Sx500 Series Stackable Switch의 Denial of Service Prevention Technology(Security Suite) 구성

목표

DoS(Denial of Service) 또는 DDoS(Distributed Denial of Service) 공격은 유효한 사용자가 네트워크를 사용하도록 제한합니다.공격자는 네트워크의 모든 대역폭을 차지하는 불필요한 요청으로 네트워크를 플러딩하여 DOS 공격을 수행합니다.DoS 공격은 네트워크 속도를 늦추거나 네트워크를 몇 시간 동안 완전히 잠글 수 있습니다. DoS 보호는 네트워크 보안을 향상시키는 주요 기능입니다.비정상적인 트래픽을 탐지하고 필터링합니다.

보안 제품군 설정에 대한 서비스 거부 구성 및 서비스 거부 방지에 사용되는 다양한 기술에 대해 설명합니다.

참고: 선택한 DoS Prevention이 System-Level 및 Interface-Level Prevention인 경우 Multage Addresses, SYN Filtering, SYN Rate Protection, ICMP Filtering 및 IP Fragment Filtering을 편집하고 구성할 수 있습니다.이러한 구성에 대해서도 이 문서에서 설명합니다.

참고: DoS 방지를 활성화하기 전에 포트에 구성된 모든 ACL(Access Control List) 또는 고급 QoS 정책을 바인딩 해제해야 합니다.포트에서 DoS 보호가 활성화되면 ACL 및 고급 QoS 정책이 활성화되지 않습니다.

