Stealthwatch® System

하드웨어 컨피그레이션 가이드

(Stealthwatch System v6.9.0용)

컨피그레이션 가이드: **Stealthwatch System v6.9.0** 어플라이언스

문서 작성 날짜: 2017년 7월 6일

Cisco 상표

목 차

1

소개

개요

이 가이드에서는 다음의 Stealthwatch® System 하드웨어를 구성하는 방법에 관해 설명합니다.

- SMC(Stealthwatch Management Console)
- Stealthwatch Flow Collector™
- Stealthwatch Flow Sensor™
- UDP Director™

이 가이드에서는 *Stealthwatch System 하드웨어 설치 가이드*의 지침에 따라 하드웨어를 이미 설치했다고 가정합니다.

VE(Virtual Edition) 제품의 컨피그레이션에 대해서는 가상 어플라이언스(SMC VE 및 Flow Collector VE, Flow Sensor VE 및 UDP Director VE)의 설치 및 컨피그레이션 가이드를 참조하십시오.

이 가이드에 대한 자세한 내용과 필요한 경우에 지원 팀에 문의하는 방법을 알아보려면 이 장을 자세히 읽어 보십시오. 이 장은 다음 섹션으로 구성되어 있습니다.

대상 독자

이 가이드의 주요 독자는 모든 Stealthwatch 실제 어플라이언스를 구성해야 하는 관리자입니다.

Stealthwatch 하드웨어 구성 요소

Stealthwatch System은 네트워크 성능 및 보안을 개선하기 위해 네트워크에 대한 정보를 수집, 분석 및 제공하는 여러 하드웨어 구성 요소로 구성됩니다. 이 섹션에서는 주요 Stealthwatch 구성 요소에 관해 설명합니다.

SMC(Stealthwatch Management Console)는 Stealthwatch의 제어 센터입니다. SMC는 시스템의 모든 다양한 구성 요소를 관리, 조정, 구성 및 조직합니다. SMC 클라이언트 소프트웨어를 사용하면 웹 브라우저 액세스가 가능한 모든 로컬 컴퓨터에서 SMC의 사용하기 편리한 GUI(graphical user interface)에 액세스할 수 있습니다. 클라이언트 GUI를 통해 엔터프라이즈 전반의 중요한 세그먼트에 대한 실시간 보안 및 네트워크 정보에 쉽게 액세스할 수 있습니다.

SMC는 다음의 기능을 제공합니다.

- 최대 25개의 Stealthwatch Flow Collector 지원
- 분산된 호스트 행동 데이터베이스에 대한 액세스 제공
- 여러 동시 사용자 지원
- 정기적인 보고를 자동화하는 보고서 스케줄러 제공
- 관련 직원 및 여러 서드파티 시스템에 직접 전달하는 이벤트 제공
- Syslog와 Stealthwatch 행동 분석을 통해 얻은 인텔리전스 간 연결 지원
- 트래픽 시각화를 지원하는 그래픽 차트 제공
- 문제 해결을 위한 드릴다운 분석 제공
- 통합된 맞춤형 보고서 제공
- 보안 침입 실시간 알림

Flow Collector

Stealthwatch Flow Collector for NetFlow는 비용 효과적인 행동 기반 네트워크 보호를 제공하기 위해 NetFlow, cFlow, J-Flow, Packeteer 2, NetStream 및 IPFIX 데이터를 수집합니다. Flow Collector for sFlow는 sFlow 데이터를 수집합니다.

Flow Collector는 엔드 투 엔드 보호를 제공하고 지리적으로 분산된 네트워크의 성능을 향상할 수 있도록 여러 네트워크 또는 네트워크 세그먼트에서 고속 네트워크 행동 데이터를 집계합니다.

Flow Collector는 데이터를 수신할 때 패킷 암호화 또는 프래그멘테이션과 관계없이 알려지거나 알려지지 않은 공격, 내부 오용 또는 잘못 구성된 네트워크 디바이스를 식별합니다. Stealthwatch가 행동을 식별하면 시스템은 그러한 행동 유형에 대해 구성한 작업이 있는 경우 해당 작업을 수행할 수 있습니다.

Flow Collector는 다음의 기능을 제공합니다.

- 모델에 따라 Flow Collector 4000까지 최대 1,000,000개의 호스트에서 초당 최대 120,000개의 플로우 레코드 처리
- Flow Collector 5000 Series는 4000개가 넘는 플로우 내보내기 디바이스를 사용하여 수백만 개의 호스트에서 초당 최대 240,000개의 플로우 처리 가능
- 플로우 데이터를 플로우 내보내기 디바이스에서 수신

- 프로세스의 중복을 제거하고 양방향 플로우 저장
- 호스트 프로파일, 호스트 쌍 데이터, Concern Index™(관심 지표) 이벤트, 인터페이스 데이터, 호스트 그룹 데이터, VM 데이터 및 TopN 통계 생성 및 저장
- 도메인 컨피그레이션 데이터 저장
- Stealthwatch Management Console로 알림 전달
- 최대 5개의 완화 디바이스 지원

Flow Sensor

Stealthwatch Flow Sensor는 SPAN(Switch Port Analyzer), 미러링 포트 또는 이더넷 TAP (Test Access Port)에 플러그인한다는 점에서 기존의 패킷 캡처 어플라이언스 또는 IDS와 유사하게 동작하는 네트워크 어플라이언스입니다. Flow Sensor는 다음의 네트워크 영역에 대한 가시성을 강화해 줍니다.

- 플로우 내보내기를 사용할 수 없는 경우.
- 플로우 내보내기를 사용할 수 있지만, 성능 메트릭 및 패킷 데이터에 대해 더욱 심층적인 가시성을 얻고자 하는 경우.

Flow Sensor를 NetFlow v9 지원 또는 IPFIX 지원 Flow Collector로 직접 연결함으로써 NetFlow에서 중요하고 자세한 트래픽 통계를 얻을 수 있습니다. 또한 Flow Sensor를 Stealthwatch Flow Collector for NetFlow와 함께 사용하면 성능 메트릭 및 행동 지표에 대한 상세 정보도 제공됩니다. 이러한 플로우 성능 지표는 네트워크 또는 서버 측 애플리케이션에서 시작된 모든 왕복 레이턴시에 대한 인사이트를 제공합니다.

Flow Sensor는 패킷 레벨 가시성을 제공하므로 TCP 세션에 대한 RTT(Round-Trip Time), SRT(Server Response Time) 및 패킷 손실을 계산할 수 있습니다. NetFlow용 Stealthwatch Flow Collector에 전송하는 NetFlow 레코드에 이러한 추가 필드가 모두 포함되어 있습니다.

UDP Director

UDP Director는 고속의 고성능 UDP 패킷 복제기입니다. UDP Director는 NetFlow, sFlow, syslog 또는 SNMP(Simple Network Management Protocol) 재배포에 매우 유용합니다. 연결되지 않은 UDP 애플리케이션에서 데이터를 수신한 다음, 이를 여러 대상에 다시 전송하고, 필요한 경우 데이터를 복제합니다.

Identity 디바이스

Stealthwatch System은 Cisco ISE-PIC를 비롯해 Identity 디바이스인 Cisco ISE(Identity Services Engine)를 포함합니다. 이러한 디바이스는 사용자 ID 데이터베이스에서 사용자 인증 정보를 수동적으로 가져와 사용자 이름과 IP 주소를 매핑합니다. SMC는 다수의 ID 어플라이언스를 완벽하게 관리합니다.

다음 표를 사용하여 Stealthwatch 어플라이언스를 구성하는 데 필요한 설정을 기록하십시오.

설정	SMC	Flow Collector	Flow Sensor	UDP Director	Identity 디바이스
호스트 이름					
IP 주소	192.168.1.11*	192.168.1.4*	192.168.1.7*	192.168.1.2*	192.168.1.100*
서브넷 마스크					
게이트웨이					
DNS 서버					
NTP 서버					
메일 릴레이					

*이것은 기본 IP 주소입니다. Flow Collector sFlow 기본값은 192.168.1.5입니다. Flow Collector 5000 Series 데이터베이스의 기본값은 192.168.1.15입니다.

또한, 다음 설정을 사용할 수 있습니다.

포트 내보내기 플로우 데이터(보통 2055) _____

SNMP 읽기 전용 커뮤니티 라우터 문자열 _____
_____.

이 가이드 사용 방법

소개 내용 외에도 이 가이드는 다음과 같은 장으로 분류되어 있습니다.

장	설명
시스템 구성	트래픽 데이터 처리를 시작하기 위해 어플라이언스를 구성하는 방법
통신 확인	SMC가 NetFlow 데이터를 수신하도록 설정하고 이를 확인하는 방법 및 SLIC Threat Feed 기능을 설정하는 방법
Identity 디바이스 추가	Identity 디바이스를 추가하는 방법
SLIC Threat Feed 기능	SMC 클라이언트에서 SLIC Threat Feed 기능

장	설명
활성화	을 활성화하는 방법

약어

이 가이드에는 다음 약어가 나와 있습니다.

약어	정의
DNS	Domain Name System(서비스 또는 서버)
dvPort	Distributed Virtual Port(분산된 가상 포트)
ESX	Enterprise Server X(엔터프라이즈 서버 X)
GB	Gigabyte(기가바이트)
IDS	Intrusion Detection System(침입 탐지 시스템)
IPS	Intrusion Prevention System(침입 방지 시스템)
IT	Information Technology(정보 기술)
MTU	Maximum Transmission Unit(최대 전송 단위)
NTP	Network Time Protocol(네트워크 타이밍 프로토콜)
OVF	Open Virtualization Format
SMC	Stealthwatch Management Console
1TB	Terabyte(테라바이트)
UUID	Universally Unique Identifier(범용 고유 식별자)
VDS	vNetwork Distributed Switch(가상 네트워크 분산형 스위치)
VE	Virtual Edition(가상 버전)
VLAN	Virtual Local Area Network
VM	Virtual Machine(가상 머신)

기타 리소스

이 가이드 외에도 다음과 같은 문서 및 온라인 자료를 유용하게 사용할 수 있습니다.

관련 문서

Stealthwatch 어플라이언스와 설치 및 컨피그레이션에 대한 정보를 확인할 수 있는 Stealthwatch 문서를 참조하십시오. Stealthwatch 제품에 대한 정보는 Cisco Stealthwatch 온라인을 참조하십시오.

추가 정보는 Stealthwatch 고객 커뮤니티 웹 사이트(http://community.lancope.com)에서 확인할 수 있습니다. 웹 사이트에 대한 로그인 액세스 권한이 없는 경우, 액세스 권한을 요청하는 이메일을 지원 팀에 보내주십시오.

Lancope 블로그

Lancope의 *Inside the Threat* 블로그(http://www.lancope.com/blog/)에서는 NetFlow, NetFlow 업계, 새로운 Stealthwatch 기능에 대한 다양한 정보와 더불어 Stealthwatch 사용에 관한 유용한 정보를 제공합니다.

지능형 사이버 보안을 위한 Lancope 리소스 & 툴

Stealthwatch에 대한 자세한 정보를 확인하려면 지능형 사이버 보안을 위한 Lancope 리소스 & 툴 사이트(https://www.lancope.com/resources)를 방문하십시오. 여기에는 온라인 비디오 라이브러리, 백서 및 웹 세미나와 같은 리소스가 포함되어 있습니다.

지원 팀에 문의

기술 지원이 필요하면 다음 방법 중 하나를 선택하십시오.

- 현지 Cisco 파트너에게 문의하십시오.
- +1800-838-6574로 연락하십시오.
- Stealthwatch 고객 커뮤니티 웹 사이트(http://community.lancope.com)에서 지원 양식을 사용하여 케이스를 제출하십시오.

문서 피드백

이 문서와 관련하여 의견이 있으시면 support@lancope.com으로 문의해 주십시오. 의견을 보내 주시면 감사하겠습니다.

2

시스템 구성

개요

이 장에서는 트래픽 데이터 처리를 시작하기 위해 어플라이언스를 구성하는 절차에 관해 설명합니다. 이 장에 나와 있는 단계를 완료하면 설치 및 컨피그레이션 프로세스가 완료됩니다.

계속 진행하기 전에 필요한 정보를 확인하려면 1페이지의 "소개"에 있는 체크리스트를 참조하십시오.

프로세스 개요

Stealthwatch System 구성에는 다음 절차를 완료하는 과정이 포함됩니다. 이 장에서 다음 절차를 살펴봅니다.

