 명령은 원격 사용자가 메시지를 수신하지 않도록 메시지 문자열을 제거합니다.

no deny-message none 명령은 연결 프로파일 정책 구성에서 특성을 제거합니다. 이 정책은 특성 값을 상속받습니다.

메시지는 최대 491자의 영숫자 문자로, 특수 문자, 공백, 구두점을 포함하나 인용 따옴표는 수에 포함하지 않습니다. 텍스트는 로그인 시 원격 사용자의 브라우저에 나타납니다. **deny-message value** 명령에 문자열을 입력하는 경우 명령이 래핑되더라도 계속 입력하십시오.

기본 거부 메시지는 다음과 같습니다. "로그인에 성공했지만 특정 기준이 충족되지 않았거나 일부 특정한 그룹 정책으로 인해 VPN 기능을 사용할 권한이 없습니다. 자세한 내용은 IT 관리자에게 문의하십시오."

다음 예에서 첫 번째 명령은 사용자 이름 모드를 시작하며 이름이 anyuser인 사용자에 대해 특성을 구성합니다. 후속 명령은 사용자 이름 webvpn 구성 모드를 시작하며 이 사용자와 연계된 거부 메시지를 수정합니다.

```
hostname(config)# username anyuser attributes
hostname(config-username)# webvpn
hostname(config-username-webvpn)# deny-message value "Your login credentials are OK. However,
 you have not been granted rights to use the VPN features. Contact your administrator for
more information."
hostname(config-username-webvpn)
```

클라이언트리스 **SSL VPN** 세션에 대한 **ACL** 지정

이 사용자에 대한 클라이언트리스 SSL VPN 세션에 사용할 ACL 이름을 지정하려면 사용자 이름 webvpn 구성 모드에서 **filter** 명령을 입력합니다. **filter none** 명령을 발행하여 생성한 null 값을 포함하는 ACL을 제거하려면 **no** 형식의 이 명령을 입력합니다. **no** 옵션을 사용하면 그룹 정책에서 값을 상속받을 수 있습니다. 필터 값 상속을 방지하려면 **filter value none** 명령을 입력합니다.

클라이언트리스 SSL VPN ACL은 이를 지정하기 위해 **filter** 명령을 입력할 때까지 적용되지 않습니다.

이 사용자에 대한 다양한 유형의 트래픽을 허용하거나 거부하도록 ACL을 구성합니다. 그런 다음 **filter** 명령을 입력하여 클라이언트리스 SSL VPN 트래픽에 대한 ACL을 적용합니다.

```
hostname(config-username-webvpn)# filter {value ACLname | none}
hostname(config-username-webvpn)# no filter
hostname(config-username-webvpn)#
```

none 키워드는 **webvpntype** ACL이 없음을 나타냅니다. 이 키워드는 null 값을 설정하므로 ACL을 허용하지 않고 다른 그룹 정책에서의 ACL 상속을 방지합니다.

value 키워드 다음에 오는 *ACLname* 문자열은 이전에 구성한 ACL의 이름을 제공합니다.

참고 클라이언트리스 SSL VPN은 **vpn-filter** 명령에 정의된 ACL을 사용하지 않습니다.

다음 예는 이름이 anyuser인 사용자 대해 acl_in이라는 ACL을 호출하는 필터를 설정하는 방법을 보여줍니다.

```
hostname(config)# username anyuser attributes
hostname(config-username)# webvpn
hostname(config-username-webvpn)# filter acl_in
hostname(config-username-webvpn)#
```

URL 목록 적용

클라이언트리스 SSL VPN 세션을 설정한 사용자의 홈 페이지에 나타나는 URL 목록을 지정할 수 있습니다. 먼저 전역 구성 모드에서 **url-list** 명령을 입력하여 하나 이상의 이름이 지정된 목록을 생성해야 합니다. 클라이언트리스 SSL VPN의 특정 사용자에게 서버 및 URL 목록을 적용하려면 사용자 이름 webvpn 구성 모드에서 **url-list** 명령을 입력합니다.

url-list none command**,** 를 사용하여 생성한 null 값을 포함하는 목록을 제거하려면 **no** 형식의 이 명령을 사용합니다. **no** 옵션을 사용하면 그룹 정책에서 값을 상속받을 수 있습니다. URL 목록 상속을 방지하려면 **url-list none** 명령을 입력합니다.

```
hostname(config-username-webvpn)# url-list {listname displayname url | none}
hostname(config-username-webvpn)# no url-list
```

이 명령에서 사용되는 키워드 및 변수는 다음과 같습니다.

- *displayname* — URL의 이름을 지정합니다. 이 이름은 클라이언트리스 SSL VPN 세션에서 포털 페이지에 나타납니다.
- listname — URL을 그룹화하는 데 사용되는 이름을 식별합니다.
- **none**— URL 목록이 없음을 나타냅니다. null 값을 설정하므로 URL 목록을 허용하지 않습니다. URL 목록 값의 상속을 방지합니다.
- *url* — 클라이언트리스 SSL VPN 사용자가 액세스 할 수 있는 URL을 지정합니다.

기본 URL 목록은 없습니다.

명령을 한 번 더 사용하면 이전 설정이 재정의됩니다.

다음 예는 이름이 anyuser인 사용자에 대해 AnyuserURL이라는 URL 목록을 설정하는 방법을 보여줍니다.

```
hostname(config)# username anyuser attributes
hostname(config-username)# webvpn
hostname(config-username-webvpn)# url-list value AnyuserURLs
hostname(config-username-webvpn)#
```

사용자에 대한 **ActiveX Relay** 활성화

ActiveX Relay를 통해 클라이언트리스 SSL VPN 세션을 설정한 사용자는 브라우저를 사용하여 Microsoft Office 애플리케이션을 시작할 수 있습니다. 이 애플리케이션은 이 세션을 사용하여 Microsoft Office 문서를 다운로드 및 업로드합니다. ActiveX Relay는 클라이언트리스 SSL VPN 세션이 종료될 때까지 그대로 실행됩니다.

클라이언트리스 SSL VPN 세션에서 ActiveX 컨트롤을 활성화하거나 비활성화하려면 사용자 이름 webvpn 구성 모드에서 다음 명령을 입력합니다.

activex-relay {**enable** | **disable**}

그룹 정책에서 **activex-relay** 명령을 상속받으려면 다음 명령을 입력합니다.

no activex-relay

다음 명령은 지정된 사용자 이름과 연계된 클라이언트리스 SSL VPN 세션에서 ActiveX 컨트롤을 활성화합니다.

```
hostname(config-username-policy)# webvpn
hostname(config-username-webvpn)# activex-relay enable
hostname(config-username-webvpn)
```

클라이언트리스 **SSL VPN** 세션에 대한 애플리케이션 액세스 활성화

이 사용자에 대한 애플리케이션 액세스를 활성화하려면 사용자 이름 webvpn 구성 모드에서 **port-forward** 명령을 입력합니다. 포트 전달은 기본적으로 비활성화되어 있습니다.

port-forward none 명령을 발행하여 생성한 null 값을 포함하여 구성에서 포트 전달 속성을 제거하려면 **no** 형식의 이 명령을 입력합니다. **no** 옵션을 사용하면 그룹 정책에서 목록을 상속받을 수 있습니다. 필터링을 허용하지 않고 포트 전달 목록의 상속을 방지하려면 **none** 키워드와 함께 **port-forward** 명령을 입력합니다.

```
hostname(config-username-webvpn)# port-forward {value listname | none}
hostname(config-username-webvpn)# no port-forward
hostname(config-username-webvpn)#
```

value 키워드 다음에 오는 *listname* 문자열은 클라이언트리스 SSL VPN의 사용자가 액세스할 수 있는 애플리케이션 목록을 식별합니다. 이 목록을 정의하려면 구성 모드에서 **port-forward** 명령을 입력합니다.

명령을 한 번 더 사용하면 이전 설정이 재정의됩니다.

애플리케이션 액세스를 활성화하기 위해 사용자 이름 webvpn 구성 모드에서 **port-forward** 명령을 입력하기 전에, 사용자가 클라이언트리스 SSL VPN 세션에서 사용할 수 있는 애플리케이션 목록을 정의해야 합니다. 이 목록을 정의하려면 전역 구성 모드에서 **port-forward** 명령을 입력합니다.

다음 예는 ports1이라는 포트 전달 목록을 구성하는 방법을 보여줍니다.

```
hostname(config-group-policy)# webvpn
hostname(config-username-webvpn)# port-forward value ports1
hostname(config-username-webvpn)#
```

포트 전달 표시 이름 구성

사용자 이름 webvpn 구성 모드에서 **port-forward-name** 명령을 사용하여 특정 사용자에 대해 엔드 유저로의 TCP 포트 전달을 식별하는 표시 이름을 구성합니다. **port-forward-name none** 명령**,** 을 사용하여 생성한 null 값을 포함하는 표시 이름을 삭제하려면 **no** 형식의 명령을 입력합니다. **no** 옵션은 기본 이름인 애플리케이션 액세스를 복원합니다. 표시 이름을 방지하려면 **port-forward none** 명령을 입력합니다.

```
hostname(config-username-webvpn)# port-forward-name {value name | none}
hostname(config-username-webvpn)# no port-forward-name
```

다음 예는 포트 전달 이름 테스트를 구성하는 방법을 보여줍니다.

```
hostname(config-group-policy)# webvpn
hostname(config-username-webvpn)# port-forward-name value test
hostname(config-username-webvpn)#
```

세션 타이머 업데이트를 무시하도록 최대 개체 크기 구성

네트워크 디바이스는 네트워크 디바이스 간에 가상 회로가 계속 활성 상태인지 확인하기 위해 짧은 킵얼라이브 메시지를 교환합니다. 이 메시지의 길이는 서로 다를 수 있습니다. **keep-alive-ignore** 명령을 사용하면 세션 타이머를 업데이트할 때 지정된 크기보다 작거나 같은 모든 메시지를 트래픽이 아니라 킵얼라이브 메시지로 간주하도록 ASA에 알려줄 수 있습니다. 범위는 0부터 900KB까지입니다. 기본값은 4KB입니다.

트랜잭션당 HTTP/HTTPS 트래픽의 상한을 지정하고 이를 무시하려면 다음과 같이 그룹 정책 속성 webvpn 구성 모드에서 **keep-alive-ignore** 명령을 사용합니다.

```
hostname(config-group-webvpn)# keep-alive-ignore size
hostname(config-group-webvpn)#
```

no 형식의 다음 명령은 구성에서 이 사양을 제거합니다.

```
hostname(config-group-webvpn)# no keep-alive-ignore
hostname(config-group-webvpn)#
```

다음은 무시하려는 개체의 최대 크기를 5KB로 설정하는 예입니다.

```
hostname(config-group-webvpn)# keep-alive-ignore 5
hostname(config-group-webvpn)#
```

자동 로그온 구성

클라이언트리스 SSL VPN의 특정 사용자의 로그인 자격 증명을 NTLM, 기본 HTTP 인증 또는 두 가지 모두를 사용하는 내부 서버에 자동으로 전송하려면 사용자 이름 webvpn 구성 모드에서 **auto-signon** 명령을 사용합니다.

auto-signon 명령은 클라이언트리스 SSL VPN 세션의 사용자를 위한 SSO(Single Sign-On) 방법입니다. 이 명령은 로그인 자격 증명(사용자 이름 및 비밀번호)을 NTLM 인증, 기본 인증 또는 두 가지 모두를 사용하는 인증을 위해 내부 서버에 전달합니다. 여러 auto-signon 명령을 입력할 수 있으며, 이는 입력 순서에 따라 처리됩니다. 즉 먼저 입력된 명령이 우선합니다.

auto-signon 기능은 webvpn 구성, webvpn 그룹 구성 또는 webvpn 사용자 이름 구성 모드의 세 가지 모드로 사용할 수 있습니다. 일반적인 우선순위 동작은 사용자 이름이 그룹을 교체하고, 그룹이 전역을 교체하는 경우 적용됩니다. 선택한 모드는 인증의 적절한 범위에 따라 다릅니다.

특정 사용자를 위한 auto-signon을 특정 서버에 대해 비활성화하려면 IP 블록 또는 URI의 원래 사양에 대해 **no** 형식의 명령을 사용합니다. 모든 서버에 대한 인증을 비활성화하려면 인수 없이 **no** 형식을 사용합니다. **no** 옵션을 사용하면 그룹 정책에서 값을 상속받을 수 있습니다.

다음 예에서 명령은 기본 인증 또는 NTLM 인증을 사용하여 클라이언트리스 SSL VPN의 이름이 anyuser인 사용자를 위한 auto-signon을 URI 마스크 https://*.example.com/*를 사용하여 정의한 서버에 구성합니다.

```
hostname(config)# username anyuser attributes
hostname(config-username)# webvpn
hostname(config-username-webvpn)# auto-signon allow uri https://*.example.com/*
 auth-type all
```

다음 예에서 명령은 기본 인증 또는 NTLM 인증을 사용하여 클라이언트리스 SSL VPN의 이름이 anyuser인 사용자를 위한 auto-signon을 서브넷 마스크 255.255.255.0을 사용하는 IP 주소 10.1.1.0인 서버에 구성합니다.

```
hostname(config)# username anyuser attributes
hostname(config-username)# webvpn
hostname(config-username-webvpn)# auto-signon allow ip 10.1.1.0 255.255.255.0
auth-type all
hostname(config-username-webvpn)#
```

HTTP 압축 지정

사용자 이름 webvpn 구성 모드에서 http-comp 명령을 입력하여 특정 사용자에 대해 클라이언트리스 SSL VPN 세션을 통한 http 데이터 압축을 활성화합니다.

```
hostname(config-username-webvpn)# http-comp {gzip | none}
hostname(config-username-webvpn)#
```

구성에서 명령을 제거하고 값을 상속받도록 하려면 **no** 형식의 다음 명령을 사용합니다.

```
hostname(config-username-webvpn)# no http-comp {gzip | none}
hostname(config-username-webvpn)#
```

이 명령의 구문은 다음과 같습니다.

- **gzip**—그룹 또는 사용자에 대해 압축을 활성화하도록 지정합니다. 이는 기본값입니다.
- **none**—그룹 또는 사용자에 대해 압축을 비활성화하도록 지정합니다.

클라이언트리스 SSL VPN 세션의 경우, 전역 구성 모드에서 구성한 **compression** 명령이 그룹 정책 및 사용자 이름 webvpn 모드에서 구성한 **http-comp** 명령을 재정의합니다.

다음은 사용자 이름인 testuser에 대해 압축을 비활성화하는 예입니다.

```
hostname(config)# username testuser internal
hostname(config)# username testuser attributes
hostname(config-username)# webvpn
hostname(config-username-webvpn)# http-comp none
hostname(config-username-webvpn)#
```

스마트 터널 액세스

다음 섹션에서는 클라이언트리스 SSL VPN 세션에서 스마트 터널 액세스를 활성화하는 방법에 대해 설명하며 해당 액세스를 통해 제공되는 애플리케이션을 지정하고 애플리케이션 사용에 대한 참고사항을 제공합니다.

스마트 터널 액세스를 구성하려면 스마트 터널 액세스에 사용할 수 있는 하나 이상의 애플리케이션을 포함하는 스마트 터널 목록과 이 목록에 연계된 엔드포인트 운영 체제를 생성합니다. 각 그룹 정책 또는 로컬 사용자 정책은 하나의 스마트 터널 목록을 지원하므로 지원할 비 브라우저 기반 애플리케이션을 스마트 터널 목록으로 그룹화해야 합니다. 목록을 생성한 후 하나 이상의 그룹 정책 또는 로컬 사용자 정책에 목록을 할당합니다.

다음 섹션에서는 스마트 터널 및 이를 구성하는 방법에 대해 설명합니다.

- 스마트 터널 정보, 375 페이지
- 스마트 터널에 대한 사전 요구 사항, 375 페이지
- 스마트 터널에 대한 지침, 376 페이지
- 스마트 터널 액세스에 사용할 수 있도록 애플리케이션 추가, 378 페이지
- 스마트 터널 목록 정보, 378 페이지
- 스마트 터널 정책 구성 및 적용, 379 페이지
- 스마트 터널의 터널 정책 구성 및 적용, 379 페이지
- 스마트 터널 자동 로그온 서버 목록 생성, 381 페이지
- 스마트 터널 자동 로그온 서버 목록에 서버 추가, 382 페이지

- 스마트 터널 액세스 자동화, 384 페이지
- 스마트 터널 액세스 활성화 및 해제, 385 페이지
- 스마트 터널 로그오프 구성, 385 페이지

스마트 터널 정보

스마트 터널은 클라이언트리스(브라우저 기반) SSL VPN 세션(보안 어플라이언스를 경로로, ASA를 프록시 서버로 사용)을 사용하는 TCP 기반 애플리케이션과 개인 사이트 간의 연결입니다. 스마트 터널 액세스 권한을 부여할 애플리케이션을 식별하고 각 애플리케이션에 대한 로컬 경로를 지정할 수 있습니다. Microsoft Windows에서 실행 중인 애플리케이션의 경우 스마트 터널 액세스 부여를 위한 조건으로 체크섬의 SHA-1 해시 일치를 요청할 수 있습니다.

Lotus SameTime 및 Microsoft Outlook은 스마트 터널 액세스 권한을 부여할 애플리케이션의 예입니다.

애플리케이션이 클라이언트 또는 웹 지원 애플리케이션인지에 따라 스마트 터널에서 다음 절차 중 하나를 수행하도록 구성합니다.

- 클라이언트 애플리케이션의 스마트 터널 목록을 하나 이상 생성한 다음 이 목록을 스마트 터널 액세스가 필요한 그룹 정책 또는 로컬 사용자 정책에 할당합니다.
- 스마트 터널 액세스에 사용할 수 있는 웹 지원 애플리케이션의 URL을 지정하는 책갈피 목록 항목을 하나 이상 생성한 다음 이 목록을 스마트 터널 액세스가 필요한 그룹 정책 또는 로컬 사용자 정책에 할당합니다.

또한 클라이언트리스 SSL VPN 세션을 통한 스마트 터널 연결에서 로그인 자격 증명 제출을 자동화하도록 웹 지원 애플리케이션을 나열할 수 있습니다.

스마트 터널의 혜택

스마트 터널 액세스를 통해 클라이언트 TCP 기반 애플리케이션에서 브라우저 기반 VPN 연결을 사용하여 서비스에 액세스할 수 있습니다. 이는 플러그인 및 레거시 기술인 포트 전달과 비교하여 사용자에게 다음과 같은 이점을 제공합니다.

- 스마트 터널은 플러그인보다 우수한 성능을 제공합니다.
- 포트 전달과 달리 스마트 터널을 사용할 경우 로컬 애플리케이션을 로컬 포트에 연결할 필요가 없으므로 사용자 환경이 간소화됩니다.
- 또한 포트 전달과 달리 스마트 터널은 사용자의 관리자 권한이 필요하지 않습니다.

플러그인의 장점은 클라이언트 애플리케이션을 원격 컴퓨터에 설치할 필요가 없다는 점입니다.

스마트 터널에 대한 사전 요구 사항

스마트 터널에서 지원하는 플랫폼 및 브라우저에 대해서는 지원되는 VPN 플랫폼, Cisco ASA 5500 Series의 내용을 참조하십시오.

다음 요건 및 제한 사항은 Windows에서의 스마트 터널 액세스에 적용됩니다.

- Windows의 ActiveX 또는 Oracle JRE(Java Runtime Environment)(JRE 6 이상이 권장됨)를 브라우저에서 활성화해야 합니다.

  ActiveX 페이지에서 연계된 그룹 정책에 **activex-relay** 명령을 입력해야 합니다. 이 명령을 입력하거나 스마트 터널 목록을 정책에 할당하고 엔드포인트에 있는 브라우저 프록시 예외 목록에서 프록시를 지정하는 경우, 사용자는 "shutdown.webvpn.relay." 항목을 이 목록에 추가해야 합니다.

- Winsock 2에서만 TCP 기반 애플리케이션을 스마트 터널 액세스에 사용할 수 있습니다.
- Mac OS X의 경우에만 Java Web Start를 브라우저에서 활성화해야 합니다.

스마트 터널에 대한 지침

- 스마트 터널은 Microsoft Windows 및 보안 어플라이언스를 실행하는 컴퓨터 사이에 위치한 프록시만 지원합니다. 스마트 터널은 Windows에서 전체 시스템에 적용되는 매개변수를 설정하는 Internet Explorer 구성을 사용합니다. 이 구성에는 프록시 정보가 포함될 수 있습니다.
  - Windows 컴퓨터에서 ASA에 액세스하는 데 프록시가 필요한 경우 클라이언트의 브라우저에 정적 프록시 항목이 있어야 하며 연결할 호스트가 클라이언트의 프록시 예외 목록에 있어야 합니다.
  - Windows 컴퓨터에서 ASA에 액세스하는 데 프록시가 필요하지 않지만 호스트 애플리케이션에 액세스하는 데 프록시가 필요한 경우, ASA가 클라이언트의 프록시 예외 목록에 있어야 합니다.

  프록시 시스템은 정적 프록시 항목의 클라이언트 구성 또는 자동 구성으로 정의되거나 PAC 파일별로 정의될 수 있습니다. 정적 프록시 구성만 스마트 터널에서 현재 지원됩니다.

- KCD(Kerberos Constrained Delegation: Kerberos 제한 위임)는 스마트 터널에 대해 지원되지 않습니다.
- Windows의 경우 명령 확인 상자에서 시작한 애플리케이션에 스마트 터널 액세스를 추가하려면 "cmd.exe"가 애플리케이션의 상위이므로 스마트 터널 목록의 단일 항목인 프로세스 이름에서 "cmd.exe"를 지정하고 다른 항목에서 애플리케이션 자체에 대한 경로를 지정해야 합니다.
- HTTP 기반 원격 액세스를 통해 일부 서브넷은 VPN 게이트웨이에 대한 사용자 액세스를 차단할 수 있습니다. 이 문제를 해결하려면 웹 및 엔드 유저 간에 트래픽을 라우팅하도록 ASA 앞에 프록시를 배치합니다. 이 프록시는 연결 방법을 지원해야 합니다. 인증이 필요한 프록시의 경우 스마트 터널은 기본 다이제스트 인증 유형만 지원합니다.
- 스마트 터널을 시작할 때 브라우저 프로세스가 동일한 경우 ASA는 기본적으로 VPN 세션을 통해 모든 브라우저 트래픽을 전달합니다. ASA는 또한 tunnel-all 정책(기본값)이 적용되는 경우 이 작업만 수행합니다. 사용자가 브라우저 프로세스의 또 다른 인스턴스를 시작하는 경우 VPN 세션을 통해 모든 트래픽을 전달합니다. 브라우저 프로세스가 동일하며 보안 어플라이언스가 URL에 대한 액세스를 제공하지 않는 경우, 사용자는 브라우저를 열 수 없습니다. 해결책으로 tunnel-all이 아닌 터널 정책을 할당합니다.

- 상태 저장 대체작동은 스마트 터널 연결을 유지하지 않습니다. 사용자는 장애 조치 후 다시 연결해야 합니다.
- 스마트 터널의 Mac 버전은 POST 책갈피, 양식 기반 자동 로그온 또는 POST 매크로 대체를 지원하지 않습니다.
- Mac OS X 사용자의 경우 포털 페이지에서 시작된 애플리케이션만 스마트 터널 연결을 설정할 수 있습니다. 이 필요 조건은 Firefox에 대한 스마트 터널 지원에도 적용됩니다. 스마트 터널을 처음 사용하는 동안 Firefox를 사용하여 Firefox의 또 다른 인스턴스를 시작하려면 csco_st라는 사용자 프로파일이 필요합니다. 이 사용자 프로파일이 없는 경우 새로 만들라는 메시지가 표시됩니다.
- Mac OS X에서 SSL 라이브러리에 동적으로 연결된 TCP를 사용하는 애플리케이션은 스마트 터널에서 작업을 수행할 수 있습니다.
- 스마트 터널은 Mac OS X에서 다음을 지원하지 않습니다.
  - 프록시 서비스
  - 자동 로그온
  - 2단계 네임 스페이스를 사용하는 애플리케이션
  - 텔넷, SSH 및 cURL 같은 콘솔 기반 애플리케이션
  - dlopen 또는 dlsym을 사용하여 libsocket 호출을 찾는 애플리케이션
  - libsocket 호출을 찾기 위해 정적으로 연결된 애플리케이션
- Mac OS X는 프로세스에 대한 전체 경로를 필요로 하며 대/소문자를 구분합니다. 각 사용자 이름에 대해 경로를 지정하는 것을 방지하려면 물결표(~)를 부분 경로 앞에 삽입합니다(예: ~/bin/vnc).
- Mac 및 Windows 디바이스의 Chrome 브라우저에서 스마트 터널을 지원하기 위한 새로운 방법이 제공되었습니다. Chrome 스마트 터널 확장자가 Chrome에서 더 이상 지원되지 않는 Netscape 플러그인 애플리케이션 프로그램 인터페이스(NPAPIs)를 대체했습니다.

  Chrome에서 이미 설치되어 있는 확장자가 없이 스마트 터널 활성화 책갈피를 클릭한 경우, 확장자를 얻도록 Chrome 웹 저장소로 리디렉션됩니다. 새 Chrome 설치 시 사용자는 확장자를 다운로드하도록 Chrome 웹 저장소로 안내를 받습니다. 확장자는 스마트 터널을 실행하는 데 필요한 ASA에서 이진 파일을 다운로드합니다.

  Chrome의 기본 다운로드 위치는 현재 사용자의 다운로드 폴더를 가리켜야 합니다. 또는 Chrome의 다운로드 설정이 '매번 묻기'인 경우, 사용자는 질문을 받을 때 다운로드 폴더를 선택해야 합니다.

  스마트 터널을 사용하는 동안 일반적인 책갈피 및 애플리케이션 구성은 새 확장자를 설치하고 다운로드 위치를 지정하는 프로세스 이외에는 변경되지 않습니다.

스마트 터널 액세스에 사용할 수 있도록 애플리케이션 추가

각 ASA의 클라이언트리스 SSL VPN 구성은 스마트 터널 목록을 지원하며 각각은 스마트 터널 액세스에 사용할 수 있는 하나 이상의 애플리케이션을 식별합니다. 각 그룹 정책 또는 사용자 이름은 하나의 스마트 터널 목록만 지원하므로 지원할 애플리케이션의 각 집합을 스마트 터널 목록으로 그룹화해야 합니다.

스마트 터널 목록 정보

각 그룹 정책 및 사용자 이름에 대해 다음 중 하나를 수행하도록 클라이언트리스 SSL VPN을 구성할 수 있습니다.

- 사용자 로그인 시 자동으로 스마트 터널 액세스를 시작합니다.
- 사용자 로그인 시 스마트 터널 액세스를 활성화하지만 사용자가 클라이언트리스 SSL VPN 포털 페이지에서 **Application Access** > **Start Smart Tunnels** 버튼을 사용하여 수동으로 시작해야 합니다.

참고 스마트 터널 로그온 옵션은 각 그룹 정책 및 사용자 이름에 대해 상호 배타적입니다. 한 가지만 사용하십시오.

다음 스마트 터널 명령은 각 그룹 정책 및 사용자 이름에 사용할 수 있습니다. 각 그룹 정책 및 사용자 이름 구성에서는 이러한 명령을 한 번에 하나씩만 지원하므로 한 가지 명령을 입력하면 ASA에서 해당 그룹 정책 또는 사용자 이름의 구성에 있는 기존 명령을 새 명령으로 교체하거나 마지막 명령인 경우 정책 그룹 또는 사용자 이름에 이미 있는 smart-tunnel 명령을 제거합니다.

