AO

TRIBUNAL DE JUSTIÇA DO ESTADO DO AMAZONAS

Pregão Eletrônico nº 039/2023-TJAM
Processo Administrativo nº 2023/000014860-00
Objeto: Registro de Preços para eventual renovação do suporte e das licenças do cluster de equipamentos de Next-Generation Firewall, assim como expansão da solução de firewall para as unidades descentralizadas do Tribunal de Justiça do Estado do Amazonas (TJAM), compreendendo suporte técnico e garantia pelo período de 60 meses, incluindo serviços de instalação, configuração e treinamento oficial do fabricante.

PROPOSTA

A empresa Servix Informática Ltda., inscrita no CNPJ sob o nº 01.134.191/0002-28, estabelecida na SIG, Quadra 04, Lote 125, Bloco A, Salas 01 e 02, Zona Industrial, Brasília – DF, telefone (11) 3525-3400 e e-mail editais@servix.com, neste ato representada pelo seu Sócio – Diretor o Sr. Fabiano Theis Nascimento, portador do documento de identidade RG nº 15.219.699-7, expedido pela SSP/SP, e inscrito no CPF sob o nº 117.670.268-89, apresenta sua proposta comercial para a execução do objeto nas condições que seguem.

ITEM	DESCRIÇÃO	QUANTIDADE	VALOR UNITÁRIO (R$)	VALOR TOTAL (R$)
1	Subscrição de Prevenção a Ameaças para solução de Plataforma de Segurança Palo Alto Networks PA-5220, pelo período de 60 meses.	2	R$ 524.780,81	R$ 1.049.561,62
2	Subscrição de Filtro de URL para solução de Plataforma de Segurança Palo Alto Networks PA-5220, pelo período de 60 meses.	2	R$ 814.039,00	R$ 1.628.078,00
3	Subscrição de Análise de Malware para solução de Plataforma de Segurança Palo Alto Networks PA-5220, pelo período de 60 meses.	2	R$ 515.851,87	R$ 1.031.703,74
4	Garantia da Solução de Plataforma de Segurança Palo Alto Networks PA-5220, com suporte Premium oficial Palo Alto Networks 24x7 em Alta Disponibilidade, pelo período de 60 meses.	2	R$ 718.910,00	R$ 1.437.820,00
5	Firewall Palo Alto PA-410	70	R$ 17.092,00	R$ 1.196.440,00
6	Subscrição CORE SECURITY SUBSCRIPTION BUNDLE (ADVANCED THREAT PREVENTION, ADVANCED URL FILTERING, ADVANCED WILDFIRE, DNSSECURITY AND SD-WAN), pelo período de 60 meses.	70	R$ 13.888,06	R$ 972.164,20
7	Garantia da Solução de Plataforma de Segurança Palo Alto Networks PA-410, com suporte Premium oficial Palo Alto Networks 24x7, pelo período de 60 meses.	70	R$ 7.894,00	R$ 552.580,00
8	Subscrição de Licença de Gerência Centralizada com suporte para 100 dispositivos Palo Alto Networks, pelo período de 60 meses.	1	R$ 139.095,00	R$ 139.095,00
9	Garantia da Solução de Panorama, com suporte Premium oficial Palo Alto Networks 24x7, pelo período de 60 meses.	1	R$ 318.562,85	R$ 318.562,85
10	Subscrição de DNS Seguro para solução de Plataforma de Segurança Palo Alto Networks PA-5220, pelo período de 60 meses	2	R$ 329.456,00	R$ 658.912,00
11	Subscrição de SD-WAN Seguro para solução de Plataforma de Segurança Palo Alto Networks PA-5220, pelo período de 60 meses.	2	R$ 329.456,00	R$ 658.912,00
12	Serviço de instalação das soluções de Next-Generation Firewall Palo Alto Networks PA-410 e PA-5410	72	R$ 5.491,22	R$ 395.367,84

13	Treinamento oficial do fabricante remoto, em língua portuguesa, com disponibilização de voucher para certificação de administração da solução Palo Alto.	4	R$ 22.565,94	R$ 90.263,76
14	Subscrição de GlobalProtect para solução de Plataforma de Segurança Palo Alto Networks PA-5220, pelo período de 60 meses	2	R$ 341.344,00	R$ 682.688,00
15	Firewall Palo Alto PA-5410	2	R$ 829.597,00	R$ 1.659.194,00
16	Subscrição CORE SECURITY SUBSCRIPTION BUNDLE (ADVANCED THREAT PREVENTION, ADVANCED URL FILTERING, ADVANCED WILDFIRE, DNS SECURITY AND SD-WAN) para PA-5410, pelo período de 60 meses.	2	R$ 1.551.534,00	R$ 3.103.068,00
17	Garantia da Solução de Plataforma de Segurança Palo Alto Networks PA-5410, com suporte Premium oficial Palo Alto Networks 24x7, pelo período de 60 meses.	2	R$ 656.016,00	R$ 1.312.032,00
18	Subscrição de GlobalProtect para solução de Plataforma de Segurança Palo Alto Networks PA-5410, pelo período de 60 meses.	2	R$ 431.808,00	R$ 863.616,00
Valor Total			R$ 17.750.059,01	

Valor total de R$ 17.750.059,01 (Dezessete Milhões e Setecentos e Cinquenta Mil e Cinquenta e Nove Reais e Um Centavo)

Validade da proposta: 60 (sessenta) dias, contados a partir da data da apresentação da proposta.

Estão inclusos nos preços supramencionados todos os custos diretos e indiretos, inclusive de embalagens, transportes ou fretes, e ainda os resultantes da incidência de quaisquer tributos, contribuições ou obrigações decorrentes da legislação trabalhista, fiscal e previdenciária a que estiver sujeito.

Para pagamento, indicamos a conta 14835-0, na agência 0383, no banco Itaú (341).

Manaus, 14 de setembro de 2023.

_____

Servix Informática Ltda.
Fabiano Theis
Sócio – Diretor

PROPOSTA TÉCNICA

LOTE ÚNICO
Marca: Palo Alto Networks
Modelo: Palo Alto NGFW PA-5220, PA-5410 e PA-410.

Objeto: renovação do suporte e das licenças do cluster de equipamentos de Next-Generation Firewall, assim como expansão da solução de firewall para as unidades descentralizadas do Tribunal de Justiça do Estado do Amazonas (TJAM), compreendendo suporte técnico e garantia pelo período de 60 meses, incluindo serviços de instalação, configuração e treinamento oficial do fabricante.

Lista de itens

ITEM	PART-NUMBER	DESCRIÇÃO	QTDE	GARANTIA
1	**Subscrição de Prevenção a Ameaças para solução de Plataforma de Segurança Palo Alto Networks PA-5220, pelo período de 60 meses**			
	PA-PAN-PA-5220-TP-5YR-HA2-R	Threat prevention subscription 5 year term renewal for device in an HA pair PA-5220	2	60 meses
2	**Subscrição de Filtro de URL para solução de Plataforma de Segurança Palo Alto Networks PA-5220, pelo período de 60 meses.**			
	PA-PAN-PA-5220-ADVURL-5YR-HA2-R	SUBSCRIPTION ADVANCED URL FILTERING, 5-YEAR, PA-5220, HA PAIR RENEWAL	2	60 meses
3	**Subscrição de Análise de Malware para solução de Plataforma de Segurança Palo Alto Networks PA-5220, pelo período de 60 meses.**			
	PA-PAN-PA-5220-WF-5YR-HA2-R	WildFire subscription 5 year term renewal for device in an HA pair PA-5220	2	60 meses
4	**Garantia da Solução de Plataforma de Segurança Palo Alto Networks PA-5220, com suporte Premium oficial Palo Alto Networks 24x7 em Alta Disponibilidade, pelo período de 60 meses.**			
	PA-PAN-SVC-PREM-5220-5YR-R	Premium support 5 year term renewal PA-5220	2	60 meses
5	**Firewall Palo Alto PA-410**			
	PAN-PA-410	PALO ALTO NETWORKS PA-410	70	60 meses
	PAN-PA-410-IOT-ENT-5YR	PA-410, ENTERPRISE IOT SUBSCRIPTION, 5 YEARS (60 MONTHS) TERM.	70	60 meses
	PAN-PA-410-OSS	ON-SITE SPARE PALO ALTO NETWORKS PA-410	2	60 meses
6	**Subscrição CORE SECURITY SUBSCRIPTION BUNDLE (ADVANCED THREAT PREVENTION, ADVANCED URL FILTERING, ADVANCED WILDFIRE, DNS SECURITY AND SD-WAN), pelo período de 60 meses.**			
	PAN-PA-410-BND-CORESEC-5YR	PA-410 Core Security Subscription Bundle Advanced Threat Prevention Advanced URL Filtering Advanced Wildfire DNS Security and SD-WAN 5 years 60 months term	70	60 meses
7	**Garantia da Solução de Plataforma de Segurança Palo Alto Networks PA-410, com suporte Premium oficial Palo Alto Networks 24x7, pelo período de 60 meses.**			
	PAN-SVC-PREM-410-5YR	PA-410 Premium support 5 years 60 months term	70	60 meses
8	**Subscrição de Licença de Gerência Centralizada com suporte para 100 dispositivos Palo Alto Networks, pelo período de 60 meses**			

	PAN-PRA-100	Panorama central management software, 100 devices	1	60 meses
9	**Garantia da Solução de Panorama, com suporte Premium oficial Palo Alto Networks 24x7, pelo período de 60 meses**			
	PAN-SVC-PREM-PRA-100-5YR	Premium support 5 year term, Panorama 100 devices	1	60 meses
10	**Subscrição de DNS Seguro para solução de Plataforma de Segurança Palo Alto Networks PA-5220, pelo período de 60 meses**			
	PAN-PA-5220-DNS-5YR-HA2	DNS Security subscription 5 year term for device in an HA pair PA-5220	2	60 meses
11	**Subscrição de SD-WAN Seguro para solução de Plataforma de Segurança Palo Alto Networks PA-5220, pelo período de 60 meses**			
	PAN-PA-5220-SDWAN-5YR-HA2	SD-WAN subscription 5 year term for device in an HA pair PA-5220	2	60 meses
12	**Serviço de instalação das soluções de Next-Generation Firewall Palo Alto Networks PA-410 e PA-5410**			
	SERVIÇO DE INSTALAÇÃO	SERVIÇO DE INSTALAÇÃO	72	60 meses
13	**Treinamento oficial do fabricante remoto, em língua portuguesa, com disponibilização de voucher para certificação de administração da solução Palo Alto**			
	PAN 210	Firewall: Essentials - Configuration and Management	4	60 meses
14	**Subscrição de GlobalProtect para solução de Plataforma de Segurança Palo Alto Networks PA-5220, pelo período de 60 meses**			
	PAN-PA-5220-GP-5YR-HA2	GlobalProtect subscription 5 year term for device in an HA pair PA-5220	2	60 meses
15	**Firewall Palo Alto PA-5410**			
	PAN-PA-5410-AC	PALO ALTO NETWORKS PA-5410 WITH REDUNDANT AC POWER SUPPLIES	2	60 meses
	PAN-PA-5410-IOT-ENT-5YR	PA-5410, ENTERPRISE IOT SUBSCRIPTION, 5 YEARS (60 MONTHS) TERM.	2	60 meses
	PAN-PA-2RU-RACK4	Palo Alto Networks PA-3220 PA-3250 PA-3260 PA-5410 PA-5420 and PA-5430 4 post rack mount kit	2	60 meses
16	**Subscrição CORE SECURITY SUBSCRIPTION BUNDLE (ADVANCED THREAT PREVENTION, ADVANCED URL FILTERING, ADVANCED WILDFIRE, DNS SECURITY AND SD-WAN) para PA-5410, pelo período de 60 meses**			
	PAN-PA-5410-BND-CORESEC-5YR	PA-5410 Core Security Subscription Bundle Advanced Threat Prevention Advanced URL Filtering Advanced Wildfire DNS Security and SD-WAN 5 years 60 months term	2	60 meses
17	**Garantia da Solução de Plataforma de Segurança Palo Alto Networks PA-5410, com suporte Premium oficial Palo Alto Networks 24x7, pelo período de 60 meses**			
	PAN-SVC-PREM-5410-5YR	Premium support 5 year term PA-5410	2	60 meses
18	**Subscrição de GlobalProtect para solução de Plataforma de Segurança Palo Alto Networks PA-5410, pelo período de 60 meses**			
	PAN-PA-5410-GP-5YR	PA-5410 GlobalProtect subscription 5 years 60 months term	2	60 meses

Tempo de Garantia da Solução: 60 meses

6.2 Funcionalidades gerais:
6.2.1 A solução consiste de appliance de proteção de rede com funcionalidades de Next Generation Firewall (NGFW), e console de gerência e monitoração;
6.2.2 As funcionalidades de proteção de rede que compõe a plataforma de segurança, funcionam em múltiplos appliances obedecendo a todos os requisitos desta especificação?";
6.2.3 A plataforma é otimizada para análise de conteúdo de aplicações em camada 7;
6.2.4 O hardware e software que executa as funcionalidades de proteção de rede, bem como a console de gerência e monitoração, é do tipo appliance. Não são equipamentos servidores e sistema operacional de uso genérico?;
6.2.5 Os dispositivos de proteção de rede possui as seguintes funcionalidades:
6.2.6 Agregação de links 802.3ad e LACP;
6.2.7 Policy based routing ou policy based forwarding;
6.2.8 Roteamento multicast (PIM-SM);
6.2.9 DHCP Relay;
6.2.10 DHCP Server;
6.2.11 Jumbo Frames;
6.2.12 Suporte a criação de objetos de rede que podem ser utilizados como endereço IP de interfaces L3;
6.2.13 Suporta sub-interfaces ethernet logicas;
6.2.14 Suporta os seguintes tipos de NAT:
6.2.15 Nat dinâmico (Many-to-1);
6.2.16 Nat dinâmico (Many-to-Many);
6.2.17 Nat estático (1-to-1);
6.2.18 NAT estático (Many-to-Many);
6.2.19 Nat estático bidirecional 1-to-1;
6.2.20 Tradução de porta (PAT);
6.2.21 NAT de Origem;
6.2.22 NAT de Destino;
6.2.23 Suporta NAT de Origem e NAT de Destino simultaneamente;
6.2.24 implementa Network Prefix Translation (NPTv6);
6.2.25 Envia log para sistemas de monitoração externos;
6.2.26 Possui a opção de enviar logs para os sistemas de monitoração externos via protocolo TCP e SSL;
6.2.27 Permite configurar certificado caso necessário para autenticação no sistema de monitoração externo de logs;
6.2.28 Proteção contra anti-spoofing;
6.2.29 Para IPv4, suporta roteamento estático e dinâmico (RIPv2, BGP e OSPFv2);
6.2.30 Para IPv6, suporta roteamento estático e dinâmico (OSPFv3);
6.2.31 Suporta a OSPF graceful restart;
6.2.32 Suporta o protocolo MP-BGP (Multiprotocol BGP) permitindo que o firewall possa anunciar rotas multicast para IPv4 e rotas unicast para IPv6;
6.2.33 Os dispositivos de proteção possuem a capacidade de operar de forma simultânea em uma única instância de firewall, mediante o uso de suas interfaces físicas nos seguintes modos: Modo sniffer (monitoramento e análise do tráfego de rede), camada 2 (l2) e camada 3 (l3);
6.2.34 Modo Sniffer, para inspeção via porta espelhada do tráfego de dados da rede;
6.2.35 Modo Camada – 2 (L2), para inspeção de dados em linha e ter visibilidade e controle do tráfego em nível de aplicação;
6.2.36 Modo Camada – 3 (L3), para inspeção de dados em linha e ter visibilidade e controle do tráfego em nível de aplicação operando como default gateway das redes protegidas;
6.2.37 Modo misto de trabalho Sniffer, L2 e L3 em diferentes interfaces físicas;
6.2.38 Suporte a configuração de alta disponibilidade Ativo/Passivo e Ativo/Ativo:
6.2.39 Em modo transparente;
6.2.40 Em layer 3;
6.2.41 A configuração em alta disponibilidade sincroniza:
6.2.41.1 Sessões;
6.2.41.2 Configurações, incluindo, mas não limitado a políticas de Firewall, NAT, QOS e objetos de rede;
6.2.41.3 Certificados de-criptografados;

