PA-4000 Series

Funzionalità principali del firewall Serie PA-4000 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 o l'acquisizione di pacchetti per lo sviluppo di App-ID.

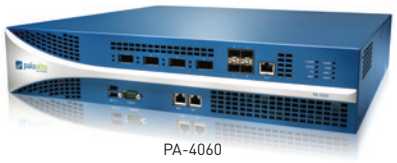
ESTENSIONE DELLE POLICY DI ABILITAZIONE SICURA DELLE APPLICAZIONI A QUALSIASI UTENTE, QUALSIASI POSIZIONE CON USER-ID™ E GLOBALPROTECT™.

- 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 locali e remoti che utilizzano piattaforme Microsoft Windows, Mac OS X, Linux, Android o iOS.

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 firme con il successivo aggiornamento disponibile.

paloalto NETWORKS
the network security company™


PA-4060


PA-4050


PA-4020

La Serie PA-4000 di Palo Alto Networks™ si compone di tre piattaforme a elevate prestazioni: PA-4060, PA-4050 e PA-4020, tutti destinati a implementazioni in data center a elevata velocità e gateway Internet. La Serie PA-4000 garantisce una velocità fino a 10 Gb/s utilizzando memoria e risorse di elaborazione dedicate per le principali aree funzionali, quali rete, protezione, prevenzione dalle minacce e gestione.

Il backplane ad alta velocità è fisicamente separato in piani di controllo e dati distinti, garantendo la disponibilità continua dell'accesso di gestione, indipendentemente dal carico di traffico. L'elemento di controllo della Serie PA-4000 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.

PRESTAZIONI E CAPACITÀ[1]	PA-4060	PA-4050	PA-4020
Velocità del firewall (con supporto per App-ID)	10 Gb/s	10 Gb/s	2 Gb/s
Velocità della prevenzione delle minacce	5 Gb/s	5 Gb/s	2 Gb/s
Velocità VPN IPSec	2 Gb/s	2 Gb/s	1 Gb/s
Nuove sessioni al secondo	60.000	60.000	60.000
N. massimo di sessioni	2.000.000	2.000.000	500.000
tunnel/interfacce tunnel VPN IPSec	4.000	4.000	2.000
GlobalProtect (VPN SSL) per utenti simultanei	10.000	10.000	5.000
Sessioni di decrittografia SSL	23.000	23.000	7.500
Certificati SSL in entrata	300	300	25
Router virtuali	125	125	20
Sistemi virtuali (standard/massimo[2])	25/125	25/125	10/20
Zone di protezione	500	500	80
N. massimo di policy	20.000	20.000	10.000

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

[2] L'aggiunta di sistemi virtuali alla quantità standard richiede l'acquisto di una licenza separata.

Per la descrizione completa del set di funzionalità del firewall Serie PA-4000 di nuova generazione, visitare il sito www.paloaltonetworks.com/literature

SPECIFICHE HARDWARE

I/O

- PA-4060: (4) 10 Gigabit XFP, (4) Gigabit SFP
- PA-4050, PA-4020: (16)10/100/1000, (8) Gigabit SFP

GESTIONE DELL'I/O

- (2) 10/100/1000 alta disponibilità, (1) 10/100/1000 gestione fuori banda, (1) porta console DB9

CAPACITÀ DI STORAGE

- HDD da 160 GB

ALIMENTAZIONE (CONSUMO MEDIO/MASSIMO)

- AC 400 W ridondante (175 W/200 W)

BTU/ORA MASSIMI

- 682

TENSIONE IN INGRESSO (FREQUENZA IN INGRESSO)

- da 100 a 240 VCA (da 50 a 60 Hz)

CONSUMO MASSIMO DI CORRENTE

- 2,5 A a 100 VCA

TEMPO MEDIO TRA I GUASTI (MTBF)

- 7,18 anni

AFFLUSSO DI CORRENTE MASSIMO

- 50A a 230 VCA, 30A a 120 VCA

MONTABILE IN RACK (DIMENSIONI)

- Rack standard a 2 U, da 19 poll. (3,5" H x 16.5" L x 17,5" P)

PESO (DISPOSITIVO AUTONOMO/COME FORNITO)

- 15 kg/18 kb

SICUREZZA

- UL, CUL, CB

EMI

- FCC Classe A, CE Classe A, VCCI Classe A, TUV

CERTIFICAZIONI

- FIPS 140 Livello 2, Common Criteria EAL2, ICSA, UCAPL

AMBIENTE

- Temperatura di esercizio da 0° a 50° C
- Temperatura non di esercizio da -20° a 70° C

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): 20.000/20.000 (PA-4060, PA-4050), 10.000/10.000 (PA-4020)
- Inoltro basato su policy
- Point-to-Point Protocol over Ethernet (PPPoE)
- Frame Jumbo: dimensione massima frame di 9.210 byte
- Multicasting: PIM-SM, PIM-SSM, IGMP v1, v2 e v3

ALTA DISPONIBILITÀ

- Modalità: Active/Active, Active/Passive
- 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: 4.096 (PA-4060, PA-4050), 2.048 (PA-4020)
- Interfacce di aggregazione (802.3ad)

NAT/PAT

- N. massimo di regole NAT: 4.000 (PA-4060, PA-4050), 1.000 (PA-4020)
- N. massimo di regole NAT (DIPP): 250 (PA-4060, PA-4050), 200 (PA-4020)
- Pool porta e IP dinamico: 254
- Pool IP dinamico: 16.234
- 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): 8 (PA-4060, PA-4050), 4 (PA-4020)
- NAT64

CABLAGGIO VIRTUALE

- N. massimo di cavi virtuali: 2.048 (PA-4060, PA-4050), 1.024 (PA-4020)
- Tipi di interfacce mappate ai cavi virtuali: fisiche e sottointerfacce

INOLTRO L2

- Dimensioni tabella ARP/dispositivo: 20.000 (PA-4060, PA-4050), 10.000 (PA-4020)
- Dimensione tabella/dispositivo MAC: 20.000 (PA-4060, PA-4050), 10.000 (PA-4020)
- Dimensioni tabella adiacente IPv6: 5.000 (PA-4060, PA-4050), 2.000 (PA-4020)

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: 12

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 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 ulteriori informazioni sul set di funzionalità del firewall di nuova generazione Serie PA-4000, 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