Serie VM

Funzionalità principali del firewall Serie VM di nuova generazione

CLASSIFICAZIONE DI TUTTE LE APPLICAZIONI, SU TUTTE LE PORTE, IN QUALSIASI MOMENTO CON APP-ID™.

- Identificazione dell'applicazione, indipendentemente da porta, crittografia (SSL o SSH) o impiego di tecniche di evasione.
- Decisioni relative alle policy di abilitazione sicura (consenso, rifiuto, pianificazione, analisi, applicazione di shaping del traffico) basate sulle applicazioni e non sulle porte.
- Categorizzazione di applicazioni non identificate per il controllo delle policy, per la raccolta di informazioni sulle minacce, per la creazione di App-ID personalizzati o per l'acquisizione di pacchetti a scopo di ulteriore indagine.

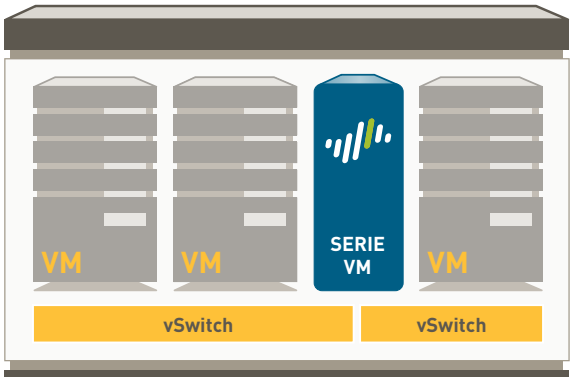
ESTENSIONE DELLE POLICY DI ABILITAZIONE SICURA DELLE APPLICAZIONI A QUALSIASI UTENTE, QUALSIASI POSIZIONE CON USER-ID™ E GLOBALPROTECT™.

- Integrazione senza agente con Active Directory, LDAP, eDirectory Citrix e Microsoft Terminal Services.
- Integrazione con NAC, 802.1X wireless e altre tipologie non standard di repository utente attraverso un'API XML.
- Distribuzione di policy coerenti a utenti che utilizzano piattaforme Microsoft Windows, Mac OS X, Linux, Android o iOS, indipendentemente dalla posizione.

PROTEZIONE CONTRO TUTTE LE MINACCE: CONOSCIUTE E SCONOSCIUTE CON CONTENT-ID™ E WILDFIRE™.

- Blocco di una gamma di minacce conosciute inclusi exploit, malware e spyware, per tutte le porte, indipendentemente dai meccanismi comuni di evasione delle minacce impiegati.
- Limitazione dei trasferimenti non autorizzati di file e dati sensibili e controllo della navigazione online non legata alle attività lavorative.
- Identificazione di malware sconosciuti, analisi di oltre 100 comportamenti dannosi, creazione automatica e distribuzione di funzionalità di protezione con il successivo aggiornamento disponibile.

paloalto NETWORKS
the network security company™



Firewall virtuale della Serie VM

La Serie VM di Palo Alto Networks™ estende l'abilitazione sicura delle applicazioni agli ambienti virtualizzati affrontando al contempo le principali sfide di protezione della virtualizzazione: monitoraggio delle policy di protezione in base allo spostamento delle macchine virtuali con oggetti indirizzo dinamici e integrazione con sistemi di orchestrazione con potenti API di gestione XML.

La Serie VM si compone di tre modelli a elevate prestazioni: VM-100, VM-200 e VM-300 che utilizzano tutti un'architettura software di tipo "single pass" per ridurre la latenza negli ambienti di data center. I piani di controllo dati e di gestione sono separati in modo da consentire agli utenti di assegnare risorse di CPU dedicate a ciascun al fine di garantire la disponibilità continua dell'accesso di gestione, indipendentemente dal carico di traffico. L'elemento di controllo della Serie VM è PAN-OS™, un sistema operativo specifico per la protezione che consente alle organizzazioni di abilitare applicazioni in tutta sicurezza utilizzando funzionalità quali App-ID, User-ID, Content-ID, GlobalProtect e WildFire.

