Stealthwatch System v6.9.0
내부 알람 ID

저작권 및 상표

알림

이 설명서의 제품 관련 사양 및 정보는 예고 없이 변경될 수 있습니다. 이 설명서의 모든 설명, 정보 및 권장 사항이 정확하다고 판단되더라도 어떠한 형태의 명시적이거나 묵시적인 보증도 하지 않습니다. 모든 제품의 해당 애플리케이션에 대한 사용은 전적으로 사용자에게 책임이 있습니다.

동봉한 제품의 소프트웨어 라이선스 및 제한된 보증은 제품과 함께 제공된 정보 패킷에 설명되어 있으며 본 문서에 참조를 통해 포함됩니다. 소프트웨어 라이선스 또는 제한된 보증을 찾을 수 없는 경우 CISCO 담당자에게 문의하여 복사본을 요청하십시오.

Cisco의 TCP 헤더 압축은 UNIX 운영 체제의 UCB 공개 도메인 버전의 일부로서 UCB(University of Berkeley)에서 개발된 프로그램을 적용하여 구현합니다. All rights reserved. Copyright © 1981, Regents of the University of California.

여기에 명시된 다른 모든 보증에도 불구하고 이러한 공급업체의 모든 문서 파일 및 소프트웨어는 모든 결점을 포함하여 "있는 그대로" 제공됩니다. CISCO 및 위에 언급된 모든 공급업체는 상품성, 특정 목적에의 적합성, 타인의 권리 비침해 또는 처리, 사용, 거래 행위로 발생하는 문제에 대한 묵시적 보증을 포함하여(단, 이에 한하지 않음) 묵시적이든 명시적이든 모든 종류의 보증을 부인합니다.

CISCO 또는 그 공급업체는 이 설명서의 사용 또는 사용할 수 없음으로 인한 모든 파생적, 부수적, 직접, 간접, 특별, 징벌적 또는 기타 모든 손해(영업 이익 손실, 영업 중단, 영업 정보 손실, 또는 그 밖의 금전적 손실로 인한 손해를 포함하되 이에 제한되지 않음)에 대하여 어떠한 경우에도 책임을 지지 않으며, 이는 CISCO 또는 그 공급업체가 그와 같은 손해의 가능성을 사전에 알고 있던 경우에도 마찬가지입니다.

이 문서에서 사용된 모든 IP(인터넷 프로토콜) 주소와 전화 번호는 실제 주소와 전화 번호가 아닙니다. 이 문서에 포함된 예제, 명령 표시 출력, 네트워크 토폴로지 다이어그램 및 다른 그림은 이해를 돕기 위한 자료일 뿐이며, 실제 IP 주소나 전화 번호가 사용되었다면 이는 의도하지 않은 우연의 일치입니다.

모든 인쇄 사본 및 소프트 카피 복제본은 비통제 사본으로 간주되며 원본 온라인 버전을 최신 버전으로 참조해야 합니다.

Cisco는 전 세계에 200개가 넘는 지사를 운영하고 있습니다. 각 지사의 주소, 전화번호 및 팩스 번호는 Cisco 웹사이트(www.cisco.com/go/offices)에서 확인하십시오.

Stealthwatch System v6.9.0 내부 알람 ID

참고: 이전에 사용된 일부 알람이 이제 사용되지 않으며, 더 이상 이 파일에 나타나지 않습니다.

1	호스트 잠금 위반
5	SYN 플러드
6	UDP 플러드
7	ICMP 플러드
8	패킷 플러드
9	대량의 이메일
10	메일 릴레이
11	스팸 소스
12	메일 거부
13	포트 감시 활성화
14	새 호스트 활성화
15	상위 대상 지표(TI)
16	높은 총 트래픽
17	최대 플로우 시작됨
18	새 플로우 시작됨
19	수신된 SYN
20	높은 파일 공유 지수(FSI)
24	의심스러운 UDP 활동
25	MAC 주소 위반
26	절반 열림 공격
28	연결됨
29	낮은 트래픽
30	높은 트래픽
31	호스트 감시 활성화
32	상위 관심 지표(CI)
33	의심스러운 긴 플로우
34	트랩된 호스트
35	웜 활동

