PA-450R

PA-450R

O PA-450R da Palo Alto Networks é um robusto firewall de última geração (NGFW) alimentado por aprendizado de máquina que apresenta recursos de última geração para aplicativos industriais em ambientes adversos.

O dispositivo robusto PA-450R protege redes industriais e de defesa em uma série de ambientes adversos, como subestações, centrais elétricas, fábricas, instalações de petróleo e gás, sistemas de gerenciamento de edifícios e redes do setor de assistência médica.

Destaques

- 1º NGFW alimentado por aprendizado de máquina do mundo
- 11 vezes líder no Magic Quadrant da Gartner para firewalls de rede
- Líder no The Forrester Wave: Firewalls empresariais, quarto trimestre de 2022
- Intervalo ampliado de temperatura operacional
- Certificado de acordo com os padrões ambientais e de teste IEC 61850-3 e IEEE 1613 para vibração, temperatura, imunidade a interferências eletromagnéticas
- Suporta alta disponibilidade com os modos ativo/ativo e ativo/passivo
- Oferece desempenho previsível com serviços de segurança
- Tem um design silencioso, sem ventoinhas e sem peças móveis
- Simplifica a implantação de um grande número de firewalls com Zero Touch Provisioning (Provisionamento sem intervenção humana – ZTP) opcional
- Suporta administração centralizada com gerenciamento centralizado Panorama e Strata Cloud Manager
- Maximiza os investimentos em segurança e evita interrupções nos negócios com o Strata™ Cloud Manager

O elemento de controle do PA-450R 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; 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.

Oferece gerenciamento e operações unificados alimentados por IA com o Strata Cloud Manager

- **Evite interrupções de rede**: Preveja a integridade da implantação e identifique proativamente os gargalos de capacidade com até sete dias de antecedência com análises preditivas para evitar proativamente interrupções operacionais.
- **Fortaleça a segurança em tempo real**: Análise de políticas e verificações de conformidade em tempo real com base em IA em relação às práticas recomendadas do setor e da Palo Alto Networks.
- **Permita o gerenciamento e as operações de segurança de rede simples e consistentes**: Gerencie a configuração e as políticas de segurança em todos os fatores de forma, incluindo SASE, firewalls de hardware e software e todos os serviços de segurança para garantir a consistência e reduzir a sobrecarga operacional.

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

A abordagem tradicional de usar ferramentas de segurança isoladas desafia as organizações, incluindo lacunas de segurança, aumento da sobrecarga para as equipes de segurança e interrupções na produtividade dos negócios. Perfeitamente integrados aos nossos NGFWs líderes do setor, nossos serviços de segurança entregues na nuvem compartilham inteligência contra ameaças para 65.000 clientes evitando ameaças conhecidas e desconhecidas em todos os vetores de ameaças em tempo real. Elimine as lacunas de segurança em toda a sua rede e aproveite os serviços de segurança em linha alimentados por IA que fornecem proteção em tempo real em qualquer lugar.

Os serviços incluem:

- **Threat Prevention avançado**: Impeça explorações conhecidas e desconhecidas e ataques de comando e controle (C2) com detecções em linha alimentadas por IA, bloqueando 60% mais ataques de injeção de dia zero e 48% mais tráfego de comando e controle altamente evasivo do que as soluções IPS tradicionais.
- **WildFire® avançado**: Garanta que os arquivos estejam seguros prevenindo automaticamente malware conhecido, desconhecido e altamente evasivo 180 vezes mais rápido do que os concorrentes 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% dos sites maliciosos pelo menos 48 horas antes de outros fornecedores.
- **Segurança de DNS**: Obtenha 68% 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.

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 recursos do PA-450R	
	PA-450R
Taxa de transferência de firewall (appmix)*	3,2 Gbps
Taxa de transferência do Threat Prevention (appmix)†	1,4 Gbps
Taxa de transferência da VPN IPsec‡	2,2 Gbps
Máximo de sessões	200000
Novas sessões por segundo§	10000
Sistemas virtuais (base/máx)‖	1/2

Observação: os resultados foram medidos no PAN-OS 11.1.

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

† 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 appmix.

‡ 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 11.1.

Tabela 2: Recursos de rede do PA-450R
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
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-450R
E/S
10/100/1000 (6), Combo [SFP ou Cobre 10/100/1000] (2)
E/S de gerenciamento
(1) Porta de gerenciamento fora de banda 10/100/1000
(1) Porta de console RJ45
(1) Porta USB
Capacidade de armazenamento
128 GB
Fonte de alimentação (consumo de energia médio/máximo)
N/A
BTU/h máximo
136
Tensão de entrada (frequência de entrada)
12 V–48 VCC
Consumo máximo de energia
6 A a 12 VCC
Corrente de ligação máxima
A definir
Dimensões
44,4 mm A x 390 mm L x 238 mm P - 1RU
Peso (dispositivo autônomo/conforme entregue)
454 gramas (estimado)/a definir
Segurança
UL 62368-1:2014, CSA C22.2 n.º 62368-1:14, IEC/EN 62368-1: 2014, IEC 62368-1: 2018
EMI
A definir
Ambiente
Temperatura operacional: -40 °C a +70 °C
Temperatura não operacional: -40 °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

strata_ds_pa-450r_020624