Visão geral do firewall de próxima geração da Palo Alto Networks

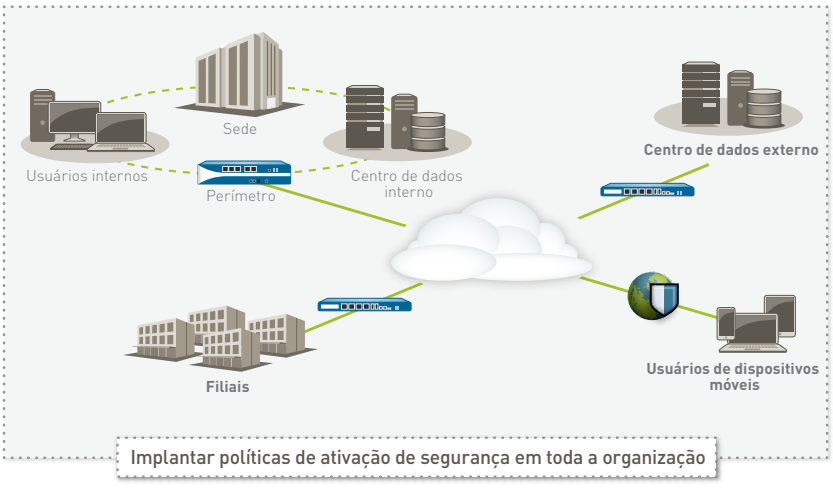
Mudanças fundamentais no panorama dos aplicativos e ameaças, assim como comportamento do usuário e infraestrutura de rede têm corroído a segurança que os firewalls tradicionais baseados em porta forneciam. Seus usuários estão acessando todos os tipos de aplicativos usando uma variedade de tipos de dispositivos, muitas vezes para fazer seu trabalho. Enquanto isso, a expansão do datacenter, virtualização, mobilidade e iniciativas baseadas em nuvem estão forçando a repensar como permitir o acesso a aplicativos, protegendo sua rede.

Respostas tradicionais incluem a tentativa de bloquear todo o tráfego de aplicativos através de uma lista cada vez maior de tecnologias de ponta, além do firewall, o que pode prejudicar seus negócios; ou permitir todos os aplicativos, o que é igualmente inaceitável, devido aos riscos crescentes aos negócios e de segurança. O desafio enfrentado é que o firewall tradicional baseado em porta, mesmo com bloqueio de aplicativos incluído, não fornece alternativa a ambas as abordagens. Para obter um equilíbrio entre permitir tudo e negar tudo, você precisa permitir aplicativos com segurança usando elementos relevantes aos negócios, como a identidade do aplicativo, quem está usando o aplicativo e o tipo de conteúdo, como critérios de política de segurança do firewall.

