VM-시리즈

VM 시리즈 차세대 방화벽의 주요 기능:

모든 포트에서 항상 APP-ID™ 로 모든 애플리케이션 분류

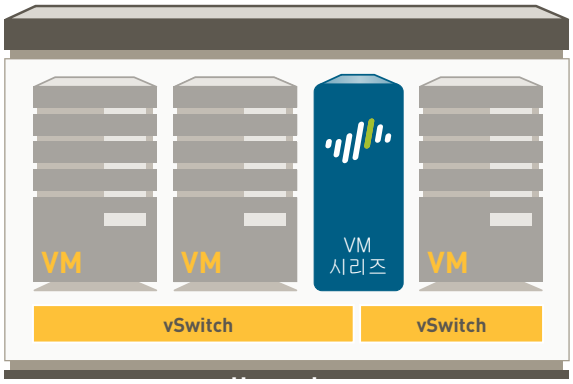
- 포트, 암호화(SSL 또는 SSH) 또는 우회 기법과 관계없이 애플리케이션을 식별합니다.
- 포트가 아닌 애플리케이션을 기반으로 트래픽 허용, 차단, 스케줄링, 위협탐지 및 트래픽 세이핑 적용 등의 모든 애플리케이션 보안 정책을 결정합니다.
- 식별되지 않는 애플리케이션을 분류해 내서 정책 제어, 위협 포렌식, 사용자 정의 App-ID 생성 또는 향후 추가 분석을 위한 패킷 캡처를 할 수 있도록 합니다.

USER-ID™ 및 GLOBALPROTECT™ 를 사용하여 모든 위치에 있는 모든 사용자에게로 애플리케이션 보안 정책 강화

- Active Directory, LDAP, eDirectory Citrix 및 Microsoft Terminal Services와 에이전트 없이 연동됩니다.
- XML API를 사용하여 NAC, 무선 및 기타 비표준 사용자 데이터베이스와 연동합니다.
- Microsoft Windows, Mac OS X, Linux, Android 또는 iOS 플랫폼 사용자에게 일관성 있는 정책을 배포합니다.

CONTENT-ID™ 및 WILDFIRE™ 를 사용하여 알려진, 또는 알려지지 않은 모든 위협으로부터 보호

- 일반적으로 사용되는 우회 기술에 관계없이 취약성 공격, 맬웨어 및 스파이웨어 등의 알려진 다양한 위협을 모든 포트에서 차단합니다.
- 파일과 민감한 데이터의 인증되지 않은 전송을 제한하고 업무와 관련 없는 웹 서핑을 제어합니다.
- 알려지지 않은 맬웨어를 식별하여 100개 이상의 악의적인 행위를 기반으로 분석한 후, 자동으로 시그니처를 생성하여 다음 업데이트를 통해 배포합니다.



VM 시리즈 가상 방화벽에서

Palo Alto Networks™ VM 시리즈는 애플리케이션 보안 구현을 가상화 환경으로 까지 확장하였으며, 동적 주소 오브젝트(Dynamic address object)를 통해 가상 머신의 이동을 추적할 수 있게 하였으며, 강력한 XML 관리 API를 통해 기존의 통합관리 시스템(Ochestration system)과 쉽게 연동할 수 있도록 하였습니다.

VM 시리즈는 고성능 모델인 VM-100, VM-200, VM-300으로 구성되며, 이 세 가지 모두 싱글 패스(Single-Pass) 소프트웨어 아키텍처를 사용하여 데이터센터 환경에서 지연을 최소화합니다. 관리 영역과 데이터 영역이 분리되어 있어서 특정 CPU를 각각에 할당할 수 있으며, 이에 따라 트래픽 부하와 관계없이 항상 매니지먼트에 접속할 수 있도록 합니다. VM 시리즈 컨트롤의 핵심은 보안 전용 OS인 PAN-OS™ 로서, 이는 App-ID, User-ID, Content-ID, GlobalProtect 및 WildFire를 사용하여 애플리케이션을 안전하게 사용할 수 있도록 합니다.

