# PA-4000 Series

## Recursos principais do firewall de próxima geração PA-4000 Series

**CLASSIFIQUE TODOS OS APLICATIVOS, EM TODAS AS PORTAS, O TEMPO TODO COM O APP-ID™.**

- Identifica o aplicativo, independentemente da porta, criptografia (SSL ou SSH) ou técnica evasiva empregada.
- Usa o aplicativo, não a porta, como a base de todas as decisões seguras sobre ativação de politica: permitir, negar, agendar, inspecionar, aplicar modelamento de tráfego.
- Classifica aplicativos não identificados em categorias, para controle de políticas, análise de ameaças, criação de App-ID personalizado ou captura de pacotes para desenvolvimento do App-ID.

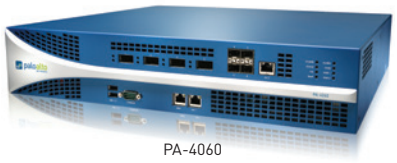
**ESTENDA AS POLÍTICAS DE PERMISSÃO DE APLICATIVO PARA QUALQUER USUÁRIO, EM QUALQUER LOCAL, COM O USER-ID™ E GLOBALPROTECT™.**

- Integração sem agente com Active Directory, LDAP, eDirectory Citrix e Microsoft Terminal Services.
- Integra-se com NAC, 802.1X sem fio e outros repositórios de usuário não padrão com um API XML.
- Implanta políticas consistentes para usuários locais e remotos que usam plataformas com Microsoft Windows, Mac OS X, Linux, Android ou iOS.

**PROTEJA CONTRA TODAS AS AMEAÇAS - CONHECIDAS E DESCONHECIDAS COM O CONTENT-ID™ E WILDFIRE™.**

- Bloqueia uma variedade de ameças conhecidas, incluindo explorações, malware e spyware, independentemente das táticas de evasão comuns empregadas pela ameaça.
- Limita a transferência não autorizada de arquivos e dados sensíveis, e controla a navegação não relacionada ao trabalho.
- Identifica malwares desconhecidos, analisa mais de 100 comportamentos mal intencionados, cria e fornece automaticamente uma assinatura na próxima atualização disponível.

paloalto NETWORKS
the network security company™


PA-4060


PA-4050


PA-4020

O PA-4000 Series da Palo Alto Networks™ é composto por três plataformas de alto desempenho, o PA-4060, o PA-4050 e o PA-4020, todos planejados para implantações de datacenter e gateway de Internet de alta velocidade. O PA-4000 Series fornece até 10 Gbps de throughput usando processamento e memória dedicados para as áreas funcionais importantes de rede, segurança, prevenção de ameaças e gerenciamento.

O hardware de alta velocidade está dividido em planos separados de dados e controle, garantindo assim que o acesso de gerenciamento esteja sempre disponível, independentemente da carga de tráfego. O elemento controlador do firewall de próxima geração PA-4000 Series é o PAN-OS™, um sistema operacional que permite que as organizações permitam aplicativos com segurança usando o App-ID, User-ID, Content-ID, GlobalProtect e WildFire.

| DESEMPENHO E CAPACIDADES[1] | PA-4060 | PA-4050 | PA-4020 |
|---|---|---|---|
| Throughput de firewall (App-ID habilitado) | 10 Gbps | 10 Gbps | 2 Gbps |
| Throughput da prevenção contra ameaças | 5 Gbps | 5 Gbps | 2 Gbps |
| Throughput VPN IPSec | 2 Gbps | 2 Gbps | 1 Gbps |
| Novas sessões por segundo | 60.000 | 60.000 | 60.000 |
| Máximo de sessões | 2.000.000 | 2.000.000 | 500.000 |
| Interfaces de túnel/túneis VPN IPSec | 4.000 | 4.000 | 2.000 |
| Usuários simultâneos do GlobalProtect (VPN SSL) | 10.000 | 10.000 | 5.000 |
| Sessões de descriptografia de SSL | 23.000 | 23.000 | 7.500 |
| Certificados SSL recebidos | 300 | 300 | 25 |
| Roteadores virtuais | 125 | 125 | 20 |
| Sistemas virtuais (base/max[2]) | 25/125 | 25/125 | 10/20 |
| Zonas de segurança | 500 | 500 | 80 |
| Número máximo de políticas | 20.000 | 20.000 | 10.000 |

[1] Desempenho e capacidades são medidos em condições ideais de teste usando o PAN-OS 5.0.