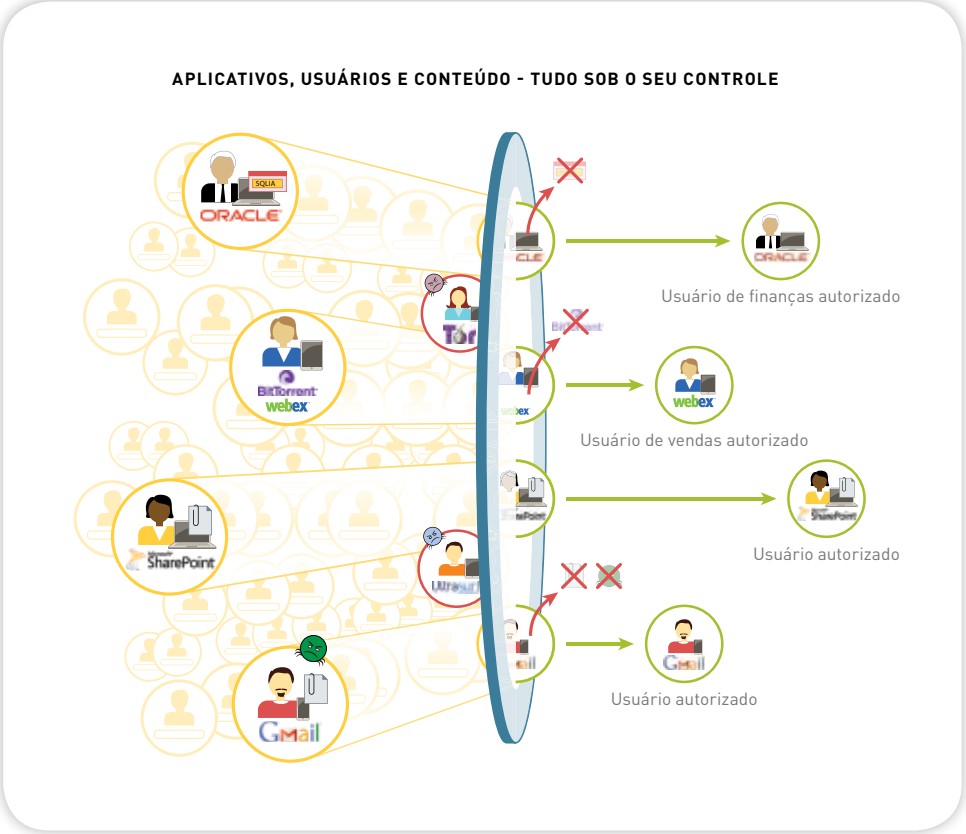
Requisitos importantes para uma permissão segura:

- **Identificar aplicativos, não portas.** Classificar o tráfego, assim que ele atinge o firewall, para determinar a identidade do aplicativo, independentemente de protocolo, criptografia ou tática de evasão. Depois usar essa identidade como base de todas as políticas de segurança.
- **Correlacionar o uso do aplicativo à identidade do usuário, não ao endereço IP, independentemente do local ou dispositivo.** Empregar informações de usuário e grupo dos diretórios da empresa e outros armazenamentos de usuários para implantar políticas de permissão consistentes para todos os seus usuários, independentemente do local ou dispositivo.
- **Proteger contra todas as ameaças - conhecidas e desconhecidas.** Evitar explorações de vulnerabilidades conhecidas, malware, spyware, URLs mal intencionados, analisando o tráfego e fornecendo proteção automaticamente contra malwares altamente direcionados e previamente desconhecidos.
- **Simplificar a política de gerenciamento.** Permitir aplicativos com segurança e reduzir esforços administrativos com ferramentas gráficas fáceis de usar, um editor de políticas unificado, templates e grupos de dispositivos.

As políticas de permissão segura de aplicativos podem ajudar a melhorar sua postura de segurança, independentemente dos locais de implantação. No perímetro, você pode reduzir sua exposição a ameaças bloqueando uma grande variedade de aplicativos indesejados e depois inspecionando se há ameaças nos aplicativos permitidos - tanto conhecidas como desconhecidas. No datacenter - tradicional ou virtualizado, a permissão de aplicativos se traduz em garantir que apenas os aplicativos de datacenter estejam sendo usados por usuários autorizados, protegendo



paloalto NETWORKS
the network security company™



o conteúdo de ameaças e lidando com desafios de segurança introduzidos pela natureza dinâmica da infraestrutura virtual. As filiais da sua empresa e usuários remotos podem ser protegidos pelo mesmo conjunto de políticas de permissão implantado na sede, garantindo assim a consistência das políticas.

Permitindo aplicativos para capacitar os negócios

A permissão segura de aplicativos com os firewalls de próxima geração da Palo Alto Networks ajuda a lidar com os riscos de negócios e de segurança associados com o rápido crescimento de aplicativos que passam pela sua rede. Ao permitir aplicativos para usuários ou grupos de usuários, tanto locais, móveis e remotos, e ao proteger o tráfego contra ameaças conhecidas e desconhecidas, é possível, ao mesmo tempo, melhorar sua postura de segurança e aumentar seus negócios.