일반 기능[1]	VM-300	VM-200	VM-100
최대 세션	250,000	100,000	50,000
IPSec VPN 터널 인터페이스	2,000	500	25
GlobalProtect(SSL VPN) 동시 사용자	500	200	25
SSL 암호 해독 세션	1024	1024	1024
SSL 인바운드 인증서	25	25	25
가상 라우터	3	3	3
보안 영역	40	20	10
최대 정책 수	5,000	2,000	250
주소 개체	10,000	4,000	2,500
성능 및 가상화 사양[1]			
성능			
방화벽 처리량(App-ID 사용)		1Gbps	
Threat Prevention 처리량		600Mbps	
IPSec VPN 처리량		250Mbps	
초당 새로운 세션		8,000	

[1] 성능 및 용량은 PAN-OS 5.0 및 8 CPU 코어를 사용하여 이상적인 테스트 조건에서 측정됩니다.

paloalto NETWORKS
the network security company™

가상화 사양	VM-300	VM-200	VM-100
HyperVisor	VMware ESXi 4.1 및 ESXi 5.0		
네트워크 드라이버	VMXNet3		
CPU 코어	2, 4 또는 8		
메모리(최소)	4GB		
디스크 드라이브 용량(최소/최대)	40GB/2TB		

네트워킹

인터페이스 모드:

- L2, L3, Tap, Virtual wire (transparent mode)

라우팅

- 모드: OSPF, RIP, BGP, Static
- 포워딩 테이블 크기(장치당/VR당 엔트리): 1000/1000
- 정책 기반 포워딩
- 멀티캐스트: PIM-SM, PIM-SSM, IGMP v1, v2 및 v3

고가용성

- 모드: 액티브/패시브(세션 동기화 없음)
- 오류 감지: 경로 모니터링, 인터페이스 모니터링

주소 할당

- 장치의 주소 할당: DHCP 클라이언트/PPPoE/정적
- 사용자의 주소 할당: DHCP 서버/DHCP 릴레이/정적

IPV6

- L2, L3, tap, virtual wire (transparent mode)
- 기능: App-ID, User-ID, Content-ID, WildFire 및 SSL 암호 해독

VLANS

- 장치당/인터페이스당 802.1q VLAN 태그: 4,094/4,094
- 최대 인터페이스: 200(VM-300), 200(VM-200), 125(VM-100)

NAT/PAT

- 최대 NAT 룰: 1,000(VM-300), 1,000(VM-200), 125(VM-100)
- 최대 NAT 룰(DIPP): 200(VM-300), 200(VM-200), 125(VM-100)
- 동적 IP 및 포트 풀: 254
- 동적 IP 풀: 32,000
- NAT 모드: 1:1 NAT, n:n NAT, m:n NAT
- DIPP 초과 구독(소스 포트 및 IP당 고유 대상 IP): 2
- NAT64

가상 와이어

- 최대 가상 와이어: 500(VM-300), 100(VM-200), 40(VM-100)
- 가상 와이어에 매핑되는 인터페이스 유형: 물리적 및 서브 인터페이스

L2 전달

- ARP 테이블 크기/장치: 1,000(VM-300), 500(VM-200), 500(VM-100)
- MAC 테이블 크기/장치: 1,000(VM-300), 500(VM-200), 500(VM-100)
- IPv6 인접 테이블 크기: 1,000(VM-300), 500(VM-200), 500(VM-100)

보안

방화벽

- 애플리케이션, 사용자 및 콘텐츠에 대한 정책 기반 제어
- 조각 난 패킷 보호
- 사전 검사 보호
- 서비스 거부(DoS)/분산 서비스 거부(DDoS) 보호
- 암호 해독: SSL(인바운드 및 아웃바운드), SSH

WILDFIRE

- 100개 이상의 악의적인 행위에 대해 목표가 설정된 알 수 없는 파일을 식별하고 분석합니다.
- 시그니처 업데이트를 통해 새로 탐지된 맬웨어에 대한 보호를 생성하고 자동으로 제공합니다.
- WildFire 시그니처 업데이트를 통합된 로깅/보고를 1시간 이내에 전달하고 일일 최대 100개의 샘플과 일일 파일 해시에 의한 최대 1,000개 보고서 쿼리를 프로그램 방식 제출을 위해 WildFire API에 액세스합니다(구독 필수).