CAPACITÀ GENERALI[1]	VM-300	VM-200	VM-100
N. massimo di sessioni	250.000	100.000	50.000
tunnel/interfacce tunnel VPN IPSec	2.000	500	25
GlobalProtect (VPN SSL) per utenti simultanei	500	200	25
Sessioni di decrittografia SSL	1024	1024	1024
Certificati SSL in entrata	25	25	25
Router virtuali	3	3	3
Zone di protezione	40	20	10
N. massimo di policy	5.000	2.000	250
Oggetti indirizzo	10.000	4.000	2.500
PRESTAZIONI[1]			
Velocità del firewall (con supporto per App-ID)	1 Gb/s		
Velocità della prevenzione delle minacce	600 Gb/s		
Velocità VPN IPSec	250 Gb/s		
Nuove sessioni al secondo	8.000		

[1] Le prestazioni e le capacità vengono misurate in condizioni di test ideali utilizzando PAN-OS 5.0 e 4 core CPU.

SPECIFICHE DI VIRTUALIZZAZIONE	VM-300 VM-200 VM-100
HyperVisor	VMware ESXi 4.1 e ESXi 5.0
Driver di rete	VMXNet3
core CPU	2, 4 o 8
Memoria (minima)	4 GB
Capacità disco rigido (minima/massima)	40 GB/2 TB

RETE

MODALITÀ INTERFACCIA:

- L2, L3, Tap, cablaggio virtuale (modalità trasparente)

ROUTING

- Modalità: OSPF, RIP, BGP, Statica
- Dimensioni della tabella di inoltro (voci per dispositivo/per VR): 1000/1000
- Inoltro basato su policy
- Multicasting: PIM-SM, PIM-SSM, IGMP v1, v2 e v3

ALTA DISPONIBILITÀ

- Modalità: Active/Passive senza sincronizzazione della sessione
- Rilevamento guasti: monitoraggio dei percorsi, monitoraggio delle interfacce

ASSEGNAZIONE INDIRIZZI

- Assegnazione indirizzi per dispositivi: Client DHCP/PPPoE/Statica
- Assegnazione indirizzi per utenti: Server DHCP/Relè DHCP/Statica

IPV6

- L2, L3, tap, cablaggio virtuale (modalità trasparente)
- Funzionalità: App-ID, User-ID, Content-ID, WildFire e decrittografia SSL

VLAN

- 802.1q VLAN tag per dispositivo/per interfaccia: 4.094/4.094
- N. massimo di interfacce: 2.000 (VM-300), 500 (VM-200), 100 (VM-100)

NAT/PAT

- N. massimo di regole NAT: 1.000 (VM-300), 1.000 (VM-200), 125 (VM-100)
- N. massimo di regole NAT (DIPP): 200 (VM-300), 200 (VM-200), 125 (VM-100)
- Pool porta e IP dinamico: 254
- Pool IP dinamico: 32.000
- Modalità NAT: 1:1 NAT, n:n NAT, m:n NAT
- Oversubscription DIPP (n. di IP con destinazione univoca per porta di origine e IP): 2 (VM-300), 1 (VM-200), 1 (VM-100)
- NAT64

CABLAGGIO VIRTUALE

- N. massimo di cavi virtuali: 1.000 (VM-300), 250 (VM-200), 50 (VM-100)
- Tipi di interfacce mappate ai cavi virtuali: fisiche e sottointerfacce

INOLTRO L2

- Dimensioni tabella ARP/dispositivo: 2.500 (VM-300), 500 (VM-200), 500 (VM-100)
- Dimensione tabella/dispositivo MAC: 2.500 (VM-300), 500 (VM-200), 500 (VM-100)
- Dimensioni tabella adiacente IPv6: 1.000 (VM-300), 500 (VM-200), 500 (VM-100)