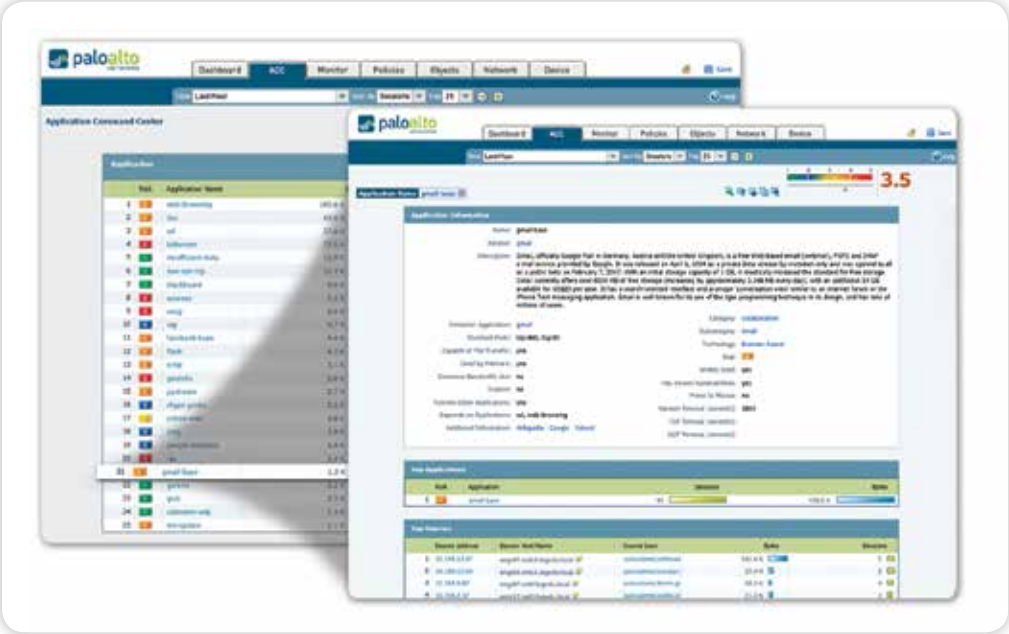
- **Classificando todos os aplicativos, em todas as portas, o tempo todo.** A classificação de tráfego precisa é a parte mais importante de qualquer firewall, com o resultado sendo a base das políticas de segurança. Hoje, os aplicativos podem facilmente contornar um firewall baseado em porta; pulando portas, usando SSL e SSH, entrando sorrateiramente pela porta 80, ou usando portas não padrão. O App-ID tem como alvo as limitações de visibilidade da classificação de tráfego que afligem os firewalls tradicionais, aplicando vários mecanismos de classificação no fluxo de tráfego, tão logo o firewall o veja, para determinar a identidade exata do aplicativo que passa pela sua rede, independentemente da criptografia de porta (SSL ou SSH) ou técnica de evasão empregada. O conhecimento exato de quais aplicativos estão passando pela rede, não só a porta e protocolo, torna-se a base de todas suas decisões de política de segurança. Aplicativos não identificados, geralmente uma porcentagem pequena de tráfego, mesmo sendo um risco potencial elevado, são categorizados automaticamente para gerenciamento sistemático - que pode incluir controle e inspeção de política, análise de ameaças, criação de um App-ID personalizado, ou captura de pacotes para desenvolvimento de App-ID da Palo Alto Networks.

- **Integrando usuários e dispositivos, não apenas endereços IP em políticas.** Criar e gerenciar políticas de segurança baseadas no aplicativo e a identidade do usuário, independentemente do dispositivo ou local, é um meio mais eficiente de proteger sua rede que confiar exclusivamente na porta e endereço IP. A integração com uma ampla variedade de repositórios de usuários da empresa fornece a identidade do usuário do Microsoft Windows, Mac OS X, Linux, Android ou iOS que acessa o aplicativo. Os usuários que estão viajando ou trabalhando remotamente são protegidos perfeitamente com as mesmas políticas consistentes que são usadas na rede local ou corporativa. A combinação de visibilidade e controle no aplicativo de um usuário significa que é possível permitir com segurança o uso do Oracle, BitTorrent ou Gmail, ou qualquer outro aplicativo que passa por sua rede, sem importar onde ou como o usuário o está acessando.