1. 개별 어플라이언스 구성
2. 시스템 구성
3. 어플라이언스 관리 인터페이스를 통한 컨피그레이션

개별 어플라이언스 구성

모든 어플라이언스의 초기 컨피그레이션은 Appliance Setup Tool(어플라이언스 설정 툴)을 사용하여 수행됩니다. 처음 어플라이언스에 액세스하면 어플라이언스 설정 툴이 나타납니다. 시스템 설정에 따라 UDP Director보다 먼저 Flow Sensor 및 Flow Collector를 구성해야 하며 마지막으로 SMC를 구성해야 합니다. SMC의 초기 설정을 완료하면 시스템 설정 툴이 열려서 Stealthwatch System을 구성할 수 있습니다.

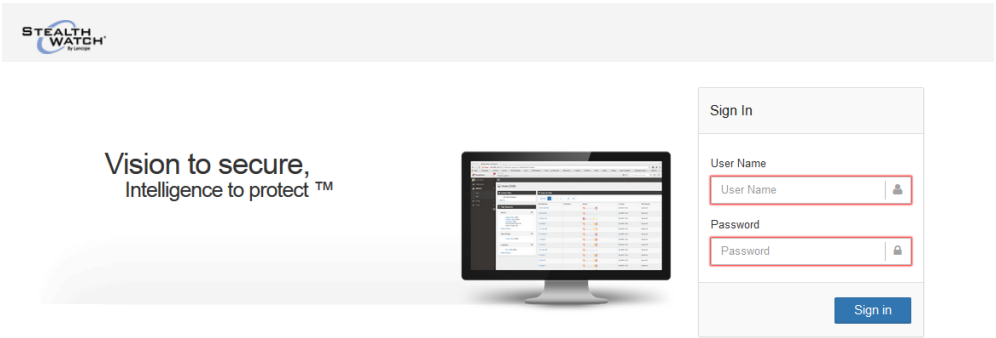
시작하기 전에 1페이지의 "소개"의 사전 요구사항 섹션에 자세히 나와 있는 정보를 수집합니다.

참고: 사용자 화면은 환경에 따라 여기에 표시된 화면과 약간 다르게 보일 수 있습니다.

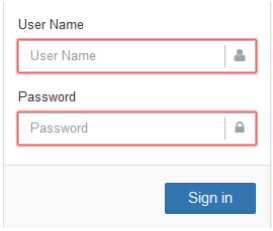
어플라이언스를 구성하려면 다음 단계를 완료합니다.

1. 브라우저의 주소 필드에 **https://**를 입력한 후에 어플라이언스의 IP 주소를 입력한 다음 **Enter** 키를 누릅니다.
2. 관리자 로그인 페이지가 열립니다. **admin** 및 **lan411cope**(두 가지 모두 대/소문자 구분)를 입력한 다음 **Login(로그인)**을 클릭합니다. 5단계로 이동합니다.

3. SMC의 경우, 랜딩 페이지가 열립니다.



로그인하려면 다음을 수행합니다.



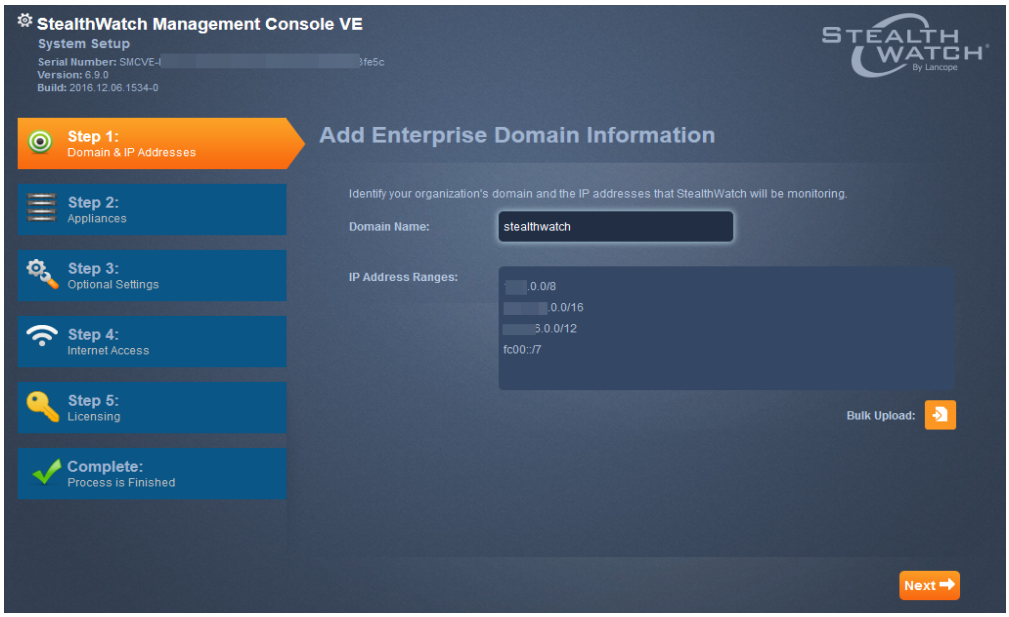
a. User Name(사용자 이름) 필드에 **admin**을 입력합니다.

b. Password(비밀번호) 필드에 **lan411cope**를 입력합니다.

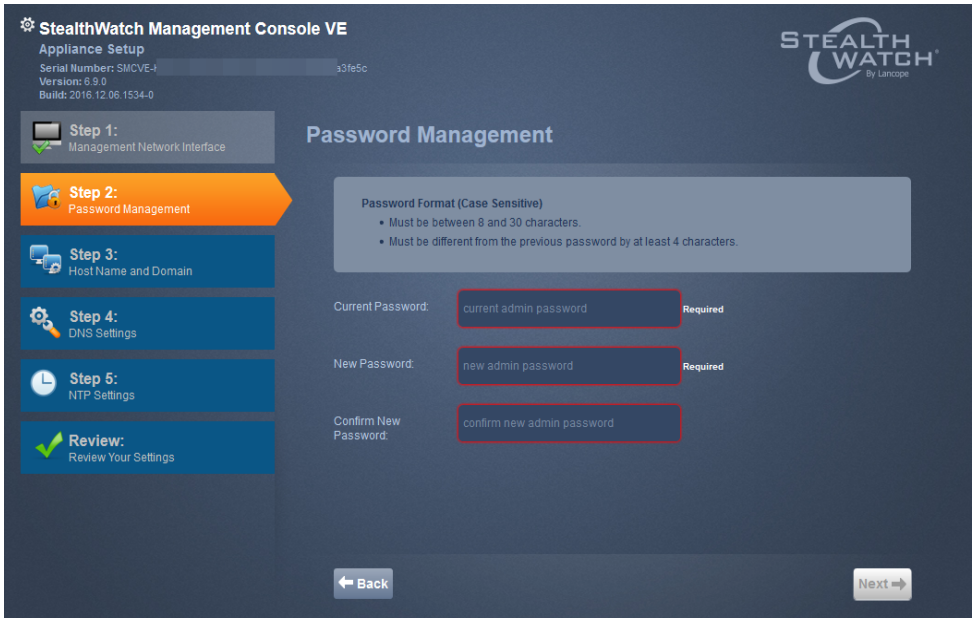
c. **Sign In(로그인)**을 클릭합니다.

5. 시작 페이지가 열립니다. **Continue(계속)**를 클릭합니다.

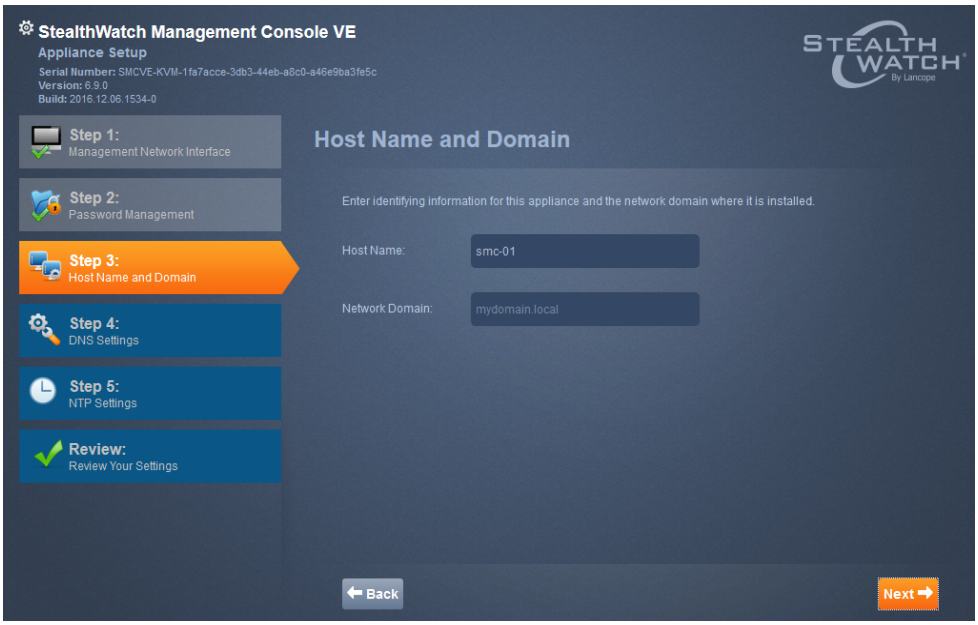
Management Network Interface(관리 네트워크 인터페이스) 페이지가 열립니다.



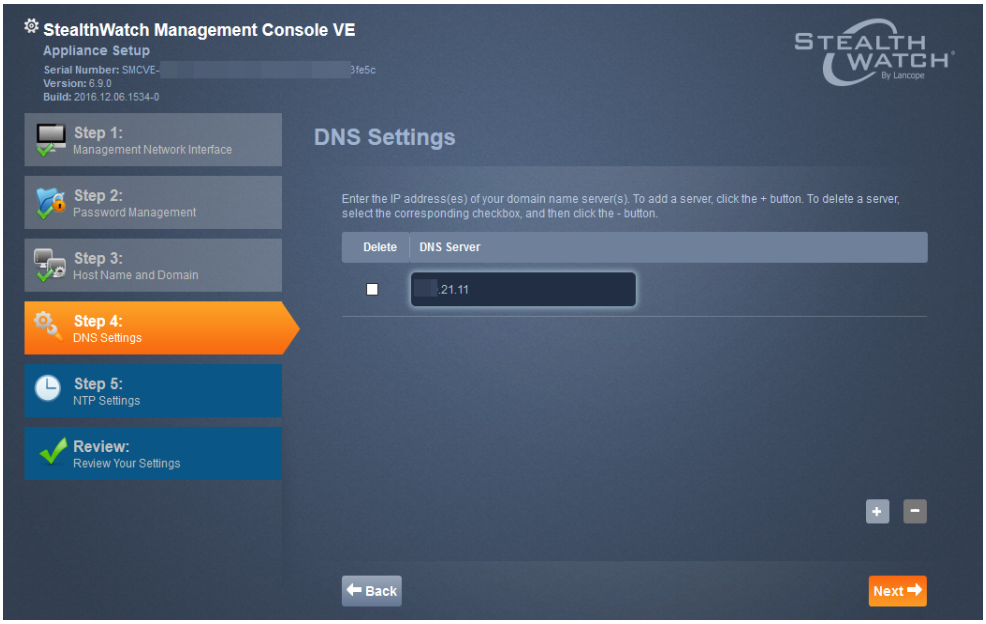
6. 어플라이언스의 IP 주소를 입력하고 **Next(다음)**를 클릭합니다. Password Management(비밀번호 관리) 페이지가 열립니다.



7. 해당 필드에 새 관리자 비밀번호를 입력하고 **Next(다음)**를 클릭합니다. Host Name and Domain(호스트 이름 및 도메인) 페이지가 열립니다.

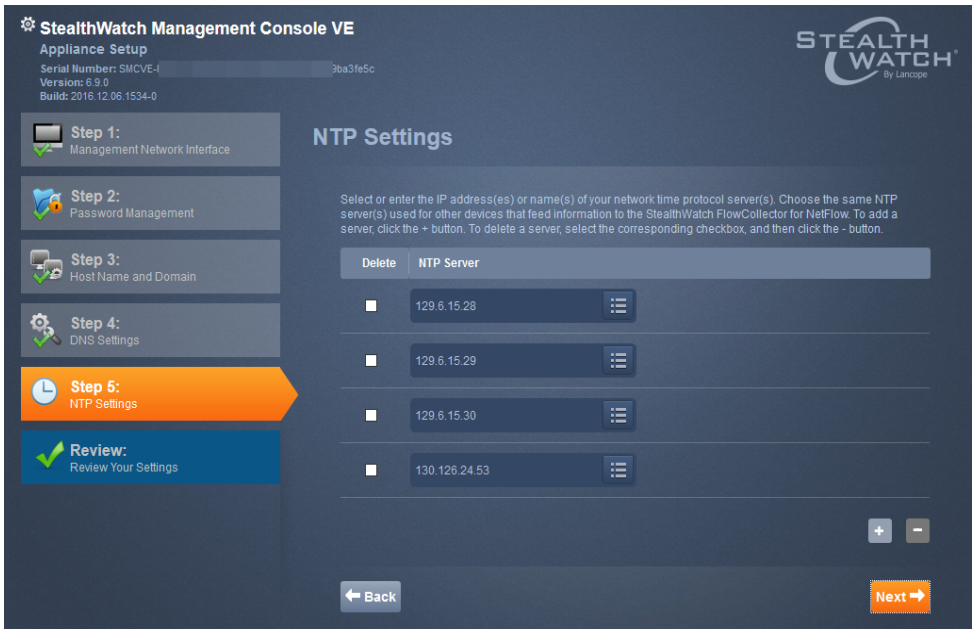


8. 해당 필드에 호스트 이름 및 네트워크 도메인 이름을 입력하고 **Next(다음)**를 클릭합니다. DNS Settings(DNS 설정) 페이지가 열립니다.