적용 가능한 디바이스

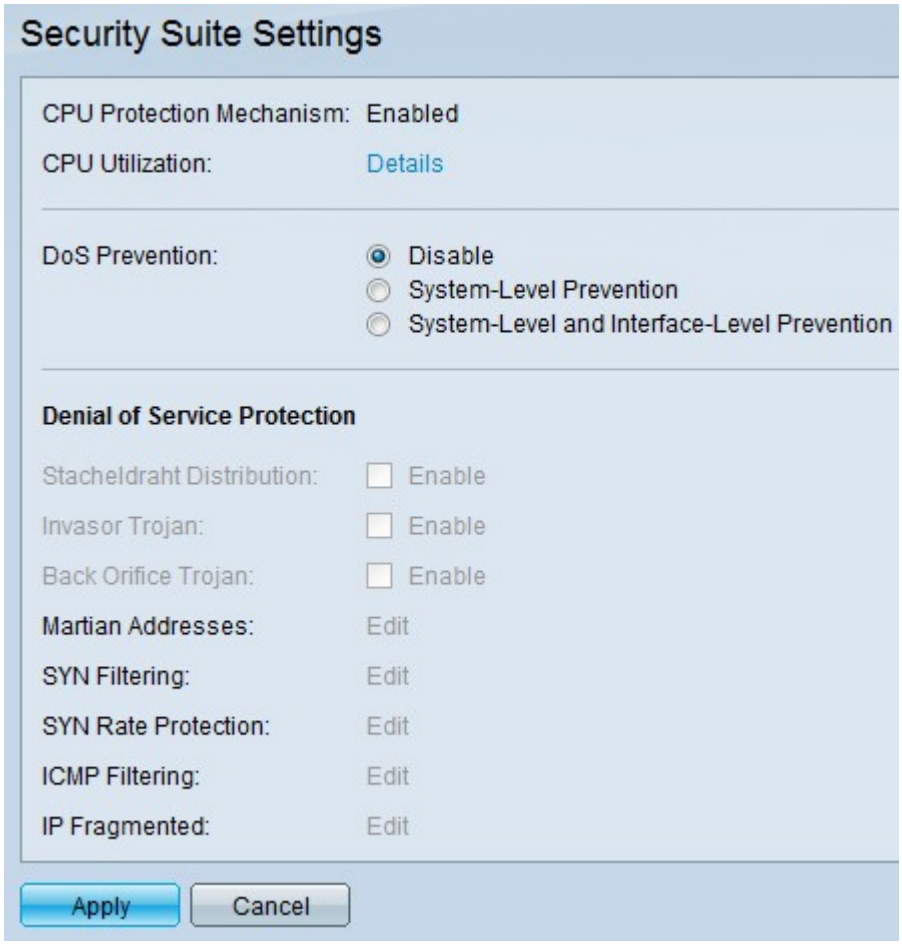
- SX500 Series Stackable Switch

소프트웨어 버전

- 1.3.0.62

보안 제품군 설정에 대한 서비스 거부 구성

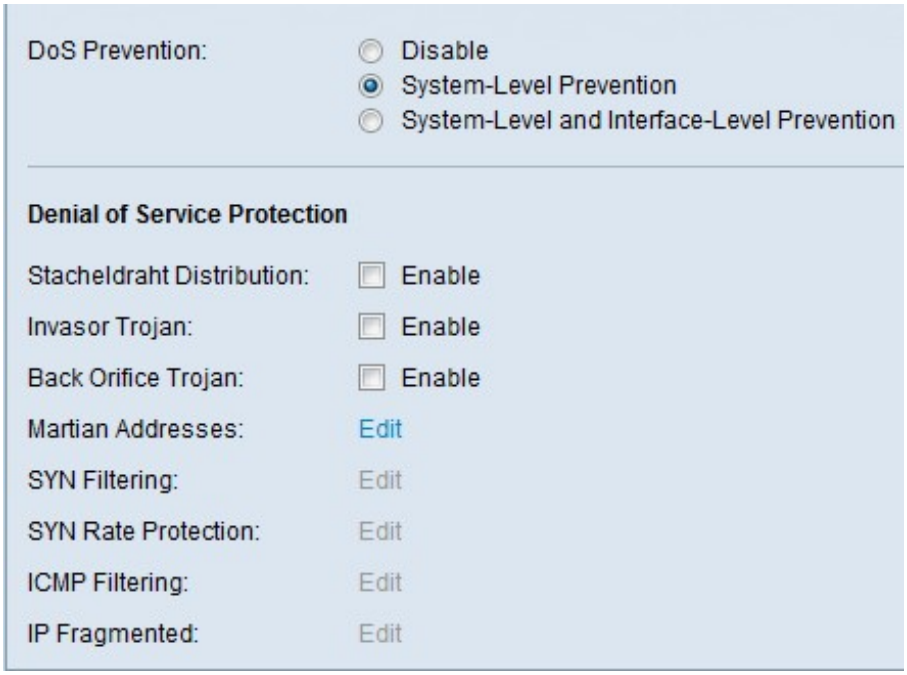
1단계. 웹 구성 유틸리티에 로그인하고 **보안 > 서비스 거부 방지 > 보안 제품군 설정을** 선택합니다.Security *Suite Settings* 페이지가 열립니다.



- CPU 보호 메커니즘 —
- **활성화됨**.이는 SCT(Security Conversion Tool)가 활성화되었음을 나타냅니다.
- CPU 사용률 — 클릭
- **CPU** 사용률 옆에 있는 세부 정보를 참조하여 CPU 리소스 사용률 정보를 확인합니다.

2단계. DoS Prevention(DoS 방지) 필드 아래에서 적절한 라디오 버튼을 클릭합니다.

- Disable — DoS 방지를 비활성화합니다.
- 시스템 레벨 방지 — Stacheldraw Distribution, Invasor Trojan 및 Back Orifice Trojan 공격을 방지합니다.
- 시스템 레벨 및 인터페이스 레벨 방지 — 스위치의 인터페이스당 공격을 방지합니다.



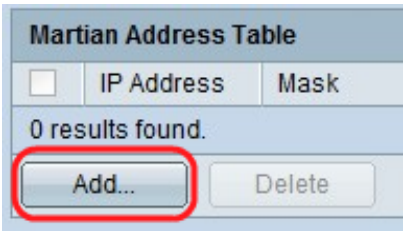
3단계. 서비스 거부 보호를 위해 다음 옵션을 선택할 수 있습니다.

- Stacheldraw 배포 — 공격자가 클라이언트 프로그램을 사용하여 네트워크 내부의 컴퓨터에 연결하는 DDoS 공격의 예입니다.그런 다음 해당 컴퓨터는 내부 서버에 여러 로그인 요청을 보내고 DDoS 공격을 시작합니다.
- Invalor Trojan — 컴퓨터가 이 공격에 감염된 경우 TCP 포트 2140이 악의적인 활동에 사용됩니다.
- Back Orifice 트로이 목마 — DoS 공격을 위해 서버 및 클라이언트 프로그램과 통신하는 데 사용되는 UDP 패킷을 버립니다.

