Cisco ASA 소프트웨어 릴리스 9.0

Cisco® ASA 소프트웨어는 Cisco ASA 보안 디바이스 제품군을 구동하는 핵심 운영 체제입니다. 엔터프라이즈급 방화벽 및 VPN 기능을 제공하고 지속적으로 변화하는 보안 요구 사항을 충족하는 포괄적인 보안 솔루션을 위해 Cisco IPS(Intrusion Prevention System), Cisco Cloud Web Security(이전의 ScanSafe), Cisco ISE(Identity Services Engine) 및 Cisco TrustSec과 통합됩니다.

15년 이상의 검증된 방화벽 및 네트워크 보안 리더십을 보유한 Cisco ASA 소프트웨어는 전 세계에 구축된 100만 대가 넘는 보안 어플라이언스에서 사용되고 있습니다. 동일한 코어 ASA 소프트웨어가 다양한 폼 팩터를 지원합니다. 여기에는 다양한 독립형 어플라이언스, 조직의 기존 네트워크 인프라에 통합되는 하드웨어 블레이드, 퍼블릭 및 프라이빗 클라우드를 보호할 수 있는 소프트웨어가 포함됩니다.

ASA 소프트웨어는 모든 규모의 회사 네트워크를 보호하고 서비스 제공자의 요구에 대응합니다.

클러스터링

고객은 Cisco ASA 소프트웨어 릴리스 9.0을 사용하여 최대 8개의 Cisco ASA 5580 또는 5585-X Adaptive Security Appliance 방화벽 모듈을 단일 클러스터에 결합하여 최대 128Gbps의 실제 처리량(최대 320Gbps)과 5,000만 개가 넘는 동시 연결을 제공할 수 있습니다. 클러스터에 배치될 때 성능이 크게 저하되는 경쟁사 오퍼링과 다르게, ASA 소프트웨어 클러스터링 솔루션은 클러스터의 유닛 수와 관계없이 일관된 배율 인수를 제공합니다. 기존 레이어 2 및 레이어 3 네트워크를 중간에서 높은 수준으로 변경해야 하는 경쟁사 플랫폼의 클러스터링과 다르게, ASA 소프트웨어는 기존 Cisco VSS(Virtual Switching System) 및 Cisco VPC(Virtual PortChannel) 기반의 데이터 센터 설계를 사용하고 표준 LACP(Link Aggregation Control Protocol)에 구축됩니다.

고성능 데이터 센터를 내부 및 외부 위협으로부터 보호하기 위해 최대 60Gbps의 IPS 처리량까지 8개의 IPS 모듈을 추가하여 8유닛 클러스터를 보강할 수 있습니다.

표 1. Cisco ASA Cluster1의 방화벽 성능 데이터[1]

플랫폼	단일 유닛	2유닛 클러스터	4유닛 클러스터	8유닛 클러스터
Cisco ASA 5585X(SSP-10 포함)	2Gbps	3.2Gbps	6.4Gbps	12.8Gbps
Cisco ASA 5585X(SSP-20 포함)	5Gbps	8Gbps	16Gbps	32Gbps
Cisco ASA 5585X(SSP-40 포함)	10Gbps	16Gbps	32Gbps	64Gbps
Cisco ASA 5585X(SSP-60 포함)	20Gbps	32Gbps	64Gbps	128Gbps

성능 이점 이외에도 클러스터는 관리 및 문제 해결이 용이합니다. 마스터 노드에 푸시된 정책은 클러스터 내 모든 유닛에 복제되며 전체 클러스터의 상태, 성능 및 용량 통계는 물론 클러스터 내의 개별 유닛을 단일 관리 콘솔에서 평가할 수 있습니다.

[1] 참고: 성능 데이터는 지침용으로만 제공됩니다. 실제 결과는 비동기 트래픽의 양과 패킷 크기에 따라 다릅니다.