6.2.41.4 Associações de Segurança das VPNs;
6.2.41.5 Tabelas FIB;
6.2.41.6 O HA (modo de Alta-Disponibilidade) possibilita monitoração de falha de link.
6.3 Funcionalidades específicas:
6.3.1 Subscrição de Prevenção a Ameaças para solução de Plataforma de Segurança Palo Alto Networks
6.3.1.1 Inclui assinaturas de prevenção de intrusão (IPS) e bloqueio de arquivos maliciosos (Antivírus e Anti-Spyware);
6.3.1.2 Tem a capacidade de bloquear ameaças desconhecidas em tempo real;
6.3.1.3 As funcionalidades de IPS, Antivírus e Anti-Spyware operam em caráter permanente, podendo ser utilizadas por tempo indeterminado, mesmo que não subsista o direito de receber atualizações ou que não haja contrato de garantia de software com o fabricante.
6.3.1.4 Sincroniza as assinaturas de IPS, Antivírus, Anti-Spyware quando implementado em alta disponibilidade ativo/ativo e ativo/passivo;
6.3.1.5 As assinaturas podem ser ativadas ou desativadas, ou ainda habilitadas apenas em modo de monitoração;
6.3.1.6 Exceções por IP de origem ou de destino são possíveis nas regras, de forma geral e assinatura a assinatura;
6.3.1.7 Permite o bloqueio de vulnerabilidades.
6.3.1.8 Permite o bloqueio de exploits conhecidos.
6.3.1.9 Inclui proteção contra ataques de negação de serviços.
6.3.1.10 Possui os seguintes mecanismos de inspeção de IPS:
6.3.1.11 Análise de padrões de estado de conexões;
6.3.1.12 Análise de decodificação de protocolo;
6.3.1.13 Análise para detecção de anomalias de protocolo;
6.3.1.14 Análise heurística;
6.3.1.15 IP Defragmentation;
6.3.1.16 Remontagem de pacotes de TCP;
6.3.1.17 Bloqueio de pacotes malformados.
6.3.1.18 Ser imune e capaz de impedir ataques básicos como: Synflood, ICMPflood, UDPfloof, etc;
6.3.1.19 Detectar e bloquear a origem de portscans com possibilidade de criar exceções para endereços IPs de ferramentas de monitoramento da organização;
6.3.1.20 Bloquear ataques efetuados por worms conhecidos, permitindo ao administrador acrescentar novos padrões;
6.3.1.21 Suportar os seguintes mecanismos de inspeção contra ameaças de rede: análise de padrões de estado de conexões, análise de decodificação de protocolo, análise para detecção de anomalias de protocolo, análise heurística, IP Defragmentation, remontagem de pacotes de TCP e bloqueio de pacotes malformados;
6.3.1.22 Possuir assinaturas específicas para a mitigação de ataques DoS e DDoS;
6.3.1.23 Possuir assinaturas para bloqueio de ataques de buffer overflow;
6.3.1.24 Possibilita a criação de assinaturas customizadas pela interface gráfica do produto;
6.3.1.25 Identifica e bloqueia comunicação com botnets;
6.3.1.26 Registra na console de monitoração as seguintes informações sobre ameaças identificadas:
6.3.1.27 O nome da assinatura ou do ataque, aplicação, usuário, origem e o destino da comunicação, além da ação tomada pelo dispositivo;
6.3.1.28 Suporta a captura de pacotes (PCAP), por assinatura de Malware e aplicação;
6.3.1.29 Permite o bloqueio de vírus, pelo menos, nos seguintes protocolos: HTTP, FTP, SMB, SMTP e POP3;
6.3.1.30 Os eventos identificam o país de onde partiu a ameaça;
6.3.1.31 Inclui proteção contra vírus em conteúdo HTML e javascript, software espião (spyware) e worms.
6.3.1.32 Proteção contra downloads involuntários usando HTTP de arquivos executáveis. maliciosos.
6.3.1.33 Rastreamento de vírus em pdf.
6.3.1.34 Permite a inspeção em arquivos comprimidos que utilizam o algoritmo deflate (zip, gzip, etc.).
6.3.2 Subscrição de Filtro de URL para solução de Plataforma de Segurança Palo Alto Networks
6.3.2.1 Suporta a capacidade de criação de políticas baseadas no controle por URL e categoria de URL;
6.3.2.2 Possui a função de exclusão de URLs do bloqueio;
6.3.2.3 Permite a customização de página de bloqueio;
6.3.2.4 Permite o bloqueio e continuação (possibilitando que o usuário acesse um site potencialmente bloqueado informando o mesmo na tela de bloqueio e possibilitando a utilização de um botão Continuar para permitir o usuário continuar acessando o site);
6.3.2.5 Permite controlar o envio de credenciais corporativas somente para categorias de URLs permitidas;
6.3.2.6 Provê análise em tempo real de páginas maliciosas e dessa forma permitir a proteção em tempo real antes mesmo da atualização das bases de dados de URLs;
6.3.3 Subscrição de Análise de Malware para solução de Plataforma de Segurança Palo Alto Networks

6.3.3.1 O dispositivo de proteção é capaz de enviar arquivos trafegados de forma automática para análise "In Cloud" ou local, onde o arquivo será executado e simulado em ambiente controlado;

6.3.3.2 É capaz de enviar para análise, arquivos tipo Executáveis, DLLs, Arquivos de Código e MSI;

6.3.3.3 É capaz de analisar arquivos maliciosos em ambiente controlado com, sistema operacional Windows, Linux, MacOS e Android;

6.3.3.4 A solução possui a capacidade de extrair e analisar em sand-box links (http e https) presentes no corpo de e-mails trafegados em SMTP e POP3. É gerado um relatório caso a abertura do link pela sand-box o identifique como site hospedeiro de exploits;

6.3.3.5 A análise de links em sand-box é capaz de classificar sites falsos na categoria de phishing e atualizar a base de filtro de URL da solução;

6.3.3.6 Permite exportar o resultado das análises de malwares de dia zero em PDF e CSV a partir da própria interface de gerência;

6.3.3.7 Permite o download dos malwares identificados a partir da própria interface de gerência;

6.3.3.8 Permite visualizar os resultados das análises de malwares de dia zero nos diferentes sistemas operacionais suportados;

6.3.3.9 Permite informar ao fabricante quanto a suspeita de ocorrências de falso-positivo e falso-negativo na análise de malwares de dia zero a partir da própria interface de gerência.

6.3.3.10 Caso sejam necessárias licenças de sistemas operacional e softwares para execução de arquivos no ambiente controlado (sand-box), as mesmas devem ser fornecidas em sua totalidade, sem custos adicionais para a contratante;

6.3.3.11 Suporta a análise de arquivos executáveis, DLLs, ZIP e criptografados em SSL no ambiente controlado;

6.3.3.12 Suporta a análise de arquivos do pacote office (.doc, .docx, .xls, .xlsx, .ppt, .pptx), arquivos java (.jar e class), Android APKs, MacOS (mach-O, DMG e PKG), Linux (ELF), RAR e 7-ZIP no ambiente de sandbox;

6.3.3.13 Atualiza a base com assinaturas para bloqueio dos malwares identificados em sand-box com frequência de, pelo menos, 5 minutos;

6.3.3.14 Permite o envio de arquivos e links para análise no ambiente controlado de forma automática via API.

6.3.3.15 Permite o envio para análise em sand-box de malwares bloqueados pelo antivírus da solução;

6.3.3.16 A solução analisa os arquivos do tipo malware em bare metal para evitar técnicas de evasão.

6.3.3.17 Previne contra-ataques sem arquivo buscando por atividade maliciosa em pelo menos nas seguintes linguagens de scripts: Powershell e Javascript.

6.3.4 Firewall Palo Alto PA-410

6.3.4.1 Possui throughput de 1 (um) Gbps com a funcionalidade de controle de aplicação para todas as assinaturas que o fabricante possuir;

6.3.4.2 Possui throughput de 650 (Seiscentos e cinquenta) Mbps com as funcionalidades de controle de aplicação, IPS, Antivírus e Anti-Spyware habilitadas simultaneamente na solução. A comprovação se dará através de documentação técnica do fabricante de acesso público informando os throughput aferidos com tráfego HTTP ou blend de protocolos definidos pelo fabricante como tráfego real;

6.3.4.3 Suporta 60.000 (Sessenta mil) conexões simultâneas;

6.3.4.4 Suporta 10.000 (dez mil) novas conexões por segundo;

6.3.4.5 Possui 6 (seis) interfaces físicas de rede de 1Gbps do tipo RJ-45;

6.3.4.6 Possui 1 (uma) interface física de rede de 1 Gbps dedicada para gerenciamento out of band, ou seja, não será utilizada interfaces genéricas e não dedicadas para o fim;

6.3.4.7 Possui 1 (uma) interface física do tipo console ou similar;

6.3.4.8 Possui armazenamento interno para registro de logs;

6.3.4.9 Possui fonte de alimentação elétrica capaz de operar entre 120 a 240 VAC;

6.3.4.10 Suporta 300 (trezentos) túneis de VPN IPSEC Gateway to Gateway simultaneamente estando, caso necessário, devidamente licenciado para este fim;

6.3.5 Subscrição de DNS Seguro para solução de Plataforma de Segurança Palo Alto Networks

6.3.5.1 Provê segurança automática para tráfego de DNS, com análise em cloud, provendo aos equipamentos, acesso a assinaturas de DNS, geradas utilizando análise preditiva e aprendizado de máquina, fornecendo dados de domínios maliciosos;

6.3.5.2 Permite configuração de categorias de assinaturas de DNS, para possibilitar a criação de políticas de segurança distintas, baseadas em fatores de risco associados com certos tipos de tráfego DNS;

6.3.5.3 Protege contra ameaças baseadas em DNS, incluindo aquelas baseadas em DNS dinâmico, domínios registrados recentemente e domínios de phishing;

6.3.5.4 Protege contra comunicações de command and control e roubo de dados baseadas em DNS.

6.3.5.5 O Dispositivo de próxima geração, em sua característica de proteção de DNS, permite o bloqueio de técnicas de Domain generation algorithms (DGA), evitando assim, que uma máquina contaminada possa tentar estabelecer em um curto espaço de tempo sessão com domínios maliciosos ou inexistentes.

6.3.6 Subscrição de SD-WAN Seguro para solução de Plataforma de Segurança Palo Alto Networks

6.3.6.1 Operacionaliza os seguintes critérios de SD-WAN:

6.3.6.2 As configurações de profiles de SD-WAN partem de um ponto central permitindo alteração e criação dos elementos primordiais para o funcionamento da solução, assim flexibilizando a configuração inicial e suas devidas manutenções;

6.3.6.3 A solução permite operar em caráter de diagrama hub-spoke;

6.3.6.4 Os dispositivos possuem a capacidade de exibir impactos por aplicação;

6.3.6.5 A solução permite ao administrador métricas de utilização de banda por circuito disponível e desta forma exibir no mínimo itens em porcentagem ou contadores, jitter, latência e perda de pacote;

6.3.6.6 O dispositivo compreende o que está causando desempenho de degradação para as aplicações e serviços ativos e assim garante que a experiência do usuário sofra o menor impacto possível;

6.3.6.7 O SD-WAN suporta os seguintes tipos de conexões WAN: ADSL/DSL, Cable Modem com Ethernet ou fibra, LTE /3G/4G/5G, MPLS, Link de rádio e Link satélite desde que a sua terminação permita conectividade com interfaces ethernet.

6.3.6.8 A solução possui inteligência para executar no mínimo as seguintes lógicas de operação:

6.3.6.9 Distribuição de tráfego por prioridade de circuito, circuitos exclusivos de contingenciamento em 3G/4G/5G serão utilizados apenas em caso de falha geral dos circuitos ADSL/MPLS;

6.3.6.10 Distribuição de tráfego de acordo com métricas definidas por origem e destino, o dispositivo permite ao administrador criar perfis com base em latência, jitter ou perda de pacotes para que uma vez que estes limites sejam atingidos o dispositivo mantenha a conexão por circuitos que apresente resultados abaixo dos limites definidos;

6.3.6.11 Distribuição de tráfego com balanceamento de sessão entre os circuitos existentes;

6.3.6.12 Distribuição orientada a qualidade, o dispositivo valida o melhor caminho disponível e utiliza-se deste path para manter sessões ativas, caso o melhor caminho entre em degradação por fatores anômalos o dispositivo entende estes fatores e distribui para os demais circuitos existentes.

6.3.6.13 A Solução de SD-WAN desempenha a função de Forward Error Correlation (FEC).

6.3.6.14 A Solução de SD-WAN desempenha a função de Packet Duplication (PD) permitindo encaminhar o pacote por mais de um circuito para em casos de falhas não haver retransmissão.

6.3.6.15 Os dispositivos suportam a funcionalidade de ZTP (Zero Touch Provisioning) para que assim, inseridos nas estruturas remotas, busquem automaticamente por suas configurações, com o objetivo de facilitar a instalação nas unidades remotas ou a troca de um dispositivo defeituoso.