- **smart-tunnel auto-start** *list*

  사용자 로그인 시 자동으로 스마트 터널 액세스를 시작합니다.

- **smart-tunnel enable***list*

  사용자 로그인 시 스마트 터널 액세스를 활성화하지만 사용자가 클라이언트리스 SSL VPN 포털 페이지에서 **Application Access** > **Start Smart Tunnels** 버튼을 사용하여 스마트 터널 액세스를 수동으로 시작해야 합니다.

- **smart-tunnel disable**

  스마트 터널 액세스를 방지합니다.

- **no smart-tunnel [auto-start list | enable list | disable]**

  그룹 정책 또는 사용자 이름 구성에서 **smart-tunnel** 명령을 제거한 다음 기본 그룹 정책에서 [**no**] **smart-tunnel** 명령을 상속받습니다. **no smart-tunnel** 명령 뒤에 오는 키워드는 선택 사항이지만 이름이 지정된 smart-tunnel 명령의 제거를 제한합니다.

스마트 터널 정책 구성 및 적용

스마트 터널 정책은 그룹 정책/사용자 이름 구성마다 필요합니다. 각 그룹 정책/사용자 이름은 네트워크의 전역으로 구성된 목록을 참조합니다. 스마트 터널이 켜져 있는 경우, 다음 2개의 CLI를 사용하여 터널 외부에서 트래픽을 허용할 수 있습니다. 하나는 네트워크(호스트 집합)를 구성하고 다른 하나는 사용자에게 정책을 적용하는 지정된 스마트 터널 네트워크를 사용합니다. 다음 명령은 스마트 터널 정책 구성에 사용할 호스트 목록을 생성합니다.

프로시저

단계 **1** 클라이언트리스 SSL VPN 구성 모드로 전환합니다.

webvpn

단계 **2** 스마트 터널 정책 구성에 사용할 호스트 목록을 생성합니다.

[no] smart-tunnel network *network name* **ip** *ip netmask*

- *network name*은 터널 정책에 적용할 이름입니다.
- *ip*는 네트워크의 IP 주소입니다.
- *netmask*는 네트워크의 넷마스크입니다.

단계 **3** *.cisco.com 등의 호스트 이름 마스크를 설정합니다.

[no] smart-tunnel network *network name* **host** *host mask*

단계 **4** 특정 사용자 또는 그룹 정책에 스마트 터널 정책을 적용합니다.

[no] smart-tunnel tunnel-policy [{excludespecified | tunnelspecified} *network name* **| tunnelall]**

- *network name*은 터널링할 네트워크 목록입니다.
- *tunnelall*은 모든 항목을 터널링(암호화됨)합니다.
- *tunnelspecified*는 네트워크 이름별로 지정한 네트워크만 터널링합니다.
- *excludespecified*는 네트워크 이름별로 지정한 네트워크 외부에 있는 네트워크만 터널링합니다.

스마트 터널의 터널 정책 구성 및 적용

SSL VPN 클라이언트에서의 스플릿 터널 구성과 같이 스마트 터널 정책은 그룹 정책/사용자 이름 구성마다 다릅니다. 각 그룹 정책/사용자 이름은 네트워크의 전역으로 구성된 목록을 참조합니다.

프로시저

단계 **1** 네트워크의 전역으로 구성된 목록을 참조합니다.

[no]smart-tunnel tunnel-policy [{excludespecified | tunnelspecified} *network name* | *tunnelall]*

- *network name*은 터널링할 네트워크 목록입니다.
- **tunnelall**은 모든 항목을 터널링(암호화됨)합니다.
- **tunnelspecified**는 네트워크 이름별로 지정한 네트워크만 터널링합니다.
- **excludespecified**는 네트워크 이름별로 지정한 네트워크 외부에 있는 네트워크만 터널링합니다.

단계 **2** 그룹 정책/사용자 정책에 터널 정책을 적용합니다.

[no] smart-tunnel network *network name* **ip** *ip netmask*

또는

[no] smart-tunnel network *network name* **host** *host mask*

한 가지 명령은 호스트를 지정하고 나머지 명령은 네트워크 IP를 지정합니다. 한 가지만 사용하십시오.

- *network name*은 터널 정책에 적용할 네트워크 이름을 지정합니다.
- *ip*는 네트워크의 IP 주소를 지정합니다.
- *netmask*는 네트워크의 넷마스크를 지정합니다.
- *host mask*는 호스트 이름 마스크를 지정합니다(예: *.cisco.com).

예제**:**

예:

인벤토리 페이지가 www.example.com(10.5.2.2)에서 호스팅된다고 가정하고 호스트의 IP 주소 및 이름을 모두 구성하려는 경우, 하나의 호스트만 포함하는 터널 정책을 생성합니다.

```
ciscoasa(config-webvpn)# smart-tunnel network inventory ip 10.5.2.2
or
ciscoasa(config-webvpn)# smart-tunnel network inventory host www.example.com
```

단계 **3** 파트너의 그룹 정책에 터널이 지정된 터널 정책을 적용합니다.

ciscoasa(config-group-webvpn)# **smart-tunnel tunnel-policy tunnelspecified inventory**

단계 **4** (선택 사항) 그룹 정책 홈 페이지를 지정하고 스마트 터널을 홈 페이지에서 활성화합니다.

예제**:**

예:

```
ciscoasa(config-group-webvpn)# homepage value http://www.example.com
ciscoasa(config-group-webvpn)# homepage use-smart-tunnel
ciscoasa(config-webvpn)# smart-tunnel notification-icon
```

참고 스크립트를 쓰거나 아무 것도 업로드하지 않고 관리자는 스마트 터널을 통해 연결할 홈 페이지를 지정할 수 있습니다.

스마트 터널 정책 구성은 공급업체가 클라이언트리스 포털을 통해 먼저 이동하지 않고 로그인 시 내부 인벤토리 서버 페이지에 대한 클라이언트리스 액세스를 파트너에게 제공하려는 경우 선택하는 것이 좋습니다.

기본적으로 스마트 터널이 활성화된 브라우저에서 시작된 모든 프로세스가 터널에 액세스 가능하기 때문에 스마트 터널 애플리케이션 구성이 필요하지 않습니다. 단, 포털이 표시되지 않으므로 로그아웃 알림 아이콘을 활성화할 수 있습니다.

스마트 터널 자동 로그온 서버 목록 생성

프로시저

단계 **1** 클라이언트리스 SSL VPN 구성 모드로 전환합니다.

webvpn

단계 **2** 서버 목록에 추가할 각 서버에 사용합니다.

smart-tunnel auto-sign-on *list* [**use-domain**] [**realm** *realm-string*] [**port** *port-num*]{ **ip** *ip-address* [*netmask*] | **host** *hostname-mask*}

- *list* - 원격 서버의 목록 이름입니다. 공백을 포함한 경우 이름 주변에 따옴표를 사용합니다. 문자열은 최대 64자까지 허용됩니다. ASA는 구성에 목록이 아직 없는 경우 목록을 생성합니다. 구성에 목록이 있으면 목록에 항목을 추가합니다. 구별하기 쉬운 이름을 할당합니다.
- use-domain(선택 사항) — 인증에 필요한 경우, Windows 도메인을 사용자 이름에 추가합니다. 이 키워드를 입력하면 스마트 터널 목록을 하나 이상의 그룹 정책 또는 사용자 이름에 할당할 때 도메인 이름이 지정됩니다.
- *realm* - 인증을 위한 영역을 구성합니다. 영역은 웹사이트의 보호 영역과 연계되며 인증 도중에 인증 확인 상자 또는 HTTP 헤더 중 하나에서 브라우저에 다시 전달됩니다. 자동 로그온이 구성되고 영역 문자열이 지정되면 사용자는 웹 애플리케이션(Outlook Web Access 등)에 영역 문자열을 구성하며 로그온하지 않고 웹 애플리케이션에 액세스할 수 있습니다.
- *port* - 어떤 포트가 자동 로그인을 수행할지 지정합니다. Firefox의 경우 포트 번호를 지정하지 않으면 자동 로그온이 HTTP 및 HTTPS에서 수행되며 기본 포트 번호 80 및 443에서 각각 액세스됩니다.
- ip - IP 주소 및 넷마스크별로 서버를 지정합니다.
- *ip-address*[netmask] - 자동 인증할 호스트의 하위 네트워크를 식별합니다.
- host- 호스트 이름 또는 와일드카드 마스크별로 서버를 지정합니다. 이 옵션을 사용하면 IP 주소의 동적 변경으로부터 구성을 보호합니다.

- *Hostname-mask* - 어떤 호스트 이름 또는 와일드카드 마스크를 자동 인증할지 지정합니다.

단계 **3** (선택 사항) 서버 목록에서 항목을 제거하여 목록 및 IP 주소 또는 호스트 이름을 모두 ASA 구성에 나타나게 지정합니다.

no smart-tunnel auto-sign-on *list* [**use-domain**] [**realm** *realm-string*] [**port** *port-num*]{ **ip** *ip-address* [*netmask*] | **host** *hostname-mask*}

단계 **4** 스마트 터널 자동 로그인 목록 항목을 표시합니다.

show running config webvpn smart-tunnel

단계 **5** config-webvpn 구성 모드로 전환합니다.

config-webvpn

단계 **6** 인증에 필요한 경우, 서브넷의 모든 호스트를 추가하고 Windows 도메인을 사용자 이름에 추가합니다.

smart-tunnel auto-sign-on HR use-domain ip 93.184.216.119 255.255.255.0

단계 **7** (선택 사항) 제거된 항목이 목록에 있는 유일한 항목인 경우 해당 목록과 HR이라는 이름의 목록에서 항목을 제거합니다.

no smart-tunnel auto-sign-on HR use-domain ip 93.184.216.119 255.255.255.0

단계 **8** ASA 구성에서 전체 목록을 제거합니다.

no smart-tunnel auto-sign-on HR

단계 **9** 인트라넷이라는 이름의 스마트 터널 자동 로그온 목록에 도메인의 모든 호스트를 추가합니다.

smart-tunnel auto-sign-on intranet host *.example.com

단계 **10** 목록에서 항목을 제거합니다.

no smart-tunnel auto-sign-on intranet host *.example.com

참고 스마트 터널 자동 로그인 서버 목록을 구성한 후에 이 목록을 활성화하려면 그룹 정책 또는 로컬 사용자 정책에 할당해야 합니다. 자세한 내용은 스마트 터널 자동 로그온 서버 목록에 서버 추가, 382 페이지를 참조해 주십시오.

스마트 터널 자동 로그온 서버 목록에 서버 추가

다음 단계는 스마트 터널 연결에서 자동 로그온을 제공하고 해당 목록을 그룹 정책 또는 로컬 사용자에게 할당할 서버 목록에 서버를 추가하는 방법에 대해 설명합니다.

시작하기 전에

- **smart-tunnel auto-sign-on** 명령을 사용하여 서버 목록을 먼저 생성합니다. 그룹 정책 또는 사용자 이름에 하나의 목록만 할당할 수 있습니다.

참고 스마트 터널 자동 로그온 기능은 Internet Explorer 및 Firefox를 사용하여 HTTP 및 HTTPS와 통신하는 애플리케이션만 지원합니다.

- FireFox를 사용 중인 경우 와일드카드, IP 주소를 사용하는 서브넷 또는 넷마스크가 있는 호스트 마스크가 아닌 정확한 호스트 이름 또는 IP 주소를 사용하여 호스트를 지정해 주십시오. 예를 들어 Firefox에서 *.cisco.com을 입력하여 email.cisco.com을 호스팅하기 위한 자동 로그온이 불가능합니다.

프로시저

단계 **1** 클라이언트리스 SSL VPN 구성 모드로 전환합니다.

webvpn

단계 **2** group policy 클라이언트리스 SSL VPN 구성 모드로 전환합니다.

group-policy webvpn

단계 **3** username 클라이언트리스 SSL VPN 구성 모드로 전환합니다.

username webvpn

단계 **4** 스마트 터널 자동 로그온 클라이언트리스 SSL VPN 세션을 활성화합니다.

smart-tunnel auto-sign-on enable

단계 **5** (선택 사항) 스마트 터널 자동 로그온 클라이언트리스 SSL VPN 세션을 해제하여 그룹 정책 또는 사용자 이름에서 제거하고 기본값을 사용합니다.

[**no**] **smart-tunnel auto-sign-on enable** *list* [**domain** *domain*]

- *list* - ASA 클라이언트리스 SSL VPN 구성에 이미 있는 스마트 터널 자동 로그인 목록의 이름입니다.
- *domain(*선택 사항*)* - 인증 동안 사용자 이름에 추가할 도메인의 이름입니다. 도메인을 입력하는 경우 목록 항목에 **use-domain** 키워드를 입력합니다.

단계 **6** SSL VPN 구성의 스마트 터널 자동 로그인 목록 항목을 보여줍니다.

show running-config webvpn smart-tunnel

단계 **7** 이름이 HR인 스마트 터널 자동 로그인 목록을 활성화합니다.

smart-tunnel auto-sign-on enable HR

단계 **8** 인증 중에 이름이 HR인 스마트 터널 자동 로그온 목록을 활성화하고 이름이 CISCO인 도메인을 사용자 이름에 추가합니다.

smart-tunnel auto-sign-on enable HR domain CISCO

단계 **9** (선택 사항) 그룹 정책에서 이름이 HR인 스마트 터널 자동 로그온 목록을 제거하고 기본 그룹 정책에서 스마트 터널 자동 로그온 목록 명령을 상속받습니다.

no smart-tunnel auto-sign-on enable HR

스마트 터널 액세스 자동화

사용자 로그인 시 스마트 터널 액세스를 자동으로 시작하려면 다음 단계를 수행하십시오.

시작하기 전에

Mac OS X의 경우 자동 시작 구성 여부에 관계없이 포털의 애플리케이션 액세스 패널에서 애플리케이션에 대한 링크를 클릭합니다.

프로시저

단계 **1** 클라이언트리스 SSL VPN 구성 모드로 전환합니다.

webvpn

단계 **2** group policy 클라이언트리스 SSL VPN 구성 모드로 전환합니다.

group-policy webvpn

단계 **3** username 클라이언트리스 SSL VPN 구성 모드로 전환합니다.

username webvpn

단계 **4** 사용자 로그인 시 자동으로 스마트 터널 액세스를 시작합니다.

smart-tunnel auto-start *list*

*list*는 이미 있는 스마트 터널 목록의 이름입니다.

예제**:**

```
hostname(config-group-policy)# webvpn
hostname(config-group-webvpn)# smart-tunnel auto-start apps1
```

이름이 apps1인 스마트 터널 목록을 그룹 정책에 할당합니다.

단계 **5** SSL VPN 구성의 스마트 터널 목록 항목을 표시합니다.

show running-config webvpn smart-tunnel

단계 **6** 그룹 정책 또는 사용자 이름에서 smart-tunnel 명령을 제거하고 기본값으로 되돌립니다.

no smart-tunnel

스마트 터널 액세스 활성화 및 해제

기본적으로 스마트 터널은 해제되어 있습니다.

프로시저

단계 **1** 클라이언트리스 SSL VPN 구성 모드로 전환합니다.

webvpn

단계 **2** group policy 클라이언트리스 SSL VPN 구성 모드로 전환합니다.

group-policy webvpn

단계 **3** username 클라이언트리스 SSL VPN 구성 모드로 전환합니다.

username webvpn

단계 **4** 스마트 터널 액세스를 활성화합니다.

smart-tunnel [enable *list* **| disable]**

*list*는 이미 있는 스마트 터널 목록의 이름입니다. 이전 테이블에서 **smart-tunnel auto-start list**를 입력한 경우 스마트 터널 액세스를 수동으로 시작할 필요가 없습니다.

예제**:**

```
hostname(config-group-policy)# webvpn
hostname(config-group-webvpn)# smart-tunnel enable apps1
```

이 예에서는 이름이 apps1인 스마트 터널 목록이 그룹 정책에 할당됩니다.

단계 **5** SSL VPN 구성의 스마트 터널 목록 항목을 표시합니다.

show running-config webvpn smart-tunnel

단계 **6** 그룹 정책 또는 로컬 사용자 정책에서 smart-tunnel 명령을 제거하고 기본 그룹 정책으로 되돌립니다.

no smart-tunnel

단계 **7** 스마트 터널 액세스를 해제합니다.

smart-tunnel disable

스마트 터널 로그오프 구성

이 섹션에서는 스마트 터널이 제대로 로그오프되었는지 확인하는 방법에 대해 설명합니다. 스마트 터널은 모든 브라우저 창이 닫힌 경우 로그오프될 수 있습니다. 또는 알림 아이콘을 마우스 오른쪽 버튼으로 클릭하고 로그아웃을 확인할 수 있습니다.

참고 포털에서 로그아웃 버튼을 사용할 것을 적극 권장합니다. 이 방법은 클라이언트리스 SSL VPN과 관련이 있고 스마트 터널의 사용 여부에 관계없이 로그오프됩니다. 알림 아이콘은 독립 실행형 애플리케이션을 브라우저 없이 사용하는 경우에만 사용해야 합니다.

상위 프로세스 종료 시 스마트 터널 로그오프 구성

이 사례에서는 로그오프하려면 모든 브라우저를 닫아야 합니다. 이제 스마트 터널 수명은 프로세스 수명의 시작과 연관이 있습니다. 예를 들어 Internet Explorer에서 스마트 터널을 시작한 경우 iexplore.exe가 실행 중이 아니면 스마트 터널이 꺼집니다. 스마트 터널은 사용자가 로그아웃하지 않고 모든 브라우저를 닫는 경우에도 VPN 세션이 종료되었는지 판단할 수 있습니다.

참고 브라우저 프로세스가 느려지는 경우 의도하지 않은 결과이며 엄격히 말해 오류의 결과입니다. Secure Desktop을 사용 중인 경우 사용자가 Secure Desktop에서 모든 브라우저를 닫은 경우에도 브라우저 프로세스가 다른 데스크톱에서 실행될 수 있습니다. 따라서 스마트 터널은 현재 데스크톱에 더 이상 창이 보이지 않는 경우 모든 브라우저 인스턴스를 gone(없음)으로 선언합니다.

프로시저

단계 **1** 관리자가 전역 기준으로 알림 아이콘을 켤 수 있습니다.

[no] smart-tunnel notification-icon

이 명령은 브라우저 창을 닫아 로그아웃을 트리거하는 것이 아니라 로그아웃 속성을 구성하고 사용자에게 로그아웃을 위해 로그아웃 아이콘 제공 여부를 제어합니다.

이 명령은 또한 상위 프로세스가 종료되는 경우 로그오프를 제어하여 알림 아이콘이 켜져 있거나 꺼져 있는 경우 자동으로 켜지거나 꺼집니다.

*notification-icon*은 언제 로그아웃 아이콘을 사용할지 지정하는 키워드입니다.

이 명령의 *no* 버전이 기본값이며 이 경우, 모든 브라우저 창을 닫으면 SSL VPN 세션에서 로그오프됩니다.

포털 로그아웃은 여전히 적용되며 영향을 받지 않습니다.

단계 **2** 프록시를 사용하고 프록시 목록 예외에 추가하는 경우 로그오프할 때 아이콘 사용 여부와 관계 없이 스마트 터널이 제대로 닫혔는지 확인합니다.

***.webvpn.**

알림 아이콘을 통한 스마트 터널 로그오프 구성

브라우저를 닫는 경우 세션이 그대로 유지되도록 상위 프로세스를 종료할 때 로그오프를 해제하도록 선택할 수 있습니다. 이 사례에서 시스템 트레이의 알림 아이콘을 사용하여 로그아웃합니다. 이 아이콘은 사용자가 로그아웃하기 위해 아이콘을 클릭할 때까지 그대로 유지됩니다. 사용자가 로그아웃하기 전에 세션이 만료된 경우 이 아이콘은 다음 연결이 시도될 때까지 그대로 유지됩니다. 시스템 트레이에서 업데이트하려면 세션 상태를 기다려야 할 수 있습니다.

참고 이 아이콘은 SSL VPN에서 로그아웃하기 위한 대체 방법입니다. VPN 세션 상태에 대한 표시기가 아닙니다.

클라이언트리스 **SSL VPN** 캡처 툴

클라이언트리스 SSL VPN CLI에는 WebVPN 연결을 통해 제대로 표시되지 않은 웹사이트에 대한 정보를 기록할 수 있는 캡처 툴이 포함되어 있습니다. 이 툴에서 기록하는 데이터는 Cisco 고객 지원 담당자가 문제를 해결하는 데 도움이 됩니다.

클라이언트리스 SSL VPN 캡처 툴의 출력은 다음과 같이 두 개의 파일로 구성됩니다.

- mangled.1, 2,3, 4... 등(웹 페이지 작업에 따라) 변조 파일은 클라이언트리스 SSL VPN 연결에서 이 페이지를 전송하는 VPN Concentrator의 html 작업을 기록합니다.
- original.1,2,3,4... 등(웹 페이지 작업에 따라) 원본 파일은 VPN Concentrator로 전송된 URL 파일입니다.

캡처 툴을 사용하여 파일 출력을 열고 보려면 Administration(관리) | File Management(파일 관리)로 이동합니다. 출력 파일을 압축하고 Cisco 지원 담당자에게 전송합니다.

참고 클라이언트리스 SSL VPN 캡처 툴을 사용하면 VPN Concentrator 성능에 영향을 줍니다. 출력 파일을 생성한 후에 캡처 툴을 해제해야 합니다.

포털 액세스 규칙 구성

이러한 개선 사항을 통해 고객은 HTTP 헤더에 있는 데이터에 기반하여 클라이언트리스 SSL VPN 세션을 허용하거나 거부하도록 전역 클라이언트리스 SSL VPN 액세스 정책을 구성할 수 있습니다. ASA가 클라이언트리스 SSL VPN 세션을 거부하는 경우 엔드포인트에 오류 코드를 즉시 반환합니다.

ASA는 엔드포인트를 ASA에 대해 인증하기 전에 이 액세스 정책을 평가합니다. 그 결과 거부 시 더 적은 수의 ASA 처리 리소스가 엔드포인트에서의 추가 연결 시도에서 소모됩니다.

시작하기 전에

ASA에 로그온하고 전역 구성 모드를 시작합니다. 전역 구성 모드에서 ASA에 `hostname(config)#`가 표시됩니다.

프로시저

단계 **1** 클라이언트리스 SSL VPN 구성 모드를 시작합니다.

webvpn

단계 **2** HTTP 헤더의 HTTP 헤더 코드 또는 문자열을 기반으로 클라이언트리스 SSL VPN 세션의 생성을 허용하거나 거부합니다.

portal-access-rule *priority* [{**permit** | **deny** [**code** *code*]} {**any** | **user-agent match** *string*}

예제**:**

```
hostname(config-webvpn)# portal-access-rule 1 deny code 403 user-agent match *Thunderbird*
hostname(config-webvpn)# portal-access-rule 1 deny code 403 user-agent match "*my agent*"
```

두 번째 예는 공백이 있는 문자열을 지정하는 데 적절한 구문을 보여줍니다. 문자열 주위에 와일드카드(*)를 사용한 다음 따옴표(" ")를 사용합니다.

클라이언트리스 SSL VPN 성능 최적화

ASA는 클라이언트리스 SSL VPN 성능 및 기능을 최적화하기 위한 여러 가지 방법을 제공합니다. 성능 개선에는 웹 개체 캐싱 및 압축이 포함됩니다. 기능 조정에는 콘텐츠 변형 및 proxy-bypass에 대한 제한 설정이 포함됩니다. APCF는 콘텐츠 변형을 조정하는 추가적인 방법을 제공합니다.

캐싱 구성

캐싱은 클라이언트리스 SSL VPN 성능을 개선합니다. 이는 자주 재사용되는 개체를 시스템 캐시에 저장하여 콘텐츠의 재작성 및 압축 반복 작업을 줄이도록 해줍니다. 이렇게 하면 클라이언트리스 SSL VPN 및 원격 서버 간에 트래픽이 줄어 들어 많은 애플리케이션이 훨씬 더 효율적으로 실행됩니다.

기본적으로 캐싱은 활성화되어 있습니다. 캐시 모드에서 캐싱 명령을 사용하여 캐싱이 환경에서 작동되는 방식을 사용자 지정할 수 있습니다.

콘텐츠 변형 구성

기본적으로 ASA는 사용자가 SSL VPN 디바이스 내부에서 또는 이와 개별적으로 애플리케이션에 액세스 중인지 여부에 따라 다른 의미 체계 및 액세스 제어 규칙을 포함할 수 있는 HTTP 트래픽을 프록

시하기 위해 JavaScript 및 Java 같은 고급 요소를 포함하는 콘텐츠 변형/재작성 엔진을 통해 모든 클라이언트리스 SSL VPN 트래픽을 처리합니다.

일부 웹 리소스는 매우 개별적으로 처리해야 합니다. 다음 섹션에서는 이러한 처리 방법을 제공하는 기능에 대해 설명합니다. 관련된 조직 및 웹 콘텐츠의 요건에 따라 이 기능 중 하나를 사용할 수 있습니다.

재작성된 **Java** 콘텐츠 서명을 위한 인증서 구성

클라이언트리스 SSL VPN에서 변형된 Java 개체는 신뢰 지점과 연계된 PKCS12 디지털 인증서를 사용하여 이후에 서명할 수 있습니다.

프로시저

단계 **1** 인증서를 가져옵니다.

crypto ca import

단계 **2** 인증서를 사용합니다.

ava-trustpoint

예제**:**

```
hostname(config)# crypto ca import mytrustpoint pkcs12 mypassphrase
Enter the base 64 encoded PKCS12.
End with the word "quit" on a line by itself.
[ PKCS12 data omitted ]
quit
INFO: Import PKCS12 operation completed successfully.
hostname(config)# webvpn
hostname(config)# java-trustpoint mytrustpoint
```

이 예는 이름이 mytrustpoint인 신뢰 지점 생성 및 Java 개체 서명에 대한 할당을 보여줍니다.

콘텐츠 재작성 해제

일부 애플리케이션과 웹 리소스(예: 공공 웹 사이트)가 ASA를 통과하는 것을 원치 않을 수도 있습니다. 따라서 ASA에서는 사용자가 ASA를 거치지 않고 특정 사이트 및 애플리케이션을 찾아볼 수 있도록 재작성 규칙을 생성할 수 있습니다. 이는 IPSec VPN 연결의 스플릿 터널링과 유사합니다.

프로시저

단계 **1** 클라이언트리스 SSL VPN 구성 모드로 전환합니다.

webvpn

단계 **2** 클라이언트리스 SSL VPN 터널 외부에 액세스하도록 애플리케이션 및 리소스를 지정합니다.

rewrite

이 명령은 여러 번 사용할 수 있습니다.

단계 **3** rewrite 명령과 함께 사용됩니다.

disable

규칙 순서 번호는 보안 어플라이언스가 가장 작은 수부터 시작하는 순서 번호에 따라 재작성 규칙을 검색하고 일치하는 첫 번째 규칙을 적용하므로 중요합니다.

프록시 우회 사용

애플리케이션 및 웹 리소스가 이 기능이 제공하는 특수한 콘텐츠 재작성에서 더욱 효율적으로 활용되는 경우 ASA가 프록시 우회를 사용하도록 구성할 수 있습니다. 프록시 우회는 원래 콘텐츠를 최소한으로 변경하는 콘텐츠 재작성의 대체 방법입니다. 사용자 지정 웹 애플리케이션에 주로 유용합니다.

proxy-bypass 명령을 여러 번 사용할 수 있습니다. 항목을 구성한 순서는 중요하지 않습니다. 인터페이스 및 경로 마스크 또는 인터페이스 및 포트는 프록시 우회 규칙을 고유하게 식별합니다.