Cisco TrustSec® 통합

ASA 소프트웨어는 향상된 가시성 및 제어를 위해 ID 기반 방화벽 보안과 Cisco TrustSec® 보안 그룹 태그의 통합을 통해 컨텍스트 인식을 제공합니다. ID 기반 방화벽 보안은 더욱 유연한 액세스 제어를 제공하여 사용자 및 그룹의 ID 및 액세스 포인트를 기반으로 정책을 시행할 수 있습니다. 또한 정책 컨피그레이션을 간소화합니다. 관리자는 비즈니스 규칙에 해당하는 정책을 작성할 수 있습니다. 이를 통해 보안이 강화되고 사용 편의성이 향상되며 관리해야 할 정책 수가 줄어듭니다. 마찬가지로, Cisco TrustSec 통합을 통해 보안 그룹 태그를 네트워크의 DNA에 포함할 수 있습니다. 이에 따라 관리자는 더 향상되고 세분화된 정책을 개발 및 시행할 수 있습니다.

Cloud Web Security 통합

ASA 소프트웨어를 Cisco Cloud Web Security와 통합하면 조직에서 로컬 네트워크 보안과 결합된 중앙 집중식 콘텐츠 보안 솔루션을 얻을 수 있습니다. 대부분의 경쟁사 오퍼링에서 사용되는 올인원(all-in-one) 접근 방식과 다르게 Cisco ASA 소프트웨어에서 사용되는 아키텍처 접근 방식은 더 나은 성능과 효율을 제공합니다. 관리자는 네트워크 주소, Microsoft Active Directory 사용자 또는 그룹 이름, 특정 보안 컨텍스트에 상주하는 호스트 등을 기준으로 트래픽 하위 집합에 대한 심층 콘텐츠 검색을 수행할 수 있습니다. 그 결과, ASA 소프트웨어는 뛰어난 성능으로 탁월한 보안을 제공할 수 있습니다.

보안 원격 액세스

ASA 소프트웨어는 Cisco AnyConnect® 3.1 이상과 함께 사용될 때 공용 인터페이스와 SSL 터널 내부에서 IPv4 및 IPv6 듀얼 스팩을 활성화합니다. IPv6 클라이언트리스 지원도 제공됩니다. 대부분의 경쟁사 오퍼링의 경우 IPv4에서 IPv6 트래픽 패턴으로 전환할 때 평균 80%의 성능 저하가 발생하지만, ASA 소프트웨어는 15% 미만의 성능 영향으로 IPv6 원격 액세스 연결을 지원합니다.

또한 ASA 소프트웨어는 IPsec 터널을 사용한 사이트 대 사이트 연결과 원격 액세스에 대한 Suite B 암호화 표준을 포함하는 종합적인 차세대 암호화 기능을 제공합니다.

기능 및 혜택

표 2. 기능 및 혜택

기능	설명	주요 혜택	지원되는 ASA 모델
클러스터링	여러 하드웨어 어플라이언스가 다음을 제공할 수 있습니다. • 최대 128Gbps 실제 처리량 • 최대 동시 연결 수 5,000만 개	• 선형적이며 예측 가능한 규모 및 처리량 증가(예: 동일한 트래픽 프로파일에 대해 2유닛 클러스터는 32Gbps를 지원하고 4유닛 클러스터는 64Gbps를 지원함) • Cisco ASDM(Application Security Device Manager)의 단일 인스턴스를 사용하여 최대 8유닛 클러스터를 구성하고 모니터링 가능 • 클러스터 멤버 간 상태 동기화. 단일 장애 지점 없음	ASA 5580 및 ASA 5585-X 어플라이언스
Cisco Cloud Web Security (Scansafe) 통합	Cisco Cloud Web Security를 통합하여 고객이 웹 보안 및 악성코드 차단을 위해 웹 트래픽을 Cisco 웹 보안 클라우드로 리디렉션하도록 합니다.	• 확인란 보안 제품과 다르게 통합은 성능 및 용량 저하를 최소화하여 포괄적인 웹 보안(URL 필터링, 웹 AVC(Application Visibility and Control) 및 악성코드 차단)을 제공합니다. • 사용자 이름, 사용자 그룹, 소스 또는 대상을 기반으로 하는 추가 분석을 위해 웹 트래픽이 Cisco Cloud Web Security 타워로 리디렉션될 수 있습니다. • 최적화된 성능을 위해 트래픽 리디렉션을 사용합니다. 고객은 트래픽을 세 개의 광범위한 카테고리로 세그먼트화할 수 있습니다. 세 개의 카테고리는 본사 또는 지사 위치로 이동하는 VPN 트래픽, 바로 인터넷으로 이동하는 화이트 리스트 트래픽 및 Cisco Cloud Web Security 타워에 심층 검사용으로 표시되는 트래픽입니다.	모든 ASA 5500 및 5500-X Series 어플라이언스 및 Cisco Catalyst 6500 Series ASA 서비스 모듈