- **Evitar todas as ameaças - conhecidas e desconhecidas.** Para proteger a rede moderna de hoje, é necessário lidar com uma mistura de explorações, malware e spyware conhecidos, assim como ameaças completamente desconhecidas e direcionadas. Esse processo se inicia com a redução da superfície de ataque da rede, permitindo aplicativos específicos e negando outros, implicitamente através de uma estratégia "negar todos, exceto" ou através de políticas explícitas. A prevenção de ameaças coordenadas pode ser então aplicada a todo o tráfego permitido, bloqueando sites de malware conhecidos, explorações de vulnerabilidade, vírus, spyware e consultas de DNS mal intencionadas em uma única passagem. Malwares personalizados ou desconhecidos são ativamente analisados e identificados através da execução de arquivos desconhecidos e observação direta de mais de 100 comportamentos mal intencionados em um ambiente de testes virtualizado. Quando um novo malware é descoberto, uma assinatura do arquivo infectado e tráfego de malware relacionado é automaticamente gerado e fornecido a você. Toda análise de prevenção de ameaças usa contexto completo de aplicativo e protocolo, garantindo que as ameaças sejam sempre encontradas, mesmo se elas tentarem se ocultar da segurança em túneis, conteúdo comprimido ou em portas não padrão.

Flexibilidade de implantação e gerenciamento

O recurso de permissão segura de aplicativo está disponível em uma plataforma de hardware construída especialmente para isso ou em formato virtualizado. Ao implantar vários firewalls da Palo Alto Networks, em formato de hardware ou virtual, você pode usar o Panorama, uma oferta opcional de gerenciamento centralizado para obter visibilidade em padrões de tráfego, implantar políticas, gerar relatórios e fornecer atualizações de conteúdo a partir de uma central.



Visibilidade do aplicativo: Exiba a atividade em um formato claro e fácil de ler. Adicione e remova filtros para saber mais sobre o aplicativo, suas funções e quem está usando.

Permissão segura de aplicativos: uma abordagem abrangente

O aplicativo seguro exige uma abordagem abrangente para proteger sua rede e aumentar seus negócios, que começa com um conhecimento profundo dos aplicativos na sua rede; quem é o usuário, independentemente da plataforma ou local; qual é o conteúdo que o aplicativo está carregando, se houver. Com um conhecimento mais completo da atividade de rede, você pode criar políticas de segurança mais significativas baseadas em elementos do aplicativo, usuário e conteúdo relevantes aos seus negócios. O local do usuário, sua plataforma e onde a política é implantada - perímetro, datacenter tradicional ou virtualizado, filiais ou usuário remoto - faz pouca, ou nenhuma diferença, em como a política é criada. Você pode agora permitir com segurança qualquer aplicativo, qualquer usuário e qualquer conteúdo.

Conhecimento completo significa políticas de segurança mais rigorosas

As práticas recomendadas de segurança ditam que o conhecimento mais completo do que está na sua rede é benéfico para implantar políticas de segurança mais rigorosas. Por exemplo, saber exatamente quais aplicativos estão passando pela sua rede, ao contrário do conjunto mais amplo de tráfego que é baseado em porta, permite que seus administradores permitam especificamente os aplicativos que permitem seus negócios, bloqueando os indesejáveis. Saber quem é o usuário, não apenas seu endereço IP, acrescenta outros critérios de política que permitem que você seja mais específico na sua atribuição de políticas. Usando um conjunto de ferramentas de visualização gráfica, seus administradores podem obter um quadro mais completo das atividades dos aplicativos, o impacto potencial na segurança e tomar decisões de política mais informadas. Os aplicativos são classificados continuamente e, à medida que seu estado muda, os resumos gráficos são atualizados dinamicamente, exibindo as informações em uma interface fácil de usar baseada na web.