6.3.7 Subscrição de GlobalProtect para solução de Plataforma de Segurança Palo Alto Networks

6.3.7.1 Suporta VPN Site-to-Site e Cliente-To-Site;

6.3.7.2 Suporta IPSec VPN;

6.3.7.3 Suporta SSL VPN;

6.3.7.4 A VPN IPSEc suporta:

6.3.7.4.1 3DES;

6.3.7.4.2 Autenticação MD5 e SHA-1;

6.3.7.4.3 Diffie-Hellman Group 1 , Group 2, Group 5 e Group 14;

6.3.7.4.4 Algoritmo Internet Key Exchange (IKEv1 e v2);

6.3.7.4.5 AES 128, 192 e 256 (Advanced Encryption Standard)

6.3.7.4.6 Autenticação via certificado IKE PKI.

6.3.7.5 Possui interoperabilidade com os seguintes fabricantes:

6.3.7.5.1 Cisco;

6.3.7.5.2 Checkpoint;

6.3.7.5.3 Juniper;

6.3.7.5.4 Palo Alto Networks;

6.3.7.5.5 Fortinet;

6.3.7.5.6 Sonic Wall;

6.3.7.6 Permite habilitar, desabilitar, reiniciar e atualizar IKE gateways e túneis de VPN IPSEc a partir da interface gráfica da solução, facilitando o processo de throubleshooting;

6.3.7.7 A VPN SSL suporta:

6.3.7.7.1 O usuário realiza a conexão por meio de cliente instalado no sistema operacional do equipamento ou por meio de interface WEB;

6.3.7.7.2 A funcionalidade de VPN SSL é atendida com ou sem o uso de agente;

6.3.7.7.3 Atribuição de endereço IP nos clientes remotos de VPN SSL;

6.3.7.7.4 Permite a atribuição de IPs fixos nos usuários remotos de VPN SSL;

6.3.7.7.5 Permite a criação de rotas de acesso e faixas de endereços IP atribuídas a clientes remotos de VPN de forma customizada por usuário AD/LDAP e grupo de usuário AD/LDAP;

6.3.7.7.6 Permite que todo o tráfego dos usuários remotos de VPN seja escoado para dentro do túnel de VPN, impedindo comunicação direta com dispositivos locais como proxies;
6.3.7.7.7 Atribuição de DNS nos clientes remotos de VPN;
6.3.7.7.8 Permite que seja definido métodos de autenticação distintos por sistema operacional do dispositivo remoto de VPN (Android, IOS, Mac, Windows e Chrome OS);
6.3.7.7.9 A solução de VPN verifica se o client que está conectando é o mesmo para o qual o certificado foi emitido inicialmente. O acesso é bloqueado caso o dispositivo não seja o correto;
6.3.7.7.10 Possui lista de bloqueio para dispositivos que forem reportados com roubado ou perdido pelo usuário;
6.3.7.7.11 Há a opção de ocultar o agente de VPN instalado no cliente remoto, tornando o mesmo invisível para o usuário;
6.3.7.7.12 Exibe mensagens de notificação customizada toda vez que um usuário remoto se conectar a VPN. Permite que o usuário desabilite a exibição da mensagem nas conexões seguintes;
6.3.7.7.13 Avisa ao usuário remoto de VPN quanto a proximidade da expiração de senha LDAP. Permite também a customização da mensagem com informações relevantes para o usuário;
6.3.7.7.14 Permite criar políticas de controle de aplicações, IPS, Antivírus, Antipyware e filtro de URL para tráfego dos clientes remotos conectados na VPN SSL;
6.3.7.7.15 A VPN SSL suporta proxy arp e uso de interfaces PPPOE;
6.3.7.7.16 Suporta autenticação via AD/LDAP, OTP (One Time Password), certificado e base de usuários local;
6.3.7.7.17 Permite a distribuição de certificado para o usuário de remoto através do portal de VPN de forma automatizada;
6.3.7.7.18 Possui lista de bloqueio para dispositivos em casos quando, por exemplo, o usuário reportar que o dispositivo foi perdido ou roubado;
6.3.7.7.19 Permite estabelecer um túnel VPN client-to-site do cliente a plataforma de segurança, fornecendo uma solução de single-sign-on aos usuários, integrando-se com as ferramentas de Windows- logon;
6.3.7.7.20 Suporta leitura e verificação de CRL (certificate revocation list);
6.3.7.7.21 Permite a aplicação de políticas de segurança e visibilidade para as aplicações que circulam dentro dos túneis SSL;
6.3.7.7.22 O agente de VPN a ser instalado nos equipamentos desktop e laptops, é capaz de ser distribuído de maneira automática via Microsoft SMS, Active Directory e ser descarregado diretamente desde o seu próprio portal, o qual reside no centralizador de VPN;
6.3.7.7.23 O agente comunica-se com o portal para determinar as políticas de segurança do usuário,
6.3.7.7.24 Permite que a conexão com a VPN SSL seja estabelecida das seguintes formas:
6.3.7.7.24.1 Antes do usuário autenticar na estação;
6.3.7.7.24.2 Após autenticação do usuário na estação;
6.3.7.7.24.3 Sob demanda do usuário;
6.3.7.7.25 Mantém uma conexão segura com o portal durante a sessão.
6.3.7.7.26 O agente de VPN SSL client-to-site é compatível com pelo menos: Windows 10, Windows 11, Mac OSx e Chrome OS;
6.3.7.7.27 O cliente de VPN SSL cliente-to-site também suporta dispositivos móveis (IOS e ANDROID) e sistemas operacionais Linux;
6.3.7.7.28 Possui mecanismos de checagem de conformidade do dispositivo remoto;
6.3.7.7.29 A checagem de conformidade permite verificar, as seguintes informações no cliente remoto: sistema operacional e patches instalados, antivírus e versão instalada, firewall no host, criptografia do disco, agente de DLP instalado, backup de disco, chaves de registros e processos ativos;
6.3.7.7.30 É possível a criação de perfis customizados de conformidade com, as seguintes opções: sistema operacional e patches instalados, antivírus e versão instalada, firewall no host, criptografia do disco, agente de DLP instalado backup de disco, chaves de registros e processos ativos;
6.3.7.7.31 O portal de VPN envia ao cliente remoto, a lista de gateways de VPN ativos para estabelecimento da conexão, os quais podem ser administrados centralmente;
6.3.7.7.32 Há a opção do cliente remoto escolher manualmente o gateway de VPN e de forma automática através da melhor rota entre os gateways disponíveis com base no tempo de resposta mais rápido;
6.3.7.7.33 Possui a capacidade de identificar se a origem da conexão de VPN é externa ou interna;
6.3.8 Subscrição de Licença de Gerência Centralizada com suporte para 100 dispositivos Palo Alto Networks
6.3.8.1 O gerenciamento centralizado é entregue como appliance físico ou virtual. Caso seja entregue em appliance físico é compatível com rack 19 polegadas e possui todos os acessórios necessários para sua instalação. Caso seja entregue em appliance virtual é compatível com Nutanix AHV;
6.3.8.2 A solução gerencia a quantidade total de equipamentos de ambos os lotes;
6.3.8.3 Caso a solução possua licenciamento relacionado ao volume de logs diários, este é entregue com a maior capacidade suportada ou ilimitada sem a necessidade de licenciamento adicional;

6.3.8.4 O gerenciamento da solução possibilita a coleta de estatísticas de todo o tráfego que passar pelos equipamentos da plataforma de segurança.

6.3.8.5 Controle sobre todos os equipamentos da plataforma de segurança em uma única console, com administração de privilégios e funções.

6.3.8.6 Permite controle global de políticas para todos os equipamentos que compõe a plataforma de segurança;

6.3.8.7 Suporta organizar os dispositivos administrados em grupos: os sistemas virtuais são administrados como dispositivos individuais, os grupos podem ser geográficos, por funcionalidade (por exemplo, IPS), e distribuição;

6.3.8.8 Implementa sistema de hierarquia entre os firewalls gerenciados, onde é possível aplicar configurações de forma granular em grupos de firewalls;

6.3.8.9 Implementa a criação de perfis de usuários com acesso a plataforma de gerenciamento com definição exata de quais informações e de quais firewalls e grupos de firewalls o usuário terá acesso referente a logs e relatórios;

6.3.8.10 Permite a criação de objetos e políticas compartilhadas;

6.3.8.11 Consolida logs e relatórios de todos os dispositivos administrados;

6.3.8.12 Permite exportar backup de configuração automaticamente via agendamento;

6.3.8.13 Permite que a configuração dos firewalls seja importada de forma automática na plataforma de gerenciamento centralizado e que possa ser usada em outros firewalls e grupos de firewalls;

6.3.8.14 Mostra os status dos firewalls em alta disponibilidade a partir da plataforma de gerenciamento centralizado;

6.3.8.15 Centraliza a administração de regras e políticas do cluster, usando uma única interface de gerenciamento;

6.3.8.16 O gerenciamento da solução suporta acesso via SSH, cliente ou WEB (HTTPS) e API aberta;

6.3.8.17 Permite substituir o certificado de fábrica no acesso HTTPS a gerência do firewall como possibilidade de uso de certificado criado localmente na própria solução ou importado de fonte externa;

6.3.8.18 Caso haja a necessidade de instalação de cliente para administração da solução o mesmo é compatível com sistemas operacionais Windows e Linux;

6.3.8.19 O gerenciamento permite/possui:

6.3.8.19.4. Criação e administração de políticas de firewall e controle de aplicação;

6.3.8.19.5. Criação e administração de políticas de IPS, Antivírus e Anti-Spyware;

6.3.8.19.6. Criação e administração de políticas de Filtro de URL;

6.3.8.19.7. Monitoração de logs;

6.3.8.19.8. Ferramentas de investigação de logs;

6.3.8.19.9. Debugging;

6.3.8.19.7. Captura de pacotes;

6.3.8.19.8. Acesso concorrente de administradores.

6.3.8.20 Permite que administradores concorrentes façam modificações, valide configurações e reverta configurações do firewall simultaneamente e que cada administrador consiga aplicar apenas as suas alterações de forma independente das realizadas por outro administrador;

6.3.8.21 Possui mecanismo busca global na solução onde é consultado por uma string tais como: nome de objetos, ID ou nome de ameaças, nome de aplicações, nome de políticas, endereços IPs, permitindo a localização e uso dos mesmo na configuração do dispositivo;

6.3.8.22 Possui um mecanismo de busca por comandos no gerenciamento via SSH, facilitando a localização de comandos;

6.3.8.23 Permite usar palavras-chaves e cores para facilitar identificação de regras;

6.3.8.24 Bloqueio de alterações, no caso acesso simultâneo de dois ou mais administradores;

6.3.8.25 Definição de perfis de acesso à console com permissões granulares como: acesso de escrita, acesso de leitura, criação de usuários, alteração de configurações;

6.3.8.26 Autenticação integrada ao Microsoft Active Directory e servidor Radius;

6.3.8.27 Localização de em quais regras um endereço IP, IP Range, subnet ou objetos estão sendo utilizados;

6.3.8.28 Atribuir sequencialmente um número a cada regra de firewall, NAT, QOS e regras de DOS;

6.3.8.29 Criação de regras que fiquem ativas em horário definido;

6.3.8.30 Criação de regras com data de expiração;

6.3.8.31 Backup das configurações e rollback de configuração para a última configuração salva;

6.3.8.32 Suportar Rollback de Sistema Operacional para a última versão local;

6.3.8.33 Habilidade de upgrade via SCP, TFTP e interface de gerenciamento;
6.3.8.34 Possui mecanismo de análise de impacto na política de segurança antes de atualizar a base com novas aplicações disponibilizadas pelo fabricante e validação de regras antes da aplicação;
6.3.8.35 Implementa mecanismo de validação de configurações antes da aplicação das mesmas permitindo identificar erros, tais como: rota de destino inválida, regras em shadowing etc;
6.3.8.36 É permitido o uso de appliance externo para permitir a validação de regras antes da aplicação.
6.3.8.37 Validação das políticas, avisando quando houver regras que, ofusquem ou conflitem com outras (shadowing);
6.3.8.38 Geração de logs de auditoria detalhados, informando a configuração realizada, o administrador que a realizou e o horário da alteração;
6.3.8.39 Tem a capacidade de gerar um relatório gráfico que permite visualizar as mudanças na utilização de aplicações na rede no que se refere a um período de tempo anterior, para permitir comparar os diferentes consumos realizados pelas aplicações no tempo presente com relação ao passado;
6.3.8.40 Geração de relatórios com mapas geográficos gerados em tempo real para a visualização de origens e destinos do tráfego gerado na instituição;
6.3.8.41 Provê relatórios com visão correlacionada de aplicações, ameaças (IPS, Antivírus e Anti-Spware), URLs e filtro de arquivos, para melhor diagnóstico e resposta a incidentes;
6.3.8.42 Permite a criação de Dashboards customizados para visibilidades do tráfego de aplicativos, usuários, categorias de URL, ameaças identificadas pelo IPS, antivírus, Anti-Spyware, malwares "Zero Day"detectados em sand-box e tráfego bloqueado;
6.3.8.43 O gerenciamento da solução possibilita a coleta de estatísticas de todo o tráfego que passar pelos dispositivos de segurança;
6.3.8.44 Permite a visualização dos logs de malwares modernos, tráfego (IP de origem, destino, usuário e porta), aplicação, IPS, antivírus, Anti-Spyware, Filtro de URL e filtro de arquivos em uma única tela.
6.3.8.45 Possui relatórios de utilização dos recursos por aplicações, URL, ameaças (IPS, Antivírus e Anti-Spware), etc;
6.3.8.46 Provê uma visualização sumarizada de todas as aplicações, ameaças (IPS, Antivírus e Anti- Spware), e URLs que passaram pela solução;
6.3.8.47 Possui mecanismo "Drill-Down" para navegação nos relatórios em Real Time;
6.3.8.48 Nas opções de "Drill-Down", é possível identificar o usuário que fez determinado acesso;
6.3.8.49 Possui relatório de visibilidade e uso sobre aplicativos (SaaS). O relatório também Mostra os riscos para a segurança do ambiente, tais como a entrega de malwares através de aplicativos SaaS com a informação do usuário responsável pelo acesso;
6.3.8.50 Os relatórios de visibilidade e uso sobre aplicativos (SaaS) podem ser extraídos por grupo de usuários apresentando o uso e consumo de aplicações por grupo de usuário;
6.3.8.51 Permite que os logs e relatórios sejam rotacionados automaticamente baseado no tempo em que estão armazenados na solução, assim como no espaço em disco usado;
6.3.8.52 Permite fazer o envio de logs para soluções externas de forma granular podendo selecionar quais campos dos logs são enviados incluindo, mas não limitado a: tipo de ameaça, usuário, aplicação, etc;
6.3.8.53 Exibição das seguintes informações, de forma histórica e em tempo real (atualizado de forma automática e contínua a cada 1 minuto):
6.3.8.53.1 Situação do dispositivo e do cluster;
6.3.8.53.2 Principais aplicações;
6.3.8.53.3 Principais aplicações por risco;
6.3.8.53.4 Administradores autenticados na gerência da plataforma de segurança;