36	웜 전파
37	최대 플로우 제공됨
38	새 플로우 제공됨
39	호스트에 경고
40	데이터 손실
41	봇 감염 호스트 - 시도된 C&C 활동(부분 일치)
42	봇 감염 호스트 - 성공적인 C&C 활동(전체 일치)
43	봇 C&C(Command & Control) 서버(제어됨)
44	느린 연결 플러드
45	데이터 유출
46	C&C(Command-and-Control)
47	정책 위반
48	의심스러운 조용한 긴 플로우
49	수신된 UDP
50	ICMP 수신됨
51	정찰
52	데이터 호딩
53	상위 대상 지표(TI)
54	상위 DDoS 소스 인덱스
55	포트 스캔
56	공격
57	이상 징후
58	무차별 대입 로그인
59	가상 호스트와의 통신
60	높은 SMB 피어
61	SSH 역방향 셸
62	위조 애플리케이션 탐지됨
63	스캐너 통신
257	Ping
258	ICMP 시간 초과
259	UDP 시간 초과
260	TCP 시간 초과

261	UDP 재설정
262	TCP 재설정
263	잘못된 플래그 모두
264	잘못된 플래그 SYN FYN
265	잘못된 플래그 예약됨(Sflow만 해당)
266	잘못된 플래그 RST
267	잘못된 플래그 ACK
268	잘못된 플래그 URG
269	잘못된 플래그 플래그 없음
271	Stealth 스캔 UDP
272	Stealth 스캔 TCP
273	소스=대상
276	주소 스캔 TCP
277	Ping 스캔
278	너무 큰 패킷 Ping
281	프래그멘테이션 패킷 너무 짧음
282	프래그멘테이션 패킷 너무 김
283	프래그멘테이션 크기가 다름
286	주소 스캔 UDP
289	연결할 수 없는 ICMP Net
290	연결할 수 없는 ICMP 호스트
291	연결할 수 없는 ICMP 프로토콜
292	연결할 수 없는 ICMP 포트
293	ICMP 프래그멘테이션 필요
294	ICMP 소스 라우팅 실패
295	알 수 없는 ICMP 대상 네트워크
296	알 수 없는 ICMP 대상 호스트
297	ICMP 소스 호스트 격리됨
298	ICMP 대상 네트워크 관리자
299	ICMP 대상 호스트 관리자
300	ICMP 네트워크 연결 불가 TOS
301	ICMP 호스트 연결 불가 TOS

302	ICMP 통신 관리자
303	ICMP 호스트 우선순위
304	ICMP 우선순위 구분
310	플로우 거부됨
315	의심스러운 데이터 호딩
316	표적 데이터 호딩
317	TOR에서 연결 시도됨
318	TOR에서 연결 성공
319	내부 TOR 종료 탐지됨
513	TOR로 연결 시도됨
514	TOR로 연결 성공
515	내부 TOR 엔트리 탐지됨
516	Bogon 주소로 연결 성공
517	Bogon 주소에서 연결 성공
518	Bogon 주소로 연결 시도됨
519	Bogon 주소에서 연결 시도됨
4010	Flow Collector 플로우 데이터 손실
4020	인터페이스 사용률이 인바운드를 초과함
4030	인터페이스 사용률이 아웃바운드를 초과함
5010	FlowSensor VE 컨피그레이션 오류
5011	FlowSensor 트래픽 손실
5012	FlowSensor RAID 실패
5013	FlowSensor RAID 다시 구성
5998	FlowSensor 시간 불일치
5999	FlowSensor 관리 채널 다운
6010	새 VM
6020	V-모션
7001	관계 높은 총 트래픽
7002	관계 높은 트래픽
7003	관계 낮은 트래픽
7004	관계 최대 플로우
7005	관계 새 플로우

7006	관계 왕복 시간
7007	관계 서버 응답 시간
7008	관계 TCP 재전송 비율
7009	관계 SYN 플러드
7010	관계 UDP 플러드
7011	관계 ICMP 플러드
9021	Flow Collector 데이터 삭제됨
9022	Flow Collector 데이터베이스 사용할 수 없음
9023	Flow Collector 데이터베이스 채널 다운
9040	Flow Collector 로그 보존 감소됨
9050	Flow Collector 엑스포터 수 초과됨
9051	Flow Collector FlowSensor VE 수 초과됨
9052	Flow Collector 플로우 비율 초과됨
9053	Flow Collector 인터페이스 수 초과됨
9100	Flow Collector RAID 실패
9102	Flow Collector RAID 다시 구성
9998	Flow Collector 성능 저하됨
9999	Flow Collector 중지됨
60000	Flow Collector 시간 불일치
60001	Cisco ISE 관리 채널 다운
60002	Flow Collector 관리 채널 다운
60003	SMC RAID 실패
60005	SMC RAID 다시 구성
60007	SMC 디스크 공간 부족
60008	SMC 중복 기본
60012	Stealthwatch Flow License 초과됨
60013	라이선스 손상됨
60014	라이선스 없는 기능
60015	SLIC 채널 다운
600016	ID 채널 다운
600017	SMC 장애 조치 채널 다운
600018	Identity Concentrator 채널 다운