VM-Series

Wesentliche Funktionen der VM Series-Firewall der nächsten Generation:

KLASSIFIZIEREN SIE MIT APP-ID™ JEDERZEIT SÄMTLICHE ANWENDUNGEN AUF ALLEN PORTS.

- Identifizieren Sie die Anwendung unabhängig vom Port, der Verschlüsselung (SSL oder SSH) oder der eingesetzten Umgehungsmethode.
- Nutzen Sie die Anwendung und nicht den Port als Basis für sämtliche Entscheidungen im Rahmen der Richtlinie zur sicheren Aktivierung: zulassen, ablehnen, planen, prüfen, Traffic-Shaping anwenden
- Kategorisieren Sie nicht identifizierte Anwendungen für die Richtlinienkontrolle, die Bedrohungsanalyse, die Erstellung benutzerdefinierter App-IDs oder die Datenaufzeichnung für eine weitere Prüfung.

ERWEITERN SIE MIT USER-ID™ UND GLOBALPROTECT™ DIE RICHTLINIEN ZUR SICHEREN ANWENDUNGSAKTIVIERUNG AUF BELIEBIGE BENUTZER UND STANDORTE.

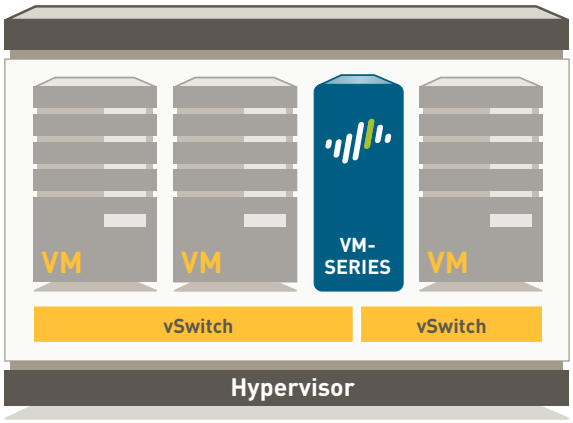
- Agentenlose Integration in Active Directory, LDAP, eDirectory Citrix und Microsoft Terminal Services.
- Integration in NAC, drahtloses 802.1X und andere nicht standardmäßige Benutzer-Repositorys mit einer XML-API.
- Bereitstellung konsistenter Richtlinien für Benutzer, die Microsoft Windows-, Mac OS X-, Linux-, Android- oder iOS-Plattformen ausführen.

MIT CONTENT-ID™ UND WILDFIRE™ KÖNNEN SIE SICH VOR SÄMTLICHEN BEKANNTEN UND UNBEKANNTEN BEDROHUNGEN SCHÜTZEN.

- Blockieren Sie eine Reihe von bekannten Bedrohungen, einschließlich Ausnutzung von Sicherheitslücken, Malware und Spyware – auf allen Ports, unabhängig von den eingesetzten Taktiken zur Vermeidung gängiger Bedrohungen.
- Beschränken Sie die Übertragung von Dateien und sensiblen Daten und kontrollieren Sie die nicht arbeitsbezogene Internetsuche.
- Identifizieren Sie unbekannte Malware und suchen Sie nach über 100 schädlichen Funktionsweisen. Mit dem nächsten verfügbaren Update ist das automatische Erstellen und Bereitstellen von Schutz möglich.

paloalto NETWORKS

the network security company™



VM-Series Virtual Firewall

Mit der Palo Alto Networks™ VM-Series ist die sichere Aktivierung von Anwendungen auch in virtualisierten Umgebungen möglich, wobei die wichtigsten Sicherheitsanforderungen bei der Virtualisierung erfüllt werden: Verfolgen der Sicherheitsrichtlinien auf die Bewegung virtueller Rechner anhand von dynamischen Adressen sowie die Integration in Orchestrierungssysteme mithilfe einer leistungsstarken XML-Management-API.

Die VM-Series-Firewall besteht aus den drei Hochleistungsmodellen VM-100, VM-200 und VM-300, die eine Single-Pass-Software-Architektur zur Minimierung von Latenz in Rechenzentrumsumgebungen nutzen. Die Management- und Datenebenen sind voneinander getrennt, sodass die Benutzer jeder entsprechende CPUs zuweisen können, um sicherzustellen, dass der Management-Zugriff unabhängig von der Höhe des Datenflusses jederzeit verfügbar ist. Die VM Series wird über PAN-OS™ gesteuert, ein sicherheitsspezifisches Betriebssystem, über das Unternehmen Anwendungen sicher unter Verwendung von App-ID, User-ID, Content-ID, GlobalProtect und WildFire aktivieren können.

