PA-5000 Series

Recursos principais do firewall de próxima geração PA-5000 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 investigação mais aprofundada.

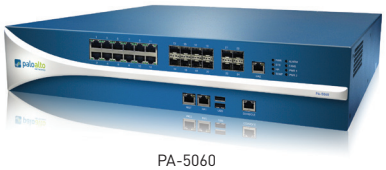
ESTENDA AS POLÍTICAS DE PERMISSÃO DE APLICATIVO PARA QUALQUER USUÁRIO, EM QUALQUER LOCAL, COM O USER-ID™ E GLOBALPROTECT™.

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

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 - em todas as portas, independentemente das táticas de evasão empregadas pela ameaça.
- Limita transferência não autorizada de arquivos e dados sensíveis, e controle a navegação não relacionada com o trabalho.
- Identifica malwares desconhecidos, analisa mais de 100 comportamentos de malware, cria e fornece automaticamente proteção na próxima atualização disponível.

paloalto NETWORKS
the network security company™



PA-5060

PA-5050

PA-5020

O PA-5000 Series da Palo Alto Networks™ é composto por três plataformas de alto desempenho, o PA-5060, o PA-5050 e o PA-5020, todos planejados para implantações de datacenter e gateway de Internet de alta velocidade.

O PA-5000 Series fornece até 20 Gbps de throughput usando processamento e memória dedicados para as áreas funcionais importantes de rede, segurança, prevenção de ameaças e gerenciamento. Para garantir que o acesso ao gerenciamento esteja sempre disponível, independentemente da carga de tráfego, os planos de dados e controle são separados fisicamente. O elemento controlador do firewall de próxima geração PA-5000 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-5060	PA-5050	PA-5020
Throughput de firewall (App-ID habilitado)	20 Gbps	10 Gbps	5 Gbps
Throughput da prevenção contra ameaças	10 Gbps	5 Gbps	2 Gbps
Throughput VPN IPSec	4 Gbps	4 Gbps	2 Gbps
Máximo de sessões	4.000.000	2.000.000	1.000.000
Novas sessões por segundo	120.000	120.000	120.000
Interfaces de túnel/túneis VPN IPSec	8.000	4.000	2.000
Usuários simultâneos do GlobalProtect (VPN SSL)	20.000	10.000	5.000
Sessões de descriptografia de SSL	90.000	45.000	15.000
Certificados SSL recebidos	1.000	300	100
Roteadores virtuais	225	125	20
Sistemas virtuais (base/max[2])	25/225*	25/125*	10/20*
Zonas de segurança	900	500	80
Número máximo de políticas	40.000	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-5000 Series, acesse www.paloaltonetworks.com/literature.

ESPECIFICAÇÕES DE HARDWARE

E/S

- PA-5060, PA-5050: (12) 10/100/1000, (8) Gigabit SFP, (4) 10 Gigabit SFP+
- PA-5020: (12)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 RJ-45

OPÇÕES DE ARMAZENAMENTO

- Unidades de disco única ou dupla de estado sólido

CAPACIDADE DE ARMAZENAMENTO

- 120GB, 240GB SSD, RAID 1

FONTE DE ALIMENTAÇÃO (CONSUMO DE ENERGIA MÉDIO/MÁXIMO)

- PA-5060: 450W CA (330W/415W) redundante
- PA-5050, PA-5020: 450W CA (270W/340W) redundante

BTU/H MÁXIMO

- PA-5060: 1.416
- PA-5050, PA-5020: 1.160

TENSÃO DE ENTRADA (FREQUÊNCIA DE ENTRADA)

- 100 a 240VCA (50-60Hz); -40 a -72 VCC

CONSUMO MÁXIMO DE CORRENTE

- 8A@100VCA, 14A@48VCC

CORRENTE DE LIGAÇÃO MÁXIMA

- 80A@230VCA; 40A@120VCA; 40A@48VCC

TEMPO MÉDIO ENTRE FALHAS (MTBF)

- 6,5 anos

MONTADO EM RACK (DIMENSÕES)

- 2U, rack padrão de 19" (3.5"A x 21"P x 17.5"L)

PESO (DISPOSITIVO AUTÔNOMO/NO ENVIO)

- 41lbs/55lbs

SEGURANÇA

- UL, CUL, CB

EMI

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

CERTIFICAÇÕES

- NEBS nível 3, FIPS nível 2, ICSA

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): 64.000/64.000
- 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-5060, PA-5050), 2.048 (PA-5020)
- Interfaces agregadas (802.3ad)

NAT/PAT

- Máximo de regras NAT: 8.000 (PA-5060), 4.000 (PA-5050), 1.000 (PA-5020)
- Máximo de regras NAT (DIPP): 450 (PA-5060), 250 (PA-5050), 200 (PA-5020)
- Pool de porta e IP dinâmico: 254
- Pool de IP dinâmico: 32.000
- 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
- NAT64

VIRTUAL WIRE

- Máximo virtual wires: 2.048 (PA-5060, PA-5050), 1.024 (PA-5020)
- Tipos de interfaces mapeadas para virtual wires: física e subinterfaces

ENCAMINHAMENTO L2

- Tamanho de tabela ARP/dispositivo: 32,000 (PA-5060, PA-5050), 20,000 (PA-5020)
- Tamanho de tabela MAC/dispositivo: 32,000 (PA-5060, PA-5050), 20,000 (PA-5020)
- Tamanho de tabela vizinha IPv6: 5,000 (PA-5060, PA-5050), 2,000 (PA-5020)

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 contra 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, 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 de geração PA-5000 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

Copyright ©2013, Palo Alto Networks, Inc. Todos os direitos reservados. A Palo Alto Networks, o logotipo da Palo Alto Networks, PAN-OS, App-ID e Panorama são marcas comerciais da Palo Alto Networks, Inc. Todas as especificações estão sujeitas a alterações sem aviso prévio. A Palo Alto Networks não assume nenhuma responsabilidade por quaisquer erros no presente documento ou qualquer obrigação de atualizar as informações contidas neste documento. A Palo Alto Networks se reserva ao direito de alterar, modificar, transferir ou revisar esta publicação sem aviso prévio. **PAN_SS_PA5000_031313**