- Aplicativos novos e conhecidos podem ser rapidamente investigados com um único clique, que exibe uma descrição do aplicativo, suas características comportamentais, e quem está usando.
- A visibilidade adicional em categorias de URL, ameaças e padrões de dados fornece um quadro completo e bem preciso da atividade de rede.
- Aplicativos desconhecidos, geralmente uma porcentagem pequena em todas as redes, mas com risco potencial alto, são categorizados para uma análise para determinar se eles são aplicativos internos, aplicativos comerciais ainda não identificados, ou ameaças.

- Com muita frequência, seus usuários estão acessando qualquer aplicativo que desejam, frequentemente para fazer seu trabalho - tornando, desta forma, o aplicativo, usuário e o conteúdo relacionado mais relevantes aos seus negócios do que nunca. Com um quadro mais completo do que está na rede, seus administradores podem traduzir essas informações em políticas de permissão de aplicativos, para reduzir o risco.

Permitindo aplicativos e reduzindo riscos

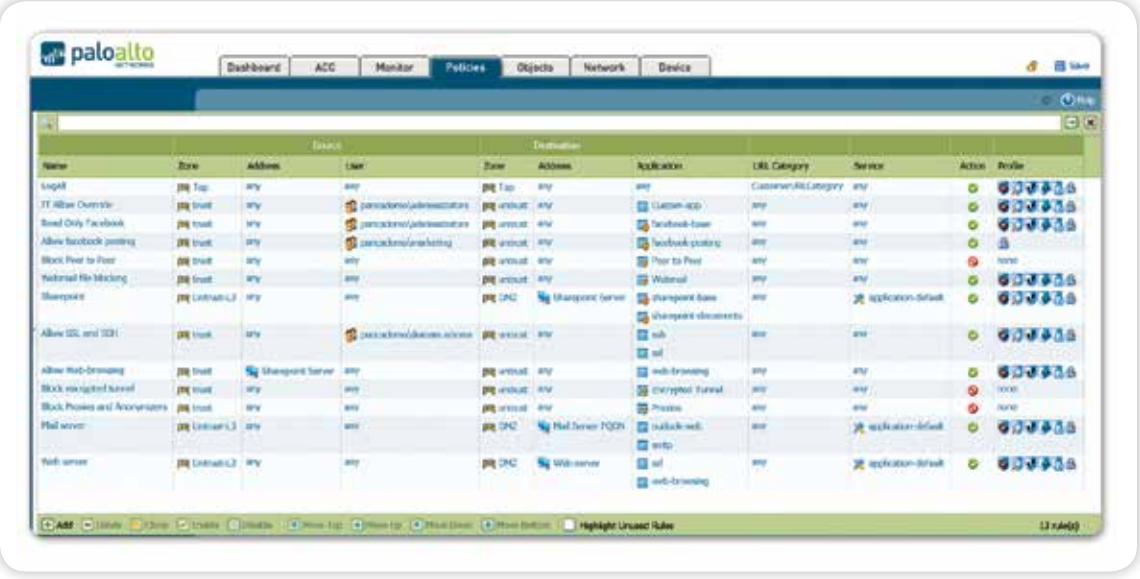
A permissão segura de aplicativos usa critérios de decisão de política que incluem aplicativos/função de aplicativos, usuários e grupos, e conteúdo, como meios de obter um equilíbrio entre a negação de aplicativos que limita os negócios, e a alternativa de alto risco de permitir todos os aplicativos.