기능	설명	주요 혜택	지원되는 ASA 모델
Trustsec	ASA 소프트웨어를 Cisco TrustSec 아키텍처에 통합하여 SGT(Security Group Tag) 및 보안 그룹 이름이 포함된 방화벽 정책 요소를 기반으로 ASA 소프트웨어 5-튜플 및 ID를 보강합니다.	• 보안 디바이스가 SGT(Security Group Tag)를 일관된 시행 요소로 사용하도록 합니다. • 고객이 ASA 소프트웨어를 사용하여 SGT를 기반으로 정책을 생성하고 시행하도록 합니다. • ASA 소프트웨어가 엔드포인트의 상태 또는 규정준수 변경 사항에 따라 적절한 정책 작업*(예: 액세스 허용, 거부, 제한)*을 수행할 수 있습니다.	모든 ASA 5500 및 5500-X Series 어플라이언스와 Cisco Catalyst 6500 Series ASA 서비스 모듈
차세대 암호화	타원 곡선, SHA-2(256, 384 및 512비트 해시)를 포함한 Suite-B 암호화 알고리즘 집합을 지원합니다. 또한 ESPv3으로 정의된 IPSecv3 및 향상된 IPSecv3 기능을 포함합니다.	• NSA 승인 Suite-B 암호화 사양을 통한 보다 작은 키 크기로 뛰어난 기밀성 및 무결성을 제공합니다.	ASA 5500-X Series 및 ASA 5585-X 어플라이언스
다중 컨텍스트 개선 사항	사이트 대 사이트 VPN 및 동적 라우팅 프로토콜에 대한 지원을 포함하도록 현재 ASA 다중 컨텍스트 기능을 강화합니다. 또한 혼합된 라우팅 및 투명 모드 다중 컨텍스트 컨피그레이션에 대한 지원을 추가합니다.	• 각 방화벽 컨텍스트가 정적 및 동적 경로에 대한 자체 라우팅 테이블을 유지할 수 있습니다. • 고객이 컨텍스트를 기반으로 라우팅 프로토콜을 혼합하고 일치시킬 수 있습니다. • IKEv1 및 IKEv2를 지원합니다. • 다중 모드에서 단일 모드 사이트 대 사이트 VPN 기능을 유지합니다. • 시스템 컨텍스트에서 유연한 VPN 리소스 할당을 허용합니다.	모든 ASA 5500 및 5500-X 어플라이언스(ASA 5505 제외)와 Cisco Catalyst 6500 Series ASA 서비스 모듈

IPv6	혼합된 IPv4/IPv6 구축에 ASA를 구축할 수 있고 고객이 이 즉시 실행 가능한 마이그레이션을 준비합니다.	• 다음을 포함한 중요한 v4에서 v6으로 변환 기능을 제공하여 고객이 IPv6으로의 마이그레이션을 준비할 수 있습니다.
		  ◦ 상태 보존형 NAT64 및 NAT66
		  ◦ DHCPv6 릴레이, DNS64
		  ◦ 혼합된 v4 및 v6 환경에서 정책 컨피그레이션을 간소화하기 위한 통합 ACL
		• IPv4 트래픽에 비해 15% 미만의 성능 영향으로 IPv6 원격 액세스 연결을 제공합니다. 반면, 경쟁사 오퍼링의 경우 IPv4에서 IPv6 트래픽 패턴으로 전환할 때 평균 80%의 성능 저하가 발생합니다.
			모든 ASA 5500 및 5500-X Series 어플라이언스 및 Cisco Catalyst 6500 Series ASA 서비스 모듈