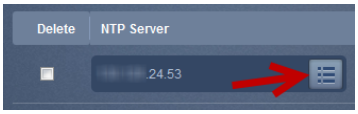


9. **+** 버튼을 클릭하고 DNS 서버의 IP 주소를 입력합니다. **Next(다음)**를 클릭합니다. NTP Settings(NTP 설정) 페이지가 열립니다.

> **참고:** 첫 번째 NTP 서버를 pool.ntp.org로 설정하십시오. 이렇게 하면 Stealthwatch 어플라이언스가 NTP 서버의 임의 ntp.org 풀에 액세스하여 어플라이언스 시간을 설정할 수 있습니다.

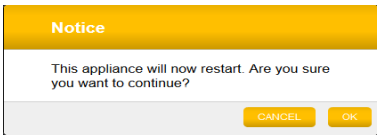


10. 기본 설정을 적용하거나, NTP 서버의 IP 주소를 입력하거나 리스트 아이콘을 클릭하고 드롭다운 리스트에서 하나를 선택하여 이름을 선택하는 방법으로 다른 서버를 입력할 수 있습니다. "어플라이언스 관리 인터페이스를 통한 컨피그레이션"을 참조하십시오



11. **Next(다음)**를 클릭합니다. Review(검토) 페이지가 열립니다.

12. 설정을 검토하고 **Apply(적용)**를 클릭합니다. 확인 대화 상자가 열립니다.



13. 새 시스템 설정이 적용될 때까지 몇 분 기다린 후 **Next(다음)**를 클릭합니다. 완료되면 어플라이언스의 로그인 페이지가 열립니다.
14. 로그인 크리덴셜을 입력하고 **Login(로그인)**을 클릭합니다.
15. 구성하려는 다른 어플라이언스가 있습니까?
    - 그렇다면, 1단계로 돌아가서 다음 어플라이언스에서도 이 절차를 반복하십시오. 기본 SMC는 마지막에 구성해야 합니다.
    - 그렇지 않다면, 다음 단계로 이동합니다.
16. 마지막 또는 유일한 SMC를 구성한 후에 다음 섹션인 "시스템 구성"을 계속 진행합니다.

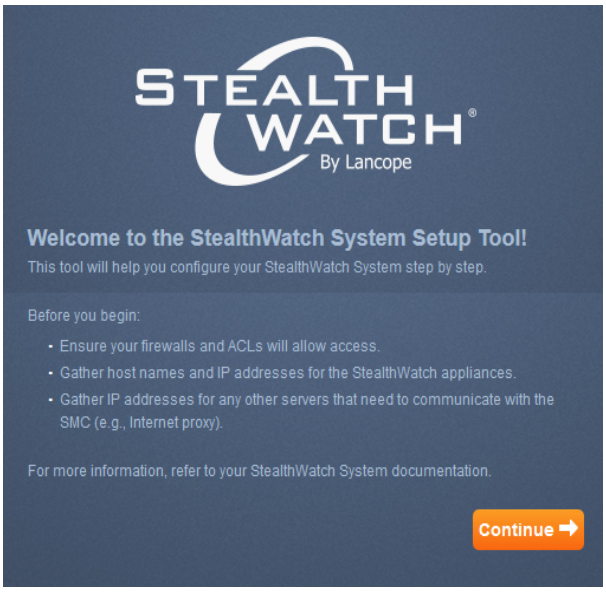
시스템 구성

SMC(VE)를 포함한 모든 어플라이언스 구성을 완료한 후에 시스템을 구성할 수 있습니다.

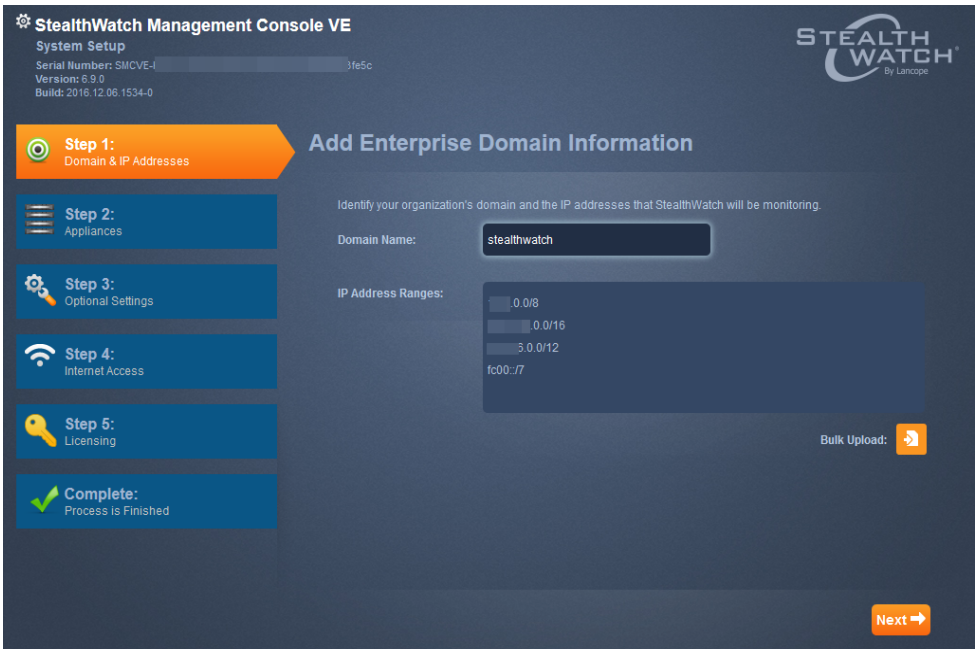
주의! SMC에서 관리되는 모든 어플라이언스를 활성화해야 합니다. 그렇지 않으면, SMC는 Flow Collector와 통신할 수 없으므로 시스템을 제대로 구성할 수 없습니다.

중요: 페일오버 SMC를 구성하는 경우, 시스템의 도메인 이름만 입력하고 나머지 페이지에서는 **Next(다음)**를 클릭해야 합니다. 이렇게 하면 기본 SMC를 구성할 때 시스템을 설정할 수 있습니다.

System Setup Tool(시스템 설정 툴)의 시작 페이지가 열립니다.



1. **Continue(계속)**를 클릭합니다. Add Enterprise Domain Information(엔터프라이즈 도메인 정보 추가) 페이지가 열립니다.

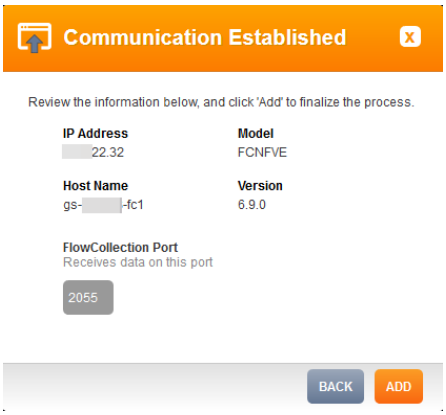


2. 시스템의 IP 주소 범위를 입력하거나(CIDR, 대시를 이용한 범위, 후행 점 서브넷 또는 IPv6 사용 가능) 대량 업로드를 사용하여 IP 주소 범위로 구성된 CSV 파일을 가져온 후 **Next(다음)**를 클릭합니다. Appliance(어플라이언스) 페이지가 열립니다.

참고: CSV 파일의 IP 주소는 쉼표, 쉼표 공백, 공백, 반환 형식 중 하나를 사용하여 구분해야 합니다.

3. + 버튼을 클릭합니다. Add Flow Collector(Flow Collector 추가) 대화 상자가 열립니다.

4. Flow Collector IP 주소를 입력하고 **Next(다음)**를 클릭합니다. Communication(통신) 대화 상자가 열립니다.



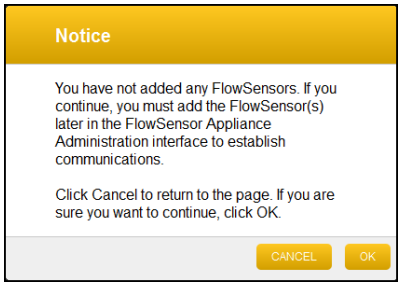
조건부 절차: 이 단계에서 Flow Collector 또는 Flow Sensor를 추가할 경우, Flow Collector 또는 Flow Sensor와 SMC(Stealthwatch Management Console) 간의 관리 채널을 먼저 만들어야 합니다. 이 작업을 수행하지 않으면 이 절차를 수행할 때 오류 메시지를 받게 됩니다. Flow Collector 및 Flow Sensor의 관리 채널을 만들려면 다음 단계를 완료합니다.

1. 브라우저와 어플라이언스의 IP 주소를 사용하여 해당하는 어플라이언스 관리 인터페이스에 로그인합니다.
2. 왼쪽 탐색 창에서 **Configuration(컨피그레이션) > Management Systems Configuration(관리 시스템 컨피그레이션)**을 클릭합니다.
3. **Add New Management System(새 관리 시스템 추가)**을 클릭합니다.
4. Management System IP Address(관리 시스템 IP 주소) 필드에 SMC IP 주소를 입력합니다.
5. **Is SMC(SMC 여부)** 확인란을 선택합니다.
6. **Apply(적용)**를 클릭합니다.
7. System Setup Tool(시스템 설정 툴)의 Error(오류) 대화 상자에서 **Cancel(취소)**을 클릭한 다음 **Apply(적용)**를 클릭합니다.

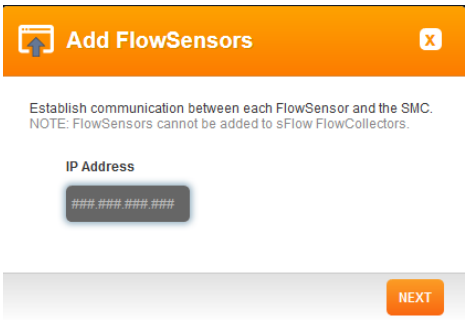
5. **Add(추가)**를 클릭합니다. Flow Collector가 시스템에 추가됩니다.

6. **Next(다음)**를 클릭합니다. Appliance > Flow Sensors(어플라이언스 > Flow Sensor) 페이지가 열립니다.

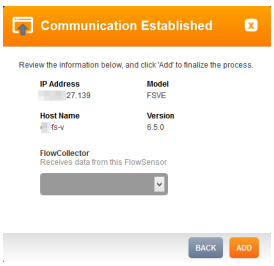
7. 추가하려는 Flow Sensor가 있습니까?
   - 그렇다면, + 버튼을 클릭하고 9단계로 이동합니다.
   - 그렇지 않다면, **Next(다음)**를 클릭하고 다음 단계로 이동합니다.
8. 경고 메시지가 표시됩니다. **OK(확인)**를 클릭합니다. 14단계로 이동합니다.



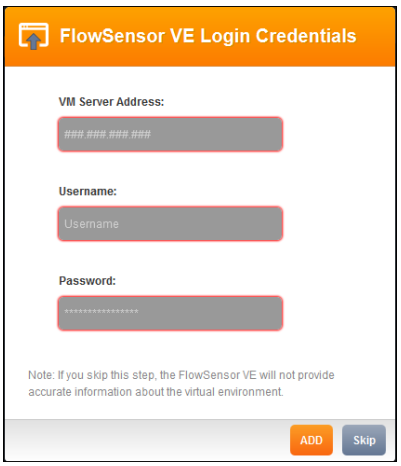
9. **+** 버튼을 클릭합니다. Add Flow Sensor(Flow Sensor 추가) 대화 상자가 나타납니다.