6.3.8.53.5 Número de sessões simultâneas;
6.3.8.53.6 Status das interfaces;
6.3.8.53.7 Uso de CPU.
6.3.8.54 Geração de relatórios. Os seguintes relatórios são gerados:
6.3.8.54.1 Resumo gráfico de aplicações utilizadas;
6.3.8.54.2 Principais aplicações por utilização de largura de banda de entrada e saída;
6.3.8.54.3 Principais aplicações por taxa de transferência de bytes;
6.3.8.54.4 Principais hosts por número de ameaças identificadas;
6.3.8.54.5 Atividades de um usuário específico e grupo de usuários do AD/LDAP, incluindo aplicações acessadas, categorias de URL, URL/tempo de utilização e ameaças (IPS, Antivírus e Anti- Spware), de rede vinculadas a este tráfego.
6.3.8.55 Permite a criação de relatórios personalizados;
6.3.8.56 Gerar alertas automáticos via:
6.3.8.56.1 Email;
6.3.8.56.2 SNMP;
6.3.8.56.3 Syslog;
6.3.9 Serviço de instalação das soluções de Next-Generation Firewall Palo Alto Networks
6.3.9.1 O Serviço de instalação das unidades é realizado da seguinte forma:
6.3.9.1.1 Para a renovação, é realizado ativação das novas licenças e atualização de versão dos appliances.
6.3.9.1.2 Os serviços de instalação dos firewalls PA-410 são feitos de forma remota pela CONTRATADA.
6.3.9.1.3 Os serviços de instalação dos firewalls PA-5410 são feitos de forma presencial na unidade definida pelo TJAM;
6.3.9.1.4 Todo o processo é realizado por profissional qualificado e certificado na solução.
6.3.9.1.5 Os serviços de instalação e configuração das soluções são supervisionados pela contratante, através de funcionário (os) designado (s) para esta atividade, preliminarmente ao início da execução, durante a execução até o término da execução da instalação e ser acompanhada por gerente de projetos da CONTRATADA visando atender os prazos definidos e suas entrega de todo lote.
6.3.9.1.6 A instalação e configuração das soluções é realizada pela equipe da própria CONTRATADA.
6.3.9.1.7 A instalação e configuração da solução não ocorrerá por empresa, equipe ou profissional diferente da CONTRATADA neste processo.
6.3.9.1.8 A instalação e configuração contempla toda parte de hardware e software conforme item e arquitetura da solução Segurança para Defesa Cibernética.
6.3.9.1.9 Entende-se como instalação e configuração a instalação dos softwares e a ativação dos equipamentos adquiridos pela contratante.
6.3.9.1.10 A CONTRATADA executa os serviços sem qualquer interferência no funcionamento regular das atividades normalmente realizadas pela contratante, garantindo a continuidade dos serviços, ou seja, não há interrupção não programada do serviço de dados atual para a entrada do novo serviço. Desta forma, executa serviços em finais de semana, feriados e horário noturno, sempre que houver necessidade para atendimento das condições expostas pela contratante nesta especificação;
6.3.9.1.11 Todas as instalações e configurações são realizadas em conformidade com a recomendação do fabricante do equipamento e os requisitos fornecidos pela contratante para o ambiente em questão;
6.3.9.1.12 Instalação logica em ambiente virtual da contratante;
6.3.9.1.13 Ao término da instalação e configuração é considerado uma sessão de perguntas e respostas no local, com o objetivo de ser abordado os pontos principais e de funcionalidades chaves dos produtos instalados.
6.3.9.1.14 A CONTRATADA segue sua metodologia própria no processo de instalação e as melhores práticas indicadas pelo fabricante.
6.3.9.1.15 A CONTRATADA responsabiliza-se pela conformidade e qualidade dos serviços e bens, bem como de cada material, matéria-prima ou componente individualmente considerado, mesmo que não sejam de sua fabricação, garantindo seu perfeito desempenho;
6.3.10 Garantia da Solução de Plataforma de Segurança Palo Alto Networks, com suporte Premium oficial 24x7:
6.3.10.1 A CONTRATADA disponibiliza uma equipe de pessoas tecnicamente capacitadas, as quais são responsáveis pelo suporte e manutenção das soluções durante todo o contrato de forma remota.
6.3.10.2 A equipe está disponível para atendimento em regime 24 horas, 7 dias na semana e 365 dias ao ano.
6.3.10.3 Responsabilidades e atividades da Equipe:
6.3.10.3.1 Realizar todos os serviços de suporte e manutenção da solução quando solicitado pela CONTRATANTE.

6.3.10.3.2 Realizar o atendimento de tickets/chamados abertos pela contratante no sistema da CONTRATADA quando solicitado pela CONTRATANTE.

6.3.10.3.3 Realizar a interface entre as necessidades da contratante e os profissionais do fabricante por executar as atividades, em caso de necessidade de intervenção do fabricante em soluções de problemas.

6.3.10.4 A CONTRATADA disponibiliza ferramenta de acompanhamento de chamados, de sua propriedade e de sua responsabilidade, que atende aos seguintes requisitos:

6.3.10.4.1 O acesso às informações é protegido por senha e conexão segura ou outro método equivalente;

6.3.10.4.2 A contratante tem acesso à ferramenta via interface WEB através da internet;

6.3.10.4.3 A ferramenta mantém identificação do projeto ou demanda, data e hora de abertura do chamado, início e término do atendimento, identificação e resolução do escopo, documentação da solução, status, recursos alocados e outras informações pertinentes;

6.3.10.4.4 A ferramenta é capaz de exportar seus dados em formato .csv;

6.3.10.5 A ferramenta é capaz de permitir a emissão de relatórios diários e/ou mensais para o controle de todas as solicitações abertas e encaminhadas pela contratante;

6.3.10.5.1 A ferramenta deverá é capaz de gerir e garantir que os níveis de serviços de atendimento sejam monitorados, de forma que o tempo de atendimento de uma solicitação comece a ser contado a partir do envio da mesma pelo usuário solicitante e seja finalizado no momento de fechamento da solicitação no sistema.

6.3.11 Firewall Palo Alto PA-5410

6.3.11.1 Possui throughput de 40 (quarenta) Gbps com a funcionalidade de controle de aplicação para todas as assinaturas que o fabricante possuir;

6.3.11.2 Possui throughput de 20 (vinte) Gbps com as funcionalidades de controle de aplicação, IPS, Antivírus e Anti-Spyware habilitadas simultaneamente na solução. A comprovação se dá através de documentação técnica do fabricante de acesso público informando os throughput aferidos com tráfego HTTP ou blend de protocolos definidos pelo fabricante como tráfego real;

6.3.11.3 Suporta 3.000(três milhões) conexões simultâneas;

6.3.11.4 Suporta 250.000 (duzentos e cinquenta mil) novas conexões por segundo;

6.3.11.5 Possui 6 (seis) interfaces físicas de rede de 1Gbps do tipo RJ-45;

6.3.11.6 Possui 6 (seis) interfaces físicas de rede de 10Gbps SFP/SFP+;

6.3.11.7 Possui 4 (quatro) interfaces físicas de rede de 10/25Gbps SFP/SFP+/SFP28;

6.3.11.8 Possui 4 (quatro) interfaces físicas de rede de 40/100Gbps QSFP+/QSFP28;

6.3.11.9 Possui 1 (uma) interface física de rede de 1 Gbps dedicada para gerenciamento out of band, ou seja, não será permitida a utilização de interfaces genéricas e não dedicadas para o fim;

6.3.11.10 Possui 1 (uma) interface física do tipo console ou similar;

6.3.11.11 Está licenciada para 10 sistemas virtuais;

6.3.11.12 Possui armazenamento interno de 480 (quatrocentos e oitenta) GB para registro de logs;

6.3.11.13 Possui fonte de alimentação elétrica redundante capaz de operar entre 120 a 240 VAC;

6.4 Controle de Aplicações

6.4.1 Os dispositivos de proteção de rede possui a capacidade de reconhecer aplicações, independente de porta e protocolo, com as seguintes funcionalidades:

6.4.2 Possibilita a liberação e bloqueio somente de aplicações sem a necessidade de liberação de portas e protocolos.

6.4.3 Reconhece pelo menos 3000 aplicações diferentes, incluindo, mas não limitado: a tráfego relacionado a peer-to-peer, redes sociais, acesso remoto, update de software, protocolos de rede, voip, áudio, vídeo, proxy, mensageiros instantâneos, compartilhamento de arquivos, e-mail;

6.4.4 Identifica o uso de táticas evasivas, ou seja, tem a capacidade de visualizar e controlar as aplicações e os ataques que utilizam táticas evasivas via comunicações criptografadas, tais como Skype e ataques mediante a porta 443.

6.4.5 Para tráfego criptografado SSL, de-criptografa pacotes a fim de possibilitar a leitura de payload para checagem de assinaturas de aplicações conhecidas pelo fabricante;

6.4.6 Permite a utilização de aplicativos para um determinado grupo de usuário e bloquear para o restante, incluindo, mas não limitado a Skype. Permite também a criação de políticas de exceção concedendo o acesso a aplicativos como Skype apenas para alguns usuários;

6.4.7 Identifica o uso de táticas evasivas via comunicações criptografadas;
6.4.8 Atualiza a base de assinaturas de aplicações automaticamente;
6.4.9 Limita a banda (download/upload) usada por aplicações (traffic shaping), baseado no IP de origem, usuários e grupos do LDAP/AD;
6.4.10 Os dispositivos de proteção de rede possui a capacidade de identificar o usuário de rede com integração ao Microsoft Active Directory, sem a necessidade de instalação de agente no Domain Controller, nem nas estações dos usuários;
6.4.11 É possível adicionar controle de aplicações em todas as regras de segurança do dispositivo, ou seja, não se limitando somente a possibilidade de habilitar controle de aplicações em algumas regras;
6.4.12 Suporta múltiplos métodos de identificação e classificação das aplicações, por pelo menos checagem de assinaturas, decodificação de protocolos e análise heurística;
6.4.13 Para manter a segurança da rede eficiente, suporta o controle sobre aplicações desconhecidas e não somente sobre aplicações conhecidas;
6.4.14 Permite nativamente a criação de assinaturas personalizadas para reconhecimento de aplicações proprietárias na própria interface gráfica da solução, sem a necessidade de ação do fabricante, mantendo a confidencialidade das aplicações do órgão;
6.4.15 O fabricante Permite a solicitação de inclusão de aplicações na base de assinaturas de aplicações;
6.4.16 Alerta o usuário quando uma aplicação for bloqueada;
6.4.17 Possibilita que o controle de portas seja aplicado para todas as aplicações;
6.4.18 Permite criar filtro na tabela de regras de segurança para exibir somente:
6.4.19 Regras que permitem passagem de tráfego baseado na porta e não por aplicação, exibindo quais aplicações estão trafegando na mesma, o volume em bytes trafegado por cada a aplicação por, pelo menos, os últimos 30 dias e o primeiro e último registro de log de cada aplicação trafegada por esta determinada regra;
6.4.20 Aplicações permitidas em regras de forma desnecessária, pois não há tráfego da mesma na determinada regra;
6.4.21 Regras de segurança onde não houve passagem de tráfego nos últimos 90 dias;
6.5 Identificação de Usuários
6.5.1 Inclui a capacidade de criação de políticas baseadas na visibilidade e controle de quem está utilizando quais aplicações através da integração com serviços de diretório, autenticação via ldap, Active Directory, E-Directory e base de dados local;
6.5.2 Possui integração com Microsoft Active Directory para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários;
6.5.3 Possui integração com Radius para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários;
6.5.4 Possui integração com Ldap para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em Usuários e Grupos de usuários;
6.5.5 Suporta o recebimento eventos de autenticação de controladoras wireless, dispositivos 802.1x e soluções NAC via syslog, para a identificação de endereços IP e usuários;
6.5.6 Permite o controle, sem instalação de cliente de software, em equipamentos que solicitem saída a internet para que antes de iniciar a navegação, expanda-se um portal de autenticação residente no firewall (Captive Portal);
6.5.7 Suporte a autenticação Kerberos;
6.5.8 Suporta autenticação via Kerberos para administradores da plataforma de segurança, captive Portal e usuário de VPN SSL;
6.5.9 Possui suporte a identificação de múltiplos usuários conectados em um mesmo endereço IP em ambientes Citrix e Microsoft Terminal Server, permitindo visibilidade e controle granular por usuário sobre o uso das aplicações que estão nestes serviços;
6.5.10 O firewall opera/suporta Security Assertion Markup Language (SAML) 2.0, com single sign-on para as funcionalidades de Captive Portal e VPN SSL (client to server), permitindo login único e interativo para fornecer acesso automático a serviços autenticados, internos e externos à organização;
6.5.11 Implementa a criação de grupos customizados de usuários no firewall, baseado em atributos do LDAP/AD;
6.6 QoS:

6.6.1 Com a finalidade de controlar aplicações e tráfego cujo consumo possa ser excessivo, (como youtube, ustream, etc) e ter um alto consumo de largura de banda, se requer que a solução, além de poder permitir ou negar esse tipo de aplicações, possui a capacidade de controlá-las por políticas de máximo de largura de banda quando forem solicitadas por diferentes usuários ou aplicações, tanto de áudio como de vídeo streaming.

