PA-200

Funzionalità principali del firewall PA-200 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.

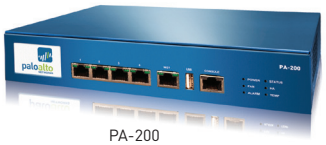
ESTENSIONE DELLE POLICY DI ABILITAZIONE SICURA DELLE APPLICAZIONI A QUALSIASI UTENTE, QUALSIASI POSIZIONE CON USER-ID™ E GLOBALPROTECT™.

- 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-200

Il firewall PA-200 di Palo Alto Networks™ è destinato a implementazioni di firewall ad alta velocità all'interno di filiali distribuite di grandi imprese. PA-200 è in grado di gestire i flussi di traffico di rete utilizzando risorse di elaborazione dedicate per la rete, la protezione, la prevenzione delle minacce e la gestione.

Il backplane ad alta velocità è suddiviso in piani di controllo e dati separati, garantendo la disponibilità continua dell'accesso di gestione indipendentemente dal carico di traffico. L'elemento di controllo del firewall PA-200 di nuova generazione 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-200
Velocità del firewall (con supporto per App-ID)	100 Mb/s
Velocità della prevenzione delle minacce	50 Mb/s
Velocità VPN IPSec	50 Mb/s
Nuove sessioni al secondo	1.000
N. massimo di sessioni	64.000
tunnel/interfacce tunnel VPN IPSec	25
GlobalProtect (VPN SSL) per utenti simultanei	25
Sessioni di decrittografia SSL	1.000
Certificati SSL in entrata	25
Router virtuali	3
Zone di protezione	10
N. massimo di policy	250

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

Per la descrizione completa del set di funzionalità del firewall PA-200 di nuova generazione, visitare il sito www.paloaltonetworks.com/literature

SPECIFICHE HARDWARE

I/O
- (4) 10/100/1000

GESTIONE DELL'I/O
- (1) porta di gestione fuori banda 10/100, (1) porta console RJ-45

CAPACITÀ DI STORAGE
- SSD da 16 GB

ALIMENTAZIONE (CONSUMO MEDIO/MASSIMO)
- 40 W (20 W/30 W)

BTU/ORA MASSIMI
- 102 BTU

TENSIONE IN INGRESSO (FREQUENZA IN INGRESSO)
- da 100 a 240 VCA (da 50 a 60 Hz)

CONSUMO MASSIMO DI CORRENTE
- 3,3 A a 100 VCA

MTBF
- 13 anni

DIMENSIONI (DISPOSITIVO AUTONOMO/COME FORNITO)
- 1,75" H x 7" P x 9,25" P

PESO
- 1,3 kg/2,3 kg (spedizione)

SICUREZZA
- UL, CUL, CB

EMI
- FCC Classe B, CE Classe A, VCCI Classe B

CERTIFICAZIONI
- ICSA

AMBIENTE
- Temperatura di esercizio da 0° a 40° 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): 1.000/1.000
- Inoltro basato su policy
- Point-to-Point Protocol over Ethernet (PPPoE)
- Multicasting: PIM-SM, PIM-SSM, IGMP v1, v2 e v3

ALTA DISPONIBILITÀ
- 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: 100

NAT/PAT
- N. massimo di regole NAT: 125
- N. massimo di regole NAT (DIPP): 125
- 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): 1
- NAT64

CABLAGGIO VIRTUALE
- N. massimo di cavi virtuali: 50
- Tipi di interfacce mappate ai cavi virtuali: fisiche e sottointerfacce

INOLTRO L2
- Dimensioni tabella ARP/dispositivo: 500
- Dimensione tabella/dispositivo MAC: 500
- Dimensioni tabella adiacente IPv6: 500

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: 4

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 PA-200 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