네트워크 구성에 따라 경로 마스크 대신 포트를 사용하여 프록시 우회를 구성한 경우, 해당 포트가 ASA에 액세스하도록 방화벽 구성을 변경해야 할 수도 있습니다. 경로 마스크를 사용하여 이러한 제한사항을 방지하십시오. 단, 경로 마스크는 변경될 수 있으므로 이러한 가능성을 없애려면 여러 경로 마스크 명령문을 사용해야 할 수도 있습니다.

경로란 URL에서 .com, .org 또는 기타 도메인 이름 유형 뒤에 나오는 모든 것입니다. 예를 들어 URL www.example.com/hrbenefits에서는 *hrbenefits*가 경로입니다. 마찬가지로 URL www.example.com/hrinsurance에서는 *hrinsurance*가 경로입니다. 모든 hr 사이트에 대한 프록시 우회를 사용하려면 /hr*와 같이 * 와일드카드를 사용하여 명령이 여러 번 사용되는 것을 방지할 수 있습니다.

프로시저

단계 **1** 클라이언트리스 SSL VPN 구성 모드로 전환합니다.

webvpn

단계 **2** 프록시 우회를 구성합니다.

proxy-bypass

18 장

클라이언트리스 SSL VPN 원격 사용자

이 장에서는 사용자 원격 시스템에 대한 구성 요건 및 작업을 간략하게 설명합니다. 또한 사용자가 클라이언트리스 SSL VPN을 시작하는 데 도움이 되는 정보를 제공합니다. 다음의 섹션이 포함됩니다.

참고 ASA가 클라이언트리스 SSL VPN에 대해 구성되어 있는지 확인하십시오.

클라이언트리스 SSL VPN 원격 사용자

이 장에서는 사용자 원격 시스템에 대한 구성 요건 및 작업을 간략하게 설명합니다. 또한 사용자가 클라이언트리스 SSL VPN을 시작하는 데 도움이 되는 정보를 제공합니다. 다음의 섹션이 포함됩니다.

참고 ASA가 클라이언트리스 SSL VPN에 대해 구성되어 있는지 확인하십시오.

사용자 이름 및 비밀번호

네트워크에 따라 원격 세션 동안 사용자는 컴퓨터, 인터넷 서비스 공급자, 클라이언트리스 SSL VPN, 메일 또는 파일 서버 또는 기업 애플리케이션 중 하나 또는 모두에 로그온해야 할 수 있습니다. 사용자는 고유한 사용자 이름 및 비밀번호 또는 PIN 같은 다양한 정보가 필요한 여러 가지 다른 상황에서 인증해야 할 수 있습니다. 사용자에게 필수 액세스 권한이 있는지 확인합니다.

다음 표에서는 클라이언트리스 SSL VPN 사용자가 알아야 할 사용자 이름 및 비밀번호 유형을 보여줍니다.

표 ***19:*** 클라이언트리스 ***SSL VPN*** 사용자에게 제공할 사용자 이름 및 비밀번호

로그인 사용자 이름/비밀번호 유형		입력 시기
컴퓨터	컴퓨터 액세스	컴퓨터 시작 시
인터넷 서비스 공급자	인터넷 액세스	인터넷 서비스 공급자에 연결 시
클라이언트리스 SSL VPN	원격 네트워크 액세스	클라이언트리스 SSL VPN 세션 시작 시
파일 서버	원격 파일 서버 액세스	원격 파일 서버에 액세스하기 위해 클라이언트리스 SSL VPN 파일 브라우징 기능 사용 시
기업 애플리케이션 로그인	방화벽 보호 내부 서버 액세스	내부의 보호되는 웹 사이트에 액세스하기 위해 클라이언트리스 SSL VPN 웹 브라우징 기능 사용 시
메일 서버	클라이언트리스 SSL VPN을 통한 원격 메일 서버 액세스	이메일 메시지 전송 또는 수신 시

보안 팁 전달

다음과 같은 보안 팁을 전달합니다.

- 항상 클라이언트리스 SSL VPN 세션에서 로그아웃하거나, 클라이언트리스 SSL VPN 툴바에서 로그아웃 아이콘을 클릭하거나, 브라우저를 닫습니다.
- 클라이언트리스 SSL VPN의 사용이 모든 사이트와의 통신 보안을 보장하는 것은 아닙니다. 클라이언트리스 SSL VPN은 원격 컴퓨터 또는 워크스테이션과 기업 네트워크에 있는 ASA 간의 데이터 전송 보안을 보장합니다. 사용자가 인터넷 또는 내부 네트워크에 있는 비 HTTPS 웹 리소스에 액세스하는 경우에는 기업 ASA에서 대상 웹 서버로의 통신 보안이 유지되지 않습니다.

클라이언트리스 **SSL VPN** 기능을 사용하도록 원격 시스템 구성

다음 표에는 클라이언트리스 SSL VPN을 사용하도록 원격 시스템 설정하는 작업, 이 작업에 대한 요구 사항/사전 요구 사항 및 권장 사용 방법이 포함되어 있습니다.

사용자 어카운트를 구성한 방식에 따라 각 클라이언트리스 SSL VPN 사용자가 사용할 수 있는 기능이 다를 수 있습니다. 또한 다음 표에는 사용자 작업별로 정보가 구성되어 있습니다.

표 ***20:*** 클라이언트리스 ***SSL VPN*** 원격 시스템 구성 및 엔드 유저 요구 사항

작업	원격 시스템 또는 엔드 유저 요건	사양 또는 사용 제안
클라이언트리스 **SSL VPN** 시작	인터넷에 연결	다음을 비롯한 모든 인터넷 연결이 지원됩니다. • 홈 DSL, 케이블 또는 다이얼업 • 공용 키오스크 • 호텔 연결 • 공항 무선 노드 • 인터넷 카페
	클라이언트리스 SSL VPN 지원 브라우저	클라이언트리스 SSL VPN에 대해 다음 브라우저를 권장합니다. 다른 브라우저는 클라이언트리스 SSL VPN 기능을 완벽하게 지원하지 않을 수 있습니다. Microsoft Windows의 경우: • Internet Explorer 8 • Firefox 8 Linux의 경우: • Firefox 8 Mac OS X의 경우: • Safari 5 • Firefox 8
	브라우저에서 사용 가능한 쿠키	쿠키는 포트 전달을 통한 애플리케이션 액세스를 위해 브라우저에서 활성화되어야 합니다.
	클라이언트리스 SSL VPN의 URL	다음 형식의 HTTPS 주소: https://address 이때 address(주소)는 클라이언트리스 SSL VPN이 활성화된 ASA(또는 로드 밸런싱 클러스터)의 인터페이스 IP 주소 또는 DNS 호스트 이름입니다. 예를 들어 https://10.89.192.163 또는 https://cisco.example.com입니다.

작업	원격 시스템 또는 엔드 유저 요건	사양 또는 사용 제안
	클라이언트리스 SSL VPN 사용자 이름 및 비밀번호	
	[선택 사항] 로컬 프린터	클라이언트리스 SSL VPN은 웹 브라우저에서 네트워크 프린터로의 인쇄를 지원하지 않습니다. 로컬 프린터로의 인쇄는 지원됩니다.
클라이언트리스 **SSL VPN** 연결에서 부동 툴바 사용		부동 툴바를 사용하면 클라이언트리스 SSL VPN 사용을 간소화할 수 있습니다. 툴바를 사용하여 URL을 입력하고 파일 위치를 찾아보며 기본 브라우저 창에 방해되지 않게 사전 구성된 웹 연결을 선택할 수 있습니다. 팝업을 차단하도록 브라우저를 구성한 경우 부동 툴바를 표시할 수 없습니다. 부동 툴바는 현재의 클라이언트리스 SSL VPN 세션을 나타냅니다. **Close** 버튼을 클릭하면 ASA는 클라이언트리스 SSL VPN 세션을 닫도록 확인 상자를 표시합니다. 팁 텍스트를 텍스트 필드에 붙여넣으려면 Ctrl-V를 사용합니다(클라이언트리스 SSL VPN 툴바에서는 마우스 오른쪽 버튼으로 클릭이 활성화되지 않습니다.).

작업	원격 시스템 또는 엔드 유저 요건	사양 또는 사용 제안
웹 브라우징	보호된 웹 사이트에 대한 사용자 이름 및 비밀번호	클라이언트리스 SSL VPN의 사용이 모든 사이트와의 통신 보안을 보장하는 것은 아닙니다. "보안 팁 전달, 392 페이지"을 참조하십시오.
		클라이언트리스 SSL VPN을 통한 웹 브라우징의 모양과 느낌은 사용자에게 익숙하지 않을 수 있습니다. 예를 들면 다음과 같습니다. • 클라이언트리스 SSL VPN의 제목 표시줄은 각각의 웹 페이지 위에 표시됩니다. • 다음 방법으로 웹 사이트에 액세스합니다. • 클라이언트리스 SSL VPN 홈 페이지의 Enter Web Address(웹 주소 입력) 필드에서 URL 입력 • 클라이언트리스 SSL VPN 홈 페이지의 사전 구성 웹사이트 링크 클릭 • 앞의 두 가지 방법 중 하나를 통해 액세스되는 웹 페이지에서 링크 클릭 또한 특정한 어카운트를 구성한 방법에 따라 다음과 같을 수도 있습니다. • 일부 웹사이트가 차단됨 • 클라이언트리스 SSL VPN 홈 페이지에서 링크로 나타나는 웹사이트만 사용 가능

작업	원격 시스템 또는 엔드 유저 요건	사양 또는 사용 제안
네트워크 브라우징 및 파일 관리	공유 원격 액세스에 대해 구성된 파일 권한	클라이언트리스 SSL VPN을 통해 공유 폴더 및 파일에만 액세스할 수 있습니다.
	보호되는 파일 서버에 대한 서버 이름 및 비밀번호	—
	폴더 및 파일이 위치한 도메인, 작업 그룹, 서버 이름	사용자는 조직 네트워크를 통해 자신의 파일을 찾는 방법에 익숙하지 않을 수 있습니다.
	—	복사가 진행 중인 동안 **Copy File to Server** 명령을 중단하거나 다른 화면으로 이동하지 마십시오. 작업을 중단하면 불완전한 파일이 서버에 저장될 수 있습니다.

작업	원격 시스템 또는 엔드 유저 요건	사양 또는 사용 제안
애플리케이션 사용 **(**포트 전달 또는 애플리케이션 액세스라고도 함**)**	참고 Mac OS X에서 Safari 브라우저만 이 기능을 지원합니다.	
	참고 이 기능을 사용하려면 Oracle JRE(Java Runtime Environment)를 설치하고 로컬 클라이언트를 구성해야 하며 이를 위해서는 로컬 시스템에 대한 관리자 권한이 필요하므로 사용자가 공용 원격 시스템에서 연결한 경우 애플리케이션을 사용하지 못할 수도 있습니다.	
	사용자는 애플리케이션 사용을 마칠 때 **Close** 아이콘을 클릭하여 항상 애플리케이션 액세스 창을 닫아야 합니다. 창을 제대로 닫지 못하면 애플리케이션 액세스 또는 애플리케이션 자체에 액세스할 수 없습니다.	
	클라이언트 애플리케이션이 설치됨	—
	브라우저에서 사용 가능한 쿠키	—
	관리자 권한	호스트 파일 수정 시 필요하므로 DNS 이름을 사용하여 서버를 지정하는 경우 사용자는 컴퓨터에 대한 관리자 액세스 권한을 지녀야 합니다.
	Oracle JRE(Java Runtime Environment)가 설치되어 있습니다. 브라우저에서 JavaScript를 활성화해야 합니다. 기본적으로 활성화되어 있습니다.	JRE가 설치되지 않은 경우 사용할 수 있는 사이트로 사용자를 안내하는 팝업 창이 표시됩니다. 드문 경우지만 포트 전달 애플릿이 Java 예외 오류로 인해 실패합니다. 이 경우 다음을 수행하십시오. **1.** 브라우저 캐시를 지우고 브라우저를 닫습니다. **2.** Java 아이콘이 컴퓨터 작업 표시줄에 없는지 확인합니다. Java의 모든 인스턴스를 닫습니다. **3.** 클라이언트리스 SSL VPN 세션을 설정하고 포트 전달 Java 애플릿을 실행합니다.

작업	원격 시스템 또는 엔드 유저 요건	사양 또는 사용 제안
	필요 시 클라이언트 애플리케이션이 구성됨 참고 Microsoft Outlook 클라이언트에는 이 구성 단계가 필요하지 않습니다. 비 Windows 클라이언트 애플리케이션은 모두 구성해야 합니다. Windows 애플리케이션에 구성이 필요한지 판단하려면 Remote Server(원격 서버)의 값을 확인하십시오. • 원격 서버에 서버 호스트 이름이 포함된 경우, 클라이언트 애플리케이션을 구성할 필요가 없습니다. • 원격 서버 필드에 IP 주소가 포함된 경우, 클라이언트 애플리케이션을 구성해야 합니다.	클라이언트 애플리케이션을 구성하려면 서버의 로컬로 매핑된 IP 주소 및 포트 번호를 사용합니다. 이 정보를 찾으려면 다음을 수행하십시오. 1. 원격 시스템에서 클라이언트리스 SSL VPN을 시작하고 클라이언트리스 SSL VPN 홈 페이지에서 Application Access(애플리케이션 액세스) 링크를 클릭합니다. 애플리케이션 액세스 창이 나타납니다. 2. 이름 열에서 사용할 서버의 이름을 찾은 다음 로컬 열에서 해당 클라이언트 IP 주소 및 포트 번호를 식별합니다. 3. 이 IP 주소 및 포트 번호를 사용하여 클라이언트 애플리케이션을 구성합니다. 구성 단계는 클라이언트 애플리케이션마다 다릅니다.
	참고 클라이언트리스 SSL VPN에서 실행 중인 애플리케이션에서 URL(예: 이메일 메시지의 URL)을 클릭해도 클라이언트리스 SSL VPN을 통해 사이트가 열리지 않습니다. 클라이언트리스 SSL VPN에서 사이트를 열려면 URL을 Enter (URL) Address((URL) 주소 입력) 필드에 붙여넣습니다.	
애플리케이션 액세스를 통한 이메일 사용	애플리케이션 액세스에 대한 요건 충족(애플리케이션 사용 참조)	메일을 사용하려면 클라이언트리스 SSL VPN 홈 페이지에서 애플리케이션을 액세스를 시작합니다. 이제 메일 클라이언트를 사용할 수 있습니다.
	참고 IMAP 클라이언트를 사용 중이며 메일 서버 연결이 손실되거나 새 연결을 설정할 수 없는 경우, IMAP 애플리케이션을 닫고 클라이언트리스 SSL VPN을 재시작합니다.	
	기타 이메일 클라이언트	Microsoft Outlook Express 5.5 및 6.0 버전의 테스트는 완료되었습니다.

작업	원격 시스템 또는 엔드 유저 요건	사양 또는 사용 제안
웹 액세스를 통한 이메일 사용	웹 기반 이메일 제품이 설치됨	지원되는 제품은 다음과 같습니다. • Outlook Web Access 최적의 결과를 위해서는 Internet Explorer 8.x 이상 또는 Firefox 8.x 이상에서 OWA를 사용하십시오. • Lotus Notes 다른 웹 기반 이메일 제품도 작동해야 하지만 이는 검증되지 않았습니다.
Using email via email Proxy	SSL 활성화 메일 애플리케이션이 설치됨 ASA SSL 버전을 TLSv1 전용으로 설정하지 마십시오. Outlook 및 Outlook Express는 TLS를 지원하지 않습니다.	지원되는 메일 애플리케이션: • Microsoft Outlook • Microsoft Outlook Express 버전 5.5 및 6.0 다른 SSL 활성화 메일 클라이언트도 작동해야 하지만 이는 검증되지 않았습니다.
	메일 애플리케이션이 구성됨	

클라이언트리스 **SSL VPN** 데이터 캡처

CLI capture 명령을 사용하여 클라이언트리스 SSL VPN 연결에서 올바르게 표시되지 않는 웹사이트에 대한 정보를 기록할 수 있습니다. 이 데이터는 Cisco 고객 지원 엔지니어가 문제를 해결하는 데 도움이 됩니다. 다음 섹션에서는 캡처 명령을 사용하는 방법에 대해 설명합니다.

• 캡처 파일 만들기, 400 페이지
• 브라우저를 사용하여 캡처 데이터 표시, 400 페이지

참고 클라이언트리스 SSL VPN 캡처를 활성화하면 ASA 성능에 영향을 줍니다. 따라서 문제 해결에 필요한 캡처 파일을 생성한 후에는 캡처를 꺼야 합니다.

캡처 파일 만들기

프로시저

단계 **1** 클라이언트리스 SSL VPN 캡처 유틸리티를 시작하여 패킷을 캡처합니다.

capture *capture-name* **type webvpn user** *csslvpn-username*

- *capture-name*은 캡처에 할당한 이름으로, 캡처 파일의 이름 앞에도 추가됩니다.
- *csslvpn-username*은 캡처하기 위해 일치시킬 사용자 이름입니다.

예제:

```
hostname# capture hr type webvpn user user2
```

단계 **2** **no** 버전의 명령을 사용하여 캡처를 중지합니다.

no capture *capture-name*

예제:

```
hostname# no capture hr
```

캡처 유틸리티는 *capture_name*.zip 파일을 생성하며 이 파일은 비밀번호 **koleso**를 사용하여 암호화됩니다.

단계 **3** 이 .zip 파일을 Cisco로 전송하거나 Cisco TAC 서비스 요청에 첨부합니다.

단계 **4** .zip 파일 내용을 보려면 비밀번호 **koleso**를 사용하여 파일의 압축을 풉니다.

브라우저를 사용하여 캡처 데이터 표시

프로시저

단계 **1** 클라이언트리스 SSL VPN 캡처 유틸리티를 시작합니다.

capture *capture-name* **type webvpn user** *csslvpn-username*

- *capture-name*은 캡처에 할당한 이름으로, 캡처 파일의 이름 앞에도 추가됩니다.
- *csslvpn-username*은 캡처하기 위해 일치시킬 사용자 이름입니다.

예제:

```
hostname# capture hr type webvpn user user2
```

단계 **2** 브라우저를 열고 주소 상자에 다음을 입력합니다.

https://*ASA*의 *IP* 주소 또는 호스트 이름/**webvpn_capture.html**

캡처된 내용이 스니퍼 형식으로 표시됩니다.

단계 **3** **no** 버전의 명령을 사용하여 캡처를 중지합니다.

no capture *capture-name*

예제**:**

```
hostname# no capture hr
```

19 장

클라이언트리스 SSL VPN 사용자

비밀번호 관리

비밀번호가 만료될 예정인 경우 선택적으로 엔드 유저에게 경고하도록 ASA를 구성할 수 있습니다.

ASA는 RADIUS 및 LDAP 프로토콜에 대한 비밀번호 관리를 지원합니다. “password-expire-in-days" 옵션은 LDAP에 대해서만 지원됩니다.

IPsec 원격 액세스 및 SSL VPN 터널 그룹에 대해 비밀번호 관리를 구성할 수 있습니다.

비밀번호 관리를 구성하는 경우, ASA는 로그인 시 원격 사용자에게 사용자의 현재 비밀번호가 만료 예정이거나 이미 만료되었음을 알립니다. 그런 다음 ASA에서는 사용자에게 비밀번호를 변경할 기회를 제공합니다. 현재 비밀번호가 아직 만료되지 않은 경우, 사용자는 이 비밀번호를 사용하여 계속 로그인할 수 있습니다.

이 명령은 이러한 알림을 지원하는 AAA 서버에 유효합니다.

ASA 릴리스 7.1 이상에서는 MS-CHAPv2를 지원하는 RADIUS 구성 또는 LDAP로 인증할 때 일반적으로 다음 연결 유형에 대한 비밀번호 관리를 지원합니다.

- AnyConnect VPN 클라이언트
- IPsec VPN Client
- 클라이언트리스 SSL VPN

RADIUS 서버(예: Cisco ACS)는 인증 요청을 다른 인증 서버로 프록시할 수 있습니다. 그러나 ASA 관점에서 보면 RADIUS 서버와만 통신하는 것입니다.

시작하기 전에

- 기본 LDAP에는 SSL 연결이 필요합니다. LDAP에 대한 비밀번호 관리를 시도하기 전에 LDAP over SSL을 활성화해야 합니다. 기본적으로 LDAP는 포트 636을 사용합니다.
- 인증을 위해 LDAP 디렉토리 서버를 사용 중인 경우, 비밀번호 관리가 Sun Java System Directory Server(이전 이름은 Sun ONE Directory Server) 및 Microsoft Active Directory에서 지원됩니다.
  - Sun - Sun 디렉터리 서버에 액세스하려면 ASA에 구성된 DN이 이 서버의 기본 비밀번호 정책에 액세스할 수 있어야 합니다. 디렉토리 관리자 또는 디렉토리 관리자 권한이 있는 사용자를 DN으로 사용할 것을 권장합니다. 또는 기본 비밀번호 정책에 ACI를 배치할 수 있습니다.
  - Microsoft - Microsoft Active Directory에서 비밀번호 관리를 활성화하려면 LDAP over SSL을 구성해야 합니다.
- MSCHAP를 지원하는 일부 RADIUS 서버는 현재 MSCHAPv2를 지원하지 않습니다. 이 명령에는 MSCHAPv2가 필요하므로 공급업체에 확인하십시오.
- Kerberos/Active Directory(Windows 비밀번호) 또는 NT 4.0 도메인의 이러한 연결 유형에 대해서는 비밀번호 관리가 지원되지 않습니다.
- LDAP의 경우 시중에 출시된 여러 LDAP 서버 전용의 비밀번호 변경 방법이 있습니다. 현재 ASA에서는 Microsoft Active Directory 및 Sun LDAP 서버에만 사용할 수 있는 독점적 비밀번호 관리 로직을 구축하고 있습니다.
- RADIUS 또는 LDAP 인증이 구성되어 있지 않으면 ASA는 이 명령을 무시합니다.
- password-management 명령은 비밀번호가 만료될 때까지 남은 일 수를 변경하는 것이 아니라 만료 며칠 전부터 ASA에서 사용자에게 비밀번호 만료가 얼마 남지 않았음을 알리기 시작할 것인지를 변경합니다.

프로시저

단계 **1** 일반 특성 모드로 전환합니다.

tunnel-group general-attributes

단계 **2** 비밀번호가 만료될 예정임을 원격 사용자에게 알립니다.

password-management password-expire-in-days *days*

예제**:**

```
hostname(config-general)# password-management password-expire-in-days 90
```

- password-expire-in-days 키워드를 지정하는 경우, 날짜 수도 지정하십시오.
- 날짜 수를 0으로 설정하면 이 명령이 해제됩니다.

이 예에서, ASA는 비밀번호가 만료되기 90일 전에 사용자에게 경고를 시작합니다.

참고 password-expire-in-days 키워드가 설정되지 않은 경우, ASA는 보류 중인 만료에 대해 사용자에게 알리지 않지만, 사용자는 비밀번호가 만료된 이후에 비밀번호를 변경할 수 있습니다.

클라이언트리스 **SSL VPN**에서 단일 로그인 사용

SAML 2.0을 사용하는 **SSO**

SSO 및 **SAML 2.0** 정보

ASA는 SAML 2.0을 지원하므로 클라이언트리스 VPN 엔드 유저가 클라이언트리스 VPN과 프라이빗 네트워크 외부의 다른 SAAS 애플리케이션 간에 전환할 때 크리덴셜을 한 번만 입력할 수 있게 됩니다.

예를 들어, 기업 고객이 PingIdentity를 SAML IdP(Identity Provider)로 활성화했고 SAML 2.0 SSO가 활성화된 Rally, Salesforce, Oracle OEM, Microsoft ADFS, onelogin 또는 Dropbox에 계정이 있는 경우, ASA에서 SAML 2.0 SSO를 SP(서비스 제공자)로 지원하도록 구성하면 엔드 유저가 한 번만 로그인하여 클라이언트리스 VPN을 포함한 이 모든 서비스에 액세스할 수 있습니다.

또한 AnyConnect 4.4 클라이언트가 SAML 2.0을 사용하여 SAAS 기반 애플리케이션에 액세스할 수 있도록 AnyConnect SAML 지원이 추가되었습니다. AnyConnect 4.6에는 이전 릴리스에 통합되어 있던 기본(외부) 브라우저 대신 제공되는 임베디드 브라우저를 포함하는 개선된 버전의 SAML 통합이 도입되었습니다. 임베디드 브라우저를 포함하여 새롭게 개선된 버전을 사용하려면 AnyConnect 4.6 및 ASA 9.7.1.24, 9.8.2.28, 또는 9.9.2.1로 업그레이드해야 합니다.

ASA는 SAML이 터널 그룹, 기본 터널 그룹 또는 다른 모든 그룹에 대한 인증 방법으로 구성되었을 때 SP가 활성화된 상태입니다. 클라이언트리스 VPN 엔드 유저는 활성화된 ASA 또는 SAML IdP에 액세스하여 Single Sign-On을 시작합니다. 이러한 각 시나리오는 다음과 같습니다.

SAML SP 시작 **SSO**

엔드 유저가 클라이언트리스 VPN을 사용하여 ASA에 액세스하는 방식으로 로그인을 시작하는 경우 다음과 같이 로그인 동작이 진행됩니다.

1. 클라이언트리스 VPN 엔드 유저가 SAML이 활성화된 터널 그룹에 액세스하거나 선택하는 경우 인증을 위해 엔드 유저가 SAML idP로 리디렉션됩니다. 사용자가 group-url에 직접 액세스하는 경우(이 경우 리디렉션이 자동 모드임)를 제외하고 사용자에게 프롬프트가 표시됩니다.

   ASA는 브라우저가 SAML IdP에 리디렉션되는 SAML 인증 요청을 생성합니다.

2. IdP에서 엔드 유저에게 크리덴셜을 요구하고 엔드 유저가 로그인합니다. 입력한 크리덴셜은 IdP 인증 구성을 충족해야 합니다.

3. IdP 응답이 브라우저에 다시 전송되고 ASA의 로그인 URL에 게시됩니다. ASA는 로그인을 완료하기 위해 응답을 확인합니다.

SAML IdP 시작 SSL

사용자가 IdP에 액세스하여 로그인을 시작하는 경우 다음과 같이 로그인 동작이 진행됩니다.

1. 엔드 유저가 IdP에 액세스합니다. IdP에서 IdP의 인증 구성에 따라 엔드 유저에게 크리덴셜을 요구합니다. 엔드 유저가 크리덴셜을 제출하고 IdP에 로그인합니다.
2. 일반적으로, 엔드 유저는 IdP로 구성되고 SAML이 활성화된 서비스의 목록을 가져옵니다. 엔드 유저가 ASA를 선택합니다.
3. SAML 응답이 브라우저에 다시 전송되고 ASA의 로그인 URL에 게시됩니다. ASA는 로그인을 완료하기 위해 응답을 확인합니다.

CoT(Circle of Trust)

ASA와 SAML IdP(Identity Provider) 간의 신뢰 관계는 구성된 인증서(ASA 트러스트 포인트)를 통해 수립되어야 합니다.

엔드 유저와 SAML IdP(Identity Provider) 간의 신뢰 관계는 IdP에 구성된 인증을 통해 설정됩니다.