No perímetro, incluindo usuários em filiais, móveis e remotos, as políticas de permissão são focadas em identificar todo o tráfego, e depois permitir seletivamente o tráfego baseado na identidade do usuário; depois verificar se há ameaças no tráfego. Exemplos de políticas:

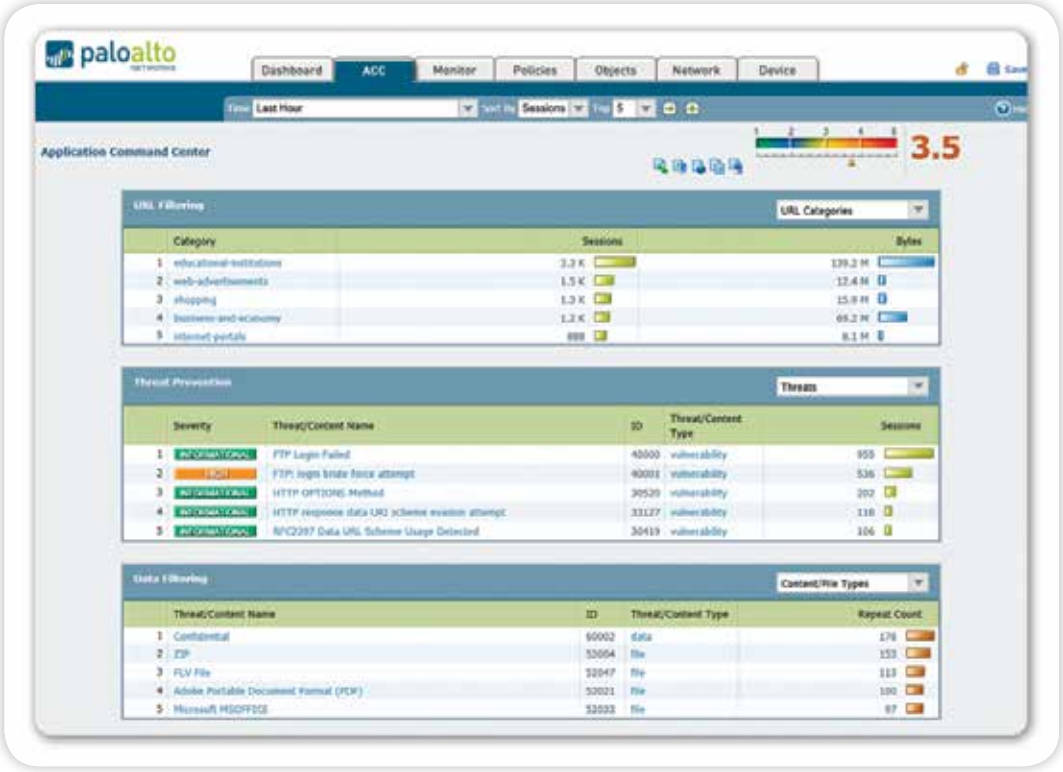
- Limitar o uso de webmail e mensagens instantâneas a umas poucas variantes; descriptografar aquelas que usam SSL, inspecionar se há explorações no tráfego e fazer o upload de arquivos desconhecidos no WildFire para análise e desenvolvimento de assinatura.
- Permitir aplicativos e websites de mídia, mas aplicar prevenção de QoS e malware para limitar o impacto de aplicativos VoIP e proteger sua rede.
- Controlar o Facebook permitindo que todos os usuários "naveguem", bloqueando jogos e plug-ins sociais do Facebook; e permitindo publicações no Facebook somente para marketing. Verificar se há malware e explorações em todo tráfego do Facebook.
- Controlar a navegação na web, permitindo e verificando tráfego para websites relacionados aos negócios, bloqueando o acesso a web sites obviamente não relacionados ao trabalho; acesso de "instrutor" a sites questionáveis através de páginas de bloqueio personalizadas.
- Aplicar segurança consistente implantando transparentemente as mesmas políticas a todos os usuários: locais, móveis ou remotos, com o GlobalProtect.
- Usar uma estratégia implícita de "negar tudo, exceto" ou bloquear explicitamente aplicativos indesejados como P2P e "bypasses" ou tráfego de países específicos para reduzir o tráfego de aplicativos que introduz risco de negócios e de segurança.

No datacenter (tradicional, virtualizado ou uma combinação deles), exemplos de permissão são focados em confirmar aplicativos, procurar por aplicativos desonestos, e proteger os dados.