10. IP 주소를 입력하고 **OK(확인)**를 클릭합니다. Communication Established(설정된 통신) 대화 상자 나타납니다.

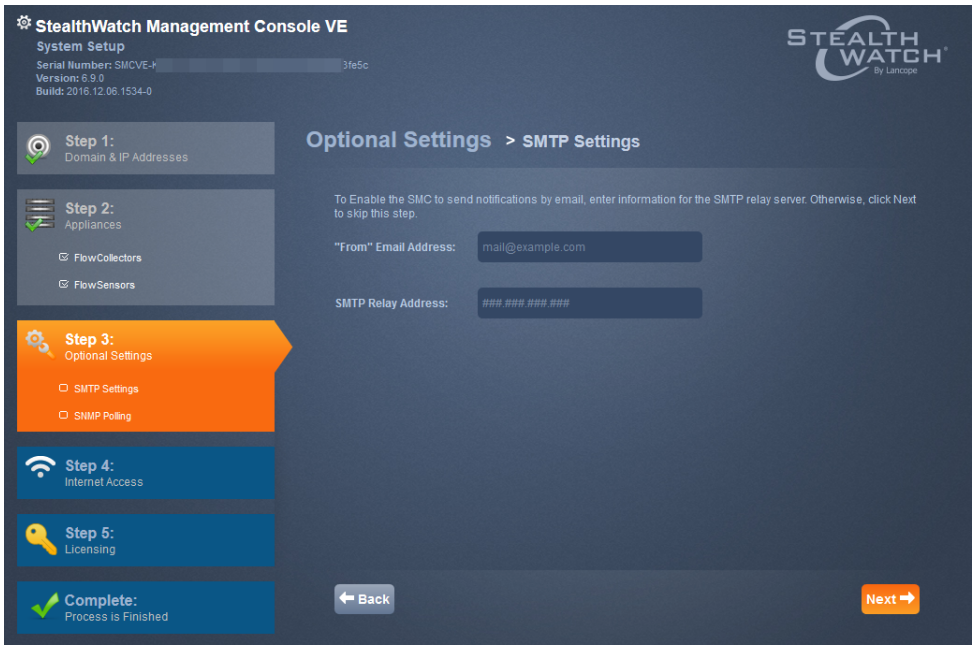


11. 드롭다운 목록에서 Flow Collector를 선택하고 **Add(추가)**를 클릭합니다.



Flow Sensor가 추가됩니다.

12. **Next(다음)**를 클릭합니다. SMTP Setting(SMTP 설정) 페이지가 열립니다.



13. SMC에서 이메일을 전송할 때 사용하고자 하는 이메일 주소를 "from(발신)" 필드에 입력합니다.
14. SMTP 릴레이 주소를 입력하고 Next(다음)를 클릭합니다. SNMP Setting(SNMP 설정) 페이지가 열립니다.

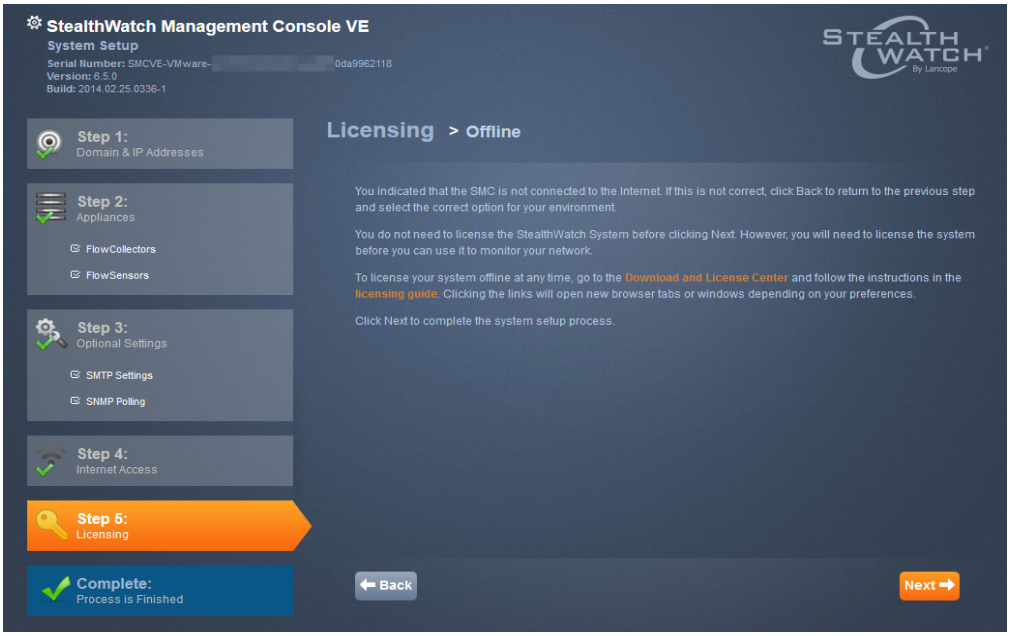
15. 필요한 경우, 설정을 수정하고(여기서는 하나의 문자열만 설정 가능) **Next(다음)**를 클릭합니다.

> **참고:** SNMP 버전 3을 선택한 경우, 사용자 이름을 입력한 후 옵션으로 인증 및 암호화를 선택할 수 있습니다.

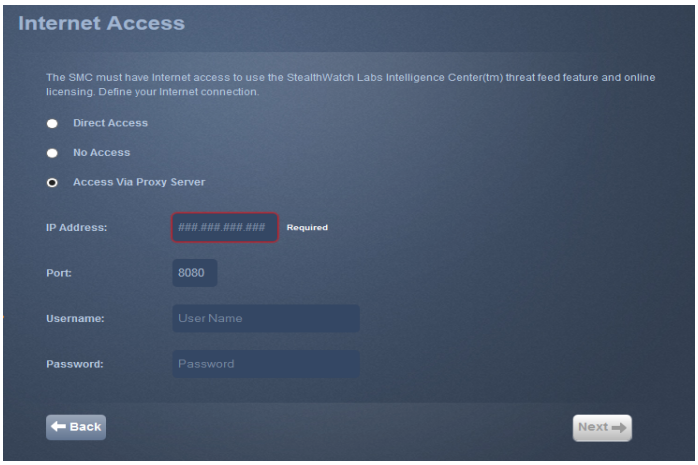
16. SMC의 경우, Internet Access(인터넷 액세스) 페이지가 열립니다.

17. 적절한 유형의 인터넷 액세스를 선택합니다.

- **No access(액세스 안 함)**: SMC를 인터넷에 연결하지 않습니다. 다운로드 및 라이선싱 센터에서 라이선스를 받기 위해 액세스 권한을 얻어야 합니다. Offline(오프라인) 페이지에서 **Next(다음)**를 클릭하여 Complete(완료) 페이지를 엽니다.

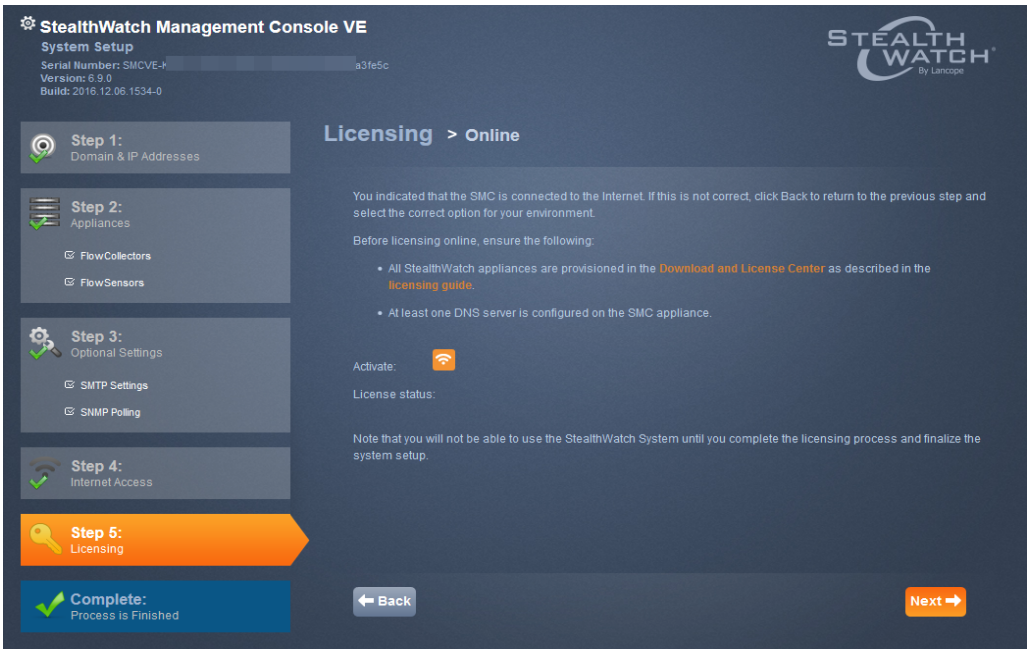


- **Access via Proxy Server(프록시 서버를 통한 액세스)**: SMC를 프록시 서버를 통해 인터넷에 연결합니다. 프록시 설정이 나타납니다.



프록시 서버의 설정을 완료하고 **Next(다음)**를 클릭합니다.

20. Direct Access(직접 액세스)를 선택했거나 프록시 설정을 완료하였다면, Licensing(라이선싱) 페이지가 열립니다.



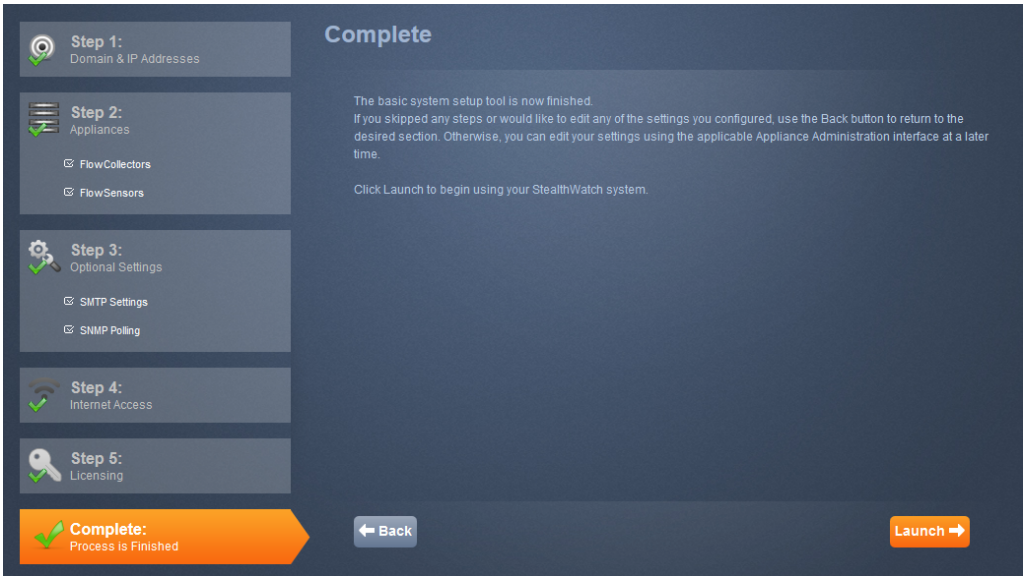
21. Download and License Center(다운로드 및 라이선스 센터) 링크를 클릭합니다. *Stealthwatch 제품 다운로드 및 라이선싱* 문서에 설명된 대로 라이선스를 획득합

니다.

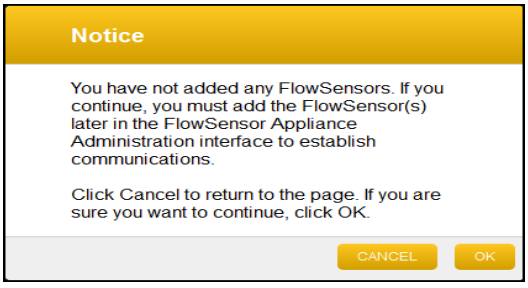
22. 라이선스를 획득한 후 **Activate(활성화)**를 클릭합니다.

> **참고:** 어플라이언스가 등록되지 않으면 메시지가 표시됩니다.

23. **OK(확인)**를 클릭합니다. Complete(완료) 페이지가 열립니다.



24. **Launch(실행)**를 클릭하여 SMC 클라이언트 랜딩 페이지로 이동합니다. 메시지가 열립니다. 어플라이언스 라이선스를 받지 않은 경우, 라이선스를 받지 않은 항목에 대한 정보가 포함된 메시지가 표시됩니다. 예시 메시지는 다음과 같습니다.



25. 오른쪽 상단 모서리에 있는 Welcome Admin User(관리 사용자 시작) 드롭다운 목록에서 **Administer Appliance(어플라이언스 관리)**를 클릭하여 어플라이언스 관리 인터페이스를 열고 다음 섹션인 27페이지의 "어플라이언스 관리 인터페이스를 통한 컨피그레이션"을 계속 진행합니다.

26. UDP Director가 설치되어 있습니까?

- 그렇다면, 다음 섹션인 "SMC에서 UDP Director 구성"을 계속 진행합니다.
- 그렇지 않다면, "어플라이언스 관리 인터페이스를 통한 컨피그레이션"을 계속 진행합니다.