[2] Adicionar sistemas virtuais à quantidade básica exige uma licença comprada separadamente.

Para obter uma descrição completa do conjunto de recursos do firewall de próxima de geração PA-4000 Series, acesse www.paloaltonetworks.com/literature.

## ESPECIFICAÇÕES DE HARDWARE

### E/S

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

### E/S DE GERENCIAMENTO

- (2) 10/100/1000 de alta disponibilidade, (1) gerenciamento fora de banda 10/100/1000, (1) porta de console DB9

### CAPACIDADE DE ARMAZENAMENTO

- 160GB em HDD

### FONTE DE ALIMENTAÇÃO (CONSUMO DE ENERGIA MÉDIO/MÁXIMO)

- 400W CA (175W/200W) redundante

### BTU/H MÁXIMO

- 682

### TENSÃO DE ENTRADA (FREQUÊNCIA DE ENTRADA)

- 100-240 VCA (50-60Hz)

### CONSUMO MÁXIMO DE CORRENTE

- 2,5A@100VCA

### TEMPO MÉDIO ENTRE FALHAS (MTBF)

- 7,18 anos

### CORRENTE DE LIGAÇÃO MÁXIMA

- 50A@230VCA; 30A@120VCA

### MONTADO EM RACK (DIMENSÕES)

- 2U, rack padrão de 19" (3.5"A x 16,5"P x 17.5"L)

### PESO (DISPOSITIVO AUTÔNOMO/NO ENVIO)

- 33lbs/40lbs

### SEGURANÇA

- UL, CUL, CB

### EMI

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

### CERTIFICAÇÕES

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

### AMBIENTE

- Temperatura operacional: 32° a 122° F, 0 a 50° C
- Temperatura não operacional: -4° a 158° F, -20° a 70° C

## REDE

### MODOS DE INTERFACE:

- L2, L3, Tap, Virtual wire (modo transparente)

### ROTEAMENTO

- Modos: OSPF, RIP, BGP, estático
- Tamanho de tabela de encaminhamento (entradas por dispositivo/por VR): 20.000/20.000 (PA-4060, PA-4050), 10.000/10.000 (PA-4020)
- Encaminhamento baseado em políticas
- Point-to-Point Protocol over Ethernet (PPPoE)
- Jumbo frames: Tamanho máximo de quadro de 9.210 bytes
- Multicast: PIM-SM, PIM-SSM, IGMP v1, v2 e v3

### ALTA DISPONIBILIDADE

- Modos: Ativo/Ativo, Ativo/Passivo
- Detecção de falhas: Monitoramento de caminho, monitoramento de interface

### ATRIBUIÇÃO DE ENDEREÇOS

- Atribuição de endereços por dispositivo: Cliente DHCP/PPPoE/Estático
- Atribuição de endereços para usuários: Servidor DHCP/Relé DHCP/Estático

### IPV6

- L2, L3, tap, virtual wire (modo transparente)
- Recursos: App-ID, User-ID, Content-ID, WildFire e descriptografia SSL

### VLANS

- Tags VLAN 802.1q por dispositivo/por interface: 4.094/4.094
- Máximo de interfaces: 4.096 (PA-4060, PA-4050), 2.048 (PA-4020)
- Interfaces agregadas (802.3ad)

### NAT/PAT

- Máximo de regras NAT: 4.000 (PA-4060, PA-4050), 1.000 (PA-4020)
- Máximo de regras NAT (DIPP): 250 (PA-4060, PA-4050), 200 (PA-4020)
- Pool de porta e IP dinâmico: 254
- Pool de IP dinâmico: 16.234
- Modos NAT: 1:1 NAT, n:n NAT, m:n NAT
- Sobreutilização de DIPP (IPs de destino único por porta de origem e IP): 8 (PA-4060, PA-4050), 4 (PA-4020)
- NAT6

### VIRTUAL WIRE

- Máximo virtual wires: 2.048 (PA-4060, PA-4050), 1.024 (PA-4020)
- Tipos de interfaces mapeadas para virtual wires: física e subinterfaces