PROTEZIONE

FIREWALL

- Controllo di applicazioni, utenti e contenuti basato su policy
- Protezione di pacchetti frammentati
- Protezione tramite scansione
- Protezione DoS (Denial of Service)/DDoS (Distributed Denial of Services)
- Decrittografia: SSL (in ingresso e in uscita), SSH

WILDFIRE

- Identificazione e analisi di file mirati e sconosciuti in base a oltre 100 comportamenti dannosi
- Generazione e distribuzione automatica di funzionalità di protezione per i nuovi malware rilevati tramite aggiornamenti delle firme
- Distribuzione di aggiornamenti della firma in meno di 1 ora, registrazione/generazione di report integrata, accesso all'API WildFire per l'inoltro programmatico di fino a 100 campioni al giorno e fino a 1.000 query report per hash file al giorno (solo in abbonamento)

FILTRAGGIO DI FILE E DATI

- Trasferimento file: controllo bidirezionale su oltre 60 tipi di file univoci
- Trasferimento dati: controllo bidirezionale sul trasferimento non autorizzato di CC# e SSN
- Protezione dai download non intenzionali

INTEGRAZIONE UTENTI (USER-ID)

- Microsoft Active Directory, Novell eDirectory, Sun One e altre directory basate su LDAP
- Microsoft Windows Server 2003/2008/2008r2, Microsoft Exchange Server 2003/2007/2010
- Microsoft Terminal Services, Citrix XenApp
- API XML per semplificare l'integrazione con repository utenti non standard

VPN IPSEC (SITO-SITO)

- Chiave di scambio: chiave manuale, IKE v1
- Crittografia: 3DES, AES (128-bit, 192-bit, 256-bit)
- Autenticazione: MD5, SHA-1, SHA-256, SHA-384, SHA-512
- Creazione tunnel VPN dinamica (GlobalProtect)

PREVENZIONE DALLE MINACCE (SOLO IN ABBONAMENTO)

- Protezione di applicazioni e sistemi operativi dalla vulnerabilità agli exploit
- Protezione basata su flussi da virus (inclusi quelli incorporati in codici HTML, Javascript, PDF e file compressi), spyware, worm

FILTRAGGIO URL (SOLO IN ABBONAMENTO)

- Categorie URL predefinite e personalizzate
- Cache dispositivo per gli URL aperti di recente
- Categoria URL inclusa nei criteri di corrispondenza per le policy di protezione
- Dati sui tempi di navigazione

QUALITY OF SERVICE (QOS)

- Shaping del traffico basato su policy in base ad applicazioni, utenti, origini, destinazioni, interfacce, tunnel VPN IPSec e altro ancora
- 8 classi di traffico con parametri per la larghezza di banda garantita, massima e prioritaria
- Monitoraggio della larghezza di banda in tempo reale
- Contrassegno diffserv in base alla policy
- Interfacce fisiche supportate per il QoS: 6 (VM-300, VM-200), 4 (VM-100)

ACCESSO VPN/REMOTO SSL (GLOBALPROTECT)

- Gateway GlobalProtect
- Portale GlobalProtect
- Trasporto: IPSec con fall-back SSL
- Autenticazione: LDAP, SecurID o DB locale
- SO client 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)
- Supporto per client di terze parti: Apple iOS, Android 4.0 e versioni successive, VPNC IPSec for Linux

STRUMENTI DI GESTIONE, GENERAZIONE DI REPORT E VISIBILITÀ

- Interfaccia Web integrata, CLI o gestione centralizzata (Panorama)
- Interfaccia utente multi-lingue
- Syslog, Netflow v9 e SNMP v2/v3
- REST API basate su XML
- Riepilogo in formato grafico di applicazioni, categorie di URL, minacce e dati (ACC)
- Visualizzazione, filtraggio ed esportazione di registri su traffico, minacce, WildFire, URL e filtraggio dei dati
- Generazione di report completamente personalizzabile

Per la descrizione completa del set di funzionalità del firewall Serie VM di nuova generazione, visitare il sito www.paloaltonetworks.com/literature.

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