SAML 시간 제한

SAML 어설션에는 다음과 같은 NotBefore 및 NotOnOrAfter가 있습니다. <saml:Conditions NotBefore="2015-03-10T19:47:41Z" NotOnOrAfter="2015-03-10T20:47:41Z">

ASA에 구성된 SAML 시간 제한은 NotBefore의 합계와 시간 제한이 NotOnOrAfter 이전인 경우 NotOnOrAfter를 재정의합니다. NotBefore + 시간 제한이 NotOnOrAfter 이후이면 NotOnOrAfter가 적용됩니다.

시간 제한은 시간 제한 이후에 어설션이 다시 사용되는 것을 방지하기 위해 매우 짧아야 합니다. SAML 기능을 사용하려면 ASA의 NTP(Network Time Protocol) 서버와 IdP NTP 서버를 동기화해야 합니다.

프라이빗 네트워크에서 지원

SAML 2.0 기반 서비스 공급자 IdP는 프라이빗 네트워크에서 지원됩니다. SAML IdP를 프라이빗 클라우드에 구축할 경우, ASA 및 기타 SAML 지원 서비스는 피어 위치 및 모든 프라이빗 네트워크에 있습니다. 서비스와 사용자 간의 게이트웨이로 ASA를 사용할 경우 IdP에서의 인증이 제한된 익명 webvpn 세션과 함께 처리되며 IdP와 사용자 간의 모든 트래픽이 변환됩니다. 사용자가 로그인할 때 ASA에서 해당 속성이 있는 세션을 수정하고 IdP 세션을 저장합니다. 크리덴셜을 다시 입력하지 않고도 프라이빗 네트워크에서 통신 사업자를 사용할 수 있습니다.

SAML IdP *NameID* 속성은 사용자의 사용자 이름을 확인하며 권한 부여, 계정 관리 및 VPN 세션 데이터베이스에 사용됩니다.

참고 프라이빗 및 퍼블릭 네트워크 간에 인증 정보를 교환할 수 없습니다. 모두 내부 및 외부 통신 사업자 모두에 대해 동일한 IdP를 사용하는 경우 개별적으로 인증해야 합니다. 외부 서비스와 내부 전용 IdP를 함께 사용할 수 없습니다. 프라이빗 네트워크에서 외부 전용 IdP는 통신 사업자와 함께 사용할 수 없습니다.

SAML 2.0에 대한 지침 및 제한 사항

- SAML 2.0 SSO는 클라이언트리스 VPN 기능을 지원하므로 다음과 같이 클라이언트리스 VPN과 동일한 제한 사항과 할당 방법을 사용합니다.
  - 다중 상황 모드 및 로드 밸런싱은 지원되지 않습니다.
  - 액티브/스탠바이 장애 조치는 지원되지만 액티브/액티브 장애 조치는 지원되지 않습니다.
  - IPv4 및 IPv6 세션은 지원됩니다.
- ASA는 모든 SAML IdP에서 지원하는 SAML 2.0 Redirect-POST 바인딩을 지원합니다.
- ASA는 SAML SP로만 작동합니다. 게이트웨이 모드 또는 피어 모드에서 IdP(Identity Provider)로 작동할 수 없습니다.
- 이 SAML SSO SP 기능은 상호 제외 인증 방법입니다. AAA 및 인증서와 함께 사용할 수 없습니다.
- 사용자 이름/비밀번호 인증, 인증서 인증 및 KCD를 기반으로 하는 기능은 지원되지 않습니다. 예를 들어, 인스턴스, 사용자 이름/비밀번호 사전 채우기, 양식 기반 자동 로그온, 매크로 대체 기반 자동 로그온, KCD SSO 등이 있습니다.
- DAP는 SAML 활성화 터널 그룹에 대해 지원되지 않습니다.
- 기존 클라이언트리스 VPN 시간 제한 설정은 SAML 세션에 계속 적용됩니다.
- ASA 관리자는 인증 어설션 및 적절한 시간 제한 동작을 적절하게 처리하기 위해 ASA와 SAML IdP 간의 클럭 동기화를 확인해야 합니다.
- ASA 관리자는 다음 사항을 고려하면서 ASA와 IdP 모두에서 유효한 서명 인증서를 유지해야 합니다.
  - ASA에서 IdP를 구성하는 경우에는 IdP 서명 인증서가 필수입니다.
  - ASA는 IdP에서 수신된 서명 인증서에서 해지 확인을 수행하지 않습니다.
- SAML 어설션에는 NotBefore 및 NotOnOrAfter 조건이 있습니다. 구성된 ASA SAML 시간 제한은 이러한 조건과 다음과 같이 상호 작용합니다.
  - 시간 제한은 NotBefore의 합계와 시간 제한이 NotOnOrAfter 이전인 경우 NotOnOrAfter를 재정의합니다.
  - NotBefore + 시간 제한이 NotOnOrAfter 이후이면 NotOnOrAfter가 적용됩니다.
  - NotBefore 속성이 없으면 ASA에서 로그인 요청을 거부합니다. NotOnOrAfter 속성이 없고 SAML 시간 제한이 설정되지 않은 경우 ASA에서 로그인 요청을 거부 합니다.
- AnyConnect와 함께 SAML을 사용할 경우, 다음과 같은 추가 지침이 있습니다.
  - 신뢰할 수 없는 서버 인증서는 임베디드 브라우저에서 허용되지 않습니다.
  - CLI 또는 SBL 모드에서는 임베디드 브라우저 SAML 통합이 지원되지 않습니다.

- 웹 브라우저에서 설정된 SAML 인증은 AnyConnect와 공유되지 않으며 반대의 경우도 마찬가지입니다.
- 구성에 따라 임베디드 브라우저가 포함된 헤드엔드에 연결할 때는 다양한 방법이 사용됩니다. 예를 들어 AnyConnect의 경우 IPv6 연결보다 IPv4 연결이 기본적으로 사용될 수 있는 반면 임베디드 브라우저의 경우 IPv6이 기본적으로 사용될 수도 있고 그 반대의 방식이 적용될 수도 있습니다. 마찬가지로 AnyConnect는 프록시 사용을 시도한 후 장애가 발생하면 프록시 없음으로 대체할 수 있는 반면 임베디드 브라우저의 경우에는 프록시 사용을 시도한 후 장애가 발생하면 탐색을 중지할 수 있습니다.
- SAML 기능을 사용하려면 ASA의 NTP(Network Time Protocol) 서버와 IdP NTP 서버를 동기화해야 합니다.
- ASDM의 VPN 마법사는 현재 SAML 구성을 지원하지 않습니다.
- 내부 IdP를 사용하여 로그인한 후에는 SSO를 사용하여 내부 서버에 액세스할 수 없습니다.
- SAML IdP NameID 속성은 사용자의 사용자 이름을 확인하며 권한 부여, 계정 관리 및 VPN 세션 데이터베이스에 사용됩니다.

SAML 2.0 IdP(Identity Provider) 구성

시작하기 전에

SAML (IdP) 제공자용 로그인 및 로그아웃 URL을 가져옵니다. 제공자의 웹 사이트에서 URL을 가져올 수도 있고, 메타데이터 파일에서 해당 정보를 제공할 수도 있습니다.

프로시저

단계 **1** Webvpn 구성 모드에서 SAML IdP(Identity Provider)를 생성하고 webvpn 아래에서 saml-idp sub-mode를 입력합니다.

[**no**] **saml idp** *idp-entityID*

idp-entityID — SAML IdP entityID는 4~256자를 포함해야 합니다.

SAML IdP를 제거하려면 **no** 형식의 이 명령을 사용하십시오.

단계 **2** IdP URL을 구성합니다.

url [**sign-in** | **sign-out**] *value*

value — IdP에 로그인하는 데 사용할 URL 또는 IdP에서 로그아웃할 때 리디렉션할 URL입니다. **sign-in** URL은 필수이고, **sign-out** URL은 선택 사항입니다. Url 값은 4~500자를 포함해야 합니다.

단계 **3** (선택 사항) 클라이언트리스 VPN 기본 URL을 구성합니다.

base-url *URL*

이 URL은 엔드 유저가 ASA로 다시 리디렉션할 서드파티 IdP에 제공됩니다.

base-url이 구성되어 있는 경우, **show saml metadata**에서 AssertionConsumerService 및 SingleLogoutService 속성의 기본 URL로 사용합니다.

base-url이 구성되지 않은 경우 이 URL은 ASA의 호스트 이름 및 도메인 이름에 따라 결정됩니다. 예를 들어, 호스트 이름이 `ssl-vpn`이고 도메인 이름이 `cisco.com`이면 `https://ssl-vpn.cisco.com`을 사용합니다.

show saml metadata를 입력할 때 base-url이나 호스트 이름/도메인 이름이 구성되어 있지 않은 경우, 오류가 발생합니다.

단계 **4** IdP와 SP(ASA) 간에 트러스트 포인트를 구성합니다.

trustpoint [**idp** | **sp**] *trustpoint-name*

idp— SAML 어설션을 확인하려면 ASA에 대한 IdP 인증서를 포함하는 트러스트 포인트를 지정합니다.

sp (선택 사항) — ASA의 서명 또는 암호화된 SAML 어설션을 확인하려면 IdP에 대한 ASA(SP)의 인증서를 포함하는 트러스트 포인트를 지정합니다.

trustpoint-name — 이전에 구성한 트러스트 포인트여야 합니다.

단계 **5** (선택 사항) SAML 시간 제한을 구성합니다.

timeout assertion*timeout in seconds*

지정된 경우 이 구성은 NotBefore의 합계와 시간 제한(초 단위)이 NotOnOrAfter 이전인 경우 NotOnOrAfter를 재정의합니다.

지정되지 않은 경우 어설션에서 NotBefore 및 NotOnOrAfter가 유효성을 확인하는 데 사용됩니다.

참고 기존 SAML IdP가 구성되어 있는 터널 그룹의 경우, SAML이 특정 터널 그룹에 대해 다시 활성화되는 경우 webvpn에서 saml idp CLI에 대한 변경 사항은 터널 그룹에만 적용됩니다. 시간 제한을 구성한 후에는 터널 그룹 webvpn 속성에서 saml identity-provider CLI를 다시 발행한 후에만 업데이트된 시간 제한이 적용됩니다.

단계 **6** (선택 사항) SAML 요청에서 서명을 활성화 또는 비활성화(기본 설정)합니다.

signature <value>

참고 2.5.1 SSO로 업그레이드하면 기본 서명 방법이 SHA1에서 SHA256으로 변경되고, *value*를 rsa-sha1, rsa sha256, sha384 rsa 또는 rsa sha512로 입력하여 원하는 서명 방법 옵션을 구성할 수 있습니다.

단계 **7** (선택 사항) IdP가 내부 네트워크인지를 결정하는 플래그를 설정하려면 **internal** 명령을 사용합니다. 그러면 ASA가 게이트웨이 모드에서 작동합니다.

단계 **8** 구성을 보려면 **show webvpn saml idp**를 사용합니다.

단계 **9** **forceauthn**을 사용하면 SAML 인증 요청이 발생하는 경우, IdP(Identity Provider)가 이전의 보안 상황을 사용하지 않고 직접 인증하게 됩니다. 이 설정은 기본값입니다. 따라서 비활성화하려면 **no forceauthn**을 사용합니다.

예

다음 예는 IdP 이름의 salesforce_idp를 구성하고 미리 구성된 트러스트 포인트를 사용합니다.

```
ciscoasa(config)# webvpn
ciscoasa(config-webvpn)#saml idp salesforce_idp

ciscoasa(config-webvpn-saml-idp)#url sign-in
https://asa-dev-ed.my.salesforce.com/idp/endpoint/HttpRedirect
ciscoasa(config-webvpn-saml-idp)#url sign-out
https://asa-dev-ed.my.salesforce.com/idp/endpoint/HttpRedirect

ciscoasa(config-webvpn-saml-idp)#trustpoint idp salesforce_trustpoint
ciscoasa(config-webvpn-saml-idp)#trustpoint sp asa_trustpoint

ciscoasa(config)#show webvpn saml idp
saml idp salesforce_idp
url sign-in https://asa-dev-ed.my.salesforce.com/idp/endpoint/HttpRedirect
url sign-out https://asa-dev-ed.my.salesforce.com/idp/endpoint/HttpRedirect
trustpoint idp salesforce_trustpoint
trustpoint  sp asa_trustpoint
```

다음 웹 페이지는 Onelogin을 위해 URL을 얻는 방법의 예를 보여줍니다.

https://onelogin.zendesk.com/hc/en-us/articles/202767260-Configuring-SAML-for-Clarizen

다음 웹 페이지는 OneLogin에서 URL을 찾을 수 있는 메타데이터를 사용하는 방법의 예입니다.

http://onlinehelp.tableau.com/current/online/en-us/saml_config_onelogin.htm

다음에 수행할 작업

SAML 2.0 서비스 공급자(SP)로 ASA 구성, 410 페이지에 설명된 대로 연결 프로파일에 SAML 인증을 적용합니다.

SAML 2.0 서비스 공급자(SP)로 ASA 구성

SAML SP로 특정 터널 그룹을 구성하려면 이 절차를 수행합니다.

참고 AnyConnect 4.4 또는 4.5를 사용하는 SAML 인증을 사용 중인 경우, ASA 버전 9.7.1.24, 9.8.2.28 또는 9.9.2.1(릴리스 날짜: 2018년 4월 18일)을 구축하는 경우 기본값이 설정된 SAML 동작은 임베디드 브라우저이며 이는 AnyConnect 4.4 및 4.5에서 지원되지 않습니다. 따라서 AnyConnect 4.4 및 4.5 클라이언트가 외부(기본) 브라우저를 사용하는 SAML로 인증하려면 터널 그룹 구성에서 **saml external-browser** 명령을 활성화해야 합니다.

saml external-browser 명령은 AnyConnect 4.6 이상으로 업그레이드하기 위한 마이그레이션 용도로 사용됩니다. 보안 제한으로 인해 AnyConnect 소프트웨어를 업그레이드 하는 동안 일시적인 마이그레이션의 일부로 서만이 솔루션을 사용 합니다. 이 명령은 나중에는 사용되지 않습니다.

시작하기 전에

IdP는 이미 구성되어 있어야 합니다. SAML 2.0 IdP(Identity Provider) 구성, 408 페이지를 참고하십시오.

프로시저

단계 **1** 터널 그룹 webvpn 하위 모드에서 IdP를 할당하려면 saml identify-provider 명령을 사용합니다.

[**no**] **saml identify-provider** *idp-entityID*

idp-entityID — 이전에 구성된 기존 IdP 중 하나여야 합니다.

SAML SP를 비활성화하려면 **no** 형식의 이 명령을 사용하십시오.

단계 **2** 현재 터널 그룹에 대한 SAML SP 기능을 활성화합니다.

authentication saml

SAML 인증 방법은 상호 배타적입니다.

예

```
ciscoasa(config)# webvpn
ciscoasa(config-webvpn)# tunnel-group-list enable
ciscoasa(config)# tunnel-group cloud_idp_onelogin type remote-access
ciscoasa(config)# tunnel-group cloud_idp_onelogin webvpn-attributes
ciscoasa(config-tunnel-webvpn)# authentication saml
ciscoasa(config-tunnel-webvpn)# group-alias cloud_idp enable
ciscoasa(config-tunnel-webvpn)# saml identity-provider
https://app.onelogin.com/saml/metadata/462950
```

SAML 2.0 및 Onelogin 예

Onelogin 정보와 이름 대신 서드파티 SAML 2.0 IdP를 사용하는 이 예를 따르십시오.

1. IdP와는 ASA(SP) 간의 시간 동기화를 설정합니다.

   ```
   ciscoasa(config)# ntp server 209.244.0.4
   ```

2. 서드파티 IdP에서 제공하는 다음 절차에 따라 IdP에서 IdP의 SAML 메타데이터를 가져옵니다.
3. IdP의 서명 인증서를 트러스트 포인트로 가져옵니다.

   ```
   ciscoasa(config)# crypto ca trustpoint onelogin
   ciscoasa(config-ca-trustpoint)# enrollment terminal
   ciscoasa(config-ca-trustpoint)# no ca-check
   ciscoasa(config-ca-trustpoint)# crypto ca authenticate onelogin
   Enter the base 64 encoded CA certificate.
   End with the word "quit" on a line by itself
   quit
   INFO: Certificate has the following attributes:
   Fingerprint:     85de3781 07388f5b d92d9d14 1e22a549
   Do you accept this certificate? [yes/no]: yes
   ```

```
Trustpoint CA certificate accepted.
% Certificate successfully imported
```

4. SP(ASA) 서명 PKCS12를 트러스트 포인트로 가져옵니다.

```
ciscoasa(config)# crypto ca import asa_saml_sp pkcs12 password
Enter the base 64 encoded pkcs12.
End with the word "quit" on a line by itself:
quit
INFO: Import PKCS12 operation completed successfully
```

5. SAML IdP를 추가합니다.

```
ciscoasa(config-webvpn)# saml idp https://app.onelogin.com/saml/metadata/462950
```

6. saml-idp sub-mode 아래에서 속성을 구성합니다.

   IdP 로그인 URL과 로그아웃 URL을 구성합니다.

```
ciscoasa(config-webvpn-saml-idp)# url sign-in
https://ross.onelogin.com/trust/saml2/http-post/sso/462950
ciscoasa(config-webvpn-saml-idp)# url sign-out
https://ross.onelogin.com/trust/saml2/http-redirect/slo/462950
```

   IdP 트러스트 포인트 및 SP 트러스트 포인트를 구성합니다.

```
ciscoasa(config-webvpn-saml-idp)# trustpoint idp onelogin
ciscoasa(config-webvpn-saml-idp)# trustpoint sp asa_saml_sp
```

   클라이언트리스 VPN 기반 URL, SAML 요청 서명 및 SAML 어설션 시간 제한을 구성합니다.

```
ciscoasa(config-webvpn-saml-idp)# base-url https://172.23.34.222
ciscoasa(config-webvpn-saml-idp)# signature
ciscoasa(config-webvpn-saml-idp)# timeout assertion 7200
```

7. 터널 그룹에 사용할 IdP를 구성하고 SAML 인증을 활성화합니다.

```
ciscoasa(config)# webvpn
ciscoasa(config-webvpn)# tunnel-group-list enable
ciscoasa(config)# tunnel-group cloud_idp_onelogin type remote-access
ciscoasa(config)# tunnel-group cloud_idp_onelogin webvpn-attributes
ciscoasa(config-tunnel-webvpn)# authentication saml
ciscoasa(config-tunnel-webvpn)# group-alias cloud_idp enable
ciscoasa(config-tunnel-webvpn)# saml identity-provider
https://app.onelogin.com/saml/metadata/462950
```

8. ASA의 SAML SP 메타데이터를 표시합니다.

   `https://172.23.34.222/saml/sp/metadata/cloud_idp_onelogin`에서 ASA의 SAML SP 메타데이터를 가져올 수 있습니다. URL에서 `cloud_idp_onelogin`는 터널 그룹 이름입니다.

9. 타사 IdP가 제공하는 절차에 따라 타사 IdP에서 SAML SP를 구성합니다.

SAML 2.0 트러블슈팅

debug webvpn saml값을 사용하여 SAML 2.0 동작을 디버깅합니다. 값에 따라 다음 SAML 메시지가 표시됩니다.

- 8 — 오류
- 16 — 경고 및 오류

• 128 또는 255 — 디버그, 경고 및 오류

HTTP 기본 또는 **NTLM** 인증을 사용하는 **SSO** 구성

이 섹션에서는 HTTP 기본 또는 NTLM 인증을 사용하는 단일 로그인에 대해 설명합니다. 이 방법 중 하나 또는 두 가지 모두를 사용하여 SSO를 구현하도록 ASA를 구성할 수 있습니다. **auto-sign-on** 명령은 클라이언트리스 SSL VPN 사용자 로그인 크리덴셜(사용자 이름 및 비밀번호)을 내부 서버에 자동으로 전달하도록 ASA를 구성합니다. **auto-sign-on** 명령을 여러 번 입력할 수 있습니다. ASA는 입력 순서(이전 명령이 우선)에 따라 명령을 처리합니다. IP 주소 및 IP 마스크 또는 URI 마스크 중 하나를 사용하여 로그인 자격 증명을 수신하도록 서버를 지정합니다.

클라이언트리스 SSL VPN 구성, 클라이언트리스 SSL VPN 그룹 정책 모드 또는 클라이언트리스 SSL VPN 사용자 이름 모드 중 하나에서 **auto-sign-on** 명령을 사용합니다. 사용자 이름은 그룹을 교체하고 그룹은 전역을 교체합니다. 다음과 같이 필수 인증 범위가 있는 모드를 선택합니다.

모드	범위
webvpn configuration	모든 전역 클라이언트리스 SSL VPN 사용자입니다.
webvpn group-policy configuration	그룹 정책에서 정의한 클라이언트리스 SSL VPN 사용자의 하위 집합입니다.
webvpn username configuration	클라이언트리스 SSL VPN의 개별 사용자입니다.

예

• NTLM 인증을 사용하여 10.1.1.0에서 10.1.1.255 범위의 IP 주소를 지닌 서버에 대해 클라이언트리스 SSL VPN의 모든 사용자용으로 auto-sign-on을 구성합니다.

```
hostname(config-webvpn)# auto-sign-on allow ip 10.1.1.1 255.255.255.0 auth-type ntlm
```

• 기본 HTTP 인증을 사용하여 URI 마스크 https://*.example.com/*로 정의된 서버에 대해 클라이언트리스 SSL VPN의 모든 사용자용으로 auto-sign-on을 구성합니다.

```
hostname(config-webvpn)# auto-sign-on allow uri https://*.example.com/* auth-type
```

• 기본 또는 NTLM 인증 중 하나를 사용하여 URI 마스크로 정의된 서버에 대해 ExamplePolicy 그룹 정책과 연계된 클라이언트리스 SSL VPN 세션용으로 auto-sign-on을 구성합니다.

```
hostname(config)# group-policy ExamplePolicy attributes
hostname(config-group-policy)# webvpn
hostname(config-group-webvpn)# auto-sign-on allow uri https://*.example.com/* auth-type
 all
```

• HTTP 기본 인증을 사용하여 10.1.1.0에서 10.1.1.255 범위의 IP 주소를 지닌 서버에 대해 사용자 이름인 *Anyuser*용으로 auto-sign-on을 구성합니다.

```
hostname(config)# username Anyuser attributes
hostname(config-username)# webvpn
hostname(config-username-webvpn)# auto-sign-on allow ip 10.1.1.1 255.255.255.0 auth-type
 basic
```

- 인증을 위해 특정 포트 및 영역에 auto-sign-on을 구성합니다.

```
smart-tunnel auto-sign-on host-list [use-domain] [realm realm string] [port port num]
[host host mask | ip address subnet mask]
```

HTTP 양식 프로토콜로 SSO 구성

이 섹션에서는 SSO를 위한 HTTP 양식 프로토콜 사용에 대해 설명합니다. HTTP 양식 프로토콜은 AAA 방법으로 자격을 부여할 수도 있는 SSO 인증에 대한 접근 방식입니다. 이는 클라이언트리스 SSL VPN의 사용자 간에 인증 정보를 교환하고 웹 서버를 인증하기 위한 안전한 방법을 제공합니다. RADIUS 또는 LDAP 서버와 같은 다른 AAA 서버와 함께 사용할 수 있습니다.

ASA는 인증 웹 서버에 대해 클라이언트리스 SSL VPN 사용자를 위한 프록시 역할을 다시 수행하지만 이 경우, 요청에 대해 HTTP 양식 프로토콜 및 POST 메소드를 사용합니다. 양식 데이터를 전송 및 수신하도록 ASA를 구성해야 합니다.

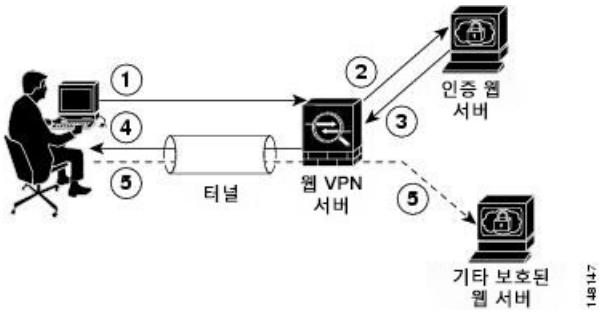
HTTP 프로토콜로 SSO를 올바르게 설정하려면 인증 및 HTTP 프로토콜 교환에 대해 완벽한 지식을 갖추어야 합니다.

공통 프로토콜로서, 다음 조건이 인증에 사용되는 웹 서버 애플리케이션에 대해 충족되는 경우에만 적용됩니다.

- 인증 쿠키를 성공적인 요청에 대해 설정해야 하며 무단 로그온에 대해서는 설정하지 않아야 합니다. 이 경우 ASA는 인증 실패와 성공을 구분할 수 없습니다.

다음 그림에서는 아래에 설명된 SSO 인증 단계를 보여줍니다.

그림 ***9: HTTP*** 양식을 사용하여 ***SSO*** 인증



1. 클라이언트리스 SSL VPN의 사용자는 ASA에서 클라이언트리스 SSL VPN 서버에 로그온하기 위해 먼저 사용자 이름 및 비밀번호를 입력합니다.
2. 클라이언트리스 SSL VPN 서버는 사용자를 위한 프록시 역할을 수행하며 양식 데이터(사용자 이름 및 비밀번호)를 POST 인증 요청을 사용하여 인증 웹 서버에 전달합니다.

3. 인증 웹 서버에서 사용자 데이터를 승인하는 경우, 사용자를 대신하여 데이터가 저장된 클라이언트리스 SSL VPN 서버로 인증 쿠키를 반환합니다.
4. 클라이언트리스 SSL VPN 서버는 사용자에게 터널을 설정합니다.
5. 사용자는 이제 사용자 이름 및 비밀번호를 재입력하지 않고 보호되는 SSO 환경 내에서 다른 웹사이트에 액세스할 수 있습니다.

ASA에서 사용자 이름 및 비밀번호 등의 POST 데이터를 포함하도록 하는 양식 매개변수 구성을 기대하지만 처음에는 웹 서버에 필요한 숨겨진 추가 매개변수를 알 수 없는 경우도 있습니다. 일부 인증 애플리케이션은 사용자에게 표시되지 않고 사용자가 입력할 수도 없는 숨겨진 데이터를 예상합니다. 그러나 중간에서 프록시 역할을 하는 ASA 없이 브라우저에서 웹 서버로 직접 인증 요청을 하는 방법을 통해 인증 웹 서버가 예상하는 숨겨진 매개변수를 발견할 수 있습니다. HTTP 헤더 분석기를 사용하여 웹 서버 응답을 분석하면 다음과 유사한 형식의 숨겨진 매개변수가 나타납니다.

```
<param name>=<URL encoded value>&<param name>=<URL encoded>
```

숨겨진 매개변수 중 일부는 필수 사항이고 나머지는 선택 사항입니다. 웹 서버가 숨겨진 매개변수에 대해 데이터를 요청하는 경우 해당 데이터를 생략하는 인증 POST 요청을 거부합니다. 헤더 분석기는 숨겨진 매개변수가 필수 사항인지 아닌지를 알려주지 않기 때문에 필수 사항인 매개변수를 판단할 때까지 모든 숨겨진 매개변수를 포함시킬 것을 권장합니다.

HTTP 양식 프로토콜을 사용하여 SSO를 구성하려면 다음 작업을 수행해야 합니다.

- 양식 데이터를 수신하고 처리하도록 인증 웹 서버에서 URI(Uniform Resource Identifier)를 구성합니다(**action-uri**).
- 사용자 이름 매개변수를 구성합니다(**user-parameter**).
- 사용자 비밀번호 매개변수를 구성합니다(**password-parameter**).

인증 웹 서버의 요건에 따라 다음 작업을 수행해야 할 수도 있습니다.