파일 및 데이터 필터링

- 파일 전송: 60개 이상의 고유한 파일 유형에 대한 양방향 제어
- 데이터 전송: CC# 및 SSN의 인증되지 않은 전송에 대한 양방향 제어
- 드라이브 바이(Drive-by) 다운로드 보호

사용자 통합(USER-ID)

- Microsoft Active Directory, Novell eDirectory, Sun One 및 기타 LDAP 기반 디렉터리
- Microsoft Windows Server 2003/2008/2008r2, Microsoft Exchange Server 2003/2007/2010
- Microsoft Terminal Services, Citrix XenApp
- 비 표준 사용자 리포지토리와의 통합을 용이하게 해주는 XML API

IPSEC VPN(사이트 간)

- 키 교환: 수동 키, IKE v1
- 암호화: 3DES, AES(128비트, 192비트, 256비트)
- 인증: MD5, SHA-1, SHA-256, SHA-384, SHA-512
- 동적 VPN 터널 생성(GlobalProtect)

위협 예방(구독 필수)

- 애플리케이션, 운영 체제 취약성 공격 방지
- 바이러스(HTML, Javascript, PDF 및 압축 파일에 내장된 바이러스 포함), 스파이웨어, 웜에 대한 스트림 기반 방지

URL 필터링(구독 필수)

- 미리 정의된 사용자 정의 URL 범주
- 가장 최근에 액세스한 URL의 장치 캐시
- 보안 정책을 위한 일치 기준의 일환으로 사용되는 URL 범주
- 시간 정보 찾아보기

서비스 품질(QOS)

- 애플리케이션, 사용자, 소스, 대상, 인터페이스, IPSec VPN 터널 등의 기준별 정책 기반 트래픽 셰이핑
- 최대 및 우선 순위 대역폭 매개변수를 보장하는 8개의 트래픽 등급
- 실시간 대역폭 모니터
- 정책 DiffServ 표시당
- QoS에 지원되는 물리적 인터페이스: 6(VM-300, VM-200), 4(VM-100)

SSL VPN/원격 액세스(GLOBALPROTECT)

- GlobalProtect 게이트웨이
- GlobalProtect 포털
- 전송: 대체 SSL이 있는 IPSec
- 인증: LDAP, SecurID 또는 로컬 DB
- 클라이언트 OS: Mac OS X 10.6, 10.7(32/64비트), 10.8(32/64비트), Windows XP, Windows Vista(32/64비트), Windows 7(32/64비트)
- 타사 클라이언트 지원: Apple iOS, Android 4.0 이상, Linux용 VPNC IPSec

관리, 보고, 가시성 도구

- 통합 웹 인터페이스, CLI 또는 중앙 관리(Panorama)
- 다국어 사용자 인터페이스
- Syslog, Netflow v9 및 SNMP v2/v3
- XML 기반 REST API
- 애플리케이션, URL 범주, 위협 및 데이터(ACC)의 그래픽 요약
- 트래픽, 위협, WildFire, URL 및 데이터 필터링 로그 보기, 필터링 및 내보내기
- 완전 사용자 정의 가능 보고

VM 시리즈 차세대 방화벽 기능에 대한 자세한 설명은 www.paloaltonetworks.com/literature를 참조하십시오.

paloalto NETWORKS
the network security company™

3300 Olcott Street
Santa Clara, CA 95054

Accueil : +1.408.573.4000
Ventes : +1.866.320.4788
Assistance : +1.866.898.9087

www.paloaltonetworks.com

PAN_SS_VM_112712