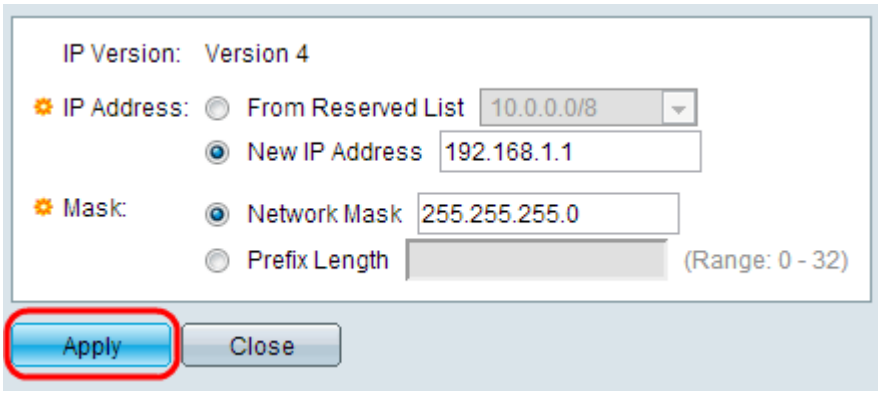
Martian 주소 구성

1단계. Martian Addresses(**Martian 주소**) 필드에서 Edit(수정)를 클릭하면 *Martian Addresses(Martian 주소)* 페이지가 열립니다.Martian Addresses는 네트워크에 대한 공격의 원인이 될 수 있는 IP 주소를 나타냅니다.이러한 네트워크에서 오는 패킷은 삭제됩니다.

2단계. Include in the Reserved Martian Addresses(예약된 **Martian 주소**에 포함)를 선택하고 **Apply(적용)를** 클릭하여 System Level Prevention(시스템 레벨 방지) 목록에 예약된 Martian 주소를 추가합니다.



3단계. Martian 주소를 추가하려면 Add(추가)를 **클릭합니다**.Add *Martian Addresses* 페이지가 표시됩니다.다음 매개변수를 입력합니다.



4단계. IP Address 필드에 거부해야 하는 IP 주소를 입력합니다.

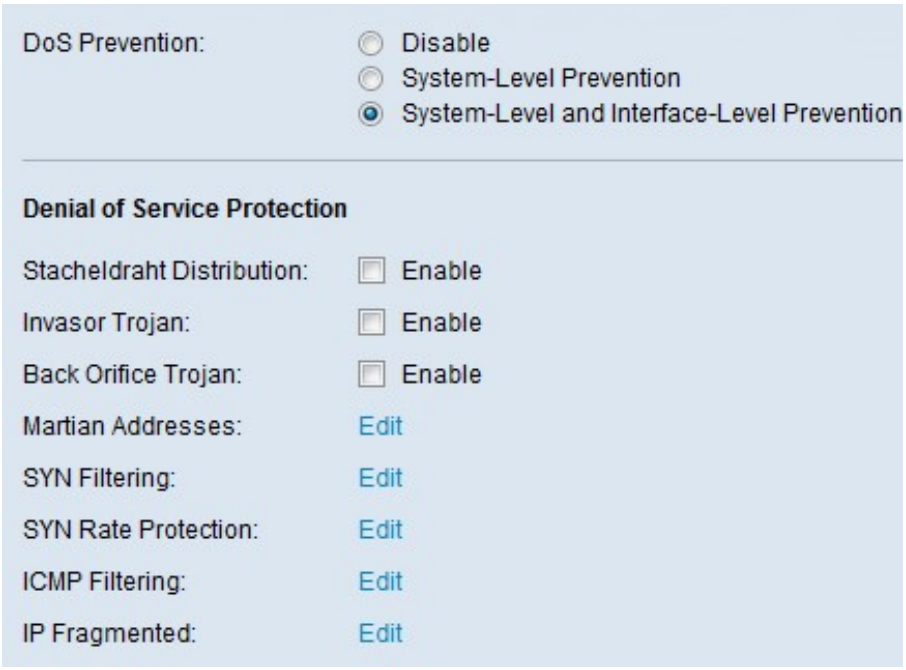
5단계. 거부해야 하는 IP 주소의 범위를 나타내는 IP 주소의 마스크.