- 인증 웹 서버에 사전 로그인 쿠키 교환이 필요한 경우 시작 URL을 구성합니다(**start-url**).
- 인증 웹 서버에 필요한 임의의 숨겨진 인증 매개변수를 구성합니다(**hidden-parameter**).
- 인증 웹 서버에서 설정한 인증 쿠키의 이름을 구성합니다(**auth-cookie-name**).

프로시저

단계 **1** aaa-server-host 구성 모드로 전환합니다.

aaa-server-host

단계 **2** 인증 웹 서버가 요청하는 경우, 인증 웹 서버에서 사전 로그인 쿠키를 검색할 URL을 지정합니다.

start-url

예제**:**

```
hostname(config)# aaa-server testgrp1 protocol http-form
```

```
hostname(config)# aaa-server testgrp1 host 10.0.0.2
hostname(config-aaa-server-host)# start-url http://example.com/east/Area.do?Page-Grp1
```

이 예는 IP 주소가 10.0.0.2인 testgrp1 서버 그룹에서 인증 웹 서버 URL인 http://example.com/east/Area.do?Page-Grp1을 지정합니다.

단계 **3** 인증 웹 서버에서 인증 프로그램에 대한 URI를 지정합니다.

action-uri

예제:

```
http://www.example.com/auth/index.html/appdir/authc/forms/MCOlogin.fcc?TYPE=33554433
&REALMOID=06-000a1311-a828-1185-ab41-8333b16a0008&GUID=&SMAUTHREASON=0&METHOD=GET&SMAGENTNA
ME=$SM$5FZmjnk3DRNwNjk2KcqVCFbIrNT9%2bJ0H0KPshFtg6rB1UV2PxkHqLw%3d%3d&TARGET=https%3A%2F%2F
auth.example.com
```

이 작업 URI를 지정하려면 다음 명령을 입력합니다.

```
hostname(config-aaa-server-host)# action-uri http://www.example.com/auth/index.htm
hostname(config-aaa-server-host)# action-uri l/appdir/authc/forms/MCOlogin.fcc?TYP
hostname(config-aaa-server-host)# action-uri 554433&REALMOID=06-000a1311-a828-1185
hostname(config-aaa-server-host)# action-uri -ab41-8333b16a0008&GUID=&SMAUTHREASON
hostname(config-aaa-server-host)# action-uri =0&METHOD=GET&SMAGENTNAME=$SM$5FZmjnk
hostname(config-aaa-server-host)# action-uri 3DRNwNjk2KcqVCFbIrNT9%2bJ0H0KPshFtg6r
hostname(config-aaa-server-host)# action-uri B1UV2PxkHqLw%3d%3d&TARGET=https%3A%2F
hostname(config-aaa-server-host)# action-uri %2Fauth.example.com
```

URI를 여러 개의 순차적인 행에 입력할 수 있습니다. 행별 최대 문자 수는 255자입니다. 전체 URI에 대한 최대 문자 수는 2048자입니다.

작업 URI에 호스트 이름과 프로토콜을 포함해야 합니다. 이 예에서는 http://www.example.com의 URI 시작 부분에 나타납니다.

단계 **4** HTTP POST 요청에 대해 userid 사용자 이름 매개변수를 구성합니다.

user-parameter

예제:

```
hostname(config-aaa-server-host)# user-parameter userid
```

단계 **5** HTTP POST 요청에 대해 user_password 사용자 비밀번호 매개변수를 구성합니다.

password-parameter

예제:

```
hostname(config-aaa-server-host)# password-parameter user_password
```

단계 **6** 인증 웹 서버와 교환하기 위해 숨겨진 매개변수를 지정합니다.

hidden-parameter

예제:

```
hostname(config)# aaa-server testgrp1 host example.com
hostname(config-aaa-server-host)# hidden-parameter SMENC=ISO-8859-1&SMLOCALE=US-EN&targe
hostname(config-aaa-server-host)# hidden-parameter t=https%3A%2F%2Fwww.example.com%2Femc
hostname(config-aaa-server-host)# hidden-parameter o%2Fappdir%2FAreaRoot.do%3FEMCOPageCo
hostname(config-aaa-server-host)# hidden-parameter de%3DENG&smauthreason=0
```

이 예는 POST 요청에서 가져온 숨겨진 매개변수의 예를 보여줍니다. 이 숨겨진 매개변수는 &로 구분되는 4개의 양식 항목 및 해당 값을 포함합니다. 항목 및 해당 값은 다음과 같습니다.

- 값이 ISO-8859-1인 SMENC
- 값이 US-EN인 SMLOCALE
- 대상(https%3A%2F%2Fwww.example.com%2Femco%2Fappdir%2FAreaRoot.do 값 포함)
- %3FEMCOPageCode%3DENG.
- smauthreason(0 값 포함)

단계 **7** 인증 쿠키 이름을 지정합니다.

auth-cookie-name *cookie-name*

예제:

```
hostname(config-aaa-server-host)# auth-cookie-name SsoAuthCookie
```

이 예는 SsoAuthCookie의 인증 쿠키 이름을 지정합니다.

단계 **8** 터널 그룹 일반 특성 구성 모드로 전환합니다.

tunnel-group general-attributes

단계 **9** 이전 단계에서 구성한 SSO 서버를 사용하도록 터널 그룹을 구성합니다.

authentication-server-group

예제:

```
hostname(config)# tunnel-group testgroup general-attributes
hostname(config-tunnel-general)#authentication-server-group testgrp1
```

이 예는 /testgroup/이라는 터널 그룹이 /testgrp1/"이라는 이름의 SSO 서버를 사용하도록 구성합니다.

단계 **10** AAA 서버 호스트 구성 모드로 전환합니다.

aaa-server-host

단계 **11** 인증 쿠키 이름을 지정합니다.

auth-cookie-name *cookie-name*

예제:

```
hostname(config-aaa-server-host)# auth-cookie-name SsoAuthCookie
```

이 예는 SsoAuthCookie의 인증 쿠키 이름을 지정합니다.

단계 **12** 터널 그룹 일반 특성 모드로 전환합니다.

tunnel-group general-attributes

단계 **13** 이전 단계에서 구성한 SSO 서버를 사용하도록 터널 그룹을 구성합니다.

authentication-server-group group

예제**:**

```
hostname(config)# tunnel-group testgroup general-attributes
hostname(config-tunnel-general)#authentication-server-group testgrp1
```

이 예는 /testgroup/이라는 터널 그룹이 /testgrp1/"이라는 이름의 SSO 서버를 사용하도록 구성합니다.

HTTP 양식 데이터 수집

이 섹션에서는 HTTP 양식 데이터를 발견하고 수집하기 위한 단계를 제시합니다. 인증 웹 서버에 필요한 매개변수를 알 수 없는 경우, 인증 교환을 분석하여 매개변수 데이터를 수집할 수 있습니다.

시작하기 전에

이 단계에서는 브라우저 및 HTTP 헤더 분석기가 필요합니다.

프로시저

단계 **1** 브라우저 및 HTTP 헤더 분석기를 시작하며 ASA를 통과하지 않고 웹 서버 로그인 페이지에 직접 연결합니다.

단계 **2** 웹 서버 로그인 페이지가 브라우저에 로드된 후에 교환할 동안 쿠키가 설정되고 있는지를 판단하려면 로그인 순서를 검사합니다. 웹 서버가 로그인 페이지에 쿠키를 로드한 경우, 이 로그인 페이지 URL을 *start-URL*로 구성합니다.

단계 **3** 사용자 이름 및 비밀번호를 입력하여 웹 서버에 로그온하고 **Enter** 키를 누릅니다. 이 작업에서는 HTTP 헤더 분석기를 사용하여 검사하는 인증 POST 요청을 생성합니다.

호스트 HTTP 헤더 및 본문이 있는 POST 요청의 예는 다음과 같습니다.

```
POST
/emco/myemco/authc/forms/MCOlogin.fcc?TYPE=33554433&REALMOID=06-000430e1-7443-125c
-ac05-83846dc90034&GUID=&SMAUTHREASON=0&METHOD=GET&SMAGENTNAME=$SM$5FZmjnk3DRNwNjk
2KcqVCFbIrNT9%2bJ0H0KPshFtg6rB1UV2PxkHqLw%3d%3d&TARGET=https%3A%2F%2Fwww.example.c
om%2Femco%2Fmyemco%2FHTTP/1.1

Host: www.example.com

(BODY)
```

```
SMENC=ISO-8859-1&SMLOCALE=US-EN&USERID=Anyuser&USER_PASSWORD=XXXXXX&target=https
%3A%2F%2Fwww.example.com%2Femco%2Fmyemco%2F&smauthreason=0
```

단계 **4** POST 요청을 검사하고 프로토콜, 호스트 및 전체 URL을 복사하여 action-uri 매개변수를 구성합니다.

단계 **5** POST 요청 본문을 검사하고 다음을 복사합니다.

a) 사용자 이름 매개변수. 이전의 예에서 이 매개변수는 *anyuser* 값이 아니라 *USERID*입니다.

b) 비밀번호 매개변수. 이전의 예에서 이 매개변수는 *USER_PASSWORD*입니다.

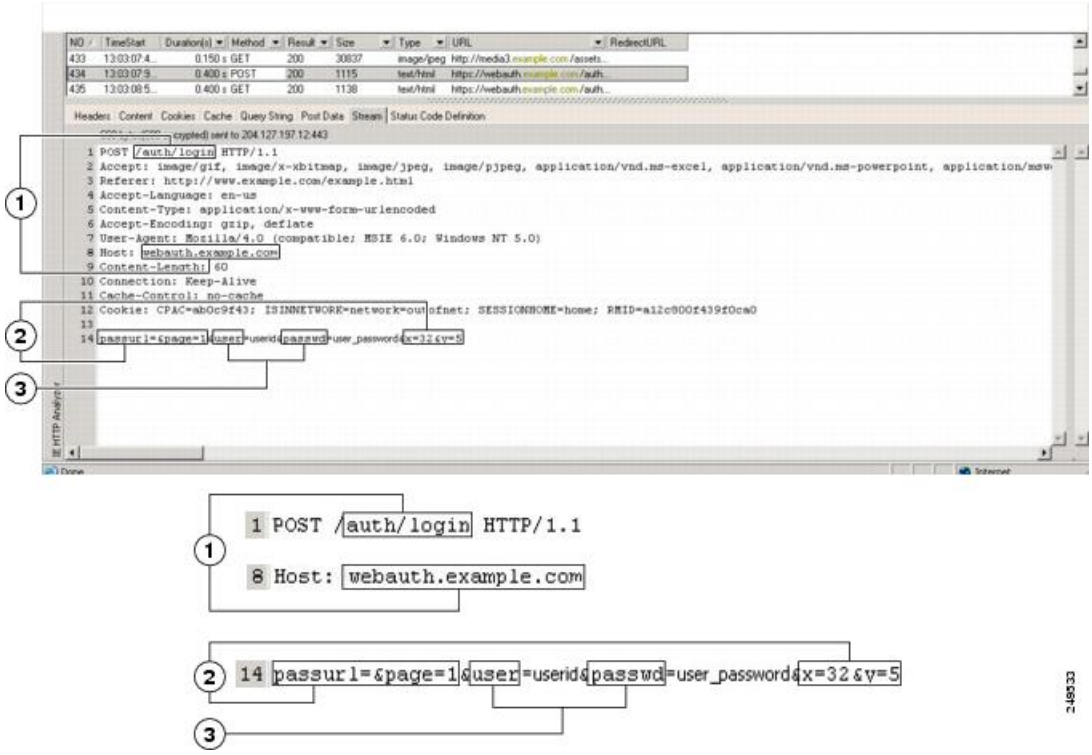
c) 숨겨진 매개변수.

이 매개변수는 사용자 이름과 비밀번호 매개변수를 제외한 POST 본문에 있는 모든 요소입니다. 이전의 예에서 숨겨진 매개변수는 다음과 같습니다.

```
SMENC=ISO-8859-1&SMLOCALE=US-EN&target=https%3A%2F%2Fwww.example.com%2
Femco%2Fmyemco%2F&smauthreason=0
```

다음 그림은 HTTP 분석기의 샘플 출력에서 작업 URI, 숨겨진 매개변수, 사용자 이름 및 비밀번호 매개변수를 강조 표시합니다. 이는 하나의 예일 뿐이며 출력은 웹사이트에 따라 매우 다양하게 나타납니다.

그림 ***10:*** 작업 ***URI,*** 숨겨진 매개변수, 사용자 이름 및 비밀번호 매개변수



1	작업 URI 매개변수
2	숨겨진 매개변수
3	사용자 이름 및 비밀번호 매개변수

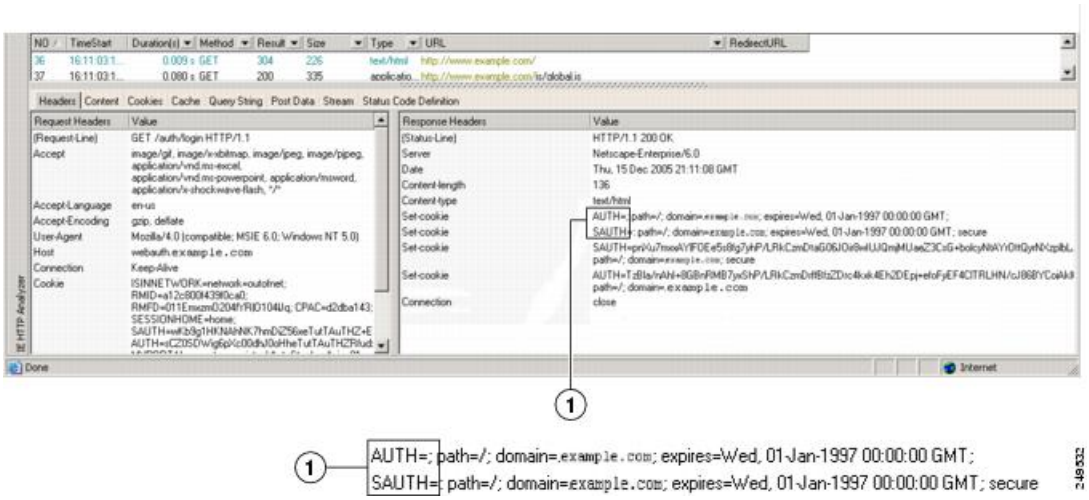
단계 **6** 웹 서버에 성공적으로 로그온한 경우, 브라우저에서 서버가 설정한 세션 쿠키의 이름을 찾으려면 HTTP 헤더 분석기를 사용하여 서버 응답을 검사합니다. **auth-cookie-name** 매개변수입니다.

다음의 서버 응답 헤더에서 세션 쿠키의 이름은 SMSESSION입니다. 값이 아니라 이름이 필요합니다.

```
Set-Cookie:
SMSESSION=yN4Yp5hHVNDgs4FT8dn7+Rwev41hsE49XlKc+1twie0gqnjbhkTkUnR8XWP3hvDH6PZ
PbHIHtWLDKTa8ngDB/lbYTjIxrbDx8WPWwaG3CxVa3adOxHFR8yjD55GevK3ZF4ujgU1lhO6fta0d
SSOSepWvnsCb7IFxCw+MGiw0o88uHa2t4l+SillqfJvcpuXfiIAO06D/gtDF4OOw5YKHEl2KhDEvv
+yQzxwfEz2cl7Ef5iMr8LgGcDK7qvMcvrgUqx68JQOK2+RSwtHQ15bCZmsDU5vQVCvSQWC8OMHNGw
pS253XwRLvd/h6S/tM0k98QMv+i3N8oOdj1V7flBqecH7+kVrU01F6oFzr0zM1kMyLr5HhlVDh7B0
k9wp0dUFZiAzaf43jupD5f6CEkuLeudYW1xgNzsR8eqtPK6t1gFJyOn0s7QdNQ7q9knsPJsekRAH9
hrLBhWBLTU/3B1QS94wEGD2YTuiW36TiP14hYwOlCAYRj2/bY3+lYzVu7EmzMQ+UefYxh4cF2gYD8
RZL2RwmP9JV5148I3XBFPNUw/3V5jf7nRuLr/CdfK3OO8+Pa3V6/nNhokErSgyxjzMd88DVzM41Lx
xaUDhbcmkoHT9ImzBvKzJX0J+o7FoUDFOxEdIqlAN4GNqk49cpi2sXDbIarALp6Bl3+tbB4MlHGH+
0CPscZXqoi/kon9YmGauHyRs+0m6wthdlAmCnvlJCDfDoXtn8DpabgiW6VDTrvl3SGPyQtUv7Wdah
uq5SxbUzjY2JxQnrUtwB977NCzYu2sOtN+dsEReWJ6ueyJBbMzKyzUB4L3i5uSYN50B4PCv1w5KdR
Ka5p3N0Nfq6RM6dfipMEJw0Ny1sZ7ohz3fbvQ/YZ7lw/k7ods/8VbaR15ivkE8dSCzuf/AInHtCzu
Q6wApzEp9CUoG8/dapWriHjNoi4llJOgCst33wEhxFxcWy2UWxs4EZSjsI5GyBnefSQTPVfma5dc/
emWor9vWr0HnTQaHP5rg5dTNqunkDEdMIHfbeP3F90cZejVzihM6igiS6P/CEJAjE;Domain=.exa
mple.com;Path=/
```

다음 그림에서는 HTTP 분석기 출력에 있는 권한 부여 쿠키의 예를 보여줍니다. 이는 하나의 예일 뿐이며 출력은 웹사이트에 따라 매우 다양하게 나타납니다.

그림 ***11:*** 샘플 ***HTTP*** 분석기 출력에 있는 권한 부여 쿠키



1	권한 부여 쿠키

단계 **7** 경우에 따라 서버는 인증의 성공 여부와 관계 없이 동일한 쿠키를 설정할 수 있으며 해당 쿠키는 SSO 목적으로 허용되지 않습니다. 쿠키가 다른지 확인하려면 유효하지 않은 로그인 크리덴셜을 사용하여 1단계부터 6단계까지 반복한 다음 "실패" 쿠키를 "성공" 쿠키와 비교합니다. 이제 필수 매개변수 데이터를 갖추었으므로 HTTP 양식 프로토콜을 사용하여 SSO에 대해 ASA를 구성합니다.

플러그인에 대한 **SSO** 구성

플러그인은 SSO(Single Sign-On: 단일 로그인)를 지원합니다. 플러그인은 입력된 동일한 자격 증명(사용자 이름 및 비밀번호)을 사용하여 클라이언트리스 SSL VPN 세션을 인증합니다. 플러그인은 매크로 대체를 지원하지 않으므로 내부 도메인 비밀번호와 같은 다른 필드나 RADIUS 또는 LDAP 서버의 특성에서 SSO를 수행하는 옵션을 제공하지 않습니다.

플러그인에 대해 SSO 지원을 구성하려면 플러그인을 설치하고 책갈피 항목을 추가하여 서버에 대한 링크를 표시하고 csco_sso=1 매개변수를 사용하여 SSO 지원을 지정합니다. 다음 예는 SSO에 대해 활성화된 플러그인 책갈피를 보여줍니다.

```
ssh://ssh-server/?cisco_sso=1
rdp://rdp-server/?Parameter1=value&Parameter2=value&csco_sso=1
```

매크로 대체를 사용하는 **SSO** 구성

이 섹션에서는 SSO를 위한 매크로 대체 사용에 대해 설명합니다. 매크로 대체를 사용하는 SSO 구성에서는 동적 값을 대체하도록 책갈피에 특정 변수를 삽입할 수 있습니다.

참고 스마트 터널 책갈피는 변수 대체가 아니라 자동 로그온을 지원합니다. 예를 들어 스마트 터널에 대해 구성된 SharePoint 책갈피는 클라이언트리스 SSL VPN에 로그온하는 데 사용한 자격 증명과 동일한 사용자 이름 및 비밀번호 자격 증명을 사용하여 애플리케이션에 로그온합니다. 변수 대체 및 자동 로그온을 동시에 또는 개별적으로 사용할 수 있습니다.

이제 일부 웹 페이지에서 자동 로그온에 대한 매크로 대체와 함께 책갈피를 사용할 수 있습니다. 이전 POST 플러그인 접근 방식은 관리자가 로그인 매크로를 사용하여 POST 책갈피를 지정하고 POST 요청을 게시하기 전에 로드하기 위해 시작 페이지를 수신하도록 생성되었습니다. 이러한 POST 플러그인 접근 방식에서는 요청 시 쿠키 또는 다른 헤더 항목이 필요하지 않습니다. 관리자는 사후 로그인 요청이 전송되는 위치를 지정하는 사전 로드 페이지 및 URL을 결정합니다. 사전 로드 페이지에서는 엔드포인트 브라우저를 자격 증명이 있는 POST 요청을 사용하는 대신 웹 서버 또는 웹 애플리케이션에 따라 전송되는 특정 정보를 가져오도록 할 수 있습니다.

다음 변수(또는 매크로)는 책갈피 및 양식 기반 HTTP POST 작업에서 대체용으로 사용할 수 있습니다.

- CSCO_WEBVPN_USERNAME — 사용자 로그인 ID
- CSCO_WEBVPN_PASSWORD — 사용자 로그인 비밀번호
- CSCO_WEBVPN_INTERNAL_PASSWORD — 사용자 내부(또는 도메인) 비밀번호 이 캐시된 자격 증명은 AAA 서버를 대상으로 인증되지 않습니다. 이 값을 입력하는 경우 보안 어플라이언스는 비밀번호 또는 기본 비밀번호 값이 아닌 자동 로그온에 대한 비밀번호로 이 값을 사용합니다.

참고 GET 기반 http(s) 책갈피에서는 이 3가지 변수 중 어떤 값도 사용할 수 없습니다. POST 기반 http(s)와 cifs 책갈피만 해당 변수를 사용할 수 있습니다.

- CSCO_WEBVPN_CONNECTION_PROFILE — 사용자 로그인 그룹 드롭다운(연결 프로파일 별칭)
- CSCO_WEBVPN_MACRO1 — RADIUS-LDAP VSA(Vendor Specific Attributes: 공급업체별 특성)를 통해 설정합니다. ldap-attribute-map 명령을 통해 LDAP에서 매핑한 경우 이 매크로에 WebVPN-Macro-Substitution-Value1 Cisco 특성을 사용합니다. http://www.cisco.com/en/US/docs/security/asa/asa83/configuration/guide/ref_extserver.html#wp1572118 에서 Active Directory ldap-attribute-mapping 예를 참조하십시오.

  RADIUS를 통한 CSCO_WEBVPN_MACRO1 매크로 대체는 VSA#223에서 수행됩니다.

표 ***21: VSA#223***

WebVPN-Macro-Value1	Y	223	문자열	단일	무제한
WebVPN-Macro-Value2	Y	224	문자열	단일	무제한

  www.cisco.com/email과 같은 값은 특정 DAP 또는 그룹 정책에 대한 https://CSCO_WEBVPN_MACRO1 또는 https://CSCO_WEBVPN_MACRO2 등의 클라이언트리스 SSL VPN 포털에서 동적으로 책갈피를 채웁니다.

- CSCO_WEBVPN_MACRO2 — RADIUS-LDAP VSA(Vendor Specific Attributes: 공급업체별 특성)를 통해 설정합니다. ldap-attribute-map 명령을 통해 LDAP에서 매핑한 경우 이 매크로에 WebVPN-Macro-Substitution-Value2 Cisco 특성을 사용합니다. http://www.cisco.com/en/US/docs/security/asa/asa83/configuration/guide/ref_extserver.html#wp1572118 에서 Active Directory ldap-attribute-mapping 예를 참조하십시오.

  RADIUS를 통한 CSCO_WEBVPN_MACRO2 매크로 대체는 VSA#224에서 수행됩니다.

클라이언트리스 SSL VPN이 엔드 유저 요청(책갈피 또는 게시 양식의 형식으로)에서 6개의 문자열 중 하나를 인지할 때마다 이 문자열을 사용자 특정 값으로 교체한 다음 이 요청을 원격 서버에 전달합니다.

사용자 이름 및 비밀번호의 조회가 ASA에서 실패하는 경우, 빈 문자열이 대체되며 자동 로그인을 사용할 수 없는 경우와 마찬가지로 동작이 다시 변환됩니다.

사용자 이름 및 비밀번호 요건

네트워크에 따라 원격 세션 동안 사용자는 컴퓨터, 인터넷 서비스 공급자, 클라이언트리스 SSL VPN, 메일 또는 파일 서버 또는 기업 애플리케이션 중 하나 또는 모두에 로그온해야 할 수 있습니다. 사용자는 고유한 사용자 이름 및 비밀번호 또는 PIN 같은 다양한 정보가 필요한 여러 가지 다른 상황에서

인증해야 할 수 있습니다. 다음 표에서는 클라이언트리스 SSL VPN 사용자가 알아야 할 사용자 이름 및 비밀번호 유형을 보여줍니다.

로그인 사용자 이름/비밀번호 유형		입력 시기
컴퓨터	컴퓨터 액세스	컴퓨터 시작 시
인터넷 서비스 공급자	인터넷 액세스	인터넷 서비스 공급자에 연결 시
클라이언트리스 SSL VPN	원격 네트워크 액세스	클라이언트리스 SSL VPN 시작
파일 서버	원격 파일 서버 액세스	원격 파일 서버에 액세스하기 위해 클라이언트리스 SSL VPN 파일 브라우징 기능 사용 시
기업 애플리케이션 로그인	방화벽 보호 내부 서버 액세스	내부의 보호되는 웹 사이트에 액세스하기 위해 클라이언트리스 SSL VPN 웹 브라우징 기능 사용 시
메일 서버	클라이언트리스 SSL VPN을 통한 원격 메일 서버 액세스	이메일 메시지 전송 또는 수신 시

보안 팁 전달

사용자에게 항상 툴바에서 로그아웃 아이콘을 클릭하여 클라이언트리스 SSL VPN 세션을 닫도록 알려주십시오. (브라우저 창을 닫아도 세션은 닫히지 않습니다.)

클라이언트리스 SSL VPN은 원격 PC 또는 워크스테이션과 기업 네트워크에 있는 ASA 간의 데이터 전송 보안을 보장합니다. 클라이언트리스 SSL VPN을 사용하는 사용자에게 모든 사이트와의 통신 보안이 보장되지는 않음을 알려주십시오. 사용자가 인터넷 또는 내부 네트워크에 있는 비 HTTPS 웹 리소스에 액세스하는 경우에는 기업 ASA에서 대상 웹 서버로의 통신은 암호화되지 않으므로 개별적인 통신이 아닙니다.

클라이언트리스 SSL VPN 기능을 사용하도록 원격 시스템 구성

이 섹션에서는 클라이언트리스 SSL VPN을 사용하도록 원격 시스템을 설정하는 방법에 대해 설명합니다.

- 클라이언트리스 SSL VPN 정보, 424 페이지
- 클라이언트리스 SSL VPN에 대한 사전 요구 사항, 424 페이지
- 클라이언트리스 SSL VPN 부동 툴바 사용, 425 페이지

사용자 어카운트를 다르게 구성할 수 있으며 다른 클라이언트리스 SSL VPN 기능을 개별 사용자가 사용할 수 있습니다.

클라이언트리스 SSL VPN 정보

다음을 비롯한 지원되는 모든 연결을 사용하여 인터넷에 연결할 수 있습니다.

- 홈 DSL, 케이블 또는 다이얼업
- 공용 키오스크
- 호텔 핫스팟
- 공항 무선 노드
- 인터넷 카페

참고 클라이언트리스 SSL VPN에서 지원되는 웹 브라우저 목록에 대해서는 지원되는 VPN 플랫폼, Cisco ASA 5500 Series의 내용을 참조하십시오.

