VM-Series

Principais recursos do firewall de próxima geração VM-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™.

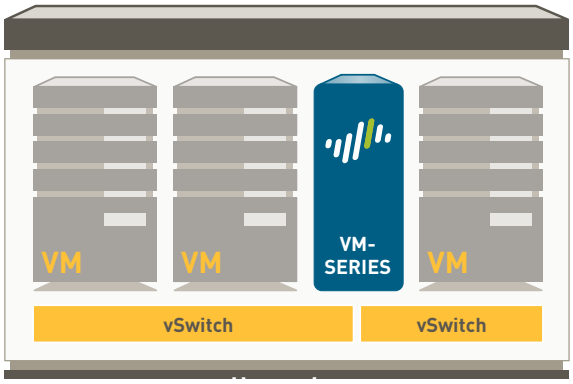
- Integração sem agente com Active Directory, LDAP, eDirectory Citrix e Microsoft Terminal Services.
- Integra-se com NAC, sem fio e outros repositórios de usuário que não sejam padrão, com um API XML.
- Implanta políticas consistentes para usuários usando plataformas Microsoft Windows, Mac OS X, Linux,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

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

- Bloqueia uma variedade de ameaças 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™



VM-Series Virtual Firewall

Os produtos da VM-Series da Palo Alto Networks™ estendem a permissão segura de aplicativos em ambientes virtuais, lidando com os desafios principais da segurança na virtualização: rastrear políticas de segurança em movimento de máquina virtual com objetos de endereço dinâmico e integração com sistemas de orquestração usando uma poderosa API de gerenciamento XML.

Os produtos da VM-Series são compostos por três modelos de alto desempenho, o VM-100, VM-200 e VM-300, os quais usam uma arquitetura de software de passagem única para reduzir a latência em ambientes de datacenter. O plano de gerenciamento e de dados são separados, de forma que os usuários podem atribuir CPUs dedicados a cada um deles como forma de garantir que o acesso ao gerenciamento esteja sempre disponível, independentemente das cargas de tráfego. O elemento controlador dos produtos da VM-Series é o PAN-OS™, um sistema operacional específico ao sistema que permite que as organizações permitam aplicativos de forma segura, usando o App-ID, User-ID, Content-ID, GlobalProtect e WildFire.

CAPACIDADES GERAIS[1]	VM-300	VM-200	VM-100
Máximo de sessões	250.000	100.000	50.000
Interfaces de túnel/túneis VPN IPSec	2.000	500	25
Usuários simultâneos do GlobalProtect (VPN SSL)	500	200	25
Sessões de descriptografia de SSL	1024	1024	1024
Certificados SSL recebidos	25	25	25
Roteadores virtuais	3	3	3
Zonas de segurança	40	20	10
Número máximo de políticas	5.000	2.000	250
Objetos de endereço	10.000	4.000	2.500
DESEMPENHO[1]			
Throughput de firewall (App-ID habilitado)	1 Gbps		
Throughput da prevenção contra ameaças	600 Mbps		
Throughput VPN IPSec	250 Mbps		
Novas sessões por segundo	8.000		

[1] Desempenho e capacidades são medidos em condições ideais de teste usando PAN-OS 5.0 e CPU com 4 núcleos.

ESPECIFICAÇÕES DE VIRTUALIZAÇÃO	VM-300 VM-200 VM-100
HyperVisor	VMware ESXi 4.1 e ESXi 5.0
Driver de rede	VMXNet3
Núcleos da CPU	2, 4 or 8
Memória (mínimo)	4GB
Capacidade da unidade de disco (Min/Max)	40GB/2TB

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): 1,000/1,000
- Encaminhamento baseado em políticas
- Multicast: PIM-SM, PIM-SSM, IGMP v1, v2 e v3

ALTA DISPONIBILIDADE

- Modos: Ativo/Passivo sem sincronização de sessão
- 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 (transparent mode)
- 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: 2.000 (VM-300), 500 (VM-200), 100 (VM-100)

NAT/PAT

- Máximo de regras NAT: 1.000 (VM-300), 1.000 (VM-200), 125 (VM-100)
- Máximo de regras NAT (DIPP): 200 (VM-300), 200 (VM-200), 125 (VM-100)
- 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): 2 (VM-300), 1(VM-200), 1 (VM-100)
- NAT64

VIRTUAL WIRE

- Máximo virtual wires: 1.000 (VM-300), 250 (VM-200), 50 (VM-100)
- Tipos de interfaces mapeadas para virtual wires: física e subinterfaces

ENCAMINHAMENTO L2

- Tamanho de tabela ARP/dispositivo: 2.500 (VM-300), 500 (VM-200), 500 (VM-100)
- Tamanho de tabela MAC/dispositivo: 2.500 (VM-300), 500 (VM-200), 500 (VM-100)
- Tamanho de tabela vizinha IPv6: 1.000 (VM-300), 500 (VM-200), 500 (VM-100)

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; acesso ao API WildFire para envio programático de até 100 amostras por dia e até 1.000 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: 6 (VM-300, VM-200), 4(VM-100)

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 VM-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