클라이언트리스 VPN과의 Citrix 상호운용성	엔드 유저가 클라이언트리스 포털을 통해 Citrix Xen 인프라에 액세스할 수 있는 기능을 제공합니다.	• 고객이 클라이언트리스 포털을 사용하여 웹 인터페이스를 통해 XenDesktop 및 XenApp에 액세스할 수 있습니다. • XenDesktop(5.0) 및 XenAp(6.0)에 대한 단일 로그인 지원을 제공합니다. • Citrix Mobile Receiver가 ASA에서 Xen 인프라로 바로 종료될 수 있습니다.	모든 ASA 5500 및 5500-X Series 어플라이언스 및 Cisco Catalyst 6500 Series ASA 서비스 모듈
클라이언트리스 VPN 개선 사항	자동 로그인 컨피그레이션을 위한 템플릿 및 툴 Java 기반 파일 브라우저 Java 플러그인에 대한 프록시 지원	• 다양한 애플리케이션에 대해 단일 로그인을 수행하도록 더 쉽고 빠르게 클라이언트리스 포털을 구성할 수 있습니다. • 여러 애플리케이션에 대한 다양한 표준 템플릿을 제공합니다. • 고객이 새로운 Java 기반 파일 브라우저를 사용하여 클라이언트리스 포털을 통해 공유 파일에 액세스할 수 있습니다. • 엔드 유저가 프록시 서버 뒤에 있는 경우에도 고객이 Java 플러그인을 사용하여 TCP/IP 애플리케이션에 액세스할 수 있습니다.	모든 ASA 5500 및 5500-X Series 어플라이언스 및 Cisco Catalyst 6500 Series ASA 서비스 모듈

소프트웨어 다운로드

Cisco ASA 소프트웨어를 다운로드하려면 Cisco Software Center를 방문하십시오.

서비스 및 지원

Cisco 서비스는 고객의 네트워크 투자를 보호하고 네트워크 운영을 최적화하며 새로운 애플리케이션에 맞는 네트워크의 준비를 통해 네트워크 인텔리전스와 고객의 비즈니스 능력 강화에 기여합니다.

Cisco Security IntelliShield Alert Manager Service, Cisco SMARTnet®, Cisco Service Provider Base 및 Cisco Services for IPS는 서비스 라이프사이클의 "운영" 단계에 포함됩니다. 이러한 서비스는 기업 고객, 상용 고객 및 서비스 공급 고객에게 적합합니다.

Cisco Security IntelliShield Alert Manager Service는 조직이 환경에 있는 잠재적 취약성에 대해 정확하고 믿을 수 있는 정보를 적시에 쉽게 액세스할 수 있도록 해주는 사용자 지정 가능한 웹 기반의 위협 및 취약성 경고 서비스를 제공합니다.

Cisco Services for IPS는 IPS 기능을 가지고 있는 모듈, 플랫폼 및 모듈과 플랫폼의 번들을 지원합니다. Cisco SMARTnet 및 Service Provider Base는 이 제품군의 다른 제품을 지원합니다.

추가 정보

자세한 내용은 다음 링크를 참조하십시오.

- Cisco ASA 5500 Series Adaptive Security Appliance: http://www.cisco.com/en/US/products/ps6120/index.html
- Cisco Cloud Web Security: http://www.cisco.com/en/US/products/ps11720/index.html
- Cisco TrustSec: http://www.cisco.com/en/US/netsol/ns1051/index.html
- Cisco AnyConnect Secure Mobility Solution: http://www.cisco.com/en/US/netsol/ns1049/index.html
- Cisco Security Manager: http://www.cisco.com/en/US/products/ps6498/index.html
- Cisco Adaptive Security Device Manager: http://www.cisco.com/en/US/products/ps6121/index.html
- Cisco Security Services: http://www.cisco.com/en/US/products/svcs/ps2961/ps2952/serv_group_home.html
- Cisco ASA 5500 Series Adaptive Security Appliance 라이센싱 정보: http://www.cisco.com/en/US/products/ps6120/products_licensing_information_listing.html

미주 지역 본부
Cisco Systems, Inc.
San Jose CA

아시아 태평양 지역 본부
Cisco Systems (USA) Pte. Ltd.
싱가포르

유럽 지역 본부
Cisco Systems International BV Amsterdam,
네덜란드

Cisco는 전 세계에 200여 개 이상의 지사가 있습니다. 각 지사의 주소, 전화 번호 및 팩스 번호는 Cisco 웹 사이트 **www.cisco.com/go/offices**에서 확인하십시오.

인쇄지: 미국 C78-714849-00 12/16