ALLGEMEINE KAPAZITÄTEN[1]	VM-300	VM-200	VM-100
Max. Anzahl an Sitzungen	250.000	100.000	50.000
IPSec-VPN-Tunnel/Tunnelschnittstellen	2.000	500	25
Gleichzeitige Benutzer von GlobalProtect (SSL VPN)	500	200	25
SSL-Entschlüsselungssitzungen	1024	1024	1024
Eingehende SSL-Zertifkate	25	25	25
Virtuelle Router	3	3	3
Sicherheitszonen	40	20	10
Max. Anzahl an Richtlinien	5.000	2.000	250
Adressobjekte	10.000	4.000	2.500
Leistung[1] und Virtualisierungsspezifikationen			
PERFORMANCE[1]			
Firewall-Durchsatz (aktivierte App-ID)	1 Gbit/s		
Bedrohungsschutz-Durchsatz	600 Gbit/s		
IPSec-VPN-Durchsatz	250 Gbit/s		
Neue Sitzungen pro Sekunde	8.000		

[1] Leistung und Kapazitäten werden unter idealen Testbedingungen mit PAN-OS 5.0 und 4 CPU gemessen.

VIRTUALISIERUNGSSPEZIFIKATIONEN	VM-300 VM-200 VM-100
HyperVisor	VMware ESXi 4.1 und ESXi 5.0
Netzwerktreiber	VMXNet3
CPU-Cores	2, 4 oder 8
Speicher (Minimum)	4 GB
Laufwerkskapazität (Min./Max.)	40 GB/2 TB

NETZWERK

SCHNITTSTELLENMODI:

- L2, L3, TAP, Virtual Wire (transparenter Modus)

ROUTING

- Modi: OSPF, RIP, BGP, Static
- Größe der Weiterleitungstabelle (Einträge pro Gerät und VR): 1000/1000
- Richtlinienbasierte Weiterleitung
- Multicase: PIM-SM, PIM-SSM, IGMP v1, v2 und v3

HOHE VERFÜGBARKEIT

- Modi: Aktiv/passiv ohne Synchronisierung der Sitzung
- Fehlererkennung: Pfadüberwachung, Schnittstellenüberwachung

ADRESSZUWEISUNG

- Adresszuweisung für Gerät: DHCP-Client/PPPoE/Static
- Adresszuweisung für Benutzer: DHCP-Server/DHCP Relay/Static

IPV6

- L2, L3, TAP, Virtual Wire (transparenter Modus)
- Funktionen: App-ID, User-ID, Content-ID, WildFire und SSL-Entschlüsselung

VLANS

- 802.1q VLAN-Tags pro Gerät und Schnittstelle: 4,094/4,094
- Max. Anzahl an Schnittstellen: 2.000 (VM-300), 500 (VM-200), 100 (VM-100)

NAT/PAT

- Max. Anzahl an NAT-Regeln: 1.000 (VM-300), 1.000 (VM-200), 125 (VM-100)
- Max. Anzahl an NAT-Regeln (DIPP): 200 (VM-300), 200 (VM-200), 125 (VM-100)
- Pool dynamischer IP-Adressen und Ports: 254
- Pool dynamischer IP-Adressen: 32.000
- NAT-Modi: 1:1 NAT, n:n NAT, m:n NAT
- DIPP-Überbelegung (Eindeutige Ziel-IPs pro Quell-Port und IP): 2 (VM-300), 1 (VM-200), 1 (VM-100)
- NAT64

VIRTUAL WIRE

- Max. Anzahl an Virtual Wires: 1,000 (VM-300), 250 (VM-200), 50 (VM-100)
- Schnittstellentypen auf Virtual Wires abgebildet: physische und Teilschnittstellen

L2-WEITERLEITUNG

- Größe der ARP-Tabelle/Gerät: 2.500 (VM-300), 500 (VM-200), 500 (VM-100)
- Größe der MAC-Tabelle/Gerät: 2.500 (VM-300), 500 (VM-200), 500 (VM-100)
- Größe der IPv6-Nachbartabelle: 1.000 (VM-300), 500 (VM-200), 500 (VM-100)

SICHERHEIT

FIREWALL

- Richtlinienbasierte Steuerung von Anwendungen, Benutzern und Inhalt
- Schutz fragmentierter Pakete
- Schutz vor Auskundschaftung
- Schutz vor Denial of Service (DoS)/Distributed Denial of Services (DDoS)
- Entschlüsselung: SSL (eingehend und ausgehend), SSH