6.6.2 Suporta a criação de políticas de QoS por:

6.6.3 Endereço de origem

6.6.4 Endereço de destino

6.6.5 Por usuário e grupo do LDAP/AD.

6.6.6 Por aplicações;

6.6.7 Por porta;

6.6.8 O QoS possibilita a definição de classes por:

6.6.9 Banda Garantida

6.6.10 Banda Máxima

6.6.11 Fila de Prioridade.

6.6.12 Suporta priorização Real Time de protocolos de voz (VOIP) como H.323, SIP, SCCP, MGCP e aplicações como Skype.

6.6.13 Suporta marcação de pacotes Diffserv, inclusive por aplicação;

6.6.14 Implementa QOS (traffic-shapping), para pacotes marcados por outros ativos na rede (DSCP). A priorização e limitação do tráfego deve ser efetuada nos dois sentidos da conexão (inbound e outbound);

6.6.15 Disponibiliza estatísticas Real Time para classes de QoS.

6.6.16 Suporta QOS (traffic-shapping), em interface agregadas;

6.6.17 Permite o monitoramento do uso que as aplicações fazem por bytes, sessões e por usuário.

16 páginas - Datas e horários baseados em Brasília, Brasil
Sincronizado com o NTP.br e Observatório Nacional (ON)
Certificado de assinaturas gerado em 14 de September de 2023, 12:35:31

Proposta comercial e Técnica Ajustada Servix TJAM pdf

Código do documento 3a862376-079a-402f-836f-d0e434b13050

Assinaturas

FABIANO THEIS NASCIMENTO:11767026889
Certificado Digital
fabiano.theis@servix.com
Assinou

Eventos do documento

14 Sep 2023, 12:31:34
Documento 3a862376-079a-402f-836f-d0e434b13050 **criado** por DENIS RANIERI (908c5191-3cfc-4cbe-9463-3d4659d2defb). Email:denis.ranieri@servix.com. - DATE_ATOM: 2023-09-14T12:31:34-03:00

14 Sep 2023, 12:32:10
Assinaturas **iniciadas** por DENIS RANIERI (908c5191-3cfc-4cbe-9463-3d4659d2defb). Email: denis.ranieri@servix.com. - DATE_ATOM: 2023-09-14T12:32:10-03:00

14 Sep 2023, 12:34:52
ASSINATURA COM CERTIFICADO DIGITAL ICP-BRASIL - FABIANO THEIS NASCIMENTO:11767026889 **Assinou** Email: fabiano.theis@servix.com. IP: 187.11.122.18 (187-11-122-18.dsl.telesp.net.br porta: 38702). Dados do Certificado: CN=FABIANO THEIS NASCIMENTO:11767026889, OU=(em branco), OU=RFB e-CPF A1, OU=Secretaria da Receita Federal do Brasil - RFB, OU=01554285000175, OU=VideoConferencia, O=ICP-Brasil, C=BR. - DATE_ATOM: 2023-09-14T12:34:52-03:00

Hash do documento original
(SHA256):42c02387550c512ca5339196c9c4111145f47738286368b7cc92f6b849e8b8a7
(SHA512):f71e92d4211abd216f5113d3acee8c99242949ae8a1da2b84415ac10f6618bb689377d84ddd1009affafd3da3592e2588fa6a2e008433df5a9a1744d4b977109

Esse log pertence **única** e **exclusivamente** aos documentos de HASH acima

Esse documento está assinado e certificado pela D4Sign

PA-460

PA-450

PA-440

PA-445

PA-410

PA-415

PA-400 Series

Os firewalls de última geração Palo Alto Networks PA-400 Series, compostos por PA-410, PA-415 , PA-410, PA-415, PA-440, PA-450 e PA-460, trazem recursos de NGFW alimentado por aprendizado de máquina para filiais distribuídas de empresas, locais de varejo e empresas de médio porte.

O primeiro firewall de última geração (NGFW) alimentado por aprendizado de máquina do mundo permite evitar ameaças desconhecidas, ter visibilidade total e garantir proteção completa, incluindo a Internet das Coisas (IoT), além de reduzir os erros com recomendações automáticas de políticas.

Destaques

- 1º NGFW alimentado por aprendizado de máquina do mundo
- Onze vezes líder no Magic Quadrant da Gartner para firewalls de rede
- Líder no The Forrester Wave: Firewalls empresariais, quarto trimestre de 2022
- Abrange uma gama de necessidades de desempenho para a empresa distribuída com uma ampla linha de produtos
- Oferece segurança em um fator de forma de desktop
- Suporta alta disponibilidade com os modos ativo/ativo e ativo/passivo
- Oferece desempenho previsível com serviços de segurança
- Apresenta um design silencioso e sem ventoinha com uma fonte de alimentação redundante opcional para filiais e escritórios em casa
- Simplifica a implantação de um grande número de firewalls com Zero Touch Provisioning (Provisionamento sem intervenção humana – ZTP) opcional
- Compatível com administração centralizada com o gerenciamento de segurança de rede Panorama
- Maximiza os investimentos em segurança e evita interrupções nos negócios com AIOps

O elemento de controle do PA-400 Series é o PAN-OS, o mesmo software que opera todos os NGFWs da Palo Alto Networks. O PAN-OS classifica nativamente todo o tráfego, inclusive de aplicativos, ameaças e conteúdo e, em seguida, vincula esse tráfego ao usuário, independentemente da localização ou do tipo de dispositivo. Assim, os aplicativos, os conteúdos e os usuários, ou seja, os elementos que permitem o funcionamento dos seus negócios, servem como base para as suas políticas de segurança, o que resulta em uma postura de segurança aprimorada e na redução do tempo de resposta a incidentes.

Principais recursos de segurança e conectividade

Firewall de última geração alimentado por aprendizado de máquina

- Incorpora aprendizado de máquina no núcleo do firewall para fornecer prevenção de ataques em linha sem assinatura no que diz respeito a ataques baseados em arquivos, além de identificar e interromper imediatamente tentativas de phishing nunca antes vistas.
- Aproveita os processos de aprendizado de máquina baseados na nuvem para enviar instruções e assinaturas com atraso zero de volta para o firewall de última geração.
- Usa análise comportamental para detectar dispositivos IoT e fazer recomendações de políticas como parte de um serviço entregue na nuvem e nativamente integrado no firewall de última geração.
- Automatiza recomendações de políticas que economizam tempo e reduzem a chance de erro humano.

Identifica e categoriza todos os aplicativos, em todas as portas e o tempo todo, com inspeção completa da Camada 7

- Identifica os aplicativos que atravessam sua rede, independentemente da porta, protocolo, técnicas evasivas ou criptografia (TLS/SSL). Além disso, descobre e controla automaticamente novos aplicativos para acompanhar o crescimento do SaaS com a assinatura Segurança SaaS.
- Usa o aplicativo, não a porta, como base para todas as decisões sobre a política de viabilização segura: permitir, rejeitar, agendar, inspecionar e aplicar a formatação do tráfego.
- Oferece a capacidade de criar tags de App-ID personalizados para aplicativos patenteados ou solicitar o desenvolvimento de App-ID para novos aplicativos da Palo Alto Networks.
- Identifica todos os dados de carga útil de um aplicativo (por exemplo, arquivos e padrões de dados) para bloquear arquivos maliciosos e impedir tentativas de transferência não autorizada de dados.
- Cria relatórios de uso de aplicativos padrão e personalizados, incluindo relatórios de Software as a Service (Software como um serviço – SaaS) que fornecem informações sobre todo o tráfego SaaS sancionado e não sancionado em sua rede.
- Permite a migração segura de conjuntos de regras obsoletas da Camada 4 para regras baseadas em App-ID com o Policy Optimizer (otimizador de políticas) integrado, oferecendo a você um conjunto de regras mais seguro e mais fácil de gerenciar.

Confira o Resumo técnico do App-ID para mais informações.

Impõe segurança para usuários em qualquer local, em qualquer dispositivo, ao adaptar a política com base na atividade do usuário

- Permite visibilidade, políticas de segurança, relatórios e perícia com base em usuários e grupos, e não apenas em endereços IP.
- Integra-se facilmente com uma ampla variedade de repositórios para aproveitar as informações do usuário: controladores de LAN sem fio, VPNs, servidores de diretório, SIEMs, proxies e muito mais.
- Permite definir grupos dinâmicos de usuários (DUGs) no firewall para realizar ações de segurança com limite de tempo sem esperar que as alterações sejam aplicadas aos diretórios do usuário.
- Aplica políticas consistentes independentemente da localização dos usuários (escritório, casa, viagem etc.) e dos dispositivos (dispositivos móveis iOS e Android, macOS, Windows, desktops Linux, laptops; Citrix e Microsoft VDI e servidores de terminal).
- Impede que as credenciais corporativas vazem para sites de terceiros e evita a reutilização de credenciais roubadas ao habilitar a autenticação multifator (MFA) na camada de rede para qualquer aplicativo, sem nenhuma alteração no aplicativo.
- Fornece ações de segurança dinâmicas com base no comportamento do usuário para restringir usuários suspeitos ou mal-intencionados.
- Autentica e autoriza consistentemente seus usuários, independentemente da localização e onde se encontre alojada a identidade do usuário, a avançar rapidamente para uma postura de segurança Confiança Zero com o Cloud Identity Engine – uma arquitetura totalmente nova baseada na nuvem para segurança baseada em identidade.

Confira o resumo da solução Cloud Identity Engine para mais informações.

Impede atividades maliciosas ocultas em tráfego criptografado

- Inspeciona e aplica a política ao tráfego criptografado por TLS/SSL, tanto de entrada quanto de saída, incluindo o tráfego que usa TLS 1.3 e HTTP/2.
- Oferece ampla visibilidade do tráfego TLS, como quantidade de tráfego criptografado, versões TLS/SSL, pacotes de codificação e muito mais, sem decriptação.
- Permite o controle sobre o uso de protocolos TLS antigos, codificações inseguras e certificados configurados incorretamente para mitigar riscos.
- Facilita a implantação simples de decriptação e permite que você use logs integrados para solucionar problemas, como aplicativos com certificados fixos.
- Permite habilitar ou desabilitar a decriptação de maneira flexível com base na categoria de URL, zona de origem e destino, endereço, usuário, grupo de usuários, dispositivo e porta, para fins de privacidade e conformidade.
- Permite criar uma cópia do tráfego descriptografado do firewall (ou seja, espelhamento de decriptação) e enviá-lo para ferramentas de coleta de tráfego para fins de perícia, histórico ou prevenção de perda de dados (DLP).
- Permite que você encaminhe de forma inteligente todo o tráfego (TLS descriptografado, TLS não descriptografado e que não seja TLS) para ferramentas de segurança de terceiros com o Network Packet Broker e otimize o desempenho da rede e reduza as despesas operacionais.

Consulte este artigo técnico sobre decriptação para saber onde, quando e como descriptografar para evitar ameaças e proteger seu negócio.

Oferece gerenciamento centralizado e visibilidade

- Beneficia-se do gerenciamento centralizado, configuração e visibilidade para vários NGFWs da Palo Alto Networks distribuídos (independentemente da localização ou escala) por meio do gerenciamento de segurança de rede Panorama™, em uma interface de usuário unificada.
- Otimiza o compartilhamento de configuração por meio do Panorama com modelos e grupos de dispositivos e dimensiona a coleta de registros conforme as necessidades de registro aumentam. PA-410, PA-415, PA-440, PA-445, PA-450 e PA-460 permitem exportar logs de sessão para Panorama e Cortex Data Lake. PA-415, PA-440, PA-445, PA-450 e PA-460 também permitem log de sessão integrado.
- Permite que os usuários, por meio do Application Command Center (ACC – Centro de comando de aplicativos), obtenham visibilidade profunda e percepções abrangentes sobre o tráfego e as ameaças da rede.

Maximize seu investimento em segurança e evite interrupções nos negócios com o AIOps

- O AIOps para NGFW oferece recomendações contínuas de melhores práticas personalizadas para sua implantação exclusiva para fortalecer sua postura de segurança e aproveitar ao máximo seu investimento em segurança.
- Prevê de forma inteligente problemas de integridade, desempenho e capacidade do firewall com tecnologia de aprendizado de máquina alimentado por dados avançados de telemetria. Também fornece informações acionáveis para resolver as interrupções previstas.

Detecte e evite ameaças avançadas com serviços de segurança entregues na nuvem

Os sofisticados ataques cibernéticos de hoje podem gerar 45.000 variantes em 30 minutos, usando vários vetores de ameaças e técnicas avançadas para enviar cargas maliciosas. A segurança tradicional isolada causa desafios para as organizações, introduzindo brechas de segurança, aumentando a sobrecarga para as equipes de segurança e prejudicando a produtividade dos negócios com acesso e visibilidade inconsistentes.

Perfeitamente integrados com nossos NGFWs líderes do setor, nossos serviços de segurança entregues na nuvem usam o efeito de rede de 80.000 clientes para coordenar instantaneamente a inteligência e proteger contra todas as ameaças em todos os vetores. Elimine as lacunas de cobertura em seus locais e aproveite as vantagens da segurança de primeira classe fornecida de forma consistente em uma plataforma para ficar protegido até mesmo das ameaças mais avançadas e evasivas.

- **Threat Prevention avançado:** Impeça explorações conhecidas, malware, spyware e ameaças de comando e controle (C2), enquanto utiliza a prevenção de ataques de dia zero pioneira no setor – evite 60% mais ataques de injeção desconhecidos e 48% mais tráfego de comando e controle altamente evasivo do que as soluções IPS tradicionais.
- **WildFire avançado:** Certifique-se de que os arquivos estejam seguros, prevenindo automaticamente malware conhecido, desconhecido e altamente evasivo 60 vezes mais rápido com o maior mecanismo de inteligência contra ameaças e prevenção de malware do setor.
- **URL Filtering avançado:** Garanta o acesso seguro à Internet e evite 40% mais ataques baseados na web com a primeira prevenção em tempo real do setor contra ameaças conhecidas e desconhecidas, interrompendo 88% das URLs maliciosas pelo menos 48 horas antes de outros fornecedores.
- **Segurança de DNS:** Obtenha 40% mais cobertura contra ameaças e interrompa 85% dos malwares que abusam do DNS para comando e controle e roubo de dados sem exigir alterações em sua infraestrutura.

- **DLP empresarial:** Minimize o risco de uma violação de dados, interrompa transferências de dados fora da política e permita a conformidade de forma consistente em toda a sua empresa, com uma cobertura 2 vezes maior de qualquer DLP empresarial entregue na nuvem.
- **Segurança de SaaS:** Fique à frente do aumento exponencial do SaaS com o único CASB de última geração do setor para ver e proteger automaticamente todos os aplicativos em todos os protocolos.
- **Segurança de IoT:** Proteja cada "coisa" e implemente segurança de dispositivo de Confiança Zero 20 vezes mais rapidamente com a segurança mais inteligente do setor para dispositivos inteligentes.

Viabiliza a funcionalidade SD-WAN

- Permite que você adote a SD-WAN com facilidade, simplesmente viabilizando-a em seus firewalls existentes.
- Possibilita que você implemente com segurança a SD-WAN, que é nativamente integrada na nossa segurança líder no setor.
- Oferece uma experiência excepcional ao usuário final, minimizando a latência, instabilidade e perda de pacotes.

Oferece uma abordagem única para processamento de pacotes com arquitetura de passagem única

- Executa serviços de rede, pesquisa de política, aplicativo e decodificação e correspondência de assinatura – para todas as ameaças e conteúdo – em uma única passagem. Isto reduz significativamente o volume da sobrecarga de processamentos necessários para executar várias funções em um único dispositivo de segurança.
- Evita a introdução de latência com a varredura do tráfego para todas as assinaturas em uma única passagem, usando correspondência de assinatura uniforme e baseada em fluxo.
- Permite um desempenho consistente e previsível quando as assinaturas de segurança estão habilitadas. (Na Tabela 1, a "taxa de transferência do Threat Prevention" é medida com várias assinaturas habilitadas).