- Isolar o repositório de números de cartão de crédito baseado em Oracle em sua própria zona de segurança; controlar o acesso a grupos de finanças, forçando o tráfego nas portas padrão, e inspecionar vulnerabilidades de aplicativos no tráfego.



Editor de política unificado: Uma aparência familiar permite a criação e implantação rápida de políticas que controlam aplicativos, usuários e conteúdo.



Visibilidade de conteúdo e ameaças: Exiba URLs, ameaças e atividade de transferência de arquivos/dados em um formato claro e fácil de ler. Adicione e remova filtros para saber mais sobre elementos individuais.

- Permitir que apenas o grupo de TI acesse o datacenter usando um conjunto fixo de aplicativos de gerenciamento remoto (p.ex., SSH, RDP, Telnet) em suas portas padrão.
- Permitir que o Microsoft SharePoint Administration seja usado apenas por sua equipe administrativa, e permitir o acesso a documentos do Microsoft SharePoint para todos os outros usuários.

Protegendo aplicativos permitidos

Permissão segura de aplicativos significa permitir acesso a certos aplicativos, e depois aplicar políticas específicas para bloquear explorações conhecidas, malware e spyware - conhecidos ou desconhecidos; controlar transferência de arquivos ou dados, e atividade de navegação na web. Táticas comuns de evasão de ameaças, como alteração de portas e tunelamento, são tratadas executando políticas de prevenção contra ameaças usando o aplicativo e contexto de protocolo gerados pelos decodificadores no App-ID. Em contraste, as soluções UTM têm uma abordagem baseada em silos para prevenção de ameaças, com cada função: firewall, IPS, AV, filtragem de URL, verificando tráfego sem compartilhar nenhum contexto, tornando-as mais suscetíveis ao comportamento evasivo.

- **Bloquear ameaças conhecidas: IPS e antivírus/anti-spyware de rede.** Um formato de assinatura uniforme e um mecanismo de verificação baseado em fluxo permite proteger sua rede de uma ampla variedade de ameaças. Os recursos do Sistema de prevenção contra invasões (IPS) bloqueiam explorações de vulnerabilidades de rede e aplicativos, buffer overflow, ataques DoS e varreduras de porta. A proteção antivírus/anti-spyware bloqueia milhões de variantes de malware, assim como qualquer tráfego de comando e controle gerado por malware, vírus em PDF e malwares ocultos em arquivos comprimidos ou tráfego web (HTTP/HTTPS comprimidos). A descriptografia SSL baseada em políticas em todos os aplicativos e portas protege contra malware que se movem através de aplicativos criptografados em SSL.

- **Bloquear malware desconhecido e direcionado: Wildfire™.** Malwares desconhecidos e direcionados são identificados e analisados pelo WildFire, que executa diretamente e observa arquivos desconhecidos em um ambiente de testes virtualizado, baseado na nuvem. O WildFire monitora mais de 100 comportamentos mal intencionados e o resultado é fornecido imediatamente ao administrador na forma de um alerta. Uma assinatura opcional do WildFire oferece melhor proteção, registros e relatórios. Como assinante, você está protegido em até uma hora, quando um novo malware é encontrado em qualquer parte do mundo, interrompendo com sucesso a disseminação de novos malwares antes que eles afetem você. Como assinante, você também obtém acesso a criação de logs e relatórios integrados no WildFire e uma API para enviar amostras à nuvem do WildFire para análises.
- **Identificar servidores infectados por bots.** O App-ID classifica todos os aplicativos, em todas as portas, incluindo qualquer tráfego desconhecido, que pode expor frequentemente anomalias e ameaças em sua rede. O relatório comportamental de botnet correlaciona tráfego desconhecido, consultas suspeitas de DNS e URL e uma variedade de comportamentos incomuns de rede para revelar dispositivos com probabilidade de estarem infectados com malware. Os resultados são exibidos em uma lista de servidores potencialmente infectados, que podem ser investigados como possíveis membros de uma botnet.
- **Limitar transferência não autorizada de arquivos e dados.** Os recursos de filtragem de dados permitem que seus administradores implantem políticas que reduzirão os riscos associados a transferências não autorizadas de arquivos e dados. As transferências de arquivos podem ser controladas dentro do arquivo (em oposição a examinar apenas a extensão do arquivo), para determinar se a ação de transferência deve ser permitida ou não. Arquivos executáveis, geralmente encontrados em downloads não intencionais, podem ser bloqueados, protegendo assim sua rede contra propagação despercebida de malware. Os recursos de filtragem de dados podem detectar e controlar o fluxo de padrões de dados confidenciais (cartões de crédito ou números da previdência social, assim como padrões personalizados).
- **Controlar a navegação na Web.** Um mecanismo de filtragem de URL personalizado e totalmente integrado permite que seus administradores apliquem políticas granulares de navegação na web, complementando as políticas de visibilidade e controle de aplicativos e protegendo a empresa contra um amplo espectro de riscos legais, regulatórios e de produtividade. Além disso, as categorias de URL podem ser aproveitadas nas políticas para fornecer mais granularidade de controle para criptografia SSL, QoS ou outras bases de regras.