WILDFIRE

- Identifizieren und analysieren Sie über 100 schädliche Funktionsweisen in zielgerichteten und unbekannten Dateien.
- Generieren Sie Schutz für neu entdeckte Malware und stellen Sie diesen automatisch über Signatur-Updates bereit
- Bereitstellung des Signatur-Updates in weniger als einer Stunde, integrierte Protokollierung/Berichterstellung, Zugriff auf WildFire-API für programmatische Eingabe von bis zu 100 Mustern und bis zu 1.000 Berichtsanfragen nach Datei-Hash pro Tag (Abonnement erforderlich)

DATEI- UND DATENFILTERUNG

- Dateiübertragung: Bidirektionale Steuerung von über 60 eindeutigen Dateitypen
- Datenübertragung: Bidirektionale Steuerung von nicht autorisierter Übertragung von CC-Nr. und SSN
- Schutz vor unbeabsichtigtem Herunterladen

BENUTZERINTEGRATION (USER-ID)

- Microsoft Active Directory, Novell eDirectory, Sun One und andere LDAP-basierte Verzeichnisse
- Microsoft Windows Server 2003/2008/2008r2, Microsoft Exchange Server 2003/2007/2010
- Microsoft Terminal Services, Citrix XenApp
- XML-API für die Integration in nicht standardmäßige Benutzer-Repositorys

IPSEC-VPN (STANDORT-ZU-STANDORT)

- Schlüsselaustausch: Manueller Schlüssel, IKE v1
- Verschlüsselung: 3DES, AES (128-Bit, 192-Bit, 256-Bit)
- Authentifizierung: MD5, SHA-1, SHA-256, SHA-384, SHA-512
- Dynamische VPN-Tunnelerstellung (GlobalProtect)

BEDROHUNGSSCHUTZ (ABONNEMENT ERFORDERLICH)

- Anwendung, Schutz vor Ausnutzung von Sicherheitslücken im Betriebssystem
- Stream-basierter Virenschutz (einschließlich Viren in HTML, Javascript, PDF und komprimierten Dateien), Spyware, Würmer

URL-FILTERUNG (ABONNEMENT ERFORDERLICH)

- Vordefinierte und benutzerdefinierte Kategorien
- Geräte-Cache für die zuletzt aufgerufenen URLs
- URL-Kategorie als Teil der Übereinstimmungskriterien für Sicherheitsrichtlinien
- Informationen zur Surfzeit

QUALITY-OF-SERVICE (QOS)

- Richtlinienbasiertes Traffic-Shaping nach Anwendung, Benutzer, Quelle, Zielort, Schnittstelle, IPSec-VPN-Tunnel und mehr
- 8 Traffic-Klassen mit garantierten, maximalen und priorisierten Bandbreitenparametern
- Bandbreitenüberwachung in Echtzeit
- Diffserv-Markierung pro Richtlinie
- Unterstützte physische Schnittstellen für QoS: 6 (VM-300, VM-200), 4 (VM-100)

SSL-VPN/REMOTE-ZUGRIFF (GLOBALPROTECT)

- GlobalProtect Gateway
- GlobalProtect Portal
- Transport: IPSec mit SSL-Fallback
- Authentifizierung: LDAP, SecurID oder lokale DB
- Client-Betriebssystem: Mac OS X 10.6, 10.7 (32/64 Bit), 10.8 (32/64 Bit), Windows XP, Windows Vista (32/64 Bit), Windows 7 (32/64 Bit)
- Client-Support von Drittanbietern: Apple iOS, Android 4.0 und höher, VPNC-IPSec für Linux

MANAGEMENT, BERICHTE, TRANSPARENZ-TOOLS

- Integrierte Webschnittstelle, CLI oder zentrale Verwaltung (Panorama)
- Mehrsprachige Benutzeroberfläche
- Syslog, Netflow v9 und SNMP v2/v3
- XML-basierte REST-API
- Grafische Zusammenfassung aller Anwendungen, URL-Kategorien, Bedrohungen und Daten (ACC)
- Protokolle zu Traffic, Bedrohung, WildFire, URL und Datenfilterung anzeigen, filtern und exportieren
- Vollständig anpassbare Berichte

Eine vollständige Beschreibung des Funktionssatzes der VM-Series-Firewall der nächsten Generation finden Sie unter www.paloaltonetworks.com/literature.

paloalto NETWORKS
the network security company™

3300 Olcott Street
Santa Clara, CA 95054

Main: +1.408.573.4000
Sales: +1.866.320.4788
Support: +1.866.898.9087

www.paloaltonetworks.com