Tabela 1: Desempenho e capacidades do PA-400 Series

	PA-410	PA-415	PA-440	PA-445	PA-450	PA-460
Taxa de transferência de firewall (HTTP/appmix)*	1,59/1,1	1,65/1,2 Gbps	2,8/2,2 Gbps	2,8/2,2 Gbps	3,5/2,9 Gbps	5,1/4,4 Gbps
Taxa de transferência do Threat Prevention (HTTP/appmix)†	0,6/0,68 Gbps	0,6/0,69 Gbps	1,0/1,0 Gbps	1,0/1,0 Gbps	1,4/1,6 Gbps	2,1/2,4 Gbps
Taxa de transferência da VPN IPsec‡	0,92 Gbps	0,92 Gbps	1,6 Gbps	1,6 Gbps	2,2 Gbps	3,0 Gbps
Máximo de sessões	64000	64000	200000	200000	300000	400000
Novas sessões por segundo§	12000	12000	37500	37500	51000	73000
Sistemas virtuais (base/máx)‖	1/1	1/1	1/2	1/2	1/5	1/5

Observação: os resultados foram medidos no PAN-OS 11.0.

* A taxa de transferência do firewall é medida com App-ID e logs ativados, usando transações HTTP/appmix de 64 KB.

† A taxa de transferência do Threat Prevention é medida com App-ID, IPS, antivírus, anti-spyware, WildFire, segurança DNS, bloqueio de arquivos e logs ativados, usando transações HTTP/appmix de 64 KB.

‡ A taxa de transferência da VPN IPSec é medida com transações HTTP de 64 KB e logs ativados.

§ Novas sessões por segundo são medidas com a substituição de aplicativo usando transações HTTP de 1 byte.

‖ Incluir sistemas virtuais na quantidade base requer uma licença comprada separadamente e como mínimo PAN-OS 11.0.

Tabela 2: Recursos de rede do PA-400 Series

Modos de interface
L2, L3, tap, fio virtual (modo transparente)
Roteamento
OSPFv2/v3 com reinício normal, BGP com reinício normal, RIP, roteamento estático
Encaminhamento baseado em políticas
Protocolo ponto a ponto por Ethernet (PPPoE)
Multicast: PIM-SM, PIM-SSM, IGMP v1, v2 e v3
SD-WAN
Medição da qualidade do caminho (instabilidade, perda de pacotes, latência)
Seleção de caminho inicial (PBF)
Mudança dinâmica de caminho

Tabela 2: Recursos de rede do PA-400 Series (continuação)
IPv6
L2, L3, tap, fio virtual (modo transparente)
Recursos: App-ID, User-ID, Content-ID, WildFire e decriptação SSL
SLAAC
IPsec VPN
Troca de chaves: chave manual, IKEv1 e IKEv2 (chave pré-compartilhada, autenticação baseada em certificado)
Criptografia: 3DES, AES (128 bits, 192 bits, 256 bits)
Autenticação: MD5, SHA-1, SHA-256, SHA-384, SHA-512
VLANs
Etiquetas VLAN 802.1Q por dispositivo/por interface: 4.094/4.094
Interfaces agregadas (802.3ad), LACP

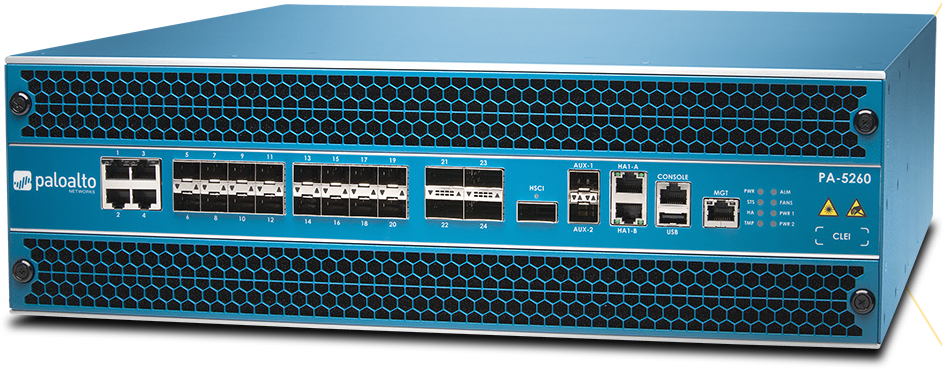
Tabela 3: Especificações de hardware do PA-400 Series
E/S
PA-410: RJ45 (7) PA-440, PA-450, PA-460: RJ45 (8) PA-415, PA-445: 1G SFP/RJ45 combo (1), RJ45 (4), RJ45/PoE (4)
E/S de gerenciamento
PA-410: (1) porta de gerenciamento fora de banda 10/100/1000, (1) porta de console RJ45, (2) porta USB Porta de gerenciamento fora de banda PA-415, PA-445 SFP/RJ45(1GB) (1), porta de console RJ-45 (1), porta USB (2), porta de console micro USB (1) PA-440, PA-450, PA-460: porta de gerenciamento fora de banda 10/100/1000 (1), porta de console RJ-45 (1), porta USB (2), porta de console Micro USB (1)
Power over Ethernet (PoE)
PA-415, PA-445 Portas PoE RJ45 (4) Orçamento total de energia PoE: 91 W Carga máxima na única porta: 60 W
Capacidade de armazenamento
PA-410: eMMC de 64 GB PA-415, PA-440, PA-445, PA-450, PA-460: eMMC de 128 GB
Fonte de alimentação (consumo de energia médio/máximo)
PA-410: 17/18 W PA-415, PA-440, PA-445: 29/34 W PA-450, PA-460: 33/41 W
BTU/h máximo
PA-410: 78 PA-415, PA-440, PA-445: 117 PA-450, PA-460: 141
Tensão de entrada (frequência de entrada)
100-240 VAC (50–60 Hz)
Consumo máximo de energia
PA-410: 1,5 A a 12 VCC PA-415, PA-440, PA-445: 2,9 A a 12 VCC PA-450, PA-460: 3,4 A a 12 VCC
Corrente de ligação máxima
PA-410: 2,1 A PA-415, PA-440, PA-445: 3,3 A PA-450, PA-460: 4,2 A

Tabela 3: Especificações de hardware do PA-400 Series (continuação)
Dimensões
PA-410: 4,1 cm x 16,3 cm x 24,2 cm (A x P x L) PA-415: 4,4 cm x 33 cm x 22,9 cm (A x P x L) PA-445: 4,2 cm x 33 cm x 22,5 cm (A x P x L) PA-440, PA-450, PA-460: 4,4 cm x 22,4 cm x 20,5 cm (A x P x L)
Peso (dispositivo autônomo/conforme entregue)
PA-410: 1,4/2,7 kg PA-415: 3,6/5,5 kg PA-445: 3,9/5,7 kg PA-440, PA-450 e PA-460: 2,3/3,5 kg
Segurança
cTUVus, CB
EMI
Classe B de FCC, Classe B de CE, Classe B de VCCI
Certificações
Consulte paloaltonetworks.com/company/certifications.html
Ambiente
Temperatura operacional: 32°F a 104°F, 0°C a 40°C Temperatura não operacional: -4°F a 158°F, -20°C a 70°C Resfriamento passivo

3000 Tannery Way
Santa Clara, CA 95054

Principal: +1.408.753.4000
Vendas: +1.866.320.4788
Suporte: +1.866.898.9087

www.paloaltonetworks.com



PA-5260

PA-5200 Series

Os firewalls de última geração (NGFWs) alimentados por aprendizado de máquina PA-5200 Series da Palo Alto Networks, incluindo o PA-5280, o PA-5260, o PA-5250 e o PA-5220, são ideais para implantações de provedores de serviço, gateways de Internet e centros de dados de alta velocidade.
O PA-5200 Series fornece até 64 Gbps de taxa de transferência usando processamento e memória dedicados para as principais áreas funcionais de rede, segurança, gerenciamento e prevenção de ameaças.

Destaques

- 1º NGFW alimentado por aprendizado de máquina do mundo
- Onze vezes líder no Magic Quadrant da Gartner para firewalls de rede
- Líder no The Forrester Wave: Firewalls empresariais, quarto trimestre de 2022
- Oferece segurança 5G nativa desenvolvida para proteger o provedor de serviços e a transformação 5G corporativa e computação de borda de acesso múltiplo (MEC)
- Amplia a visibilidade e a segurança para todos os dispositivos, incluindo dispositivos de IoT não gerenciados, sem a necessidade de implantar sensores adicionais
- Suporta alta disponibilidade com os modos ativo/ativo e ativo/passivo
- Oferece desempenho previsível com serviços de segurança
- Compatível com administração centralizada com o gerenciamento de segurança de rede Panorama
- Maximiza os investimentos em segurança e evita interrupções nos negócios com AIOps

O primeiro firewall de última geração (NGFW) alimentado por aprendizado de máquina do mundo permite evitar ameaças desconhecidas, ter visibilidade total e garantir proteção completa, incluindo a Internet das Coisas (IoT), além de reduzir os erros com recomendações automáticas de políticas. O elemento de controle do PA-5200 Series é o PAN-OS, o mesmo software que opera todos os NGFWs da Palo Alto Networks. O PAN-OS classifica nativamente todo o tráfego, inclusive de aplicativos, ameaças e conteúdo e, em seguida, vincula esse tráfego ao usuário, independentemente da localização ou do tipo de dispositivo. Assim, os aplicativos, os conteúdos e os usuários, ou seja, os elementos que permitem o funcionamento dos seus negócios, servem como base para suas políticas de segurança, o que resulta em uma postura de segurança aprimorada e na redução do tempo de resposta a incidentes.

Principais recursos de segurança e conectividade

Firewall de última geração alimentado por aprendizado de máquina

- Incorpora aprendizado de máquina no núcleo do firewall para fornecer prevenção de ataques em linha sem assinatura no que diz respeito a ataques baseados em arquivos, além de identificar e interromper imediatamente tentativas de phishing nunca antes vistas.
- Aproveita os processos de aprendizado de máquina baseados na nuvem para enviar instruções e assinaturas com atraso zero de volta para o firewall de última geração.
- Usa análise comportamental para detectar dispositivos IoT e fazer recomendações de políticas; serviço fornecido na nuvem e nativamente integrado no firewall de última geração.
- Automatiza recomendações de políticas que economizam tempo e reduzem a chance de erro humano.

Identifica e categoriza todos os aplicativos, em todas as portas e o tempo todo, com inspeção completa da Camada 7

- Identifica os aplicativos que atravessam sua rede, independentemente da porta, protocolo, técnicas evasivas ou criptografia (TLS/SSL).
- Descobre e controla automaticamente novos aplicativos para acompanhar o crescimento do SaaS com a assinatura Segurança SaaS.
- Usa o aplicativo, não a porta, como base para todas as decisões sobre a política de viabilização segura: permitir, rejeitar, agendar, inspecionar e aplicar a formatação do tráfego.
- Oferece a capacidade de criar tags de App-ID personalizados para aplicativos patenteados ou solicitar o desenvolvimento de App-ID para novos aplicativos da Palo Alto Networks.
- Identifica todos os dados de carga útil do aplicativo (por exemplo, arquivos e padrões de dados) para bloquear arquivos maliciosos e impedir tentativas de transferência não autorizada de dados.
- Cria relatórios de uso de aplicativos padrão e personalizados, incluindo relatórios de Software as a Service (Software como um serviço – SaaS) que fornecem informações sobre todo o tráfego SaaS sancionado e não sancionado em sua rede.
- Permite a migração segura de conjuntos de regras obsoletas da Camada 4 para regras baseadas em App-ID com o Policy Optimizer (otimizador de políticas) integrado, oferecendo a você um conjunto de regras mais seguro e mais fácil de gerenciar.
- Confira o Resumo técnico do App-ID para mais informações.

Impõe segurança para usuários em qualquer local, em qualquer dispositivo, ao adaptar a política com base na atividade do usuário

- Permite visibilidade, políticas de segurança, relatórios e perícia com base em usuários e grupos, e não apenas em endereços IP.
- Integra-se facilmente com uma ampla variedade de repositórios para aproveitar as informações do usuário: controladores de LAN sem fio, VPNs, servidores de diretório, SIEMs, proxies e muito mais.
- Permite definir grupos dinâmicos de usuários (DUGs) no firewall para realizar ações de segurança com limite de tempo sem esperar que as alterações sejam aplicadas aos diretórios do usuário.
- Aplica políticas consistentes independentemente da localização dos usuários (escritório, casa, viagem etc.) e dos dispositivos (dispositivos móveis iOS e Android, macOS, Windows, desktops Linux, laptops; Citrix e Microsoft VDI e servidores de terminal).
- Impede que as credenciais corporativas vazem para sites de terceiros e evita a reutilização de credenciais roubadas ao habilitar a autenticação multifator (MFA) na camada de rede para qualquer aplicativo, sem nenhuma alteração no aplicativo.
- Fornece ações de segurança dinâmicas com base no comportamento do usuário para restringir usuários suspeitos ou mal-intencionados.

- Autentica e autoriza consistentemente seus usuários, independentemente da localização e onde se encontre alojada a identidade do usuário, a avançar rapidamente para uma postura de segurança Confiança Zero com o Cloud Identity Engine – uma arquitetura totalmente nova baseada na nuvem para segurança baseada em identidade.
- Confira o resumo da solução Cloud Identity Engine para mais informações.

Impede atividades maliciosas ocultas em tráfego criptografado

- Inspeciona e aplica a política ao tráfego criptografado por TLS/SSL, tanto de entrada quanto de saída, incluindo o tráfego que usa TLS 1.3 e HTTP/2.
- Oferece ampla visibilidade do tráfego TLS, como quantidade de tráfego criptografado, versões TLS/SSL, pacotes de codificação e muito mais, sem decriptação.
- Permite o controle sobre o uso de protocolos TLS antigos, codificações inseguras e certificados configurados incorretamente para mitigar riscos.
- Facilita a implantação simples de decriptação e permite que você use logs integrados para solucionar problemas, como aplicativos com certificados fixos.
- Permite habilitar ou desabilitar a decriptação de maneira flexível com base na categoria de URL e zona de origem e destino, endereço, usuário, grupo de usuários, dispositivo e porta, para fins de privacidade e conformidade regulatória.
- Permite criar uma cópia do tráfego descriptografado do firewall (ou seja, espelhamento de decriptação) e enviá-lo para ferramentas de coleta de tráfego para fins de perícia, histórico ou prevenção de perda de dados (DLP).
- Permite que você encaminhe de forma inteligente todo o tráfego (TLS descriptografado, TLS não descriptografado e que não seja TLS) para ferramentas de segurança de terceiros com o Network Packet Broker e otimize o desempenho da rede e reduza as despesas operacionais.
- Consulte este artigo técnico sobre decriptação para saber onde, quando e como descriptografar para evitar ameaças e proteger seu negócio.

Oferece gerenciamento centralizado e visibilidade

- Beneficia-se do gerenciamento centralizado, configuração e visibilidade para vários NGFWs da Palo Alto Networks distribuídos (independentemente da localização ou escala) por meio do gerenciamento de segurança de rede Panorama™, em uma interface de usuário unificada.
- Otimiza o compartilhamento de configuração por meio do Panorama com modelos e grupos de dispositivos e dimensiona a coleta de registros conforme as necessidades de registro aumentam.
- Permite que os usuários, por meio do Application Command Center (ACC – Centro de comando de aplicativos), obtenham visibilidade profunda e percepções abrangentes sobre o tráfego e as ameaças da rede.