클라이언트리스 SSL VPN에 대한 사전 요구 사항

- 쿠키는 포트 전달을 통한 애플리케이션 액세스를 위해 브라우저에서 활성화되어야 합니다.
- 클라이언트리스 SSL VPN의 URL이 있어야 합니다. URL은 https://*address* 형식의 https 주소여야 하며 이때 *address*는 SSL VPN이 활성화된 ASA(또는 로드 밸런싱 클러스터) 인터페이스의 IP 주소 또는 DNS 호스트 이름입니다. 예를 들어, https://cisco.example.com입니다.
- 클라이언트리스 SSL VPN 사용자 이름과 비밀번호가 있어야 합니다.

참고 클라이언트리스 SSL VPN은 로컬 인쇄를 지원하지만 기업 네트워크에 있는 프린터에 대해 VPN을 통한 인쇄는 지원하지 않습니다.

클라이언트리스 SSL VPN 부동 툴바 사용

부동 툴바를 사용하면 클라이언트리스 SSL VPN 사용을 간소화할 수 있습니다. 툴바를 사용하여 URL을 입력하고 파일 위치를 찾아보며 기본 브라우저 창에 방해되지 않게 사전 구성된 웹 연결을 선택할 수 있습니다.

부동 툴바는 현재의 클라이언트리스 SSL VPN 세션을 나타냅니다. **Close** 버튼을 클릭하면 ASA는 클라이언트리스 SSL VPN 세션을 닫도록 확인 상자를 표시합니다.

팁 텍스트를 텍스트 필드에 붙여 넣으려면 Ctrl-V를 사용합니다(클라이언트리스 SSL VPN 세션 동안 표시되는 툴바에서는 마우스 오른쪽 버튼 클릭이 해제됩니다.).

참고 팝업을 차단하도록 브라우저를 구성한 경우 부동 툴바를 표시할 수 없습니다.

웹 브라우징

클라이언트리스 SSL VPN의 사용이 모든 사이트와의 통신 보안을 보장하는 것은 아닙니다. 보안 팁 전달, 423 페이지를 참고하십시오.

클라이언트리스 SSL VPN을 통한 웹 브라우징의 모양과 느낌은 사용자에게 익숙하지 않을 수 있습니다. 예를 들면 다음과 같습니다.

- 클라이언트리스 SSL VPN의 제목 표시줄은 각각의 웹 페이지 위에 나타납니다.
- 다음 방법으로 웹사이트에 액세스합니다.
  - 클라이언트리스 SSL VPN 홈 페이지의 **Enter Web Address(**웹 주소 입력**)** 필드에서 URL 입력
  - 클라이언트리스 SSL VPN 홈 페이지의 사전 구성 웹사이트 링크 클릭
  - 앞의 두 가지 방법 중 하나를 통해 액세스되는 웹 페이지에서 링크 클릭
  - 보호 웹사이트에 대한 사용자 이름 및 비밀번호가 필요합니다.

특정 어카운트를 구성하는 방법에 따라 다음과 같은 결과가 발생할 수 있습니다.

- 일부 웹사이트가 차단됨
- 클라이언트리스 SSL VPN 홈 페이지에서 링크로 나타나는 웹사이트만 사용 가능

또한 특정한 어카운트를 구성한 방법에 따라 다음과 같을 수도 있습니다.

- 일부 웹사이트가 차단됨
- 클라이언트리스 SSL VPN 홈 페이지에서 링크로 나타나는 웹사이트만 사용 가능

네트워크 브라우징(파일 관리)

사용자는 조직 네트워크를 통해 자신의 파일을 찾는 방법에 익숙하지 않을 수 있습니다.

참고 복사가 진행 중인 동안 **Copy File to Server** 명령을 중단하거나 다른 화면으로 이동하지 마십시오. 작업을 중단하면 불완전한 파일이 서버에 저장될 수 있습니다.

다음 사항을 기억하는 것이 중요합니다.

- 공유 원격 액세스를 위한 파일 권한을 구성해야 합니다.
- 보호 파일 서버에 대해 서버 이름 및 비밀번호가 있어야 합니다.
- 폴더 및 파일이 위치한 도메인, 작업 그룹 및 서버 이름이 있어야 합니다.

참고 클라이언트리스 SSL VPN을 통해 공유 폴더 및 파일에만 액세스할 수 있습니다.

원격 파일 탐색기 사용

원격 파일 탐색기는 웹 브라우저에서 기업 네트워크를 찾아보는 방법을 사용자에게 제공합니다. 사용자가 Cisco SSL VPN 포털 페이지에서 원격 파일 시스템 아이콘을 클릭하면 트리 및 폴더 보기로 원격 파일 시스템을 표시하는 사용자 시스템에서 애플릿이 실행됩니다.

참고 이 기능을 위해서는 Oracle JRE(Java Runtime Environment)가 사용자 컴퓨터에 설치되고 이 Java가 웹 브라우저에서 활성화되어 있어야 합니다. 원격 파일을 실행하려면 JRE 1.6 이상이 필요합니다.

브라우저에서 사용자는 다음을 수행할 수 있습니다.

- 원격 파일 시스템 찾아보기
- 파일 이름 바꾸기
- 원격 파일 시스템 내에서 원격 및 로컬 파일 시스템 간에 파일 이동 또는 복사
- 파일의 대용량 업로드 및 다운로드

  브라우저에서 파일을 클릭한 후 Operations(작업) > Download(다운로드)를 선택하고 Save(저장) 대화 상자에서 파일을 저장할 위치 및 이름을 제공하여 파일을 다운로드할 수 있습니다.

  대상 폴더를 클릭한 후 Operations(작업) > Upload(업로드)를 선택하고 Open(열기) 대화 상자에서 파일의 위치 및 이름을 제공하여 파일을 업로드할 수 있습니다.

  이 기능에는 다음과 같은 제한 사항이 있습니다.

  - 사용자는 액세스가 허용되지 않는 하위 폴더를 볼 수 없습니다.

- 사용자 액세스가 허용되지 않는 파일은 브라우저에 표시되는 경우에도 이동하거나 복사할 수 없습니다.
- 중첩된 폴더의 최대 깊이는 32입니다.
- 트리 보기는 끌어 놓기 복사 방법을 지원하지 않습니다.
- 파일을 원격 파일 탐색기의 여러 인스턴스 간에 이동하는 경우 모든 인스턴스는 동일한 서버(root 공유)를 탐색 중이어야 합니다.
- 원격 파일 탐색기는 최대 1500개의 파일 및 폴더를 단일 폴더에서 표시할 수 있습니다. 폴더가 이 한계를 초과하는 경우 표시할 수 없습니다.

포트 전달 사용

포트 전달을 사용하려면 클라이언트 애플리케이션을 구성하고 서버의 로컬로 매핑된 IP 주소 및 포트 번호를 사용해야 합니다.

- 사용자는 애플리케이션 사용을 마칠 때 **Close** 아이콘을 클릭하여 항상 애플리케이션 액세스 창을 닫아야 합니다. 창을 제대로 종료하지 못하면 애플리케이션 액세스 또는 애플리케이션 자체가 해제될 수 있습니다.

시작하기 전에

- Mac OS X에서 Safari 브라우저만 이 기능을 지원합니다.
- 클라이언트 애플리케이션이 설치되어 있어야 합니다.
- 브라우저에서 쿠키를 활성화해야 합니다.
- 호스트 파일 수정 시 필요하므로 DNS 이름을 사용하여 서버를 지정하는 경우 PC에서 관리자 액세스 권한이 있어야 합니다.
- Oracle JRE(Java Runtime Environment)가 설치되어 있어야 합니다.

  JRE가 설치되지 않은 경우 사용할 수 있는 사이트로 사용자를 안내하는 팝업 창이 표시됩니다. 드문 경우지만 포트 전달 애플릿이 Java 예외 오류로 인해 실패합니다. 이 경우 다음을 수행하십시오.

  1. 브라우저 캐시를 지우고 브라우저를 닫습니다.
  2. Java 아이콘이 컴퓨터 작업 표시줄에 없는지 확인합니다.
  3. Java의 모든 인스턴스를 닫습니다.
  4. 클라이언트리스 SSL VPN 세션을 설정하고 포트 전달 Java 애플릿을 실행합니다.

- 브라우저에서 JavaScript를 활성화해야 합니다. 기본적으로 활성화되어 있습니다.
- 필요 시 클라이언트 애플리케이션을 구성해야 합니다.

참고 Microsoft Outlook 클라이언트에는 이 구성 단계가 필요하지 않습니다. 비 Windows 클라이언트 애플리케이션은 모두 구성해야 합니다. Windows 애플리케이션에 구성이 필요한지를 판단하려면 Remote Server(원격 서버) 필드의 값을 확인하십시오. 원격 서버 필드에 서버 호스트 이름이 포함된 경우, 클라이언트 애플리케이션을 구성할 필요가 없습니다. 원격 서버 필드에 IP 주소가 포함된 경우, 클라이언트 애플리케이션을 구성해야 합니다.

프로시저

단계 **1** 클라이언트리스 SSL VPN 세션을 시작하고 홈 페이지에서 **Application Access(**애플리케이션 액세스**)** 링크를 클릭합니다. 애플리케이션 액세스 창이 나타납니다.

단계 **2** 이름 열에서 사용할 서버의 이름을 찾은 다음 로컬 열에서 해당 클라이언트 IP 주소 및 포트 번호를 식별합니다.

단계 **3** 이 IP 주소 및 포트 번호를 사용하여 클라이언트 애플리케이션을 구성합니다. 구성 단계는 클라이언트 애플리케이션마다 다릅니다.

참고 클라이언트리스 SSL VPN 세션에서 실행 중인 애플리케이션에서 URL(예: 이메일 메시지의 URL)을 클릭해도 해당 세션에 사이트가 열리지 않습니다. 세션에서 사이트를 열려면 URL을 Enter Clientless SSL VPN(URL) Address(클라이언트리스 SSL VPN(URL) 주소 입력) 필드에 붙여 넣습니다.

포트 전달을 통한 이메일 사용

메일을 사용하려면 클라이언트리스 SSL VPN 홈 페이지에서 애플리케이션을 액세스를 시작합니다. 이제 메일 클라이언트를 사용할 수 있습니다.

참고 IMAP 클라이언트를 사용 중이며 메일 서버 연결이 손실되거나 새 연결을 설정할 수 없는 경우, IMAP 애플리케이션을 닫고 클라이언트리스 SSL VPN을 재시작합니다.

애플리케이션 액세스 및 기타 메일 클라이언트의 요건을 모두 충족해야 합니다.

Microsoft Outlook Express 5.5 및 6.0 버전의 테스트는 완료되었습니다.

웹 액세스를 통한 이메일 사용

다음 이메일 애플리케이션이 지원됩니다.

- Exchange Server 2010에 대한 Microsoft Outlook Web App

OWA에는 Internet Explorer 7 이상 또는 Firefox 3.01 이상이 필요합니다.

- Exchange Server 2007, 2003 및 2000에 대한 Microsoft Outlook Web Access

  최적의 결과를 위해 Internet Explorer 8.x 이상 또는 Firefox 8.x 이상에서 OWA를 사용하십시오.

- Lotus iNotes

참고 웹 기반 이메일 제품이 설치되어 있어야 하고 다른 웹 기반 이메일 애플리케이션도 작동해야 하지만 아직 검증되지 않았습니다.

이메일 프록시를 통한 이메일 사용

다음 레거시 이메일 애플리케이션이 지원됩니다.

- Microsoft Outlook 2000 및 2002
- Microsoft Outlook Express 5.5 및 6.0

클라이언트리스 SSL VPN을 통한 이메일 사용, 354 페이지에서 메일 애플리케이션에 대한 지침과 예를 참조하십시오.

시작하기 전에

SSL 활성화 메일 애플리케이션이 설치되어 있어야 합니다.

ASA SSL 버전을 TLSv1 전용으로 설정하지 마십시오. Outlook 및 Outlook Express는 TLS를 지원하지 않습니다.

보유한 메일 애플리케이션이 제대로 구성되어 있어야 합니다.

다른 SSL 활성화 클라이언트도 작동해야 하지만 이는 검증되지 않았습니다.

스마트 터널 사용

스마트 터널을 사용하는 데 관리자 권한은 필요하지 않습니다.

참고 Java는 포트 전달자로 자동으로 다운로드되지 않습니다.

- 스마트 터널에는 Windows의 ActiveX 또는 JRE와 Mac OS X의 Java Web Start 중 하나가 필요합니다.
- 브라우저에서 쿠키를 활성화해야 합니다.
- 브라우저에서 JavaScript를 활성화해야 합니다.
- Mac OS X는 전면 프록시를 지원하지 않습니다.

- 지원되는 운영 체제 및 브라우저만 사용하십시오.
- TCP 소켓 기반 애플리케이션만 지원됩니다.

20 장

모바일 디바이스를 통한 클라이언트리스 SSL VPN

모바일 디바이스에서 클라이언트리스 SSL VPN 사용

Pocket PC 또는 기타 인증 모바일 디바이스에서 클라이언트리스 SSL VPN에 액세스할 수 있습니다. ASA 관리자 또는 클라이언트리스 SSL VPN 사용자는 인증된 모바일 디바이스에서 클라이언트리스 SSL VPN을 사용하기 위해 특별한 작업을 수행할 필요가 없습니다.

Cisco에서는 다음의 모바일 디바이스 플랫폼을 인증했습니다.

- HP iPaq H4150
- Pocket PC 2003
- Windows CE 4.20.0, 빌드 14053
- PIE(Pocket Internet Explorer)
- ROM 버전 1.10.03ENG
- ROM 날짜: 2004년 7월 16일

클라이언트리스 SSL VPN의 모바일 디바이스 버전에는 몇 가지 차이점이 있습니다.

- 배너 웹 페이지는 클라이언트리스 SSL VPN 팝업 창을 대체합니다.
- 아이콘 막대는 표준 클라이언트리스 SSL VPN 부동 툴바를 대체합니다. 이 막대는 Go(이동), Home(홈) 및 Logout(로그아웃) 버튼을 표시합니다.
- Show Toolbar(툴바 표시) 아이콘은 기본 클라이언트리스 SSL VPN 포털 페이지에 포함되지 않습니다.
- 클라이언트리스 SSL VPN에서 로그아웃하는 즉시 경고 메시지에서 PIE 브라우저를 제대로 닫기 위한 지침을 제공합니다. 이 지침을 준수하지 않고 일반적인 방법으로 브라우저 창을 닫은 경

우, PIE는 클라이언트리스 SSL VPN 또는 HTTPS를 사용하는 보안 웹사이트로부터 연결을 끊지 않습니다.

모바일을 통한 클라이언트리스 **SSL VPN**의 제한 사항

- 클라이언트리스 SSL VPN은 OWA 2000 및 OWA 2003 기본 인증을 지원합니다. 기본 인증이 OWA 서버에 구성되어 있지 않고 클라이언트리스 SSL VPN 사용자가 해당 서버에 액세스하려고 시도하는 경우 액세스가 거부됩니다.
- 지원되지 않는 클라이언트리스 SSL VPN 기능:
  - 애플리케이션 액세스 및 기타 Java 종속 기능
  - HTTP 프록시
  - Citrix Metaframe 기능(PDA에 해당하는 Citrix ICA 클라이언트 소프트웨어가 없는 경우)

21 장

클라이언트리스 SSL VPN 사용자 지정

클라이언트리스 SSL VPN 엔드 유저 설정

이 섹션은 엔드 유저에 대해 클라이언트리스 SSL VPN을 설정하는 시스템 관리자를 위한 내용입니다. 이 섹션에서는 엔드 유저 인터페이스를 사용자 지정하는 방법에 대해 설명하고 원격 시스템을 위한 구성 요구 사항 및 작업을 요약합니다. 이 요약에는 클라이언트리스 SSL VPN을 사용하여 원격 시스템을 시작하기 위해 사용자와 통신하는 정보가 지정되어 있습니다.

엔드 유저 인터페이스 정의

클라이언트리스 SSL VPN 엔드 유저 인터페이스는 일련의 HTML 패널로 구성됩니다. 사용자는 ASA 인터페이스 IP 주소를 https://*address* 형식으로 입력하여 클라이언트리스 SSL VPN에 로그온합니다. 가장 먼저 표시되는 패널은 로그인 화면입니다.

클라이언트리스 SSL VPN 홈 페이지 보기

사용자가 로그인하면 포털 페이지가 열립니다.

홈 페이지에 구성한 클라이언트리스 SSL VPN 기능이 모두 표시되며 이 모양에는 선택한 로고, 텍스트 및 색상이 반영되어 있습니다. 이 샘플 홈 페이지에는 특정 파일 공유 식별을 제외한 모든 사용 가능한 클라이언트리스 SSL VPN 기능이 포함되어 있습니다. 이 페이지를 통해 사용자는 네트워크를 찾아보고 URL을 입력하며 특정 웹 사이트에 액세스하고 애플리케이션 액세스(포트 전달 및 스마트 터널)를 사용하여 TCP 애플리케이션에 액세스할 수 있습니다.

클라이언트리스 SSL VPN Application Access 패널 보기

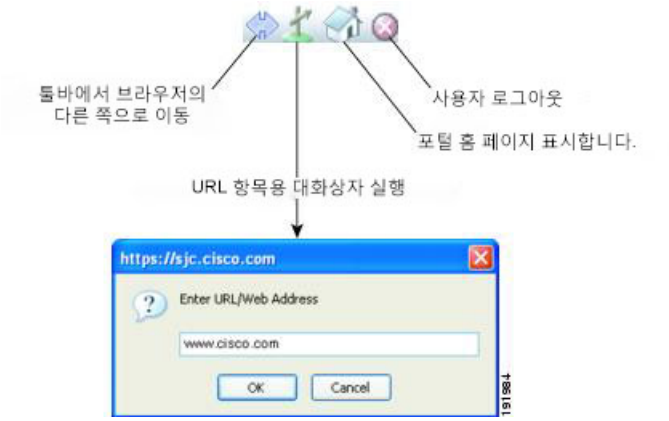
포트 전달 또는 스마트 터널을 시작하기 위해 사용자는 Application Access(애플리케이션 액세스) 상자에서 **Go(**이동**)** 버튼을 클릭합니다. Application Access 창이 열리고 이 클라이언트리스 SSL VPN 연결에 대해 구성된 TCP 애플리케이션이 표시됩니다. 이 패널이 열린 상태에서 애플리케이션을 사용하기 위해 사용자는 일반적인 방식으로 애플리케이션을 시작합니다.

참고 상태 저장 장애 조치는 애플리케이션 액세스를 사용하여 설정된 세션을 그대로 유지하지 않습니다. 사용자는 장애 조치 후 다시 연결해야 합니다.

부동 툴바 보기

다음 그림에 표시된 부동 툴바는 현재의 클라이언트리스 SSL VPN 세션을 나타냅니다.

그림 ***12:*** 클라이언트리스 ***SSL VPN***의 부동 툴바



부동 툴바의 다음 특성에 유의하십시오.

- 툴바를 사용하여 URL을 입력하고 파일 위치를 찾아보며 기본 브라우저 창에 방해되지 않게 사전 구성된 웹 연결을 선택할 수 있습니다.
- 팝업을 차단하도록 브라우저를 구성한 경우 부동 툴바를 표시할 수 없습니다.
- 툴바를 닫으면 ASA에서 클라이언트리스 SSL VPN 세션을 종료하라는 메시지가 표시됩니다.

클라이언트리스 **SSL VPN** 페이지 사용자 지정

클라이언트리스 SSL VPN 사용자에게 표시되는 포털 페이지의 모양을 변경할 수 있습니다. 예를 들어 사용자가 보안 어플라이언스에 연결할 때 표시되는 로그인 페이지, 보안 어플라이언스가 사용자를 인증한 이후에 사용자에게 표시되는 홈 페이지, 사용자가 애플리케이션을 시작할 때 표시되는 애플리케이션 액세스 창 및 사용자가 클라이언트리스 SSL VPN 세션을 로그아웃할 때 표시되는 로그아웃 페이지가 포함됩니다.

포털 페이지를 사용자 지정한 후에 사용자 지정을 저장하고 특정 연결 프로파일, 그룹 정책 또는 사용자에게 이를 적용할 수 있습니다. ASA를 다시 로드하거나 클라이언트리스 SSL을 해제한 다음 활성화할 때까지 변경 사항은 적용되지 않습니다.

개별 사용자 또는 사용자 그룹에 대한 포털 페이지 모양을 변경하도록 보안 어플라이언스가 활성화하여 많은 사용자 지정 개체를 생성하고 저장할 수 있습니다.

사용자 지정 정보

ASA는 맞춤형 개체를 사용하여 사용자 화면의 모양을 정의합니다. 사용자 지정 개체는 원격 사용자에게 표시되는 사용자 지정 가능한 화면의 모든 항목에 대한 XML 태그를 포함하는 XML 파일에서 컴파일됩니다. ASA 소프트웨어에는 원격 PC에 내보낼 수 있는 맞춤형 템플릿이 포함되어 있습니다. 이 템플릿을 수정하고 새 맞춤형 개체로 ASA에 다시 가져올 수 있습니다.

사용자 지정 개체를 내보내면 XML 태그를 포함한 XML 파일이 지정된 URL에 생성됩니다. 사용자 지정 개체 *Template*을 통해 생성된 XML 파일은 빈 XML 태그를 포함하고 있으며 새로운 사용자 지정 개체를 만들기 위한 기본 사항을 제공합니다. 이 개체는 변경하거나 캐시 메모리에서 삭제할 수 없으나 내보내거나 수정하거나 새 맞춤형 개체로 다시 ASA에 가져오는 것은 가능합니다.

사용자 지정 개체, 연결 프로파일 및 그룹 정책

사용자가 처음 연결할 때 연결 프로파일(터널 그룹)에서 식별한 이름이 *DfltCustomization*인 기본 사용자 지정 개체에서 로그온 화면이 어떻게 표시될지 결정됩니다. 연결 프로파일 목록이 활성화되어 있고 사용자가 고유한 사용자 지정이 있는 다른 그룹을 선택하면 화면이 새로운 그룹에 대해 사용자 지정 개체를 반영하도록 변경됩니다.

원격 사용자가 인증되면 그룹 정책에 사용자 지정 개체가 할당되었는지 여부에 따라 화면 모양이 결정됩니다.

사용자 지정 템플릿 내보내기

사용자 지정 개체를 내보낼 때 XML 파일은 지정한 URL에서 생성됩니다. 이름이 *Template*인 사용자 지정 템플릿은 빈 XML 태그를 포함하며 새 사용자 지정 개체를 생성하기 위한 기초를 제공합니다. 이 개체는 변경하거나 캐시 메모리에서 삭제할 수 없으나 내보내거나 수정하거나 새 맞춤형 개체로 다시 ASA에 가져오는 것은 가능합니다.

프로시저

단계 **1** 사용자 지정 개체를 내보내고 XML 태그를 변경합니다.

export webvpn customization

단계 **2** 파일을 새 개체로 가져옵니다.

import webvpn customization

예제**:**

다음은 기본 사용자 지정 개체(DfltCustomization)를 내보내고 *dflt_custom*이라는 이름의 XML 파일을 생성하는 예입니다.

```
hostname# export webvpn customization DfltCustomization tftp://209.165.200.225/dflt_custom
!!!!!!!!!!!!!!!!INFO: Customization object 'DfltCustomization' was exported to
tftp://10.86.240.197/dflt_custom
hostname#
```

사용자 지정 템플릿 수정

이 섹션에는 사용자 지정 템플릿의 콘텐츠를 보여주며 정확한 XML 태그를 신속하게 선택하고 화면에 적용되는 변경을 수행하는 데 도움이 되는 편리한 그림이 수록되어 있습니다.

