

PA-2000 Series

Recursos principais do firewall de próxima geração PA-2000 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 política: 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 ameaças 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.



PA-2050



PA-2020

O PA-2000 Series da Palo Alto Networks™ é composto por duas plataformas de alto desempenho, o PA-2050 e o PA-2020, ambos planejados para implantações de gateway de Internet de alta velocidade. O PA-2000 Series gerencia fluxos de tráfego de rede usando processamento e memória dedicados à 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-2000 Series é o PAN-OS™, um sistema operacional que permite que as organizações ativem os aplicativos com segurança usando o App-ID, User-ID, Content-ID, GlobalProtect e WildFire.

DESEMPENHO E CAPACIDADES ¹	PA-2050	PA-2020
Throughput de firewall (App-ID habilitado)	1 Gbps	500 Mbps
Throughput da prevenção contra ameaças	500 Mbps	200 Mbps
Throughput VPN IPSec	300 Mbps	200 Mbps
Novas sessões por segundo	15.000	15.000
Máximo de sessões	250.000	125.000
Interfaces de túnel/túneis VPN IPSec	2.000	1.000
Usuários simultâneos do GlobalProtect (VPN SSL)	1.000	500
Sessões de descriptografia de SSL	1.000	1.000
Certificados SSL recebidos	25	25
Roteadores virtuais	10	10
Sistemas virtuais (base/max ²)	1/6	1/6
Zonas de segurança	40	40
Número máximo de políticas	5.000	2.500

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-2000 Series, acesse www.paloaltonetworks.com/literature.

ESPECIFICAÇÕES DE HARDWARE**E/S**

- PA-2050: (16) 10/100/1000, (4) gigabit ótico SFP
- PA-2020: (12) 10/100/1000, (2) gigabit ótico SFP

E/S DE GERENCIAMENTO

- (1) Porta de gerenciamento fora de banda 10/100/1000, (1) porta de console RJ-45

CAPACIDADE DE ARMAZENAMENTO

- 160GB em HDD

FONTE DE ALIMENTAÇÃO (CONSUMO DE ENERGIA MÉDIO/MÁXIMO)

- 250W (105W/120W)

BTU/H MÁXIMO

- 409

TENSÃO DE ENTRADA (FREQUÊNCIA DE ENTRADA)

- 100-240 VCA (50-60Hz)

CONSUMO MÁXIMO DE CORRENTE

- 3A@100VCA

TEMPO MÉDIO ENTRE FALHAS (MTBF)

- 7,3 anos

CORRENTE DE LIGAÇÃO MÁXIMA

- 70A@230VCA; 35A@115VCA

MONTADO EM RACK (DIMENSÕES)

- 1U, rack padrão de 19" (1.75"A x 17"P x 17"L)

PESO (DISPOSITIVO AUTÔNOMO/NO ENVIO)

- 15lbs/20lbs

SEGURANÇA

- UL, CUL, CB

EMI

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

CERTIFICAÇÕES

- FIPS 140 nível 2, Common Criteria EAL2, ICESA, 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): 5.000/2.500 (PA-2050), 2.500/2.500 (PA-2020)
- Encaminhamento baseado em políticas
- Point-to-Point Protocol over Ethernet (PPPoE)
- 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: 2.048 (PA-2050), 1.024 (PA-2020)
- Interfaces agregadas (802.3ad)

NAT/PAT

- Máximo de regras NAT: 1.000
- Máximo de regras NAT (DIPP): 200
- 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): 2
- NAT64

VIRTUAL WIRE

- Máximo virtual wires: 1.024 (PA-2050), 512 (PA-2020)
- Tipos de interfaces mapeadas para virtual wires: física e subinterfaces

ENCAMINHAMENTO L2

- Tamanho de tabela ARP/dispositivo: 2.500 (PA-2050), 1.000 (PA-2020)
- Tamanho de tabela MAC/dispositivo: 2.500 (PA-2050), 1.000 (PA-2020)
- Tamanho de tabela vizinha IPv6: 1.000

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)
- Criptografia: 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: 4

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, Netflow v9 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 uma descrição completa do conjunto de recursos do firewall de próxima geração PA-2000 Series, acesse www.paloaltonetworks.com/literature.