Maximize seu investimento em segurança e evite interrupções nos negócios com o AIOps

- O AIOps para NGFW oferece recomendações contínuas de melhores práticas personalizadas para sua implantação exclusiva para fortalecer sua postura de segurança e aproveitar ao máximo seu investimento em segurança.
- Prevê de forma inteligente problemas de integridade, desempenho e capacidade do firewall com tecnologia de aprendizado de máquina alimentado por dados avançados de telemetria. Também fornece informações acionáveis para resolver as interrupções previstas.

Detecta e evita ameaças avançadas com serviços de segurança entregues na nuvem

Os sofisticados ataques cibernéticos de hoje podem gerar 45.000 variantes em 30 minutos, usando vários vetores de ameaças e técnicas avançadas para enviar cargas maliciosas. A segurança tradicional isolada causa desafios para as organizações, introduzindo brechas de segurança, aumentando a sobrecarga para as equipes de segurança e prejudicando a produtividade dos negócios com acesso e visibilidade inconsistentes.

Perfeitamente integrados com nossos NGFWs líderes do setor, nossos serviços de segurança entregues na nuvem usam o efeito de rede de 80.000 clientes para coordenar instantaneamente a inteligência e proteger contra todas as ameaças em todos os vetores. Elimine as lacunas de cobertura em seus locais e aproveite as vantagens da segurança de primeira classe fornecida de forma consistente em uma plataforma para ficar protegido até mesmo das ameaças mais avançadas e evasivas. Os serviços incluem:

- **Threat Prevention avançado**: Impeça explorações conhecidas, malware, spyware e ameaças de comando e controle (C2), enquanto utiliza a prevenção de ataques de dia zero pioneira no setor – evite 60% mais ataques de injeção desconhecidos e 48% mais tráfego de comando e controle altamente evasivo do que as soluções IPS tradicionais.
- **WildFire avançado**: Certifique-se de que os arquivos estejam seguros, prevenindo automaticamente malware conhecido, desconhecido e altamente evasivo 60 vezes mais rápido com o maior mecanismo de inteligência contra ameaças e prevenção de malware do setor.

- **URL Filtering avançado**: Garanta o acesso seguro à Internet e evite 40% mais ataques baseados na web com a primeira prevenção em tempo real do setor contra ameaças conhecidas e desconhecidas, interrompendo 88% das URLs maliciosas pelo menos 48 horas antes de outros fornecedores.
- **DNS Security**: Obtenha 40% mais cobertura contra ameaças e interrompa 85% dos malwares que abusam do DNS para comando e controle e roubo de dados sem exigir alterações em sua infraestrutura.
- **DLP empresarial**: Minimize o risco de uma violação de dados, interrompa transferências de dados fora da política e permita a conformidade de forma consistente em toda a sua empresa, com uma cobertura 2 vezes maior de qualquer DLP empresarial entregue na nuvem.
- **Segurança de SaaS**: Fique à frente do aumento exponencial do SaaS com o único CASB de última geração do setor para ver e proteger automaticamente todos os aplicativos em todos os protocolos.
- **IoT Security**: Proteja cada "coisa" e implemente segurança de dispositivo de Confiança Zero 20 vezes mais rapidamente com a segurança mais inteligente do setor para dispositivos inteligentes.

Oferece uma abordagem única para processamento de pacotes com arquitetura de passagem única

- Executa serviços de rede, pesquisa de política, aplicativo e decodificação e correspondência de assinatura – para todas as ameaças e conteúdo – em uma única passagem. Isto reduz significativamente o volume da sobrecarga de processamentos necessários para executar várias funções em um único dispositivo de segurança.
- Evita a introdução de latência com a varredura do tráfego para todas as assinaturas em uma única passagem, usando correspondência de assinatura uniforme e baseada em fluxo.
- Permite um desempenho consistente e previsível quando as assinaturas de segurança estão habilitadas. (Na Tabela 1, a "taxa de transferência do Threat Prevention" é medida com várias assinaturas habilitadas).

Viabiliza a funcionalidade SD-WAN

- Permite que você adote a SD-WAN com facilidade, simplesmente viabilizando-a em seus firewalls existentes.
- Possibilita que você implemente com segurança a SD-WAN, que é nativamente integrada na nossa segurança líder no setor.
- Oferece uma experiência excepcional ao usuário final, minimizando a latência, instabilidade e perda de pacotes.

Tabela 1: Desempenho e capacidades do PA-5200 Series

	PA-5220	PA-5250	PA-5260	PA-5280
Taxa de transferência de firewall (HTTP/appmix)*	13,9/15,6 Gbps	32,1/36,7 Gbps	47,2/55,2 Gbps	47,2/55,2 Gbps
Taxa de transferência do Threat Prevention (HTTP/appmix)†	7,1/8,8 Gbps	16,6/21,4 Gbps	24,8/31,4 Gbps	24,8/31,4 Gbps
Taxa de transferência da VPN IPsec†	9,5 Gbps	18,4 Gbps	26,3 Gbps	26,3 Gbps
Máximo de sessões	4 M	8 M	32 M	64 M
Novas sessões por segundo§	150000	368000	500000	500000
Sistemas virtuais (base/máx)‖	10/20	25/125	25/225	25/225

Observação: os resultados foram medidos no PAN-OS 11.0.

* A taxa de transferência de firewall é medida com o App-ID e os logs ativados, usando transações HTTP/appmix de 64 KB.

† A taxa de transferência do Threat Prevention é medida com App-ID, IPS, antivírus, anti-spyware, WildFire, bloqueio de arquivos e logs ativados, usando transações HTTP/appmix de 64 KB.

‡ A taxa de transferência da VPN IPSec é medida com transações HTTP de 64 KB e logs ativados.

§ Novas sessões por segundo são medidas com a substituição de aplicativo usando transações HTTP de 1 byte.

‖ Incluir sistemas virtuais na quantidade base requer uma licença comprada separadamente.

Tabela 2: Recursos de rede do PA-5200 Series

Modos de interface
L2, L3, tap, fio virtual (modo transparente)
Roteamento
OSPFv2/v3 com reinício normal, BGP com reinício normal, RIP, roteamento estático
Encaminhamento baseado em políticas
Protocolo ponto a ponto por Ethernet (PPPoE) e DHCP com suporte para a atribuição de endereços dinâmicos
Multicast: PIM-SM, PIM-SSM, IGMP v1, v2 e v3
Detecção de encaminhamento bidirecional (BFD)

Tabela 2: Recursos de rede do PA-5200 Series (continuação)
SD-WAN
Medição da qualidade do caminho (instabilidade, perda de pacotes, latência)
Seleção de caminho inicial (PBF)
Mudança dinâmica de caminho
IPv6
L2, L3, tap, fio virtual (modo transparente)
Recursos: App-ID, User-ID, Content-ID, WildFire e decriptação SSL
SLAAC
IPsec VPN
Troca de chaves: chave manual, IKEv1 e IKEv2 (chave pré-compartilhada, autenticação baseada em certificado)
Criptografia: 3DES, AES (128 bits, 192 bits, 256 bits)
Autenticação: MD5, SHA-1, SHA-256, SHA-384, SHA-512
VPN de grande escala GlobalProtect para configuração e gerenciamento simplificados
VLANs
Etiquetas VLAN 802.1Q por dispositivo/por interface: 4.094/4.094
Interfaces agregadas (802.3ad), LACP
Network address translation (tradução de endereço de rede - NAT)
Modos de NAT (IPv4): IP estático, IP dinâmico, IP dinâmico e porta (conversão de endereço de porta)
NAT64, NPTv6
Recursos NAT adicionais: reserva de IP dinâmico, IP dinâmico ajustável e reutilização de porta
Alta disponibilidade
Modos: ativo/ativo, ativo/passivo, sistema de alta disponibilidade (HA)
Detecção de falhas: monitoramento de caminho, monitoramento de interface
Infraestrutura de redes móveis*
Segurança de GTP
Segurança de SCTP

* Para obter informações adicionais, consulte nossa folha de dados NGFWs alimentados por aprendizado de máquina para 5G.

Tabela 3: Especificações de hardware do PA-5200 Series
E/S
PA-5220: (4) 100/1000/10G Cu, (16) 1G/10G SFP/ SFP+, (4) 40G/ QSFP PA-5280/PA-5260/PA-5250: (4) 100/1000/10G Cu, (16) 1G/10G SFP/ SFP+, (4) 40G/100G QSFP28
E/S de gerenciamento
PA-5220: (2) 10/100/1000, (1) 40G/ QSFP HA, (1) gerenciamento fora de banda 10/100/1000, (1) porta do console RJ45 PA-5280/PA-5260/PA-5250: (2) 10/100/1000, (1) 40G/100G QSFP28 HA, (1) gerenciamento fora de banda 10/100/1000, (1) porta do console RJ45
Capacidade de armazenamento
SSD 240 GB, RAID1, armazenamento do sistema 2 TB HDD, RAID1, armazenamento de log

Tabela 3: Especificações de hardware do PA-5200 Series (cont.)
Fonte de alimentação (consumo de energia médio/máximo)
571/685 W
BTU/h máximo
2340
Fontes de alimentação (base/máximo)
1:1 Totalmente redundante (2/2)
Tensão de entrada CA (Hz de entrada)
100-240 VCA (50-60 Hz)
Saída da fonte de alimentação CA
1.200 watts/fonte de alimentação
Consumo máximo de energia
CA: 8,5 A a 100 VCA, 3,6 A a 240 VCA CC: 19 A a -40 VCC, 12,7 A a -60 VCC
Corrente de ligação máxima
CA: 50 A a 230 VCA, 50 A a 120 VCA CC: 200 A a 72 VCC
CC: 200 A a 72 VCC
9,23 anos
Montável em rack (dimensões)
3U, rack padrão de 19” 5,25” x 20,5” x 17,25” (A x P x L)
Peso (dispositivo autônomo/conforme entregue)
46 lbs/62 lbs
Segurança
cTUVus, CB
EMI
Classe A de FCC, Classe A de CE, Classe A de VCCI
Certificações
Consulte paloaltonetworks.com/company/certifications.html
Ambiente
Temperatura operacional: 32°F a 122°F, 0°C a 50°C Temperatura não operacional: -4°F a 158°F, -20°C a 70°C

3000 Tannery Way
Santa Clara, CA 95054

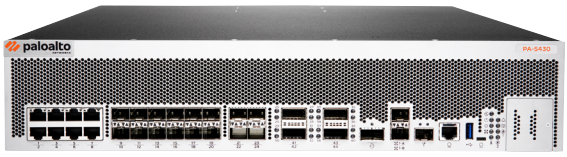
Principal: +1.408.753.4000
Vendas: +1.866.320.4788
Suporte: +1.866.898.9087

www.paloaltonetworks.com

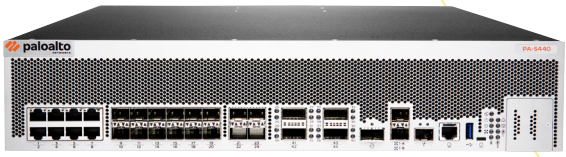
strata_ds_pa-5200-series_012323

PA-5410

PA-5420



PA-5430



PA-5440

PA-5400 Series

Os firewalls PA-5400 Series alimentados por aprendizado de máquina da Palo Alto Networks de última geração, incluindo o PA-5440, PA-5430, PA-5420 e PA-5410, são ideais para implantações de provedores de serviço, gateways de Internet e centros de dados de alta velocidade. Os dispositivos PA-5400 Series protegem todo o tráfego, inclusive o tráfego criptografado.

Destaques

- 1º NGFW alimentado por aprendizado de máquina do mundo
- Onze vezes líder no Magic Quadrant da Gartner para firewalls de rede
- Líder no The Forrester Wave: Firewalls empresariais, quarto trimestre de 2022
- Oferece segurança 5G nativa desenvolvida para proteger o provedor de serviços e a transformação 5G corporativa e computação de borda de acesso múltiplo (MEC)
- Amplia a visibilidade e a segurança para todos os dispositivos, incluindo dispositivos de IoT não gerenciados, sem a necessidade de implantar sensores adicionais
- Suporta alta disponibilidade com os modos ativo/ativo e ativo/passivo
- Oferece desempenho previsível com serviços de segurança
- Compatível com administração centralizada com o gerenciamento de segurança de rede Panorama
- Maximiza os investimentos em segurança e evita interrupções nos negócios com AIOps

O primeiro firewall de última geração (NGFW) alimentado por aprendizado de máquina do mundo permite evitar ameaças desconhecidas, ter visibilidade total e garantir proteção completa, incluindo a Internet das Coisas (IoT), além de reduzir os erros com recomendações automáticas de políticas.

O elemento de controle do PA-5400 Series é o PAN-OS, o mesmo software que opera todos os NGFWs da Palo Alto Networks. O PAN-OS classifica nativamente todo o tráfego, inclusive de aplicativos, ameaças e conteúdo e, em seguida, vincula esse tráfego ao usuário, independentemente da localização ou do tipo de dispositivo. Assim, os aplicativos, os conteúdos e os usuários, ou seja, os elementos que permitem o funcionamento dos seus negócios, servem como base para suas políticas de segurança, o que resulta em uma postura de segurança aprimorada e na redução do tempo de resposta a incidentes.

Principais recursos de segurança e conectividade

Firewall de última geração alimentado por aprendizado de máquina

- Incorpora aprendizado de máquina no núcleo do firewall para fornecer prevenção de ataques em linha sem assinatura no que diz respeito a ataques baseados em arquivos, além de identificar e interromper imediatamente tentativas de phishing nunca antes vistas.
- Aproveita os processos de aprendizado de máquina baseados na nuvem para enviar instruções e assinaturas com atraso zero de volta para o firewall de última geração.
- Usa análise comportamental para detectar dispositivos IoT e fazer recomendações de políticas; serviço fornecido na nuvem e nativamente integrado no firewall de última geração.
- Automatiza recomendações de políticas que economizam tempo e reduzem a chance de erro humano.