텍스트 편집기 또는 XML 파일을 수정하는 XML 편집기를 사용할 수 있습니다. 다음 예는 사용자 지정 템플릿의 XML 태그를 보여줍니다. 일부 중복 태그는 더 쉽게 볼 수 있도록 제거되었습니다.

```
<custom>
   <localization>
      <languages>en,ja,zh,ru,ua</languages>
      <default-language>en</default-language>
   </localization>
    <auth-page>
      <window>
          <title-text l10n="yes"><![CDATA[SSL VPN Service</title-text>
      </window>
      <full-customization>
          <mode>disable</mode>
          <url></url>
      </full-customization>
      <language-selector>
        <mode>disable</mode>
        <title l10n="yes">Language:</title>
        <language>
          <code>en</code>
          <text>English</text>
        </language>
        <language>
          <code>zh</code>
          <text>(Chinese)</text>
        </language>
        <language>
          <code>ja</code>
          <text>(Japanese)</text>
        </language>
        <language>
          <code>ru</code>
          <text>(Russian)</text>
        </language>
        <language>
          <code>ua</code>
          <text>(Ukrainian)</text>
        </language>
      </language-selector>
      <logon-form>
          <title-text l10n="yes"><![CDATA[Login</title-text>
          <title-background-color><![CDATA[#666666</title-background-color>
          <title-font-color><![CDATA[#ffffff</title-font-color>
          <message-text l10n="yes"><![CDATA[Please enter your username and
password.</message-text>
          <username-prompt-text l10n="yes"><![CDATA[USERNAME:</username-prompt-text>
          <password-prompt-text l10n="yes"><![CDATA[PASSWORD:</password-prompt-text>
          <internal-password-prompt-text l10n="yes">Internal
Password:</internal-password-prompt-text>
          <internal-password-first>no</internal-password-first>
          <group-prompt-text l10n="yes"><![CDATA[GROUP:</group-prompt-text>
          <submit-button-text l10n="yes"><![CDATA[Login</submit-button-text>
          <title-font-color><![CDATA[#ffffff</title-font-color>
          <title-background-color><![CDATA[#666666</title-background-color>
          <font-color>#000000</font-color>
```

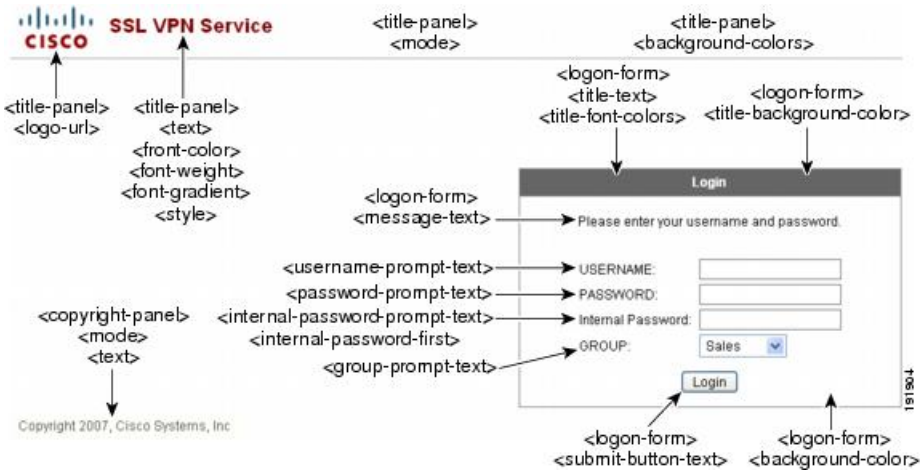
```
            <background-color>#ffffff</background-color>
            <border-color>#858A91</border-color>
        </logon-form>
        <logout-form>
            <title-text l10n="yes"><![CDATA[Logout</title-text>
            <message-text l10n="yes"><![CDATA[Goodbye.<br>

For your own security, please:<br>

<li>Clear the browser's cache

<li>Delete any downloaded files

<li>Close the browser's window</message-text>
            <login-button-text l10n="yes">Logon</login-button-text>
            <hide-login-button>no</hide-login-button>
            <title-background-color><![CDATA[#666666</title-background-color>
            <title-font-color><![CDATA[#ffffff</title-font-color>
            <title-font-color><![CDATA[#ffffff</title-font-color>
            <title-background-color><![CDATA[#666666</title-background-color>
            <font-color>#000000</font-color>
            <background-color>#ffffff</background-color>
            <border-color>#858A91</border-color>
        </logout-form>
        <title-panel>
           <mode>enable</mode>
           <text l10n="yes"><![CDATA[SSL VPN Service</text>
           <logo-url l10n="yes">/+CSCOU+/csco_logo.gif</logo-url>
           <gradient>yes</gradient>
           <style></style>
           <background-color><![CDATA[#ffffff</background-color>
           <font-size><![CDATA[larger</font-size>
           <font-color><![CDATA[#800000</font-color>
           <font-weight><![CDATA[bold</font-weight>
        </title-panel>
        <info-panel>
          <mode>disable</mode>
          <image-url l10n="yes">/+CSCOU+/clear.gif</image-url>
          <image-position>above</image-position>
          <text l10n="yes"></text>
        </info-panel>
        <copyright-panel>
           <mode>disable</mode>
           <text l10n="yes"></text>
        </copyright-panel>
      </auth-page>
      <portal>
        <title-panel>
           <mode>enable</mode>
           <text l10n="yes"><![CDATA[SSL VPN Service</text>
           <logo-url l10n="yes">/+CSCOU+/csco_logo.gif</logo-url>
           <gradient>yes</gradient>
           <style></style>
           <background-color><![CDATA[#ffffff</background-color>
           <font-size><![CDATA[larger</font-size>
           <font-color><![CDATA[#800000</font-color>
           <font-weight><![CDATA[bold</font-weight>
        </title-panel>
        <browse-network-title l10n="yes">Browse Entire Network</browse-network-title>
        <access-network-title l10n="yes">Start AnyConnect</access-network-title>
        <application>
           <mode>enable</mode>
           <id>home</id>
           <tab-title l10n="yes">Home</tab-title>
```

```
   <order>1</order>
</application>
<application>
   <mode>enable</mode>
   <id>web-access</id>
   <tab-title l10n="yes"><![CDATA[Web Applications</tab-title>
   <url-list-title l10n="yes"><![CDATA[Web Bookmarks</url-list-title>
   <order>2</order>
</application>
<application>
   <mode>enable</mode>
   <id>file-access</id>
   <tab-title l10n="yes"><![CDATA[Browse Networks</tab-title>
   <url-list-title l10n="yes"><![CDATA[File Folder Bookmarks</url-list-title>
   <order>3</order>
</application>
<application>
   <mode>enable</mode>
   <id>app-access</id>
   <tab-title l10n="yes"><![CDATA[Application Access</tab-title>
   <order>4</order>
</application>
<application>
   <mode>enable</mode>
   <id>net-access</id>
   <tab-title l10n="yes">AnyConnect</tab-title>
   <order>4</order>
</application>
<application>
   <mode>enable</mode>
   <id>help</id>
   <tab-title l10n="yes">Help</tab-title>
   <order>1000000</order>
</application>
<toolbar>
   <mode>enable</mode>
   <logout-prompt-text l10n="yes">Logout</logout-prompt-text>
   <prompt-box-title l10n="yes">Address</prompt-box-title>
   <browse-button-text l10n="yes">Browse</browse-button-text>
   <username-prompt-text l10n="yes"></username-prompt-text>
</toolbar>
<column>
   <width>100%</width>
   <order>1</order>
</column>
<pane>
   <type>TEXT</type>
   <mode>disable</mode>
   <title></title>
   <text></text>
   <notitle></notitle>
   <column></column>
   <row></row>
   <height></height>
</pane>
<pane>
   <type>IMAGE</type>
   <mode>disable</mode>
   <title></title>
   <url l10n="yes"></url>
   <notitle></notitle>
   <column></column>
   <row></row>
   <height></height>
```

```
        </pane>
        <pane>
           <type>HTML</type>
           <mode>disable</mode>
           <title></title>
           <url l10n="yes"></url>
           <notitle></notitle>
           <column></column>
           <row></row>
           <height></height>
        </pane>
        <pane>
           <type>RSS</type>
           <mode>disable</mode>
           <title></title>
           <url l10n="yes"></url>
           <notitle></notitle>
           <column></column>
           <row></row>
           <height></height>
        </pane>
        <url-lists>
           <mode>group</mode>
        </url-lists>
        <home-page>
           <mode>standard</mode>
           <url></url>
        </home-page>
     </portal>
</custom>
```

다음 그림에서는 로그온 페이지 및 사용자 지정 XML 태그를 보여줍니다. 이러한 모든 태그는 더 높은 수준의 태그인 <auth-page> 안에 중첩됩니다.

그림 ***13:*** 로그온 페이지 및 연계된 ***XML*** 태그



다음 그림은 로그온 페이지에서 사용 가능한 언어 선택기 드롭다운 목록 및 이 기능을 사용자 지정하는 XML 태그를 보여줍니다. 모든 해당 태그는 더 높은 수준의 <auth-page> 태그 안에 중첩됩니다.

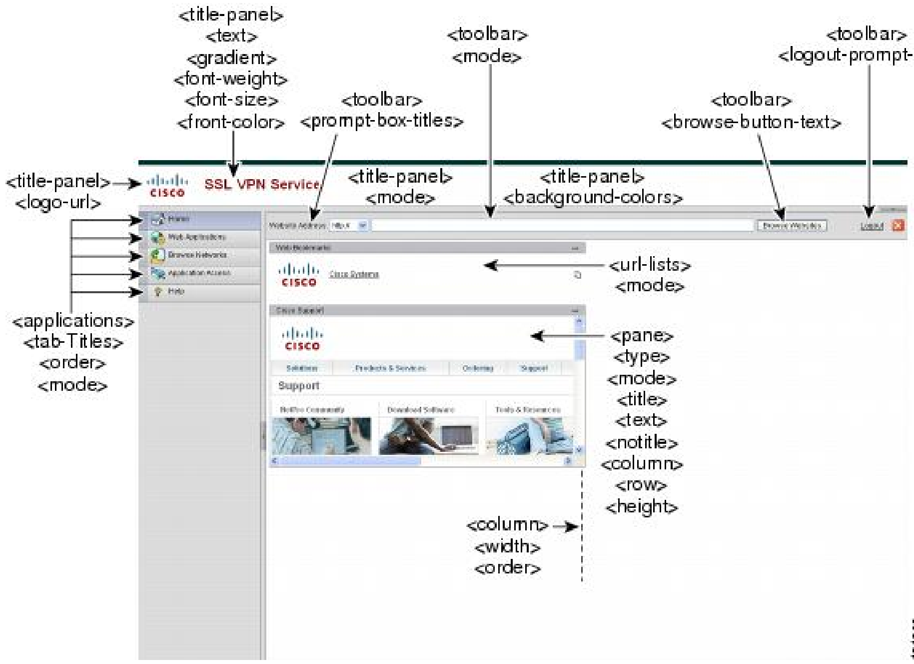
그림 *14:* 로그온 화면의 언어 선택기 및 연계된 ***XML*** 태그

다음 그림은 로그온 페이지에서 사용 가능한 정보 패널 및 이 기능을 사용자 지정하는 XML 태그를 보여줍니다. 이 정보는 로그인 상자의 왼쪽 또는 오른쪽에 나타날 수 있습니다. 해당 태그는 더 높은 수준의 <auth-page> 태그 안에 중첩됩니다.

그림 *15:* 로그온 화면의 정보 패널 및 연계된 ***XML*** 태그

다음 그림에서는 포털 페이지 및 이 기능을 사용자 지정하는 XML 태그를 보여줍니다. 해당 태그는 더 높은 수준의 <auth-page> 태그 안에 중첩됩니다.

그림 16: 포털 페이지 및 연계된 **XML** 태그



사용자 지정 개체 가져오기

XML 파일을 수정 및 저장한 후에는 ASA의 캐시 메모리로 가져옵니다. 맞춤형 개체를 가져올 때 ASA에서는 XML 코드의 유효성을 검사합니다. 코드가 유효한 경우 ASA는 캐시 메모리의 숨겨진 위치에 개체를 저장합니다.

import webvpn customization

다음 예에서는 URL 209.165.201.22/customization에서 사용자 지정 개체 *General.xml*을 가져와서 이름을 *custom1*로 지정하는 방법을 보여줍니다.

```
hostname# import webvpn customization custom1
tftp://209.165.201.22/customization /General.xml
Accessing
tftp://209.165.201.22/customization/General.xml...!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Writing file disk0:/csco_config/97/custom1...
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
329994 bytes copied in 5.350 secs (65998 bytes/sec)
```

연결 프로파일, 그룹 정책 및 사용자에 사용자 지정 적용

맞춤화를 생성한 이후에 **customization** 명령을 사용하여 연결 프로파일(터널 그룹), 그룹 또는 사용자에게 맞춤화를 적용할 수 있습니다. 이 명령을 사용하여 표시되는 옵션은 사용자의 현재 모드에 따라 다릅니다.

참고 포털 페이지를 맞춤화한 이후에 ASA를 다시 로드하거나 클라이언트리스 SSL을 비활성화한 다음 활성화할 때까지 변경 사항은 적용되지 않습니다.

프로시저

단계 **1** 클라이언트리스 SSL VPN 구성 모드로 전환합니다.

webvpn

단계 **2** tunnel-group, group-policy 또는 username 클라이언트리스 SSL VPN 구성으로 전환합니다.

tunnel-group webvpn또는 **group-policy webvpn** 또는**username webvpn**

단계 **3** 연결 프로파일에 적용할 사용자 지정 이름으로 연결 프로파일에 사용자 지정을 적용합니다.

customization *name*

또는 그룹 또는 사용자에 사용자 지정을 적용합니다. 다음 옵션이 포함됩니다.

- **none** 그룹 또는 사용자에 대해 맞춤화를 비활성화하고 값을 상속받는 것을 방지하며 기본 클라이언트리스 SSL VPN 페이지를 표시합니다.
- **value** 그룹 또는 사용자에 대한 맞춤화의 이름입니다.

예제**:**

이 예에서는 tunnel-group 클라이언트리스 SSL VPN 구성 모드로 진입하여 사용자 지정 *cisco*를 연결 프로파일 *cisco_telecommutes*에 대해 활성화합니다.

```
hostname(config)# tunnel-group cisco_telecommuters webvpn-attributes
hostname(tunnel-group-webvpn)# customization cisco
```

이 예에서는 group-policy 클라이언트리스 SSL VPN 구성 모드로 진입하여 보안 어플라이언스에서 사용자 지정 목록을 조회하고, 그룹 정책 *cisco_sales*에 대해 사용자 지정 *cisco*를 활성화합니다.

```
hostname(config)# group-policy cisco_sales attributes
hostname(config-group-policy)# webvpn
hostname(config-username-webvpn)# customization value ?
config-username-webvpn mode commands/options:
Available configured customization profiles:
 DfltCustomization
 cisco
hostname(config-group-webvpn)#customization value cisco
```

이 예에서는 username 클라이언트리스 SSL VPN 구성 모드로 진입하여 맞춤화 *cisco*를 사용자 *cisco_employee*에 대해 활성화합니다.

```
hostname(config)# username cisco_employee attributes
hostname(config-username)# webvpn
hostname(config-username-webvpn)#customization value cisco
```

단계 **4** (선택 사항) (선택 사항) 구성에서 명령을 제거하고 연결 프로필에서 맞춤화를 제거합니다.

[**no**] **customization** *name*

단계 **5** (선택 사항) (선택 사항) 구성에서 명령을 제거하고 기본값으로 되돌립니다.

[**no**] **customization** {**none** | **value** *name*}

단계 **6** 기존 사용자 지정 목록을 보여 줍니다.

customization ?

로그인 화면 고급 사용자 지정

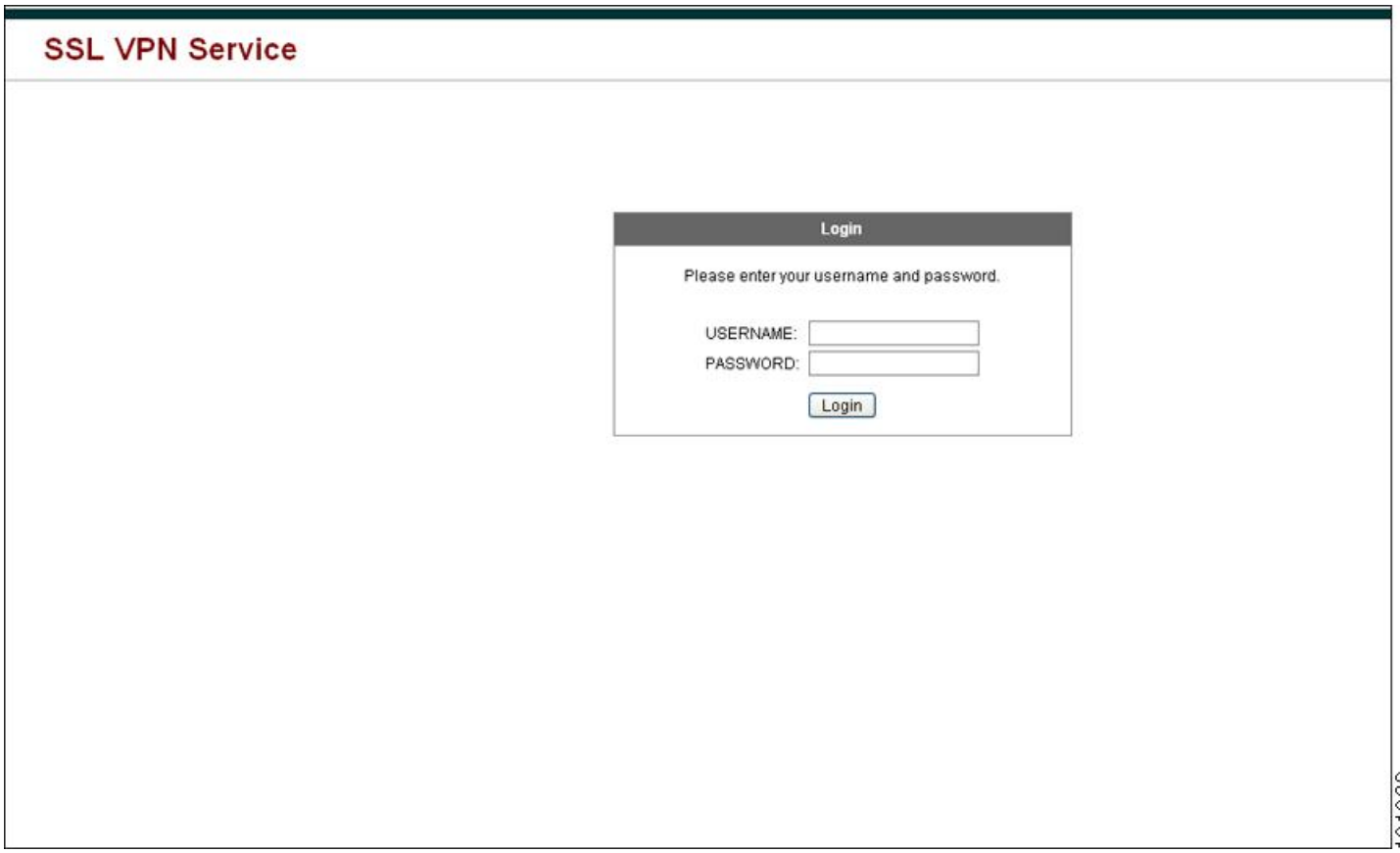
제공되는 로그인 페이지의 특정한 화면 요소를 변경하는 대신 고유한 사용자 지정 로그인 화면을 사용하려는 경우, Full Customization(전체 사용자 지정) 기능을 사용하여 이러한 고급 사용자 지정을 수행할 수 있습니다.

전체 맞춤형을 사용하여 고유한 로그인 화면에 HTML을 제공하고 ASA에서 로그인 양식 및 언어 선택기 드롭다운 목록을 생성하는 함수를 호출하는 Cisco HTML 코드를 삽입합니다.

이 섹션에서는 HTML 코드에 필요한 수정사항 및 코드를 사용하도록 ASA를 구성하는 데 필요한 작업에 대해 설명합니다.

다음 그림은 클라이언트리스 SSL VPN 사용자에게 표시되는 표준 Cisco 로그인 화면을 보여줍니다. 로그인 양식은 HTML 코드로 호출되는 함수를 사용하여 표시됩니다.

그림 ***17:*** 표준 ***Cisco*** 로그인 페이지

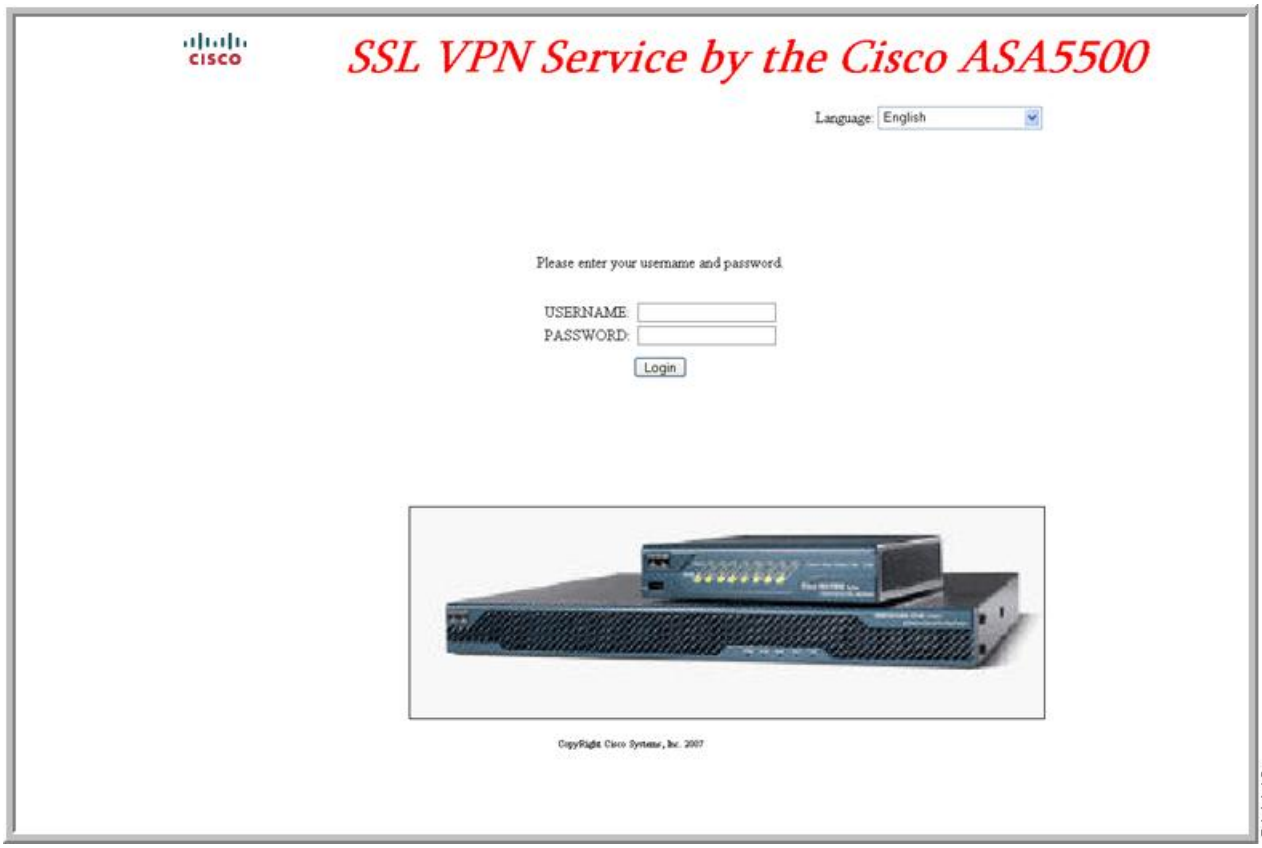


다음 그림에서는 언어 선택기 드롭다운 목록을 보여줍니다. 이 기능은 클라이언트리스 SSL VPN 사용자에 대한 옵션이며 로그인 화면의 HTML 코드에 있는 함수를 사용하여 호출됩니다.

그림 ***18:*** 언어 선택기 드롭다운 목록

다음 그림은 전체 사용자 지정 기능을 통해 활성화된 사용자 지정 로그인 화면의 간단한 예를 보여줍니다.

그림 ***19:*** 로그인 화면의 전체 사용자 지정 예



다음은 HTML 코드의 예이며 다음과 같은 형식으로 표시됩니다.

```
<head>
<meta http-equiv="Content-Type" content="text/html; charset=UTF-8">
<title>New Page 3</title>
<base target="_self">
</head>

<p align="center">
<img border="0" src="/+CSCOU+/cisco_logo.jpg" width="188" height="48"><font face="Snap ITC"
 size="6" color="#FF00FF">
</font><font face="Snap ITC" color="#FF00FF" size="7"> </font><i><b><font color="#FF0000"
size="7" face="Sylfaen"> SSL VPN Service by the Cisco ASA5500</font></b></i></p>

<body onload="csco_ShowLoginForm('lform');csco_ShowLanguageSelector('selector')">

<table>

<tr><td colspan=3 height=20 align=right><div id="selector" style="width:
300px"></div></td></tr>
<tr><td></td><td></td><td></td></tr>
<tr>
<td height="379"></td>
<td height="379"></td>
<td align=middle valign=middle>
<div id=lform >
<p> </p>
```

```
<p> </p>
<p> </p>
<p>Loading...</p>
</div>
</td>
</tr>
<tr>
<td width="251"></td>
<td width="1"></td>
<td align=right valign=right width="800">
<img border="1" src="/+CSCOU+/asa5500.jpg" width="660" height="220" align="middle">
</td></tr>

</table>
```

들여쓰기한 코드는 화면에서 로그인 양식 및 언어 선택기를 삽입합니다. 이 기능은 **csco_ShowLoginForm('lform')** 로그온 양식을 삽입합니다. **csco_ShowLanguageSelector('selector')** 는 언어 선택기를 삽입합니다.

HTML 파일 수정

프로시저

단계 **1** 파일 이름을 logon.inc로 지정합니다. 파일을 가져올 때 ASA는 로그온 화면에서 이 파일 이름을 인식합니다.

단계 **2** /+CSCOU+/를 포함하도록 파일에서 사용되는 이미지의 경로를 수정합니다.

경로 /+CSCOU+/로 표시된 ASA 캐시 메모리의 특정 영역에서 인증을 수행하기 전에 원격 사용자에게 표시되는 파일입니다. 따라서 파일에 있는 각 이미지의 소스에 이 경로가 포함되어야 합니다.

예를 들면 다음과 같습니다.

src="/+CSCOU+/asa5520.gif"

단계 **3** 아래의 특수한 HTML 코드를 삽입합니다. 이 코드에는 화면에 로그인 양식과 언어 선택기를 삽입하는 앞서 설명한 Cisco 함수가 포함되어 있습니다.

```
<body onload="csco_ShowLoginForm('lform');csco_ShowLanguageSelector('selector')">

<table>

<tr><td colspan=3 height=20 align=right><div id="selector" style="width:
300px"></div></td></tr>
<tr><td></td><td></td><td></td></tr>
<tr>
<td height="379"></td>
<td height="379"></td>
<td align=middle valign=middle>
<div id=lform >
<p> </p>
<p> </p>
<p> </p>
<p>Loading...</p>
</div>
```

```
</td>
</tr>
<tr>
<td width="251"></td>
<td width="1"></td>
<td align=right valign=right width="800">
<img border="1" src="/+CSCOU+/asa5500.jpg" width="660" height="220" align="middle">
</td></tr>

</table>
```

책갈피 도움말 사용자 지정

ASA는 선택한 각 책갈피에 대해 애플리케이션 패널에 도움말 콘텐츠를 표시합니다. 이 도움말 파일을 사용자 지정하거나 다른 언어로 도움말 파일을 생성할 수 있습니다. 그런 다음 도움말 파일을 플래시 메모리로 가져와서 후속 세션 동안 표시할 수 있습니다. 또한 이전에 가져온 도움말 콘텐츠 파일을 검색하고, 수정하고, 플래시 메모리로 다시 가져올 수 있습니다.

각 애플리케이션 패널에서는 미리 정해진 파일 이름을 사용하여 고유의 도움말 파일 콘텐츠를 표시합니다. 각각의 예상 위치는 /+CSCOE+/help/*language*/URL에 있으며 이는 ASA의 플래시 메모리 내에 있습니다. 다음 표에서는 사용자가 VPN 세션을 위해 유지 관리할 수 있는 도움말 파일 각각에 대한 세부사항을 보여줍니다.

표 ***22: VPN*** 애플리케이션 도움말 파일

애플리케이션 유형	패널	보안어플라이언스의 플래시 메모리에 있는 도움말 파일의 **URL**	**Cisco**에서 영어로 된 도움말 파일을 제공했습니까**?**
표준	Application Access	/+CSCOE+/help/*language*/app-access-hlp.inc	예
표준	Browse Networks	/+CSCOE+/help/*language*/file-access-hlp.inc	예
표준	AnyConnect Client	/+CSCOE+/help/*language*/net-access-hlp.inc	예
표준	Web Access	/+CSCOE+/help/*language*/web-access-hlp.inc	예
플러그인	MetaFrame Access	/+CSCOE+/help/*language*/ica-hlp.inc	아니요
플러그인	Terminal Servers	/+CSCOE+/help/*language*/rdp-hlp.inc	예
플러그인	Telnet/SSH Servers	/+CSCOE+/help/*language*/ssh,telnet-hlp.inc	예
플러그인	VNC Connections	/+CSCOE+/help/*language*/vnc-hlp.inc	예

*language*는 브라우저에서 렌더링한 언어의 약어입니다. 이 필드는 파일 변환에 사용되지 않으며 파일에서 사용된 언어를 표시합니다. 특정 언어 코드를 지정하려면 브라우저에서 렌더링한 언어 목록에서 언어 약어를 복사합니다. 예를 들어 대화 창은 다음 절차 중 하나를 사용하는 경우 언어 및 연계된 언어 코드를 표시합니다.

- Internet Explorer를 열고 **Tools(**도구**) > Internet Options(**인터넷 옵션**) > Languages(**언어**) > Add(**추가**)**를 선택합니다.
- Mozilla Firefox를 열어 **Tools(**도구**) > Options(**옵션**) > Advanced(**고급**) > General(**일반**)**을 선택하고 Language(언어) 옆에 있는 **Choose(**선택**)**를 클릭한 다음 **Select a language to add(**추가할 언어 선택**)**를 클릭합니다.

플래시 메모리로 도움말 파일 가져오기

프로시저

클라이언트리스 SSL VPN 세션 동안 표시할 도움말 콘텐츠 파일을 플래시 메모리로 가져옵니다.

import webvpn webcontent *destination_url source_url*

- *destination_url*은 보안 어플라이언스 열의 플래시 메모리에 있는 도움말 파일의 URL에 있는 문자열입니다.
- *source_url*은 가져올 파일의 URL입니다. 유효한 접두사는 ftp://, http:// 및 tftp://입니다.