- IP 버전 — 지원되는 IP 버전입니다.현재는 IPv4만 허용됩니다.
- 예약된 목록에서 — 예약된 목록에서 알려진 IP 주소를 선택합니다.
- 새 IP 주소 — IP 주소를 입력합니다.
- 네트워크 마스크 — 점으로 구분된 십진수 형식의 네트워크 마스크입니다.
- Prefix Length — Denial of Service Prevention이 활성화된 IP 주소의 범위를 정의하는 IP 주소의 접두사.

6단계. **Apply**를 클릭하면 Martian 주소가 실행 중인 구성 파일에 기록됩니다.

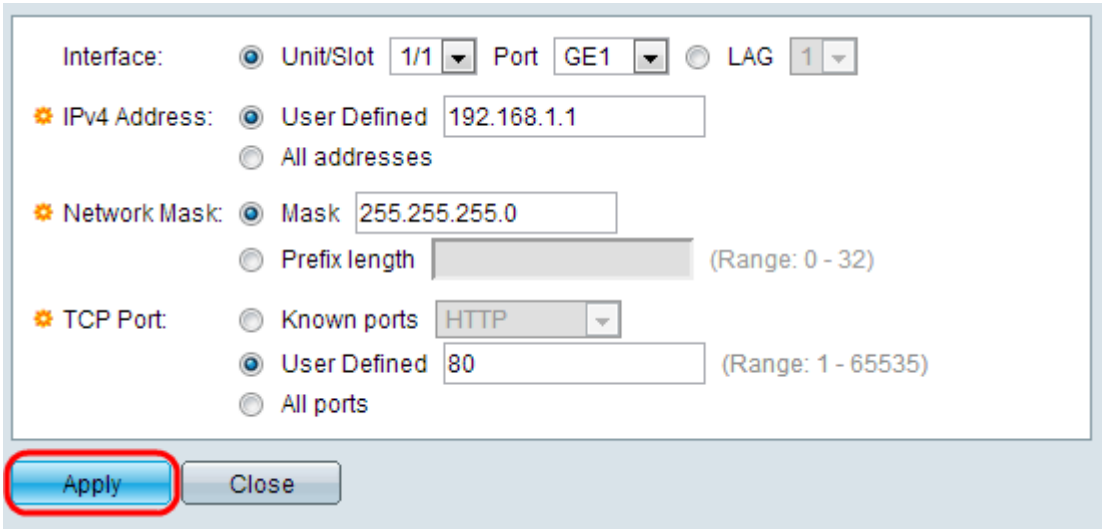
SYN 필터링 구성

SYN 필터링을 사용하면 네트워크 관리자가 SYN 플래그가 있는 잘못된 TCP 패킷을 삭제할 수 있습니다.SYN 포트 필터링은 포트별로 정의됩니다.



1단계. SYN 필터링을 구성하려면 **Edit(편집)**를 클릭하고 *SYN Filtering(SYN 필터링)* 페이지가 열립니다.

2단계. **추가**를 클릭합니다.Add *SYN filtering* 페이지가 표시됩니다.표시된 필드에 다음 매개변수를 입력합니다.

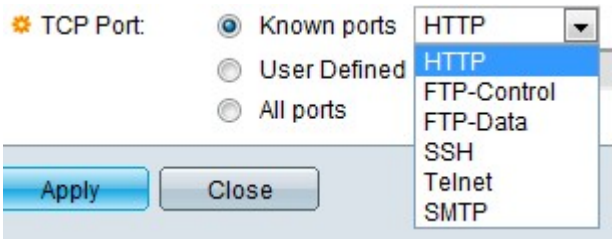


3단계. 필터를 정의해야 하는 인터페이스를 선택합니다.

4단계. **User Defined(사용자 정의)**를 클릭하여 필터가 정의된 IP 주소를 지정하거나 All Addresses(**모든 주소**)를 클릭합니다.

5단계. 필터가 활성화된 네트워크 마스크입니다.Prefix **Length**를 클릭하여 길이를 지정하거나, 범위는 0~32이고, **Mask**를 클릭하여 점으로 구분된 십진수 표기법으로 서브넷 마스크를 입

력합니다.



