

# 300 Series Managed Switch의 SYN 속도 보호

## 목표

DOS(Denial of Service) 방지는 네트워크 보안을 강화하는 네트워크 기술입니다. SYN 속도 보호는 포트 또는 LAG에서 수신할 수 있는 SYN 패킷의 수를 제한하는 DOS 방지 기능입니다. 이는 네트워크에서 SYN 플러드를 방지하는 데 사용됩니다. SYN 플러드는 공격자가 네트워크에 여러 SYN 요청 패킷을 전송할 때 발생하는 DOS 공격의 유형입니다. 이렇게 하면 네트워크가 실제 트래픽에 응답하지 않게 되는 네트워크 리소스가 오버로드됩니다.

이 기능을 사용하려면 *Security Suite Settings* 페이지에서 System-Level 및 Interface-Level Prevention에 DoS Prevention을 활성화해야 합니다. 자세한 내용은 *300 Series Managed Switches의 Security Suite 설정* 문서를 참조하십시오.

이 문서에서는 300 Series Managed Switch의 인터페이스에 SYN 속도 제한을 구성하고 적용하는 방법에 대해 설명합니다.

## 적용 가능한 디바이스

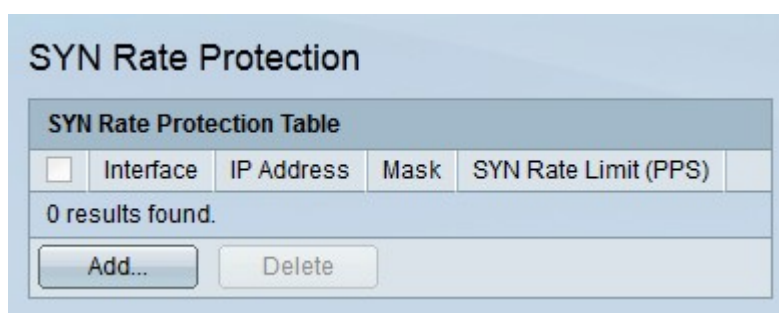
·SF/SG 300 Series Managed Switch

## 소프트웨어 버전

·v1.2.7.76

## SYN 속도 보호

1단계. 웹 구성 유틸리티에 로그인하고 **Security(보안) > Denial of Service Prevention(서비스 거부 방지) > SYN Rate Protection(SYN 속도 보호)**을 선택합니다. *SYN Rate Protection* 페이지가 열립니다.



2단계. **Add(추가)**를 클릭하여 SYN Rate Protection을 추가합니다. *Add SYN Rate Protection* 창이 나타납니다.

Interface:  Port FE1  LAG 1

IP Address:  User Defined 192.168.1.1  All addresses

Network Mask:  Mask 255.255.255.0  Prefix length (Range: 0 - 32)

SYN Rate Limit: 250 PPS (Range: 199 - 1000)

Apply Close

3단계. Interface 필드에서 원하는 인터페이스에 해당하는 라디오 버튼을 클릭합니다.

- Port — Port(포트) 드롭다운 목록에서 SYN 속도 보호를 적용할 포트를 선택합니다.
- LAG — LAG 드롭다운 목록에서 SYN 속도 보호를 적용할 LAG를 선택합니다.

4단계. IP 주소 필드에서 원하는 IPv4 주소에 해당하는 라디오 버튼을 클릭합니다.이러한 IP 주소의 패킷은 SYN 속도 보호에 의해 제한됩니다.

- 사용자 정의 — IPv4 주소를 입력합니다.
- 모든 주소 — 모든 IPv4 주소가 적용됩니다.

5단계. Network Mask(네트워크 마스크) 필드에서 원하는 네트워크 마스크에 해당하는 라디오 버튼을 클릭합니다.

- 마스크 — 네트워크 마스크를 IP 주소 형식으로 입력합니다.이렇게 하면 IP 주소의 서브넷 마스크가 정의됩니다.
- 접두사 길이 — 접두사 길이(0~32 범위의 정수)를 입력합니다. 이렇게 하면 IP 주소의 접두사 길이로 서브넷 마스크가 정의됩니다.

6단계. SYN Rate Limit 필드에 값을 입력합니다.인터페이스에서 초당 수신할 수 있는 최대 SYN 패킷 수입니다.

7단계. 적용을 클릭합니다.SYN 속도 제한이 인터페이스에 적용됩니다.

**SYN Rate Protection**

SYN Rate Protection Table				
<input type="checkbox"/>	Interface	IP Address	Mask	SYN Rate Limit (PPS)
<input type="checkbox"/>	FE1	192.168.1.1	255.255.255.0	250

Add... Delete