예

이 예에서는 TFTP 서버 209.165.200.225에서 플래시 메모리로 도움말 파일 *app-access-help.inc*를 복사합니다. URL에는 영어를 나타내는 약어 *en*이 포함됩니다.

```
hostname# import webvpn webcontent /+CSCOE+/help/en/app-access-hlp.inc
tftp://209.165.200.225/app-access-hlp.inc
```

이전에 플래시 메모리에서 가져온 도움말 파일 내보내기

프로시저

추가로 수정할 이전에 가져온 도움말 파일을 검색합니다.

export webvpn webcontent *source_url destination_url*

- *source_url*은 "보안 어플라이언스의 플래시 메모리에 있는 도움말 파일의 URL"에 있는 문자열입니다.

- *destination_url*은 **the target URL**입니다. 유효한 접두사는 ftp:// 및 tftp://입니다. 최대 문자 수는 255자입니다.

예

이 예에서는 Browser Networks(네트워크 찾아보기) 패널에 표시된 영어 도움말 파일 file-access-hlp.inc를 TFTP 서버 209.165.200.225로 복사합니다.

```
hostname# export webvpn webcontent /+CSCOE+/help/en/file-access-hlp.inc
tftp://209.165.200.225/file-access-hlp.inc
```

언어 변환 이해

ASA는 전체 클라이언트리스 SSL VPN 세션에 언어 변환을 제공합니다. 언어 변환에는 로그인, 로그아웃 배너와 플러그인 및 AnyConnect와 같은 인증 후에 표시되는 포털 페이지가 포함됩니다. 원격 사용자에게 표시되는 기능 영역 및 메시지는 변환 도메인으로 구성됩니다. 다음 표는 번환 도메인 및 번환되는 기능 영역을 보여줍니다.

언어 변환 도메인 옵션

변환 도메인	변환되는 기능 영역
AnyConnect	Cisco AnyConnect VPN Client의 사용자 인터페이스에 표시되는 메시지입니다.
banners	VPN 액세스가 클라이언트리스 연결에 대해 거부되는 경우 표시되는 메시지
CSD	CSD(Cisco Secure Desktop)의 메시지입니다.
customization	로그인 및 로그아웃 페이지, 포털 페이지 및 사용자가 사용자 지정할 수 있는 모든 메시지
plugin-ica	Citrix 플러그인의 메시지입니다.
plugin-rdp	Remote Desktop Protocol 플러그인의 메시지입니다.
plugin-rdp2	Java 원격 데스크톱 프로토콜 플러그인에 대한 메시지입니다.
plugin-telnet,ssh	Telnet 및 SSH 플러그인의 메시지입니다.
plugin-vnc	VNC 플러그인의 메시지입니다.
PortForwarder	포트 전달 사용자에게 표시되는 메시지

변환 도메인	변환되는 기능 영역
url-list	사용자가 포털 페이지에서 URL 북마크에 대해 지정하는 텍스트입니다.
webvpn	모든 Layer 7, AAA 및 사용자 지정 불가능한 포털 메시지입니다.

ASA에는 표준 기능의 일부인 각 도메인에 대한 변환 테이블 템플릿이 포함되어 있습니다. 플러그인용 템플릿은 플러그인에 포함되어 있으며 고유한 변환 도메인을 정의합니다.

제공하는 URL에서 템플릿의 XML 파일을 생성하는 변환 도메인에 대해 템플릿을 내보낼 수 있습니다. 이 파일의 메시지 필드는 비어 있습니다. 플래시 메모리에 있는 새로운 변환 테이블 개체를 생성하기 위해 이 메시지를 수정하고 템플릿을 가져올 수 있습니다.

또한 기존의 변환 테이블을 내보낼 수 있습니다. 생성한 XML 파일에 이전에 수정한 메시지가 표시됩니다. 동일한 언어 이름의 이 XML 파일을 다시 가져오면 새 버전의 변환 테이블 개체가 생성되고 이전 메시지를 덮어씁니다.

일부 템플릿은 정적이지만 일부는 ASA의 구성에 기초하여 변경됩니다. 클라이언트리스 사용자에 대해 URL 책갈피, 포털 페이지, 로그온 및 로그아웃 페이지를 맞춤화할 수 있으므로 **ASA generates the customization** 및 **url-list**는 변환 도메인 템플릿을 동적으로 생성하고 템플릿은 자동으로 이 기능 영역의 변경 사항을 반영합니다.

변환 테이블을 생성한 후, 그룹 정책 또는 사용자 특성을 생성하고 적용하는 사용자 지정 개체에 사용할 수 있습니다. AnyConnect 변환 도메인을 예외로 하면 변환 테이블에 아무런 영향을 주지 않으며, 사용자 지정 개체를 생성하고 해당 개체에 사용할 변환 테이블을 식별하며 그룹 정책 또는 사용자에 대한 사용자 지정을 지정할 때까지 메시지가 사용자 화면에서 변환되지 않습니다. AnyConnect 도메인에 대한 변환 테이블 변경 사항은 AnyConnect 클라이언트 사용자에게 바로 표시됩니다.

변환 테이블 생성

다음과 같이 단일 상황 모드 또는 다중 상황 모드 두 가지에서 변환 테이블을 생성할 수 있습니다.

프로시저

단계 **1** 컴퓨터로 변환 테이블 템플릿을 내보냅니다.

export webvpn translation-table

예제**:**

이 예에서는 사용 가능한 변환 테이블 템플릿을 보여 주고 사용자 지정 도메인에 대해 내보냅니다. 이렇게 하면 클라이언트리스 SSL VPN 세션에서 사용자에게 표시되는 메시지가 영향을 받습니다. 생성된 XML 파일의 이름은 *portal*(사용자 지정)이며 빈 메시지 필드를 포함합니다.

```
hostname# show import webvpn translation-table
Translation Tables' Templates:
customization
```

```
AnyConnect

PortForwarder
url-list
webvpn
Citrix-plugin
RPC-plugin
Telnet-SSH-plugin
VNC-plugin

Translation Tables:

hostname#  export webvpn translation-table customization template
tftp://209.165.200.225/portal
```

단계 **2** 변환 테이블 XML 파일을 수정합니다.

예제**:**

이 예에서는 *portal*로 내보낸 템플릿의 일부를 보여줍니다. 이 출력의 끝부분에는 사용자가 클라이언트리스 SSL VPN 세션을 설정할 때 포털 페이지에 표시되는 메시지에 대한 메시지 ID 필드(msgid) 및 메시지 문자열 필드(msgstr)가 포함되어 있습니다. 전체 템플릿에는 다음과 같이 여러 쌍의 메시지 필드가 포함되어 있습니다.

```
# Copyright (C) 2006 by Cisco Systems, Inc.
#
#, fuzzy
msgid ""
msgstr ""
"Project-Id-Version: ASA\n"
"Report-Msgid-Bugs-To: vkamyshe@cisco.com\n"
"POT-Creation-Date: 2007-03-12 18:57 GMT\n"
"PO-Revision-Date: YEAR-MO-DA HO:MI+ZONE\n"
"Last-Translator: FULL NAME <EMAIL@ADDRESS>\n"
"Language-Team: LANGUAGE <LL@li.org>\n"
"MIME-Version: 1.0\n"
"Content-Type: text/plain; charset=UTF-8\n"
"Content-Transfer-Encoding: 8bit\n"

#: DfltCustomization:24 DfltCustomization:64
msgid "Clientless SSL VPN Service"
msgstr ""
```

단계 **3** 변환 테이블을 가져옵니다.

import webvpn translation-table

예제**:**

이 예에서는 XML 파일을 가져옵니다. *es-us*는 미국에서 사용되는 스페인어의 약어입니다.

```
hostname# import webvpn translation-table customization language es-us
tftp://209.165.200.225/portal
hostname# !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
hostname# show import webvpn translation-table
Translation Tables' Templates:
AnyConnect
PortForwarder
```

```
customization
keepout
url-list
webvpn
Citrix-plugin
RPC-plugin
Telnet-SSH-plugin
VNC-plugin

Translation Tables:
es-us customization
```

AnyConnect 도메인에 대해 변환 테이블을 가져오는 경우 변경 사항이 즉시 적용됩니다. 다른 도메인에 대해 변환 테이블을 가져오는 경우, 사용자 지정 개체를 생성하고 해당 개체에 사용할 변환 테이블을 식별하고 그룹 정책 또는 사용자에 대해 사용자 지정 개체를 지정합니다.

사용자 지정 개체의 언어 참조

이 섹션에서는 사용자 지정 템플릿을 내보내고 수정하여 사용자 지정 개체로 가져오고 참조할 수 있는 방법에 대해 설명합니다.

시작하기 전에

사용자 지정 개체에 대해 이 변환 테이블을 올바르게 호출하려면 이 테이블을 동일한 이름을 사용하여 미리 가져와야 합니다. 이 이름은 브라우저의 언어 옵션과 호환되어야 합니다.

프로시저

단계 **1** 맞춤형 템플릿을 수정할 수 있는 위치의 URL로 내보냅니다.

export webvpn customization template

이 예에서는 템플릿을 내보내고 지정된 URL에서 사본 *sales*를 만듭니다.

```
hostname# export webvpn customization template tftp://209.165.200.225/sales
```

단계 **2** 사용자 지정 템플릿에 있는 XML 코드의 2개 영역은 변환 테이블과 관련이 있습니다. 사용자 지정 템플릿을 수정하고 이전에 가져온 변환 테이블을 참조합니다.

이 예에서는 사용할 변환 테이블을 지정합니다.

- XML 코드의 <languages> 태그 뒤에는 변환 테이블의 이름이 옵니다. 이 예에서는 en, ja, zh, ru 및 ua입니다.
- <default-language> 태그는 ASA에 연결할 때 원격 사용자에게 처음으로 표시되는 언어를 지정합니다. 위의 코드 예에서 기본 언어는 영어입니다.

```
<localization>
      <languages>en,ja,zh,ru,ua</languages>
      <default-language>en</default-language>
   </localization>
```

이 예는 언어 선택기 표시에 영향을 미치며, 언어 선택기를 활성화하고 사용자 지정하는 <language selector> 태그 및 관련 <language> 태그를 포함하고 있습니다.

- 태그의 <language-selector> 그룹에 언어 선택기 표시를 활성화하고 비활성화하는 <mode> 태그와 <title> 언어를 나열하는 드롭다운 상자의 제목을 지정하는 태그가 포함되어 있습니다.
- 태그의 <language> 그룹은 언어 선택기 드롭다운 상자에 표시된 언어 이름을 특정 변환 테이블에 매핑하는 <code> 및 <text> 태그를 포함합니다.

```
<auth-page>
     ....
         <language-selector>
            <mode>enable</mode>
            <title l10n="yes">Language:</title>
          <language>
             <code>en</code>
             <text>English</text>
          </language>
          <language>
            <code>es-us</code>
            <text>Spanish</text>
          </language>
       </language-selector>
```

단계 **3** 변경 후 파일을 저장합니다.

단계 **4** 사용자 지정 템플릿을 새 개체로 가져옵니다.

import webvpn customization

예제**:**

단계 **5** 새로운 사용자 지정 개체 *sales*를 표시합니다.

show import webvpn customization

예제**:**

```
hostname# import webvpn customization sales tftp://209.165.200.225/sales
hostname# !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
```

사용자 지정 개체를 사용하도록 그룹 정책 또는 사용자 특성 변경

이 섹션에서는 특정 그룹 또는 사용자에 대해 변경 사항을 활성화하는 방법에 대해 설명합니다.

프로시저

단계 **1** 클라이언트리스 SSL VPN 구성 모드로 전환합니다.

webvpn

단계 **2** group-policy 클라이언트리스 SSL VPN 구성 모드로 전환합니다.

group-policy webvpn

단계 **3** 맞춤형 개체를 활성화합니다.

customization

예

이 예에서는 그룹 정책 sales에서 활성화된 사용자 지정 개체 sales를 보여줍니다.

```
hostname(config)# group-policy sales attributes
hostname(config-group-policy)# webvpn
hostname(config-group-webvpn)# customization value sales
```

22 장

클라이언트리스 SSL VPN 문제 해결

애플리케이션 액세스 사용 시 호스트 파일 오류 복구

애플리케이션 액세스를 방해할 수 있는 호스트 파일 오류를 방지하기 위해 애플리케이션 액세스 사용을 마치면 Application Access(애플리케이션 액세스) 창을 올바르게 닫습니다. 이렇게 하려면 닫기 아이콘을 클릭합니다.

애플리케이션 액세스가 비정상적으로 종료되는 경우 `hosts` 파일은 클라이언트리스 SSL VPN 사용자 지정 상태로 유지됩니다. 클라이언트리스 SSL VPN은 hosts.webvpn 파일을 검색하여 다음에 애플리케이션 액세스를 시작하는 상태를 확인합니다. 파일을 발견한 경우, `Backup HOSTS File Found` 오류 메시지가 나타나고 애플리케이션 액세스가 일시적으로 해제됩니다.

애플리케이션 액세스를 잘못 종료하면 원격 액세스 클라이언트/서버 애플리케이션이 불안정한 상태로 남습니다. 클라이언트리스 SSL VPN을 사용하지 않고 이 애플리케이션을 시작하려고 하는 경우, 제대로 작동하지 않을 수 있습니다. 이 경우 정상적으로 연결된 호스트를 사용하지 못할 수 있습니다. 이러한 상황은 일반적으로 집에서 원격으로 애플리케이션을 실행하는 경우, 컴퓨터를 종료하기 전에 애플리케이션 액세스 창을 종료하지 못하고 나중에 사무실에서 애플리케이션을 실행하려고 시도하는 경우 발생할 수 있습니다.

Application Access(애플리케이션 액세스) 창을 제대로 닫지 않은 경우 다음 오류가 발생할 수 있습니다.

- 다음에 애플리케이션 액세스를 시작하려고 시도하는 경우, 애플리케이션 액세스가 해제되고 `Backup HOSTS File Found` 오류 메시지가 표시될 수 있습니다.
- 애플리케이션을 로컬로 실행 중인 경우에도 애플리케이션이 해제되거나 제대로 작동하지 않을 수 있습니다

이러한 오류는 부적절한 방법으로 애플리케이션 액세스 창을 종료하는 경우 발생할 수 있습니다. 예를 들면 다음과 같습니다.

- 애플리케이션 액세스 사용 중에 브라우저 충돌
- 애플리케이션 액세스 사용 중에 정전 또는 시스템 종료 발생
- 작업 중에 애플리케이션 액세스 창을 최소화한 다음, 창이 활성화되어 있는 상태(단, 최소화된 상태)에서 컴퓨터 종료

호스트 파일 이해

로컬 시스템의 호스트 파일은 IP 주소를 호스트 이름에 매핑합니다. 애플리케이션 액세스를 시작하는 경우, 클라이언트리스 SSL VPN은 클라이언트리스 SSL VPN 특정 항목을 추가하여 이 호스트 파일을 수정합니다. Application Access(애플리케이션 액세스) 창을 올바르게 닫아 애플리케이션 액세스를 중지하면 이 파일이 원래 상태로 되돌아갑니다.

애플리케이션 액세스 호출 전...	호스트 파일은 원래 상태입니다.
애플리케이션 액세스 시작 시....	• 클라이언트리스 SSL VPN은 호스트 파일을 hosts.webvpn에 복사한 다음 백업을 생성합니다. • 클라이언트리스 SSL VPN은 클라이언트리스 SSL VPN 특정 정보를 삽입하여 호스트 파일을 수정합니다.
애플리케이션 액세스 중지 시...	• 클라이언트리스 SSL VPN은 백업 파일을 `hosts` 파일에 복사한 다음 호스트 파일을 원래 상태로 복원합니다. • 클라이언트리스 SSL VPN은 hosts.webvpn을 삭제합니다.
애플리케이션 액세스 완료 후...	호스트 파일은 원래 상태입니다.

참고 Microsoft 안티스파이웨어 소프트웨어는 포트 전달 Java 애플릿이 호스트 파일을 변경하는 것을 차단합니다. 안티스파이웨어 소프트웨어를 사용 중인 경우 호스트 파일 변경사항을 허용하는 방법에 대해서는 www.microsoft.com을 참조하십시오.

클라이언트리스 SSL VPN을 사용하여 호스트 파일 자동으로 재구성

원격 액세스 서버에 연결할 수 있는 경우, 다음 단계에 따라 호스트 파일을 다시 구성하고 애플리케이션에 액세스와 애플리케이션을 모두 다시 활성화합니다.

프로시저

단계 **1** 클라이언트리스 SSL VPN을 시작하고 로그인합니다.

Applications Access(애플리케이션 액세스**)** 링크를 클릭합니다.

단계 **2** 다음 옵션 중 하나를 선택합니다.

- **Restore from backup(**백업에서 복원**)** — 클라이언트리스 SSL VPN이 정상 종료를 강제로 실행합니다. hosts.webvpn 백업 파일을 `hosts` 파일에 복사하여 이 파일을 원래 상태로 복원한 다음 hosts.webvpn을 삭제합니다. 그런 다음 애플리케이션 액세스를 다시 시작해야 합니다.
- **Do Nothing(**작업 수행 안 함**)** — 애플리케이션 액세스를 시작하지 않습니다. 원격 액세스 홈 페이지가 다시 표시됩니다.
- **Delete backup(**백업 삭제**)** — 클라이언트리스 SSL VPN이 hosts.webvpn 파일을 삭제하여 호스트 파일이 해당 클라이언트리스 SSL VPN 사용자 지정 상태가 됩니다. 원래 `hosts` 파일 설정이 손실됩니다. 그런 다음 클라이언트리스 SSL VPN 사용자 지정 호스트 파일을 새 원본으로 사용하여 애플리케이션 액세스가 시작됩니다. 호스트 파일 설정이 손실되어도 문제가 없는 경우에만 이 옵션을 선택합니다. 애플리케이션 액세스가 잘못 종료된 이후에 직접 또는 사용하는 프로그램에서 호스트 파일을 수정한 경우, 다른 옵션 중 하나를 선택하거나 호스트 파일을 수동으로

호스트 파일 수동 재구성

현재 위치에서 원격 액세스 서버에 연결할 수 없거나 호스트 파일을 사용자 지정했으며 수정사항이 손실되는 것을 원치 않는 경우, 다음 단계에 따라 호스트 파일을 다시 구성하고 애플리케이션에 액세스와 애플리케이션을 모두 다시 활성화합니다.

프로시저

단계 **1** 호스트 파일을 찾아 수정합니다. 가장 일반적인 위치는 c:\windows\sysem32\drivers\etc\hosts입니다.

단계 **2** 다음 문자열을 포함하는 행이 있는지 확인: `# added by WebVpnPortForward` 이 문자열을 포함하는 행이 있는 경우, 호스트 파일이 클라이언트리스 SSL VPN에 맞춤화되어 있는 것입니다. 호스트 파일이 클라이언트리스 SSL VPN 사용자 지정 파일인 경우, 다음 예와 유사합니다.

```
server1 # added by WebVpnPortForward
server1.example.com invalid.cisco.com # added by WebVpnPortForward
server2 # added by WebVpnPortForward
server2.example.com invalid.cisco.com # added by WebVpnPortForward
server3 # added by WebVpnPortForward
server3.example.com invalid.cisco.com # added by WebVpnPortForward

# Copyright (c) 1993-1999 Microsoft Corp.
#
# This is a sample HOSTS file used by Microsoft TCP/IP for Windows.
#
```

```
# This file contains the mappings of IP addresses to hostnames. Each
# entry should be kept on an individual line. The IP address should
# be placed in the first column followed by the corresponding hostname.
# The IP address and the hostname should be separated by at least one
# space.
#
# Additionally, comments (such as these) may be inserted on individual
# lines or following the machine name denoted by a '#' symbol.
#
# For example:
#
#      102.54.94.97     cisco.example.com          # source server
#       38.25.63.10     x.example.com              # x client host

123.0.0.1       localhost
```

단계 **3** `# added by WebVpnPortForward` 문자열을 포함하는 행을 삭제합니다.

단계 **4** 파일을 저장하고 닫습니다.

단계 **5** 클라이언트리스 SSL VPN을 시작하고 로그인합니다.

단계 **6** **Application Access(**애플리케이션 액세스**)** 링크를 클릭합니다.

WebVPN 조건부 디버깅

원격 액세스 VPN에서 실행 중인 다중 세션에서는 지정된 로그의 크기 때문에 트러블슈팅이 어려울 수 있습니다. **debug webvpn condition** 명령을 사용하여 더 정확하게 디버그 프로세스를 대상으로 필터를 설정할 수 있습니다.

debug webvpn condition { **group** *name* | **p-ipaddress** *ip_address* [{ **subnet** *subnet_mask* | **prefix** *length*}] | **reset** | **user** *name*}

여기서 각 항목은 다음을 나타냅니다.

- 그룹 정책(터널 그룹 또는 연결 프로파일 이외)의 **group** *name* 필터.
- 클라이언트의 공용 IP 주소에 대한 **p-ipaddress** *ip_address* [{ **subnet** *subnet_mask* | **prefix** *length*}] 필터. 서브넷 마스크(IPv4용) 또는 접두사(IPv6용)는 선택 사항입니다.
- **reset** 모든 필터 재설정. **no debug webvpn condition** 명령을 사용하여 특정 필터를 끌 수 있습니다.
- 사용자 이름을 기준으로 하는 **user** *name* 필터.

조건을 여러 개 구성하는 경우 조건이 결합되어(AND로 처리되어) 모든 조건이 충족될 경우에만 디버그가 표시됩니다.

조건 필터를 설정한 후 기본 **debug webvpn** 명령을 사용하여 디버그를 켭니다. 조건을 설정하는 것만으로 디버그가 활성화되지는 않습니다. 현재 디버깅 상태를 보려면 **show debug** 및 **show webvpn debug-condition** 명령을 사용합니다.

ASA VPN에서 여러 세션을 실행 중인 경우 단일 사용자 세션 트러블슈팅이 복잡해집니다. 조건부 디버깅은 필터 조건 설정에 따라 특정 세션의 로그 확인을 활성화합니다. SAML, WebVPN 요청/응답, Anyconnect는 조건부 디버깅을 지원하는 모듈입니다.

참고 IPv4 및 IPv6 서브넷에 대한 "any, any" 지원이 제공됩니다.

다음은 사용자 jdoe에 대해 조건부 디버그를 활성화하는 예를 보여줍니다.

```
asa3(config)# debug webvpn condition user jdoe

asa3(config)# show webvpn debug-condition
INFO: Webvpn conditional debug is turned ON
INFO: User name filters:
INFO: jdoe

asa3(config)# debug webvpn
INFO: debug webvpn  enabled at level 1.

asa3(config)# show debug
debug webvpn  enabled at level 1
INFO: Webvpn conditional debug is turned ON
INFO: User name filters:
INFO: jdoe
```

데이터 캡처

CLI 캡처 명령을 사용하여 클라이언트리스 SSL VPN 세션에서 올바르게 표시되지 않는 웹사이트에 대한 정보를 기록할 수 있습니다. 이 데이터는 Cisco 고객 지원 엔지니어가 문제를 해결하는 데 도움이 됩니다.

사전 요구 사항

클라이언트리스 SSL VPN 캡처를 활성화하면 보안 어플라이언스의 성능에 영향을 미칩니다. 따라서 문제 해결에 필요한 캡처 파일을 만든 후에는 캡처를 해제해야 합니다.

캡처 파일 만들기

프로시저

단계 **1** 클라이언트리스 SSL VPN에 대한 캡처 유틸리티를 시작하고 user2에 대한 트래픽을 파일에 캡처하는 hr이라는 이름의 캡처 파일을 만듭니다.

capture capture_name type webvpn user webvpn_username

*capture_name*은 캡처에 할당한 이름으로, 캡처 파일의 이름 앞에도 추가됩니다.

*webvpn_user*는 캡처하기 위해 일치시킬 사용자 이름입니다.

예제:

```
hostname# capture hr type webvpn user user2
WebVPN capture started.
   capture name   hr
   user name      user2
hostname# no capture hr
```

단계 **2** (선택 사항) 사용자가 로그인하여 클라이언트리스 SSL VPN 세션을 시작한 후 캡처 유틸리티에서 패킷을 캡처하는 것을 중지합니다. 캡처 유틸리티는 *capture_name.zip* 파일을 생성하며 이 파일은 비밀번호 **koleso**를 사용하여 암호화됩니다.

no capture capture_name

단계 **3** 이 .zip 파일을 Cisco Systems로 전송하거나 Cisco TAC 서비스 요청에 첨부합니다.

단계 **4** *koleso* 비밀번호를 사용하여 파일의 압축을 풉니다.

브라우저를 사용하여 캡처 데이터 표시

프로시저

단계 **1** 클라이언트리스 SSL VPN에 대한 캡처 유틸리티를 시작합니다.

capture capture_name type webvpn user webvpn_username

- *capture_name*은 캡처에 할당한 이름으로, 캡처 파일의 이름 앞에도 추가됩니다.
- *webvpn_user*는 캡처하기 위해 일치시킬 사용자 이름입니다.

단계 **2** (선택 사항) 사용자가 로그인하여 클라이언트리스 SSL VPN 세션을 시작한 후 캡처 유틸리티에서 패킷을 캡처하는 것을 중지합니다.

no capture capture_name

단계 **3** 브라우저를 열고 hr이라는 이름의 캡처를 스니퍼 형식으로 표시합니다.

https://**asdm_enabled_interface_of_the_security_appliance**:*port*/**admin/capture/***capture_name*/pcap

예제:

```
https://192.0.2.1:60000/admin/capture/hr/pcap
```

클라이언트리스 **SSL VPN** 세션 쿠키 보호

외부 애플리케이션뿐만 아니라 Flash 애플리케이션 및 Java 애플릿과 같은 내장된 개체는 일반적으로 기존 세션 쿠키를 기반으로 서버와 함께 작동합니다. 이러한 애플리케이션은 초기화될 때 일부 JavaScript를 사용하여 브라우저에서 쿠키를 가져옵니다. 클라이언트리스 SSL VPN 세션 쿠키에 httponly 플래그를 추가하면 클라이언트 쪽 스크립트가 아닌 브라우저에만 세션 쿠키가 표시되므로, 세션 공유가 불가능해집니다.

시작하기 전에

- 활성 클라이언트리스 SSL VPN 세션이 없는 경우에만 VPN 세션 쿠키 설정을 변경합니다.
- **show vpn-sessiondb webvpn** 명령을 사용하여 클라이언트리스 SSL VPN 세션의 상태를 확인합니다.
- 모든 클라이언트리스 SSL VPN 세션에서 로그아웃하려면 **vpn-sessiondb logoff webvpn** 명령을 사용합니다.
- 다음 클라이언트리스 SSL VPN 기능은 **http-only-cookie** 명령이 활성 상태일 때 작동하지 않습니다.
  - Java 플러그인
  - Java 재작성기
  - 포트 전달
  - 파일 브라우저
  - 데스크톱 애플리케이션(예: MS Office 애플리케이션)을 필요로 하는 Sharepoint 기능
  - AnyConnect 웹 실행
  - Citrix Receiver, XenDesktop 및 Xenon
  - 기타 비 브라우저 기반 애플리케이션 및 브라우저 플러그인 기반 애플리케이션

서드파티에서 Javascript와 같은 클라이언트 측 스크립트를 통해 클라이언트리스 SSL VPN 세션 쿠키에 액세스하는 것을 방지하려면 다음 단계를 수행합니다.

프로시저

클라이언트리스 SSL VPN 세션 쿠키에 대한 httponly 플래그를 활성화합니다. 기본적으로 활성화되어 있습니다.

http-only-cookie

예제**:**

```
hostname(config)# webvpn
hostname(config-webvpn)# http-only-cookie
```

참고 Cisco TAC에서 조언한 경우에만 이 명령을 사용합니다. 지침 섹션에 나와 있는 클라이언트리스 SSL VPN 기능은 경고 없이 작동하지 않으므로 이 명령을 사용하면 보안 위험에 노출됩니다.