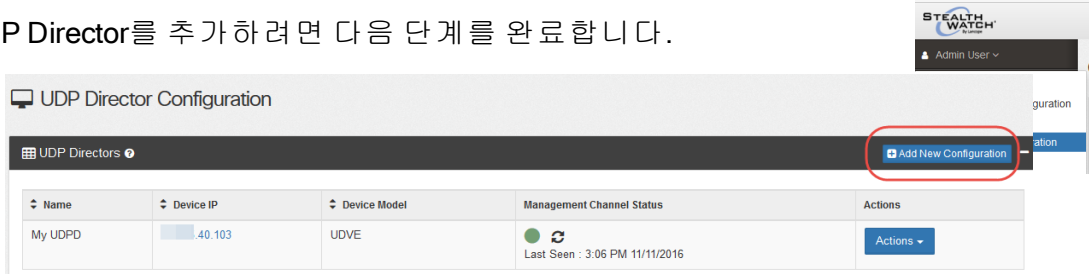
SMC에서 UDP Director 구성

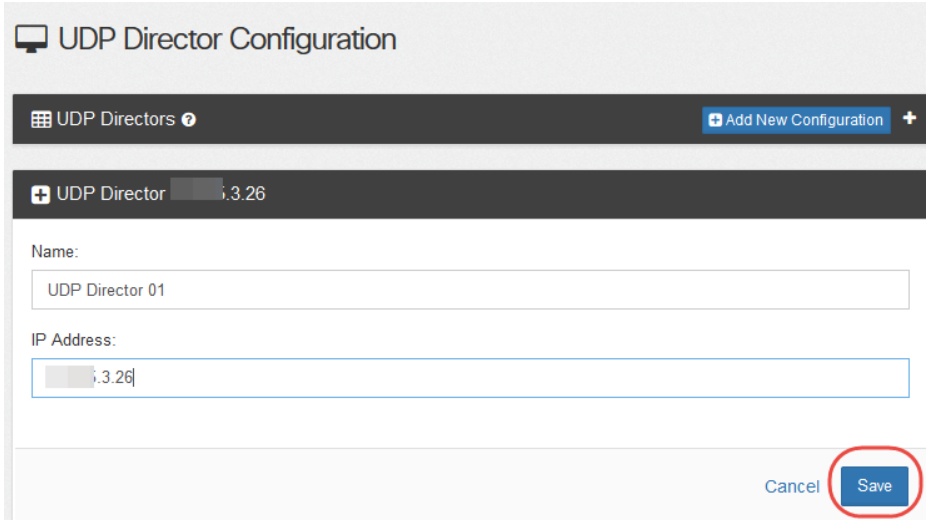
Stealthwatch System에 UDP Director가 설치되어 있는 경우, SMC에서 UDP Director를 관리할 수 있도록 SMC 웹 애플리케이션에서 UDP Director를 구성할 수 있습니다. UDP Director에서 직접 관리하려면 "UDP Director 규칙 구성"을 참조하십시오로 이동합니다.

참고: SSL은 메시지를 UDP Director에서 SMC(Stealthwatch Management Console)에 전송하는 데 사용됩니다.

UDP Director 추가

UDP Director를 추가하려면 다음 단계를 완료합니다.

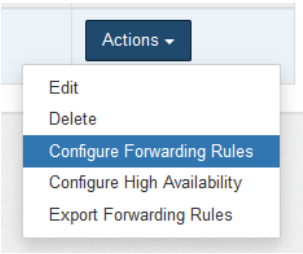




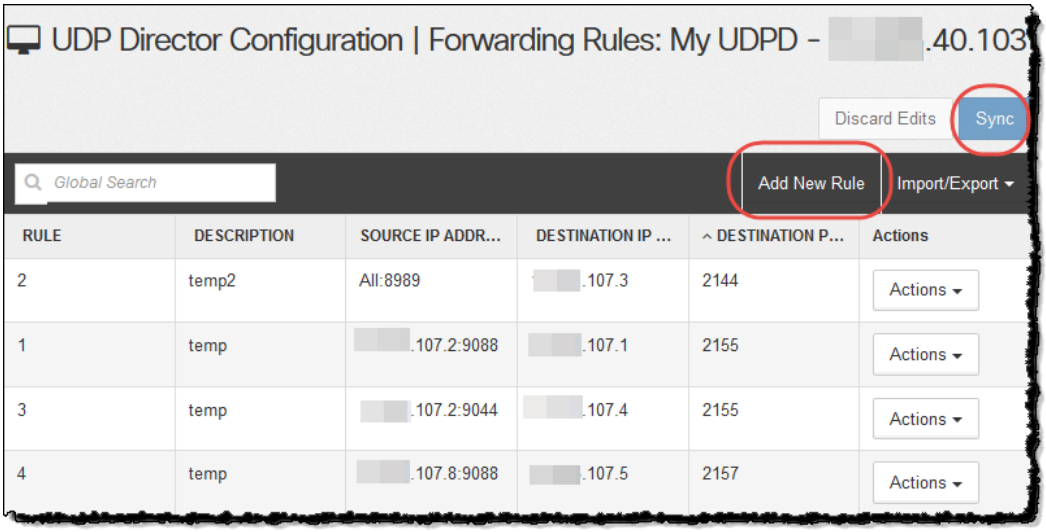
전달 규칙 구성

UDP Director를 추가한 후 관련된 전달 규칙을 구성할 수 있습니다.

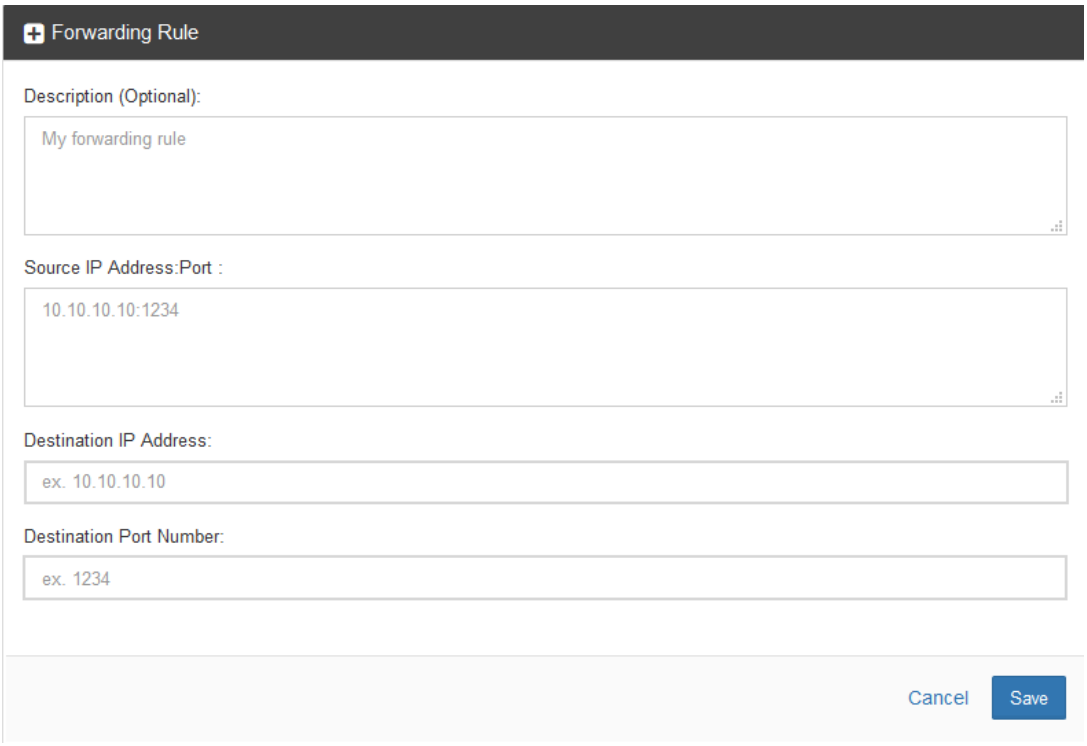
UDP Director의 전달 규칙을 구성하려면 다음 단계를 완료합니다.



1. **Actions(작업) > Configuring Forwarding Rules(전달 규칙 구성)**를 선택합니다. Forwarding Rules(전달 규칙) 페이지가 열립니다.



2. **Add New Rule(새 규칙 추가)**을 클릭합니다.



3. Description(설명) 필드에 규칙을 식별하기 위한 간략한 설명을 입력합니다.
4. Source IP Address:Port List(소스 IP 주소:포트 목록) 필드에 UDP Director에 데이터를 전송하는 디바이스의 IP 주소를 입력하고 그 뒤에 데이터를 전송할 때 사용할 포트 번호를 입력합니다.

참고:

- 아래 예와 같이 [IP 주소]:[포트 번호] 구문을 사용합니다.
- CIDR(Classless Inter-Domain Routing) 표시법을 사용하여 IP 주소 범위를 입력할 수 있습니다.
- "All(모두)"을 입력하여 이 포트에서 모든 소스 IP 주소의 데이터를 수락할 수 있습니다.
- 새 라인에 소스 IP 주소:포트 조합을 추가하여 규칙 내에 이를 추가할 수 있습니다.

예:

- 10.11.16.38:5322
- 192.168.0.0/16:9000
- All:2055

5. Destination IP Address(대상 IP 주소) 필드에 UDP Director에서 데이터를 수신하는 디바이스의 IP 주소를 입력합니다.

6. Destination Port Number(대상 포트 번호) 필드에 수신 중인 디바이스의 포트 번호를 입력합니다.
7. **Save(저장)**를 클릭합니다. 새로운 규칙이 Forwarding Rules(전달 규칙) 페이지의 테이블에 추가됩니다.
8. 변경 사항을 동기화하시겠습니까?

   a. 그렇다면, 페이지의 상단에 있는 Sync(동기화) 버튼을 클릭합니다. 새 규칙이 저장됩니다.

   b. 그렇지 않다면, 페이지의 상단에 있는 Discard Edits(편집 내용 취소) 버튼을 클릭합니다. Configuration(컨피그레이션) 대화 상자가 표시되면 **Yes(예)**를 클릭합니다.

8. 필요에 따라 이 과정을 반복하여 전달 규칙을 추가합니다.
9. 다음 섹션인 "어플라이언스 관리 인터페이스를 통한 컨피그레이션"을 계속 진행합니다.

참고: 보조 UDP Director를 사용하려면 하나 이상의 전달 규칙과 함께 추가해야 합니다. 먼저 기본 UDP Director를 구성한 다음 보조 UDP Director에서 컨피그레이션 단계를 반복해야 합니다. HA 어플라이언스 구성에 대한 지침을 확인하려면 36 페이지의 “기본 UDP Director HA 구성”으로 이동하십시오.

어플라이언스 관리 인터페이스를 통한 컨피그레이션

이 섹션에서는 어플라이언스 관리 인터페이스를 사용하여 가상 어플라이언스의 컨피그레이션을 완료하는 다음 절차에 관해 설명합니다.

1. 어플라이언스 관리 인터페이스 로그인
2. 시스템 시간 구성
3. 시스템 구성
4. UDP Director HA 구성
5. 어플라이언스 재시작

어플라이언스 관리 인터페이스 로그인

어플라이언스 관리 인터페이스에 로그인하려면 다음 단계를 완료합니다.

참고:

- Stealthwatch에서 지원되는 브라우저는 Internet Explorer 버전 9 이상과 Firefox 버전 3 이상입니다.

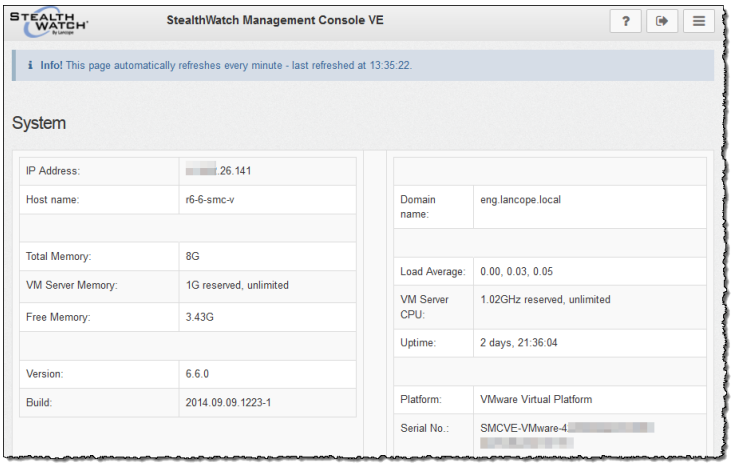
- 페이지를 로드하는 데 문제가 있으면, 브라우저 캐시를 지우고, 브라우저를 닫은 다음 다시 연 후, 다시 로그인합니다.