Identifica e categoriza todos os aplicativos, em todas as portas e o tempo todo, com inspeção completa da Camada 7

- Identifica os aplicativos que atravessam sua rede, independentemente da porta, protocolo, técnicas evasivas ou criptografia (TLS/SSL). Além disso, descobre e controla automaticamente novos aplicativos para acompanhar o crescimento do SaaS com a assinatura Segurança SaaS.
- Usa o aplicativo, não a porta, como base para todas as decisões sobre a política de viabilização segura: permitir, rejeitar, agendar, inspecionar e aplicar a formatação do tráfego.
- Oferece a capacidade de criar tags de App-ID personalizados para aplicativos patenteados ou solicitar o desenvolvimento de App-ID para novos aplicativos da Palo Alto Networks.
- Identifica todos os dados de carga útil do aplicativo (por exemplo, arquivos e padrões de dados) para bloquear arquivos maliciosos e impedir tentativas de transferência não autorizada de dados.
- Cria relatórios de uso de aplicativos padrão e personalizados, incluindo relatórios de Software as a Service (Software como um serviço – SaaS) que fornecem informações sobre todo o tráfego SaaS sancionado e não sancionado em sua rede.
- Permite a migração segura de conjuntos de regras obsoletas da Camada 4 para regras baseadas em App-ID com o Policy Optimizer (otimizador de políticas) integrado, oferecendo a você um conjunto de regras mais seguro e mais fácil de gerenciar.

Confira o Resumo técnico do App-ID para mais informações.

Impõe segurança para usuários em qualquer local, em qualquer dispositivo, ao adaptar a política com base na atividade do usuário

- Permite visibilidade, políticas de segurança, relatórios e perícia com base em usuários e grupos, e não apenas em endereços IP.
- Integra-se facilmente com uma ampla variedade de repositórios para aproveitar as informações do usuário: controladores de LAN sem fio, VPNs, servidores de diretório, SIEMs, proxies e muito mais.
- Permite definir grupos dinâmicos de usuários (DUGs) no firewall para realizar ações de segurança com limite de tempo sem esperar que as alterações sejam aplicadas aos diretórios do usuário.
- Aplica políticas consistentes independentemente da localização dos usuários (escritório, casa, viagem etc.) e dos dispositivos (dispositivos móveis iOS e Android, macOS, Windows, desktops Linux, laptops; Citrix e Microsoft VDI e servidores de terminal).
- Impede que as credenciais corporativas vazem para sites de terceiros e evita a reutilização de credenciais roubadas ao habilitar a autenticação multifator (MFA) na camada de rede para qualquer aplicativo, sem nenhuma alteração no aplicativo.
- Fornece ações de segurança dinâmicas com base no comportamento do usuário para restringir usuários suspeitos ou mal-intencionados.
- Autentica e autoriza consistentemente seus usuários, independentemente da localização e onde se encontre alojada a identidade do usuário, a avançar rapidamente para uma postura de segurança Confiança Zero com o Cloud Identity Engine – uma arquitetura totalmente nova baseada na nuvem para segurança baseada em identidade.

Confira o resumo da solução Cloud Identity Engine para mais informações.

Impede atividades maliciosas ocultas em tráfego criptografado

- Inspeciona e aplica a política ao tráfego criptografado por TLS/SSL, tanto de entrada quanto de saída, incluindo o tráfego que usa TLS 1.3 e HTTP/2.
- Oferece ampla visibilidade do tráfego TLS, como quantidade de tráfego criptografado, versões TLS/SSL, pacotes de codificação e muito mais, sem decriptação.
- Permite o controle sobre o uso de protocolos TLS antigos, codificações inseguras e certificados configurados incorretamente para mitigar riscos.
- Facilita a implantação simples de decriptação e permite que você use logs integrados para solucionar problemas, como aplicativos com certificados fixos.
- Permite habilitar ou desabilitar a decriptação de maneira flexível com base na categoria de URL e zona de origem e destino, endereço, usuário, grupo de usuários, dispositivo e porta, para fins de privacidade e conformidade regulatória.
- Permite criar uma cópia do tráfego descriptografado do firewall (ou seja, espelhamento de decriptação) e enviá-lo para ferramentas de coleta de tráfego para fins de perícia, histórico ou prevenção de perda de dados (DLP).
- Permite que você encaminhe de forma inteligente todo o tráfego (TLS descriptografado, TLS não descriptografado e que não seja TLS) para ferramentas de segurança de terceiros com o Network Packet Broker e otimize o desempenho da rede e reduza as despesas operacionais.

Consulte este artigo técnico sobre decriptação para saber onde, quando e como descriptografar para evitar ameaças e proteger seu negócio.

Oferece gerenciamento centralizado e visibilidade

- Beneficia-se do gerenciamento centralizado, configuração e visibilidade para vários NGFWs da Palo Alto Networks distribuídos (independentemente da localização ou escala) por meio do gerenciamento de segurança de rede Panorama™, em uma interface de usuário unificada.
- Otimiza o compartilhamento de configuração por meio do Panorama com modelos e grupos de dispositivos e dimensiona a coleta de registros conforme as necessidades de registro aumentam.
- Permite que os usuários, por meio do Application Command Center (ACC – Centro de comando de aplicativos), obtenham visibilidade profunda e percepções abrangentes sobre o tráfego e as ameaças da rede.

Maximize seu investimento em segurança e evite interrupções nos negócios com o AIOps

- O AIOps para NGFW oferece recomendações contínuas de melhores práticas personalizadas para sua implantação exclusiva para fortalecer sua postura de segurança e aproveitar ao máximo seu investimento em segurança.
- Prevê de forma inteligente problemas de integridade, desempenho e capacidade do firewall com tecnologia de aprendizado de máquina alimentado por dados avançados de telemetria. Também fornece informações acionáveis para resolver as interrupções previstas.

Detecta e evita ameaças avançadas com serviços de segurança entregues na nuvem

Os sofisticados ataques cibernéticos de hoje podem gerar 45.000 variantes em 30 minutos, usando vários vetores de ameaças e técnicas avançadas para enviar cargas maliciosas. A segurança tradicional isolada causa desafios para as organizações, introduzindo brechas de segurança, aumentando a sobrecarga para as equipes de segurança e prejudicando a produtividade dos negócios com acesso e visibilidade inconsistentes.

Perfeitamente integrados com nossos NGFWs líderes do setor, nossos serviços de segurança entregues na nuvem usam o efeito de rede de 80.000 clientes para coordenar instantaneamente a inteligência e proteger contra todas as ameaças em todos os vetores. Elimine as lacunas de cobertura em seus locais e aproveite as vantagens da segurança de primeira classe fornecida de forma consistente em uma plataforma para ficar protegido até mesmo das ameaças mais avançadas e evasivas.

Os serviços incluem:

- **Threat Prevention avançado**: Impeça explorações conhecidas, malware, spyware e ameaças de comando e controle (C2), enquanto utiliza a prevenção de ataques de dia zero pioneira no setor – evite 60% mais ataques de injeção desconhecidos e 48% mais tráfego de comando e controle altamente evasivo do que as soluções IPS tradicionais.
- **WildFire avançado**: Certifique-se de que os arquivos estejam seguros, prevenindo automaticamente malware conhecido, desconhecido e altamente evasivo 60 vezes mais rápido com o maior mecanismo de inteligência contra ameaças e prevenção de malware do setor.
- **URL Filtering avançado**: Garanta o acesso seguro à Internet e evite 40% mais ataques baseados na web com a primeira prevenção em tempo real do setor contra ameaças conhecidas e desconhecidas, interrompendo 88% das URLs maliciosas pelo menos 48 horas antes de outros fornecedores.
- **DNS Security**: Obtenha 40% mais cobertura contra ameaças e interrompa 85% dos malwares que abusam do DNS para comando e controle e roubo de dados sem exigir alterações em sua infraestrutura.

- **DLP empresarial**: Minimize o risco de uma violação de dados, interrompa transferências de dados fora da política e permita a conformidade de forma consistente em toda a sua empresa, com uma cobertura 2 vezes maior de qualquer DLP empresarial entregue na nuvem.
- **Segurança de SaaS**: Fique à frente do aumento exponencial do SaaS com o único CASB de última geração do setor para ver e proteger automaticamente todos os aplicativos em todos os protocolos.
- **IoT Security**: Proteja cada "coisa" e implemente segurança de dispositivo de Confiança Zero 20 vezes mais rapidamente com a segurança mais inteligente do setor para dispositivos inteligentes.

Oferece uma abordagem única para processamento de pacotes com arquitetura de passagem única

- Executa serviços de rede, pesquisa de política, aplicativo e decodificação e correspondência de assinatura – para todas as ameaças e conteúdo – em uma única passagem. Isto reduz significativamente o volume da sobrecarga de processamentos necessários para executar várias funções em um único dispositivo de segurança.
- Evita a introdução de latência com a varredura do tráfego para todas as assinaturas em uma única passagem usando correspondência de assinatura uniforme e baseada em fluxo.
- Permite um desempenho consistente e previsível quando as assinaturas de segurança estão habilitadas. (Na Tabela 1, a "taxa de transferência do Threat Prevention" é medida com várias assinaturas habilitadas).

Viabiliza a funcionalidade SD-WAN

- Permite que você adote a SD-WAN com facilidade, simplesmente viabilizando-a em seus firewalls existentes.
- Possibilita que você implemente com segurança a SD-WAN, que é nativamente integrada na nossa segurança líder no setor.
- Oferece uma experiência excepcional ao usuário final, minimizando a latência, instabilidade e perda de pacotes.

Tabela 1: Desempenho e capacidades do PA-5400 Series

	PA-5410	PA-5420	PA-5430	PA-5440
Taxa de transferência de firewall (HTTP/appmix)*	52,4/43,5 Gbps	68,0/56,0 Gbps	79,0/61,0 Gbps	93,5/72,0 Gbps
Taxa de transferência do Threat Prevention (HTTP/appmix)†	26,0/26,7 Gbps	33,0/32,0 Gbps	43,0/40,0 Gbps	61,5/52,0 Gbps
Taxa de transferência da VPN IPsec†	21 Gbps	28,7 Gbps	42 Gbps	58 Gbps
Máximo de sessões	3.6M	5M	7.2M	12M
Novas sessões por segundo§	270000	370000	380000	390000
Sistemas virtuais (base/máx)‖	10/20	15/65	25/125	25/225

Observação: os resultados foram medidos no PAN-OS 11.0.

* A taxa de transferência do firewall é medida com App-ID e logs ativados, usando transações HTTP/appmix de 64 KB.

† A taxa de transferência do Threat Prevention é medida com App-ID, IPS, antivírus, anti-spyware, WildFire, segurança DNS, bloqueio de arquivos e logs ativados, usando transações HTTP/appmix de 64 KB.

‡ A taxa de transferência da VPN IPSec é medida com transações HTTP de 64 KB e logs ativados.

§ Novas sessões por segundo são medidas com a substituição de aplicativo usando transações HTTP de 1 byte.

‖ Incluir sistemas virtuais na quantidade base requer uma licença comprada separadamente.

Tabela 2: Recursos de rede do PA-5400 Series

Modos de interface
L2, L3, tap, fio virtual (modo transparente)
Roteamento
OSPFv2/v3 com reinício normal, BGP com reinício normal, RIP, roteamento estático
Encaminhamento baseado em políticas
Protocolo ponto a ponto por Ethernet (PPPoE) e DHCP com suporte para a atribuição de endereços dinâmicos
Multicast: PIM-SM, PIM-SSM, IGMP v1, v2 e v3
Detecção de encaminhamento bidirecional (BFD)

Tabela 2: Recursos de rede do PA-5400 Series (continuação)
SD-WAN
Medição da qualidade do caminho (instabilidade, perda de pacotes, latência)
Seleção de caminho inicial (PBF)
Troca de chaves: chave manual, IKEv1 e IKEv2 (chave pré-compartilhada, autenticação baseada em certificado)
IPv6
L2, L3, tap, fio virtual (modo transparente)
Recursos: App-ID, User-ID, Content-ID, WildFire e decriptação SSL
SLAAC
IPsec VPN
Troca de chaves: chave manual, IKEv1 e IKEv2 (chave pré-compartilhada, autenticação baseada em certificado)
Criptografia: 3DES, AES (128 bits, 192 bits, 256 bits)
Autenticação: MD5, SHA-1, SHA-256, SHA-384, SHA-512
VLANs
Etiquetas VLAN 802.1Q por dispositivo/por interface: 4.094/4.094
Interfaces agregadas (802.3ad), LACP
Network address translation (tradução de endereço de rede - NAT)
Modos de NAT (IPv4): IP estático, IP dinâmico, IP dinâmico e porta (conversão de endereço de porta)
NAT64, NPTv6
Recursos NAT adicionais: reserva de IP dinâmico, IP dinâmico ajustável e reutilização de porta
Alta disponibilidade
Modos: ativo/ativo, ativo/passivo, sistema de alta disponibilidade (HA)
Detecção de falhas: monitoramento de caminho, monitoramento de interface
Infraestrutura de redes móveis*
Segurança 5G
Segurança 5G MEC (computação de borda de acesso múltiplo - multiaccess edge computing)
Segurança de GTP
Segurança de SCTP

* Para obter informações adicionais, consulte nossa folha de dados NGFWs alimentados por aprendizado de máquina para 5G.

Tabela 3: Especificações de hardware do PA-5400 Series
I/O
1G/2.5G/5G/10G (8), 1G/10G SFP/SFP+ (12), 1G/10G/25G SFP/SFP+/SFP28 (4), 40G/100G QSFP+/QSFP28 (4)
E/S de gerenciamento
Porta de gerenciamento fora de banda 1G SFP (1), 1G SFP alta disponibilidade (2), 40G QSFP+ alta disponibilidade (1), Porta do console RJ-45 (1), Micro USB
Capacidade de armazenamento
Par SSD 480 GB, armazenamento do sistema
Fonte de alimentação (consumo de energia médio/máximo)
630/760 W

Tabela 3: Especificações de hardware do PA-5400 Series (continuação)
BTU/h máximo
1638
Fontes de alimentação (base/máximo)
1:1 Totalmente redundante (2/2)
Tensão de entrada CA (Hz de entrada)
100-240 VCA (50-60 Hz)
Saída da fonte de alimentação CA
1.200 watts/fonte de alimentação
Consumo máximo de energia
CA: 7 A a 100 VCA, 3 A a 240 VCA
CC: 15 A a -48 VCC, 12 A a -60 VCC
Corrente de ligação máxima
CA: 50 A a 230 VCA, 50 A a 120 VCA
CC: 200 A a 72 VCC
Tempo médio entre falhas (MTBF)
22 anos
Montável em rack (dimensões)
Rack padrão 2U, 19" (3,45" A x 22,5" P x 17,34" L)
Peso (dispositivo autônomo/conforme entregue)
35,2 lbs/48,8 lbs
Segurança
cTUVus, CB
EMI
Classe A de FCC, Classe A de CE, Classe A de VCCI
Certificações
Consulte paloaltonetworks.com/company/certifications.html
Ambiente
Temperatura operacional: 32°F a 122°F, 0°C a 50°C
Temperatura não operacional: -4°F a 158°F, -20°C a 70°C
Tolerância de umidade: 10% a 90%
Altitude máxima: 10.000 pés/3.048 m
Fluxo de ar: da frente para trás

3000 Tannery Way
Santa Clara, CA 95054

Principal: +1.408.753.4000
Vendas: +1.866.320.4788
Suporte: +1.866.898.9087

www.paloaltonetworks.com