시작하기

이 장에서는 Cisco Secure Firewall의 기능 및 지원되는 SD-WAN 기능에 대해 간략하게 설명합니다.

이 발행물에 관하여

이 가이드에서는 Cisco Secure Firewall에서 지원되는 SD-WAN 기능을 사용하는 주요 활용 사례를 자세히 설명합니다.

이러한 접근 방식은 가능한 모든 네트워크 요구 사항을 해결하지는 않습니다. 대신, 네트워크를 패턴화할 수 있는 모델을 제공합니다. 예시에 나와 있는 기능을 사용하지 않도록 선택할 수도 있고, 필요에 더 적합한 기능을 추가 또는 대체할 수도 있습니다.

이 가이드에서는 사용자가 Cisco Secure Firewall에 대해 잘 알고 있다고 가정합니다. 설정에 대한 자세한 정보는 Cisco Secure Firewall Management Center 관리 가이드, 7.3 및 Cisco Secure Firewall Management Center 디바이스 설정 가이드, 7.3을 참조하십시오.

Cisco Secure Firewall

Cisco Secure Firewall은 Snort IPS, URL 필터링, 악성코드 방어 등의 첨단 기능을 갖춘 매우 강력한 방화벽 솔루션입니다.

이 포괄적인 제품은 물리적, 프라이빗 및 퍼블릭 클라우드 환경에서 일관된 보안 정책을 적용하여 위협 방지를 크게 간소화합니다.

또한 네트워크 인프라에 대한 광범위한 가시성을 제공하므로, 잠재적인 위협의 출처와 활동을 신속하게 식별할 수 있습니다. 이러한 정보를 파악하면 운영이 중단되기 전에 공격을 중지하기 위한 조치를 즉시 취할 수 있습니다.

기존 방화벽 기능 외에도 다음과 같은 기능을 제공합니다.

1. AVC(Application Visibility and Control)

2. 사용자 ID 인식 및 제어
3. 침입 방지 및 침입 탐지
4. SSL/TLS 암호 해독
5. 평판 기반 차단
6. 파일 및 악성코드 보호
7. VPN(Virtual Private Network)

네트워크 구축을 더욱 보호하기 위해 Cisco Secure Firewall은 이후 릴리스에서 다음과 같은 추가 보안 기능을 제공합니다.

- EVE(Encrypted Visibility Engine) - 전체 MITM(main-in-the-middle) 암호 해독을 구현할 필요 없이 암호화된 트래픽 검사를 개선합니다.
- 엘리펀트 플로우 탐지 - 엘리펀트 플로우(일반적으로 1GB/10초보다 큰 플로우)를 탐지하고 해결하여 높은 CPU 사용률 및 패킷 삭제를 방지합니다.
- CSDAC(Secure Dynamic Attribute Connector) - 기존 IP/네트워크 기반 정책 구성에 대해 태그와 레이블을 활용하여 보안 정책 관리에 민첩성과 인텔리전스를 제공합니다.

SD-WAN 기능 개요

조직이 여러 브랜치에서 운영을 확장하면서 안전하고 간소화된 연결을 보장하는 것이 무엇보다 중요해졌습니다. 안전한 브랜치 네트워크 인프라 구축에는 복잡한 설정 및 관리 프로세스가 포함되며, 이 프로세스에는 시간이 많이 걸리고 제대로 처리하지 않을 경우 보안 취약점에 노출되기 쉽습니다. 그러나 조직에서는 간소화되고 안전한 브랜치 구축을 위한 보안 방화벽 솔루션을 활용하여 이러한 문제를 해결할 수 있습니다.

이 가이드에서 강력한 방화벽 솔루션을 사용하여 보안 브랜치 구축을 간소화하는 개념을 살펴봅니다. 보안 방화벽을 브랜치 네트워크 아키텍처의 기본 구성 요소로 통합함으로써 조직은 구축 프로세스를 간소화하는 동시에 강력한 보안 베이스라인을 설정할 수 있습니다. 조직에서는 이 접근 방식을 통해 통합 보안 정책을 시행하고 트래픽 라우팅을 최적화하며 복원력 있는 연결을 보장할 수 있습니다.

Cisco Secure Firewall에서 지원되는 일부 SD-WAN 기능은 다음과 같습니다.

- 보안 탄력적 연결:
  - 본사(허브)와 브랜치(스포크) 간 경로 기반(VTI) VPN 터널
  - IPv4 및 IPv6 BGP, IPv4 및 IPv6 OSPFv2/v3, 그리고 IPv4 EIGRP over VTI
  - 정적 또는 동적 IP 스포크에 대한 DVTI 지원
- 네트워크 다운타임이 거의 없는 고가용성:
  - 듀얼 ISP 구성

- 애플리케이션 기반 인터페이스 모니터링을 기반으로 최적의 경로 선택

- 사용 가능한 대역폭 증가**:**
  - 여러 ISP 간 로드 밸런싱을 위한 ECMP 지원
  - SVTI에 대한 ECMP 지원
  - PBR을 사용하는 애플리케이션 기반 로드 밸런싱
- 퍼블릭 클라우드 및 게스트 사용자를 위한 직접 인터넷 액세스**:**
  - 애플리케이션을 일치 기준으로 사용하는 정책 기반 라우팅
  - Umbrella용 로컬 터널 ID 지원
- 간소화된 관리**:**
  - SASE Umbrella 자동 터널 구축
  - DVTI 허브 스포크 토폴로지 간소화

기능

이 표에는 일반적으로 사용되는 몇 가지 WAN 기능이 나와 있습니다.

기능	도입 버전
VTI에 대한 루프백 인터페이스 지원	릴리스 7.3
사이트 간 VPN을 통한 동적 VTI(DVTI) 지원	릴리스 7.3
Umbrella 자동 터널	릴리스 7.3
VTI에 대한 IPv4 및 IPv6 BGP, IPv4 및 IPv6 OSPFv2/v3, IPv4 EIGRP 지원	릴리스 7.3
허브 및 스포크 토폴로지를 사용하는 경로 기반 사이트 간 VPN	릴리스 7.2
경로 모니터링을 사용하는 정책 기반 라우팅	릴리스 7.2
사이트 간 VPN 모니터링 대시보드	릴리스 7.1
직접 인터넷 액세스/정책 기반 라우팅	릴리스 7.1
WAN 인터페이스가 있는 ECMP(Equal-Cost-Multi-Path) 영역	릴리스 7.1
VTI 인터페이스를 사용하는 ECMP(Equal-Cost-Multi-Path) 영역	릴리스 7.1
경로 기반 사이트 간 VPN을 위한 백업 VTI	릴리스 7.0

기능	도입 버전
사이트 간 VPN을 통한 정적 VTI(SVTI) 지원	릴리스 6.7