1. 브라우저의 주소 필드에 **https://**를 입력한 후에 어플라이언스의 IP 주소를 입력한 다음 **Enter** 키를 누릅니다.
2. SMC 어플라이언스 관리 인터페이스를 열고 있습니까?

   - 그렇다면, 랜딩 페이지가 열립니다. 오른쪽 상단 모서리에서 **Settings(설정)** 아이콘을 클릭한 다음 **Administer Appliance(어플라이언스 관리)**를 클릭합니다.

   - 그렇지 않다면, 가상 어플라이언스 **Login(로그인)** 페이지가 열립니다.

3. **User Name(사용자 이름)** 필드에 **admin**을 입력합니다.
4. **Password(비밀번호)** 필드에 어플라이언스 설정에서 생성한 admin 비밀번호를 입력합니다.
5. **Login(로그인)**을 클릭합니다. 어플라이언스 관리 인터페이스 홈 페이지가 열립니다.



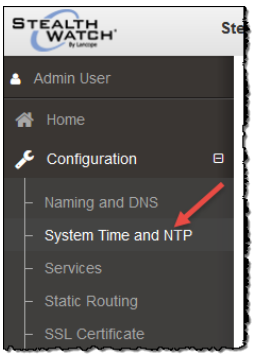
6. 다음 섹션인 "시스템 시간 구성"을 계속 진행합니다.

시스템 시간 구성

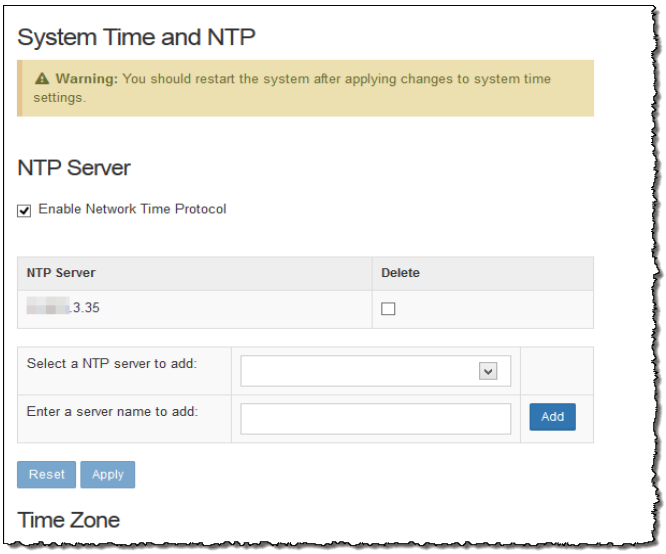
어플라이언스에서 NTP(Network Time Protocol) 및 시스템 시간(표준 시간대) 설정을 구성하려면 다음 단계를 완료합니다.

주의! Flow Collector와 SMC에 정보를 제공하는 기타 디바이스에 사용한 것과 동일한 NTP 서버를 사용합니다. Flow Collector 5000 Series 어플라이언스를 사용하는 경우, NTP 및 시스템 시간 설정을 데이터베이스 및 엔진에서 동일하게 구성합니다.

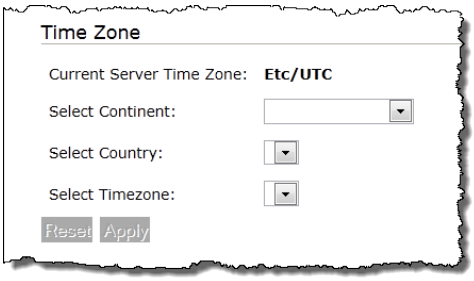
1. 어플라이언스 관리 인터페이스 탐색 창에서 **Configuration(컨피그레이션)** 옆에 있는 더하기 기호(+)를 클릭한 다음 **System Time and NTP(시스템 시간 및 NTP)**를 클릭합니다.



NTP Server(NTP 서버) 페이지가 열리고 Appliance Setup Tool(어플라이언스 설정 툴)을 사용하여 초기 컨피그레이션에서 설정한 NTP 서버가 표시됩니다.



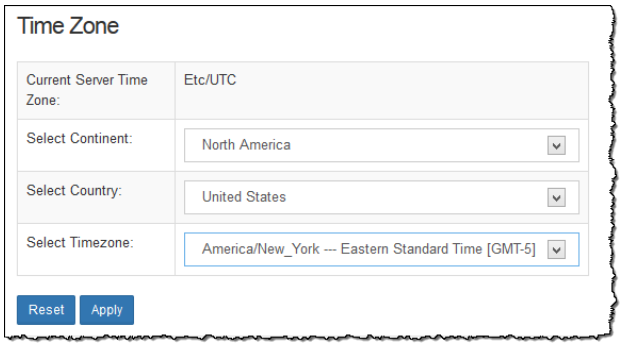
2. 어플라이언스 시스템 시간을 구성하려면 아래로 스크롤하여 해당 페이지의 Time Zone(표준 시간대) 섹션으로 이동합니다.



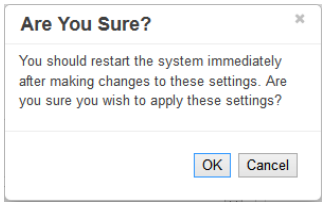
3. 다음을 수행합니다.

   - 드롭다운 목록에서 Continent(대륙)를 선택합니다.
   - 드롭다운 목록에서 Country(국가)를 선택합니다.
   - 드롭다운 목록에서 Timezone(표준 시간대)을 선택합니다.

   Apply(적용) 알림이 나타납니다.



4. 변경 사항을 영구적으로 적용하려면 **Apply(적용)**를 클릭합니다. 확인 창이 열립니다.



5. **OK(확인)**를 클릭합니다.

6. Flow Sensor 또는 UDP Director를 구성하고 있습니까?

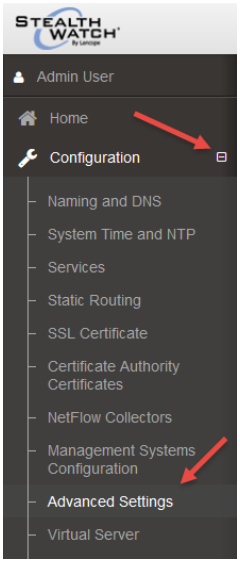
   - Flow Sensor를 구성하는 중이면 다음 섹션인 "Flow Sensor 구성"을 계속 진행합니다.
   - UDP Director를 구성하는 중이면 다음 섹션인 "UDP Director 규칙 구성"을 계속 진행합니다.
   - 그렇지 않다면, 어플라이언스 재시작 섹션을 계속 진행합니다.

Flow Sensor 구성

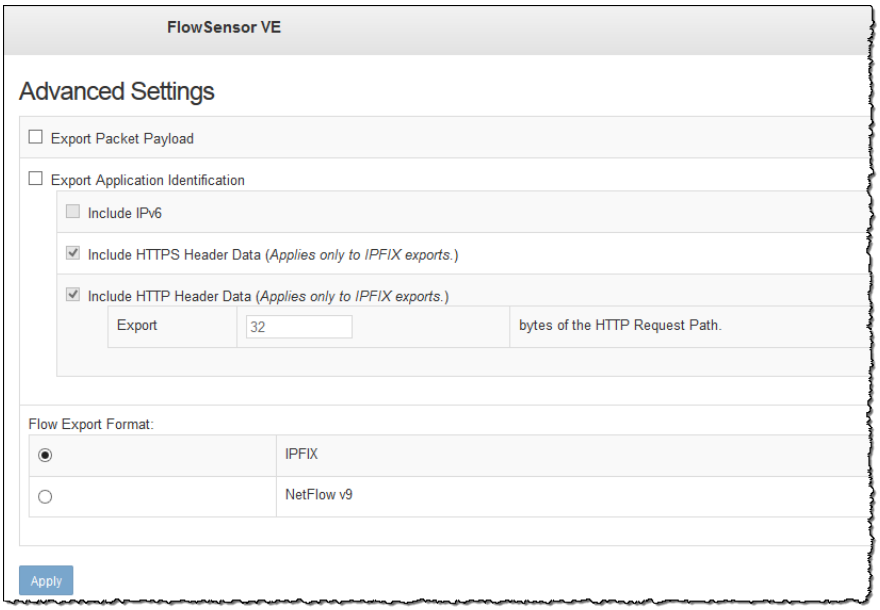
Flow Sensor 컨피그레이션에는 애플리케이션 ID와 페이로드를 구성하는 추가 단계가 필요합니다.

Flow Sensor에서 애플리케이션 ID와 페이로드 데이터를 내보내는 방법을 구성하려면 다음 단계를 완료합니다.

1. 탐색 창에서 Configuration(컨피그레이션) 메뉴 옆에 있는 더하기 기호(+)를 클릭한 다음 **Advanced Settings(고급 설정)**를 클릭합니다.



Export(내보내기) 설정 페이지가 열립니다.



2. 적절한 네트워크 설정을 선택합니다.

항목	설명
패킷 페이로드 내보내기	Flow Sensor에서 Collector로 전송하는 데이터에 첫 26바이트의 바이너리 페이로드 데이터를 포함할지를 지정할 수 있습니다.
애플리케이션 ID	Flow Sensor에서 Collector로 데이터를 전송하기 전에 애플리케이션

항목	설명
내보내기	을 식별할지를 지정할 수 있습니다. 또한, 이 설정은 다음 설정을 적용하기 위해 활성화되어야 합니다. **IPv6 포함** - Flow Sensor에서 IPv4 및 IPv6 패킷을 분석할지를 지정할 수 있습니다. 이 설정을 비활성화하면 Flow Sensor에서는 IPv4 패킷만 분석합니다. **HTTPS 헤더 데이터 내보내기** - Flow Sensor에서 Collector로 전송하는 데이터에 HTTPS 플로우의 헤더 데이터를 포함할지를 지정할 수 있습니다. 이 데이터는 SSL 일반 이름 및 SSL 조직 이름을 포함합니다. 이 설정에서는 플로우 유형을 IPFIX로 설정해야 합니다. 최대값은 256바이트입니다. **HTTP 헤더 데이터 내보내기** - Flow Sensor에서 Collector로 전송하는 데이터에 HTTP 플로우의 헤더 데이터를 포함할지를 지정할 수 있습니다. 이 설정을 선택하면 보조 필드를 통해 Flow Sensor에서 플로우 데이터의 일부로 포함하는 HTTP 경로(바이트 단위)의 최대 길이를 지정할 수 있습니다. 이 설정에서는 플로우 유형을 IPFIX로 설정해야 합니다.
플로우 내보내기 형식	Flow Sensor에서 Collector로 플로우 데이터를 전송하기 위해 IPFIX 또는 NetFlow v9를 사용할지를 지정할 수 있습니다.
캐시 모드	다음 설정 중 하나를 선택할 수 있습니다. **모든 모니터링 포트에 단일 공유 캐시 사용 -** • 비대칭 라우팅이 있는 경우에 사용합니다. • 애플리케이션 및 레이턴시 계산을 위한 단일 상태 테이블입니다. • 적은 메모리를 사용합니다. • 전반적인 pps 처리 속도가 낮습니다. • 여러 인터페이스 전반에서 생성된 하나의 NetFlow 이벤트가 발생합니다. • Flow Sensor에 두 개의 포트만 있고 TAP에 의해 연결되는 경우에만 사용합니다. **각 모니터링 포트에 독립적 캐시 사용 -** • 각 Flow Sensor 인터페이스 전반에서 패킷 중복 제거를 허용합니다. • 많은 메모리를 사용합니다. • 전반적인 pps 처리 속도가 높습니다. • 각 인터페이스는 고유한 레이턴시 및 애플리케이션 데이터베이스를 유지 관리합니다. • 각 인터페이스에 대해 지정된 패킷을 보여주는 고유한 NetFlow 레코드가 생성됩니다.

3. **Apply(적용)**를 클릭하여 설정을 저장합니다.
4. 38페이지의 "어플라이언스 재시작" 섹션을 계속 진행합니다.

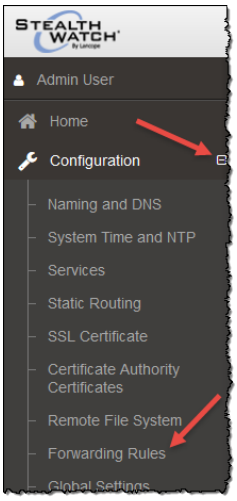
UDP Director 규칙 구성

SMC에서 UDP Director를 관리하지 않는 경우, 어플라이언스 관리 페이지에서 전달 규칙을 구성할 수 있습니다. UDP Director의 경우, 엑스포터가 eth0의 IP 주소로 전달하도록 플로우를 전송하게 구성해야 합니다. UDP Director는 전달된 패킷에 대해 각 엑스포터의 원래 IP 및 MAC 주소를 보존하면서 eth0에서 온 플로우를 전달합니다.