Gerenciamento e análise contínuos

As práticas recomendadas de segurança ditam que seus administradores obtenham um equilíbrio entre gerenciar proativamente o firewall, seja um ou centenas de dispositivos, e ser reativo, investigando, analisando e relatando incidentes de segurança.

- **Gerenciamento:** Cada plataforma da Palo Alto Networks pode ser gerenciada individualmente através de uma interface de linha de comando (CLI) ou interface baseada em navegador cheia de recursos. Em implantações em grande escala, o Panorama pode ser licenciado e implantado como uma solução de gerenciamento centralizado que permite equilibrar o controle global e centralizado com a necessidade de flexibilidade de política local, usando recursos como templates e políticas compartilhadas. Suporte adicional para ferramentas baseadas em padrões como um SMP, e APIs baseados em REST, permite a integração com ferramentas de gerenciamento de terceiros. Seja usando a interface web do dispositivo ou do Panorama, a aparência da interface é idêntica, garantindo que não há curva de aprendizado ao mover de uma para outra. Seus administradores podem usar qualquer uma das interfaces fornecidas para fazer alterações a qualquer momento, sem necessidade de se preocupar com questões de sincronização. A administração baseada em funções é suportada por todas as mídias de gerenciamento, permitindo atribuir recursos e funções a indivíduos específicos.
- **Relatórios:** Relatórios predefinidos podem ser usados "como estão", personalizados ou agrupados como um relatório para atender a necessidades específicas. Todos os relatórios podem ser exportados para formato CSV ou PDF, e podem ser executados e enviados por e-mail em um intervalo programado.
- **Criação de logs:** A filtragem de logs em tempo real facilita uma análise investigativa em cada sessão que passa por sua rede. Os resultados da filtragem de log podem ser exportados em arquivos CSV ou enviados a um servidor syslog para arquivo offline ou mais análises.

Hardware especialmente construído ou plataformas virtualizadas

A Palo Alto Networks oferece uma linha completa de plataformas em hardware especialmente construídas que vão desde o PA-200, projetado para escritórios remotos empresariais até o PA-5060, que é projetado para datacenters de alta velocidade. A arquitetura da plataforma é baseada em um mecanismo de software de passagem única e usa processamento de funções específicas para rede, segurança, prevenção de ameaças e gerenciamento para fornecer um desempenho previsível. A mesma funcionalidade de firewall que é fornecida nas plataformas em hardware está disponível também no firewall virtual VM-Series, permitindo proteger seus ambientes de computação virtualizado e baseado em rede, usando as mesmas políticas aplicadas ao seu firewall de perímetro ou de escritórios remotos.

paloalto NETWORKS
the network security company™

3300 Olcott Street
Santa Clara, CA 95054

Main: +1.408.573.4000
Sales: +1.866.320.4788
Support: +1.866.898.9087

www.paloaltonetworks.com