### ENCAMINHAMENTO L2

- Tamanho de tabela ARP/dispositivo: 20.000 (PA-4060, PA-4050), 10.000 (PA-4020)
- Tamanho de tabela MAC/dispositivo: 20.000 (PA-4060, PA-4050), 10.000 (PA-4020)
- Tamanho de tabela vizinha IPv6: 5.000 (PA-4060, PA-4050), 2.000 (PA-4020)

## SEGURANÇA

### FIREWALL

- Controle baseado em políticas sobre aplicativos, usuários e conteúdo
- Proteção de pacote fragmentado
- Proteção de verificação por reconhecimento
- Proteção contra Negação de serviço (DoS)/Negação distribuída de serviços (DDoS)
- Descriptografia: SSL (entrada e saída), SSH

### WILDFIRE

- Identifica e analisa mais de 100 comportamentos mal intencionados em arquivos alvo e desconhecidos
- Gera e fornece automaticamente proteção para malwares recém descobertos através de atualizações de assinatura
- Fornecimento de atualização da assinatura em menos de 1 hora; criação de registro e relatório integrados; acesso ao API WildFire para envio programático de até 100 amostras por dia e até 250 consultas de relatório por hash de arquivo por dia (assinatura obrigatória)

### FILTRAGEM DE ARQUIVOS E DADOS

- Transferência de arquivo: Controle bidirecional sobre mais de 60 tipos únicos de arquivos
- Transferência de dados: Controle bidirecional sobre transferência não autorizada de CC# e SSN
- Proteção contra downloads não autorizados

### INTEGRAÇÃO DO USUÁRIO (USER-ID)

- Microsoft Active Directory, Novell eDirectory, Sun One e outros diretórios baseados em LDAP
- Microsoft Windows Server 2003/2008/2008r2, Microsoft Exchange Server 2003/2007/2010
- Microsoft Terminal Services, Citrix XenApp
- API XML para facilitar a integração com repositórios de usuário não padrão

### VPN IPSEC (ENTRE SITES)

- Troca de chaves: Chave manual, IKE v1
- Criptografia: 3DES, AES (128-bit, 192-bit, 256-bit)
- Autenticação: MD5, SHA-1, SHA-256, SHA-384, SHA-512
- Criação de túnel VPN dinâmico (GlobalProtect)

### PREVENÇÃO CONTRA AMEAÇAS (ASSINATURA OBRIGATÓRIA)

- Proteção contra exploração das vulnerabilidades do sistema operacional e de aplicativos
- Proteção baseada em stream contra vírus (incluindo aqueles embutidos em HTML, Javascript, PDF e comprimidos), spyware, worms

### FILTRAGEM DE URL (ASSINATURA OBRIGATÓRIA)

- Categorias de URL predefinidas e personalizadas
- Cache do dispositivo dos URLs acessados mais recentemente
- Categoria do URL como parte do critério de correspondência de políticas de segurança
- Informações sobre o tempo de navegação

### QUALIDADE DE SERVIÇO (QOS)

- Modelamentos de tráfego baseado em políticas por aplicativo, usuário, fonte, destino, interface, túnel VPN IPSec e mais
- 8 classes de tráfego com parâmetros de largura de banda garantida, máxima e prioritária
- Monitor de largura de banda em tempo real
- Por marcação diffserv de política
- Interfaces físicas suportadas para QoS: 12

### VPN SSL/ACESSO REMOTO (GLOBALPROTECT)

- Gateway GlobalProtect
- Portal GlobalProtect
- Transporte: IPSec com fall-back SSL
- Autenticação: LDAP, SecurID ou DB local
- SO do cliente: 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)
- Suporte a clientes de terceiros: Apple iOS, Android 4.0 e superior, VPNC IPSec para Linux

### FERRAMENTAS DE GERENCIAMENTO, RELATÓRIO E VISIBILIDADE

- Interface web integrada, CLI ou gerenciamento central (Panorama)
- Interface de usuário multilíngue
- Syslog e SNMP v2/v3
- API REST baseado em XML
- Resumo gráfico de aplicativos, categorias de URL, ameaças e dados (ACC)
- Exibir, filtrar e exportar logs de tráfego, de ameaças, do WildFire, de URL e de dados de filtragem.
- Relatórios totalmente personalizáveis

Para obter mais informações sobre o conjunto de recursos do firewall de próxima de geração PA-4000 Series, acesse 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