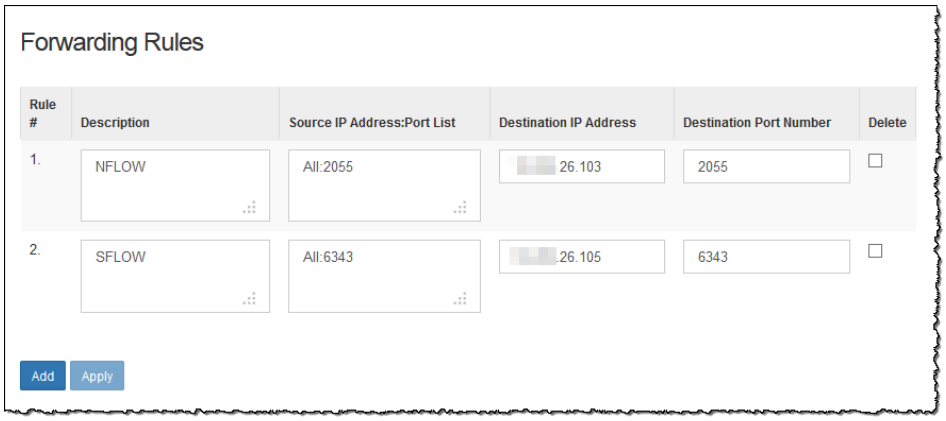
참고: 프로미스큐어스 모드의 수신에 대해 Lancope는 관심 있는 모든 트래픽에 스팬 필터를 사용할 것을 권장합니다. 이 네트워크에서는 엑스포터에서 UDP Director를 거쳐 수신기로 전송되는 데 사용되는 포트에 대한 트래픽을 허용해야 합니다(ACL).

UDP Director의 규칙을 구성하려면 다음 단계를 완료합니다.

1. 탐색 창에서 **Configuration(컨피그레이션)** 메뉴 옆에 있는 더하기 기호(+)를 클릭한 다음 **Forwarding Rules(전달 규칙)**를 클릭합니다.



Forwarding Rules(전달 규칙) 페이지가 열립니다.



2. Description(설명) 필드에 규칙에 대한 설명을 입력합니다.
3. Source IP Address:Port List(소스 IP 주소:포트 목록) 필드에 UDP Director에 데이터를 전송하는 디바이스의 IP 주소를 입력하고 그 뒤에 데이터를 전송할 때 사용할 포트 번호를 입력합니다. 다음 구문을 사용합니다.

[IP 주소]:[포트 번호] 예: 10.201.1.41:2057

참고:

- 특정 포트에서 모든 디바이스의 모든 트래픽을 수신하려면 **All:[포트 번호]**를 입력합니다. 예를 들어, **All:3123**을 입력합니다.
- CIDR(Classless Inter-Domain Routing) 표시법을 사용하여 IP 주소 범위를 입력할 수도 있습니다. 예를 들어, **172.200.1.0/16:9000**을 입력합니다.

정보:

- "All"을 사용하거나, 엔진에 필요한 구문 분석의 양을 제한하려면 가능한 경우 CIDR 범위를 입력합니다. 많은 개별 IP 주소를 입력하면 엔진이 더 많은 작업을 수행하게 됩니다.
- 또한, 입력 트래픽에 대한 대체 포트를 사용하여 해당 트래픽을 원하는 출력 포트에 리디렉션할 수 있습니다. 예를 들어, 하나의 규칙에 모든 포트 55431 트래픽을 전송하는 대신, 이전에 포트 55431을 사용했던 엑스포터의 1/3에서 44440 더미 포트를 대신 사용하도록 설정하여 해당 트래픽을 분할할 수 있습니다. 그런 다음, 엑스포터의 다른 1/3에서 포트 44441을 사용하게 하고, 엑스포터의 나머지 1/3에서 포트 44442를 사용하게 할 수 있습니다. 그런 다음, 포트 44440, 44441 및 44442에 대한 모든 트래픽을 단일 대상 포트 55431로 리디렉션합니다.

4. 다른 항목을 추가하려면 **Enter** 키를 누르고 다음 IP 주소와 포트 번호를 입력합니다.

5. Destination IP Address(대상 IP 주소) 필드에 UDP Director에서 데이터를 수신하는 디바이스의 IP 주소를 입력합니다.
6. Destination Port Number(대상 포트 번호) 필드에 수신 중인 디바이스의 포트 번호를 입력합니다.
7. 다른 수신 디바이스에 전달하도록 UDP Director에 데이터를 전송하는 디바이스가 둘 이상 있는 경우, **Add(추가)**를 클릭합니다.

   설정을 입력할 수 있는 새로운 라인이 표시됩니다. 이 UDP Director에 대해 모든 디바이스를 입력할 때까지 이 단계를 반복합니다.

8. 입력을 마치면 **Apply(적용)**를 클릭합니다. UDP Director 컨피그레이션 화면이 새로 고침되고 시스템에서 컨피그레이션 파일을 업데이트합니다. 오류는 화면 상단에 나타납니다.
9. UDP Director HA를 구성하고 있습니까?

   - 그렇다면, 다음 섹션인 UDP Director HA 구성을 계속 진행합니다.
   - 그렇지 않다면, 38페이지의 "어플라이언스 재시작"을 계속 진행합니다.

UDP Director HA 구성

UDP Director HA(High Availability)를 통해 이중 UDP Director 2000 설정을 구성할 수 있습니다. 두 노드 모두 완전히 이중화되었으나, 한 번에 한 노드만 온라인 상태가 됩니다. 이 쌍에서 온라인 노드는 기본 노드이며 오프라인 노드는 보조 노드입니다. 이 쌍의 기본 노드에 오류가 발생하면 보조 노드가 이를 대체하여 기본 노드가 됩니다.

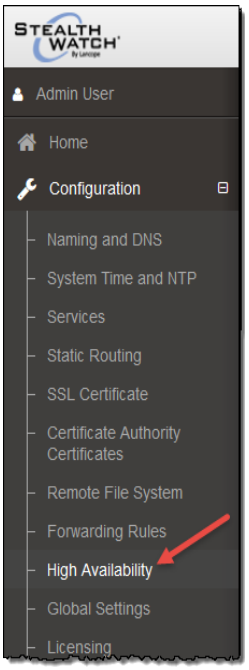
중요: HA 시스템에서는 UDP Director에 하나 이상의 규칙이 있어야 합니다. UDP Director에 이미 구성된 규칙이 있는 경우, UDP Director 규칙을 내보내고(규칙 컨피그레이션 파일 저장) 해당 파일을 두 번째 UDP Director에 가져와 규칙이 각각 일치하는지 확인합니다.

먼저 기본 UDP Director를 구성한 다음 보조 UDP Director에서 컨피그레이션 단계를 반복해야 합니다. 두 UDP Director를 모두 새로 만든 경우, 이 가이드의 절차를 각각 따르십시오. 그러나, 보조 UDP Director가 Stealthwatch System에서 어플라이언스로 이미 구성된 경우, 보조 UDP Director에 로그인하여 이 가이드에 설명된 대로 HA 구성 요소를 구성해야 합니다.

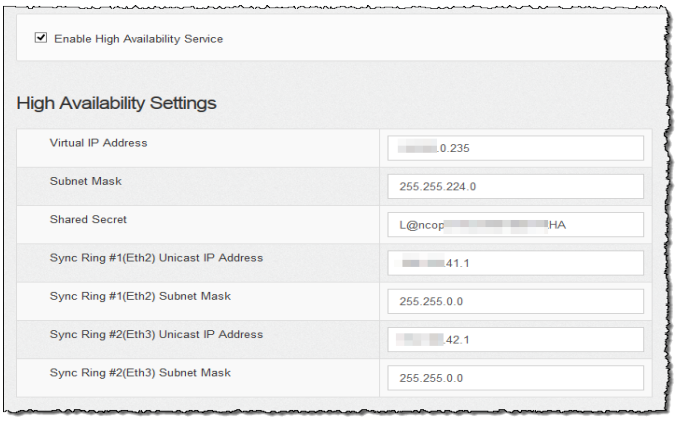
기본 UDP Director HA 구성

기본 UDP Director를 구성하려면 다음을 수행합니다.

1. UDP Director 관리 인터페이스의 탐색 창에서 **Configuration(컨피그레이션)** 옆에 있는 더하기 기호(+)를 클릭한 다음 **High Availability(HA)**를 클릭합니다.



2. Enable High Availability Cluster(HA 클러스터 활성화) 페이지의 High Availability Settings(HA 설정)에서 Enable High Availability(HA 활성화) 확인란을 선택합니다.



3. Virtual IP Address(가상 IP 주소) 및 Subnet Mask(서브넷 마스크) 필드에 기본 UDP Director의 IP 주소를 입력합니다. (보조 UDP Director에서도 이 단계를 동일하게 수행합니다.)

> **참고:** 가상 IP 주소는 유니캐스트 주소와 동일한 서브넷에 있어야 합니다.

4. Shared Secret(공유 암호) 필드에 두 UDP Director에 대한 문자열을 입력합니다. (이것은 보안 전송을 위해 암호화됩니다.)

5. Sync Ring 1 (Eth2) Unicast IP Address(Sync Ring 1(Eth2) 유니캐스트 IP 주소) 필드에 IP 주소와 서브넷 마스크를 입력합니다. (유니캐스트 IP 주소는 단일 네트워크 대상을 식별합니다.)
6. Sync Ring 2 (Eth3) Unicast IP Address(Sync Ring 2(Eth3) 유니캐스트 IP 주소) 필드에 IP 주소와 서브넷 마스크를 입력합니다.

> **참고:** 각 IP 주소(eth0, eth02, eth03)는 고유한 개별 유니캐스트 서브넷에 있어야 합니다.

7. 설정을 검토한 후에 **Apply(적용)**를 클릭하여 컨피그레이션을 설정합니다.
8. 클러스터의 두 번째 UDP Director를 구성하려면 다음 섹션을 계속 진행합니다.

보조 UDP Director HA 구성

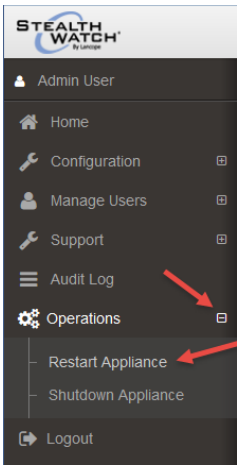
보조 UDP Director를 구성하려면 다음 단계를 완료합니다.

1. HA 쌍의 보조 UDP Director 2000의 어플라이언스 관리 인터페이스에 로그인합니다.
2. 이 화면의 모든 파라미터(첫 번째 어플라이언스에서 변경한 모든 고급 파라미터 포함)를 다음을 제외한 모든 필드에 대해 첫 번째 어플라이언스와 똑같이 구성합니다.
   - Sync Ring 1(Eth2) 유니캐스트 IP 주소 - 기본 UDP Director의 이 필드에 구성한 것과는 다른 IP 주소를 입력합니다. 단, 이는 Sync Ring 1 유니캐스트 주소와 동일한 서브넷에 있어야 합니다.
   - Sync Ring 2(Eth3) 유니캐스트 IP 주소 - 기본 UDP Director의 이 필드에 구성한 것과는 다른 IP 주소를 입력합니다. 단, 이는 Sync Ring 2 유니캐스트 주소와 동일한 서브넷에 있어야 합니다.
3. 변경 사항을 저장하고 이 어플라이언스에서 클러스터링 서비스를 시작하려면 **Apply(적용)**를 클릭합니다.
4. 기본 어플라이언스를 지정하려면 Promote(승격) 버튼을 클릭합니다.
5. 다음 섹션을 계속 진행합니다.

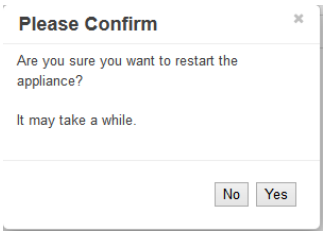
어플라이언스 재시작

어플라이언스를 재시작하려면 다음 단계를 완료합니다.

1. 어플라이언스 관리 인터페이스 메뉴에서 **Operations(작업) > Restart Appliance(어플라이언스 재시작)**를 선택합니다.



확인 대화 상자가 열립니다.