6단계. 필터링 중인 대상 TCP 포트를 클릭합니다.이러한 유형은 다음과 같습니다.

- Known Ports(알려진 포트) - 목록에서 포트를 선택합니다.
- 사용자 정의 — 포트 번호를 입력합니다.
- All Ports(모든 포트) - 모든 포트가 필터링되었음을 나타내려면 클릭합니다.

7단계. **Apply(적용)**를 클릭하면 SYN 필터링이 실행 중인 컨피그레이션 파일에 기록됩니다.

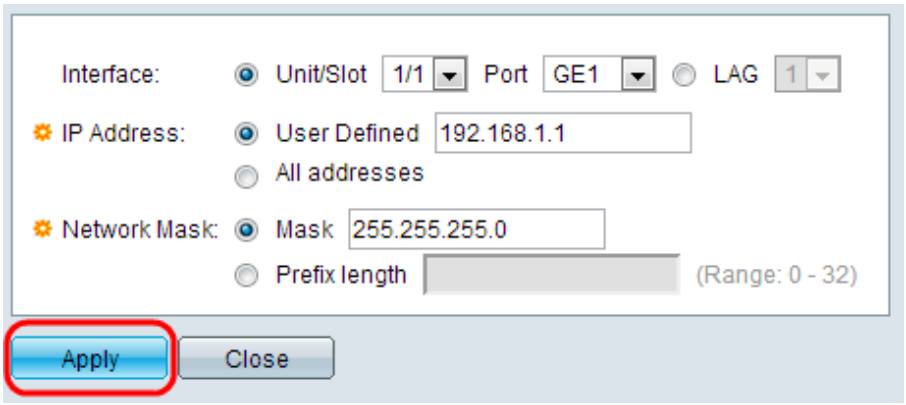
ICMP 필터링 구성

ICMP(Internet Control Message Protocol)는 가장 중요한 인터넷 프로토콜 중 하나입니다.네트워크 레이어 프로토콜입니다.ICMP는 요청된 서비스를 사용할 수 없거나 특정 호스트에 연결할 수 없음을 알리기 위해 운영 체제에서 오류 메시지를 보내는 데 사용됩니다.진단 메시지를 보내는 데에도 사용됩니다.ICMP는 시스템 간에 데이터를 교환하는 데 사용할 수 없습니다.일반적으로 IP 데이터그램의 일부 오류에 대한 응답으로 생성됩니다.

ICMP 트래픽은 매우 중요한 네트워크 트래픽이지만 악의적인 공격자가 네트워크에 대해 사용하는 경우 많은 네트워크 문제를 야기할 수 있습니다.따라서 인터넷에서 오는 ICMP 트래픽을 엄격하게 필터링해야 할 필요성이 대두됩니다.ICMP *Filtering* 페이지에서는 특정 소스의 ICMP 패킷을 필터링할 수 있습니다.이렇게 하면 ICMP 공격이 있을 경우 네트워크의 로드가 최소화됩니다.

1단계. ICMP 필터링을 구성하려면 **Edit(편집)**를 클릭하고 *ICMP Filtering(ICMP 필터링)* 페이지가 열립니다.

2단계. **추가**를 클릭합니다.Add *ICMP Filtering* 페이지가 표시됩니다.표시된 필드에 다음 매개변수를 입력합니다.



3단계. ICMP 필터링이 정의된 인터페이스를 선택합니다.

4단계. ICMP 패킷 필터링이 활성화된 IPv4 주소를 입력하거나 **All Addresses(모든 주소)**를 클릭하여 모든 소스 주소에서 ICMP 패킷을 차단합니다.IP 주소를 입력한 경우 마스크 또는 접두사 길이를 입력합니다.

5단계. 속도 보호가 활성화된 네트워크 마스크입니다.소스 IP 주소의 네트워크 마스크 형식을 선택하고 필드 중 하나를 클릭합니다.

- 마스크 — 소스 IP 주소가 속한 서브넷을 선택하고 점으로 구분된 십진수 형식으로 서브넷 마스크를 입력합니다.
- 길이를 지정하고 소스 IP 주소 접두사로 구성된 비트 수를 입력하려면 **Prefix Length**를 클릭합니다. 비트 범위는 0~32입니다.