2. **Yes(예)**를 클릭합니다.
3. Flow Collector를 구성했습니까?
   - 그렇다면, 다음 장인 "통신 확인"을 계속 진행합니다.
   - 그렇지 않다면, 다음 단계로 이동합니다.
6. Flow Sensor 또는 UDP Director를 구성했습니까?
   - 그렇다면, 축하합니다. 어플라이언스 설치 및 구성을 완료했습니다. 재시작하면 Flow Sensor가 VM 환경에서 데이터를 수집하고 NetFlow Collector에 해당 데이터를 전송하기 시작합니다. 재시작하면 UDP가 데이터를 수집하고 해당 데이터를 구성한 대상으로 전송하기 시작합니다.
   - 그렇지 않다면, 다음 단계로 이동합니다.
7. Identity 디바이스가 있습니까?
   - 그렇다면, 다음 장인 "Identity 디바이스 추가"로 이동합니다.
   - 그렇지 않다면, 다음 단계로 이동합니다.
8. SLIC 기능을 사용하고 있습니까?

- 그렇다면, "SLIC Threat Feed 기능 활성화" 장으로 이동합니다.
- 그렇지 않다면, 축하합니다. SMC 컨피그레이션을 완료했습니다. 재시작하면 Flow Collector와의 통신이 시작됩니다.

3

통신 확인

개요

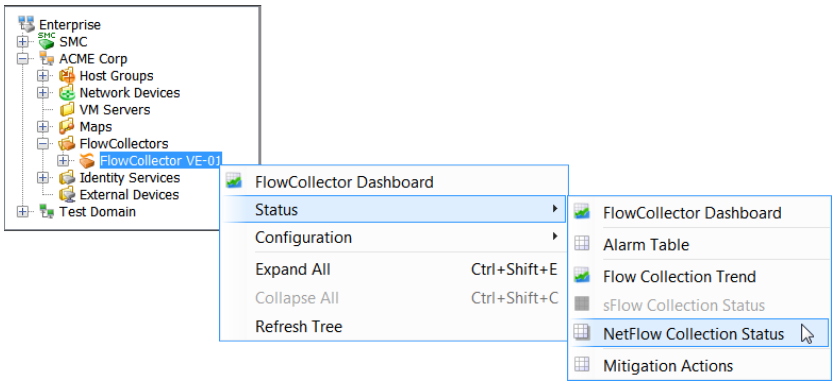
Stealthwatch 어플라이언스 라이선스를 받은 후에 NetFlow 데이터를 수신하고 있는지 확인해야 합니다. 이를 확인하려면 이 장에 설명되어 있는 다음 절차를 완료합니다.

주의! 이 섹션의 절차를 시작하기 전에 각 어플라이언스에 대해 이전 섹션에 나와 있는 라이선싱 절차를 모두 완료한 후에 30분 정도 기다리십시오.

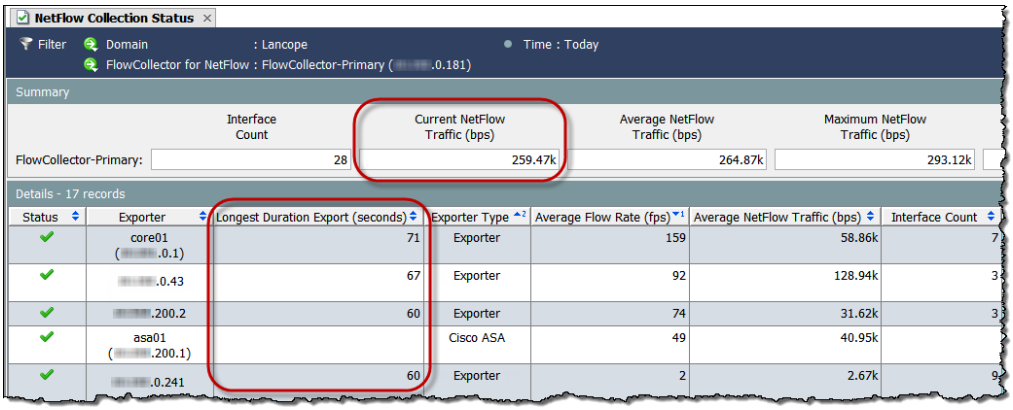
NetFlow 데이터 수집 확인

Flow Collector를 SMC에 추가한 후에 Flow Collector는 SMC에 플로우 정보를 전달하며, 이 정보는 다양한 문서에서 사용자 친화적인 방법으로 표시됩니다. 실제로 NetFlow 데이터를 수집하고 있는지 확인하려면 다음 단계를 완료합니다.

1. Enterprise(엔터프라이즈) 트리에서 Flow Collector를 마우스 오른쪽 단추로 클릭하고
   Status(상태) > NetFlow Collection Status(NetFlow 수집 상태)를 선택합니다.



NetFlow Collection Status(NetFlow 수집 상태) 문서가 열립니다.



2. 문서 상단에 있는 **Current NetFlow Traffic(현재 NetFlow 트래픽)** 필드를 살펴봅니다. 이 통계는 관찰 중인 NetFlow 트래픽의 양을 보여줍니다. 플로우 트래픽을 확인할 수 있습니까?

   - 그렇다면, 다음 단계로 이동합니다.
   - 그렇지 않다면, 엑스포터/라우터 컨피그레이션을 확인합니다. (지원에 대한 내용은 *SMC 클라이언트 온라인 도움말*을 참조하십시오.) 그런 다음, 다음 단계로 이동합니다.

3. **Longest Duration Export(최장 기간 내보내기)** 열을 확인합니다. 열 제목을 마우스 오른쪽 단추로 클릭하고 팝업 메뉴에서 **Longest Duration Export(최장 기간 내보내기)**를 선택하여 이 열을 추가해야 할 수도 있습니다. 각 엑스포터 값이 100 미만입니까?

   - 그렇다면, 캐시 내보내기 타이머가 정상입니다.
   - 그렇지 않고 값이 높은 경우, 캐시 내보내기 타이머가 잘못된 것이며 이로 인해 비현실적인 알람을 유발할 수 있습니다. 엑스포터/라우터 컨피그레이션을 확인합니다. (지원에 대한 내용은 *SMC 클라이언트 온라인 도움말*을 참조하십시오.)

4. Identity 디바이스가 있습니까?

   - 그렇다면, 다음 장인 "Cisco ISE 추가"로 이동합니다.
   - 그렇지 않다면, 다음 단계로 이동합니다.

5. SLIC 기능을 사용하고 있습니까?

   - 그렇다면, "SLIC Threat Feed 기능 활성화" 장으로 이동합니다.
   - 그렇지 않다면, 축하합니다. 어플라이언스 컨피그레이션을 완료했습니다.

4

Cisco ISE 추가

개요

Identity 디바이스를 사용하는 경우, 이를 SMC에 추가할 수 있습니다. 이 장에는 Cisco ISE(Identity Services Engine)를 추가하는 절차에 관해 설명합니다.

Cisco ISE 추가

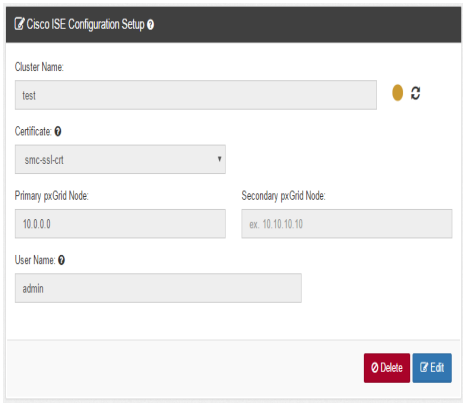
참고:

- 여러 독립된 Cisco ISE 클러스터를 도메인에 추가할 수 있습니다.
- Stealthwatch System에 Cisco ISE-PIC를 추가하는 절차는 아래 설명과 같습니다. Cisco ISE-PIC 설정에 관한 자세한 정보는 Cisco ISE 문서를 참조하십시오.

Cisco ISE를 추가하려면 다음 단계를 완료합니다.

1. SMC 웹 애플리케이션 인터페이스 메뉴에서 **Deploy(구축) > Cisco ISE Configuration(Cisco ISE 컨피그레이션)**을 선택합니다.

Add Cisco ISE(Cisco ISE 추가) 대화 상자가 열립니다.



2. Cisco ISE 클러스터 이름을 입력합니다. Cisco ISE 클러스터를 사용할 Stealthwatch System 도메인마다 클러스터를 구성해야 합니다.
3. 해당하는 인증서를 선택합니다. 이것은 어플라이언스 관리 인터페이스의 SSL 인증서 페이지("ID 업로드" 섹션 내)의 Friendly Name(고유 이름) 필드에 입력한 이름과 동일합니다. 이 인터페이스를 통해 어플라이언스가 클라이언트로서의 자신의 ID를 인증할 수 있습니다(즉, SMC가 ISE에 제공하는 클라이언트 인증서입니다).
4. 어플라이언스에서 통합하려는 ISE 클러스터에 대한 기본 pxGrid 노드의 IP 주소를 입력합니다.
5. (선택 사항) 어플라이언스에서 통합하려는 ISE 클러스터에 대한 보조 pxGrid 노드의 IP 주소를 입력합니다. 이 노드는 페일오버를 위해 사용됩니다. 기본 노드 연결에 실패하면 보조 노드가 사용됩니다.
6. Cisco ISE 디바이스에서 사용자 계정에 대해 구성한 사용자 이름을 입력합니다. 이 이름은 ISE 어플라이언스의 ISE 클러스터에 있는 pxGrid 클라이언트 목록에 표시됩니다.
7. **Add(추가) > OK(확인)**를 클릭합니다. Cisco ISE는 Identity Services 폴더의 도메인에 추가됩니다.
8. SLIC 기능을 사용하고 있습니까?
   - 그렇다면, 다음 장인 "SLIC Threat Feed 기능 활성화"를 계속 진행합니다.
   - 그렇지 않다면, 축하합니다. 어플라이언스 컨피그레이션을 완료했습니다.

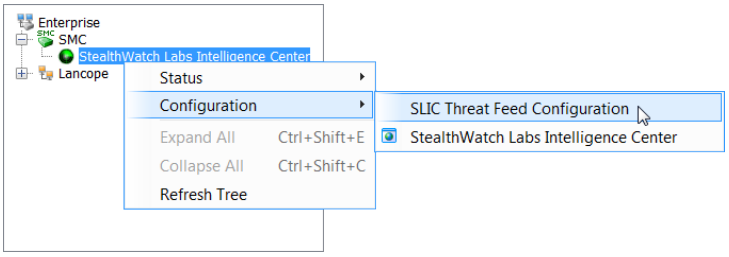
4

SLIC THREAT FEED 기능 활성화

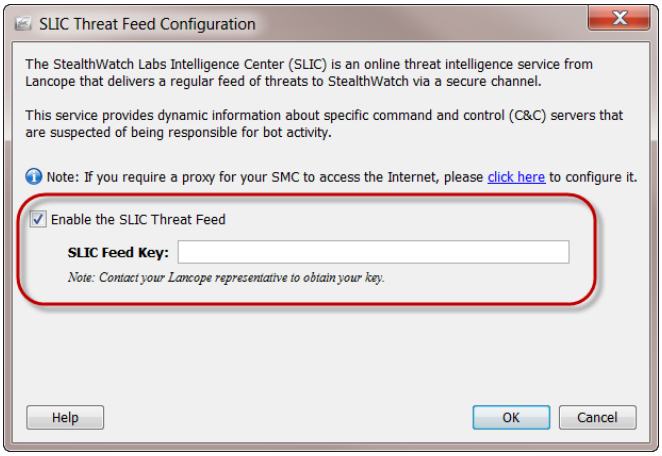
Stealthwatch 패키지 설치 및 구성의 마지막 단계는 SMC 클라이언트 인터페이스를 통해 SLIC Threat Feed를 활성화하는 것입니다.

다음 단계를 완료합니다.

1. Enterprise(엔터프라이즈) 트리에서 **Stealthwatch Labs Intelligence Center** 브랜치를 마우스 오른쪽 버튼으로 클릭한 다음 **Configuration(컨피그레이션) >> SLIC Threat Feed Configuration(SLIC Threat Feed 컨피그레이션)**을 선택합니다.



SLIC Threat Feed Configuration(SLIC Threat Feed 컨피그레이션) 대화 상자가 열립니다.



2. “Enable the SLIC Threat Feed(SLIC Threat Feed 활성화)” 확인란을 선택합니다.
3. SLIC Feed Key(SLIC Feed 키) 필드에 키를 입력합니다.
4. **OK(확인)**를 클릭합니다. 10분 이내에 Enterprise(엔터프라이즈) 트리에서 C&C (Command & Control) 서버 호스트 그룹 브랜치를 업데이트하여 지금까지 확인된 활성 C&C 서버의 목록을 표시합니다.

축하합니다! 이제 Stealthwatch System이 제공하는 여러 가지 보안 및 네트워킹 모니터링 이점을 누리실 수 있습니다. 추가 지원에 대해서는 *Stealthwatch Management Console 사용자 가이드* 또는 SMC 클라이언트 인터페이스 온라인 도움말을 참조하십시오. 내용을 보려면 **도움말**을 클릭하십시오.