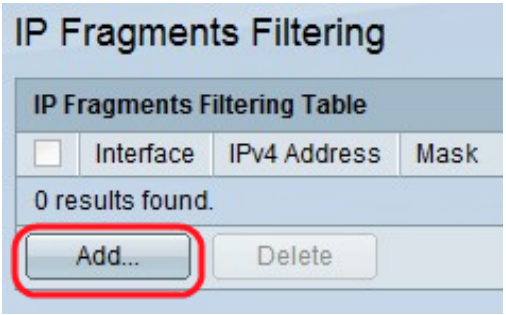
6단계. **Apply**를 클릭하여 ICMP 필터링을 실행 중인 컨피그레이션 파일에 기록합니다.

IP 프래그먼트 필터링 구성

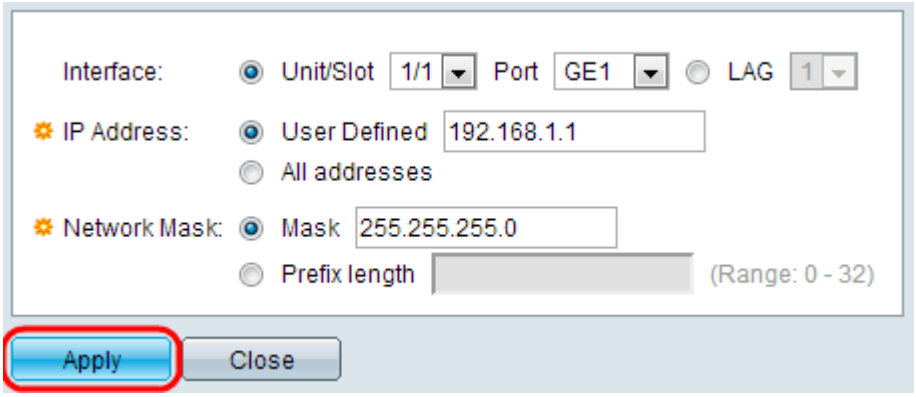
모든 패킷의 MTU(Maximum Transmission Unit) 크기가 있습니다.MTU는 네트워크에서 전송할 수 있는 가장 큰 패킷의 크기입니다.IP는 프래그먼트화의 장점을 활용하여 패킷이 형성될 수 있도록 합니다. 이렇게 하면 원래 패킷 크기보다 작은 MTU로 링크를 통과할 수 있습니다.따라서 링크의 허용되는 MTU보다 큰 패킷은 링크를 통과하도록 허용하려면 더 작은 패킷으로 분할해야 합니다.

반면 단편화는 많은 보안 문제를 야기할 수 있습니다.따라서 때때로 IP 프래그먼트가 시스템 보안 침해의 원인이 될 수 있으므로 이를 차단하는 것이 필요합니다.

1단계. IP 프래그먼트 필터링을 구성하려면 **Edit(편집)**를 클릭하고 *ICMP Fragments Filtering(ICMP 프래그먼트 필터링)* 페이지가 열립니다.



2단계. **추가**를 클릭합니다.Add *IP Fragment Filtering* 페이지가 표시됩니다.표시된 필드에 다음 매개변수를 입력합니다.



3단계. 인터페이스 — IP 단편화가 정의된 인터페이스를 선택합니다.

4단계. IP Address — IP 프래그먼트화가 활성화된 IP 주소를 입력하거나 **All Addresses(모든 주소)를** 클릭하여 모든 소스 주소에서 IP 프래그먼트된 패킷을 차단합니다.IP 주소를 입력한 경우 마스크 또는 접두사 길이를 입력합니다.

5단계. 네트워크 마스크 — IP 단편화가 차단된 네트워크 마스크입니다.소스 IP 주소의 네트워크 마스크 형식을 선택하고 필드 중 하나를 클릭합니다.

- 마스크 — 소스 IP 주소가 속한 서브넷을 선택하고 점으로 구분된 십진수 형식으로 서브넷 마스크를 입력합니다.
- 길이를 지정하고 소스 IP 주소 접두사로 구성된 비트 수를 입력하려면 **Prefix Length**를 클릭합니다. 비트 범위는 0~32입니다.

6단계. **Apply(적용)**를 클릭하여 IP 프래그먼트 필터링을 실행 중인 컨피그레이션 파일에 기록합니다.