VISÃO GERAL DO FIREWALL

Firewalls de última geração da Palo Alto Networks

Mudanças fundamentais no uso do aplicativo, comportamento do usuário e na infraestrutura complexa e complicada criam um cenário de ameaças que expõem os pontos fracos da segurança da rede tradicional baseada em porta. Seus usuários querem ter acesso a um número cada vez maior de aplicativos, usam vários dispositivos e, frequentemente, não prestam muita atenção aos riscos para a segurança e a empresa. Enquanto isso, a expansão do centro de dados, a segmentação de rede, a virtualização e as iniciativas de mobilidade forçam você a repensar como dar acesso a aplicativos e dados, enquanto protege sua de uma nova categoria de ameaças novas, mais sofisticadas e avançadas que iludem os mecanismos de segurança tradicionais.

Historicamente, você tem duas opções básicas: bloquear tudo em prol da segurança de rede ou ativar tudo em prol de sua empresa. Estas escolhas deixaram pouco espaço para concessões. A plataforma de segurança de última geração da Palo Alto Networks® oferece uma maneira para ativar com segurança os aplicativos que os seus usuários precisam ao dar acesso e, ao mesmo tempo, evitar ameaças à segurança cibernética.

Nosso firewall de última geração é o coração da plataforma de segurança de última geração, desenvolvida desde o início para enfrentar as ameaças mais sofisticadas. O firewall de última geração inspeciona todo o tráfego – inclusive de aplicativos, ameaças e conteúdo – e o vincula ao usuário, independentemente da localização ou do tipo de dispositivo. O aplicativo, o conteúdo e o usuário – os elementos que fazem sua empresa funcionar – tornam-se componentes integrantes da política de segurança da sua empresa. O resultado é a capacidade de alinhar a segurança às suas principais iniciativas empresariais. Com nossa plataforma de segurança de última geração você reduz os tempos de resposta a incidentes, descobre ameaças desconhecidas e agiliza a implantação da rede de segurança.

Figura 1: Plataforma de segurança de última geração da Palo Alto Networks

- Ative com segurança aplicativos, usuários e conteúdo, ao classificar todo o tráfego, definir o caso de uso da empresa e atribuir políticas para permitir e proteger o acesso aos aplicativos relevantes, incluindo aplicativos de software como um serviço (SaaS).
- Evite ameaças ao excluir aplicativos indesejados para reduzir sua área de cobertura de ameaças e aplique políticas voltadas à segurança para bloquear a exploração de vulnerabilidades, vírus, spyware, botnets e malware desconhecido (APTs).
- Proteja seus centros de dados através da validação de aplicativos, isolamento de dados, controle sobre aplicativos suspeitos e prevenção contra ameaças de alta velocidade.
- Proteja os ambientes de computação em nuvem pública e privada com maior visibilidade e controle; implante, aplique e mantenha políticas de segurança no mesmo ritmo que as suas máquinas virtuais.
- Adote a computação móvel segura ao ampliar a plataforma de segurança de última geração aos usuários e dispositivos, independentemente da sua localização.

- Agilize o gerenciamento de dispositivo, rede e da política com recursos de gerenciamento intuitivo para que correspondam à sua estrutura organizacional.

A plataforma de segurança de última geração ajuda a sua organização a gerenciar um espectro de requisitos de segurança baseado em um princípio comum. Ao usar uma combinação equilibrada de segurança de rede com inteligência de ameaça global e proteção de endpoint, a sua empresa pode dar suporte às iniciativas empresariais, enquanto aprimora sua postura geral de segurança e reduz o tempo de resposta ao incidente relacionado à segurança.

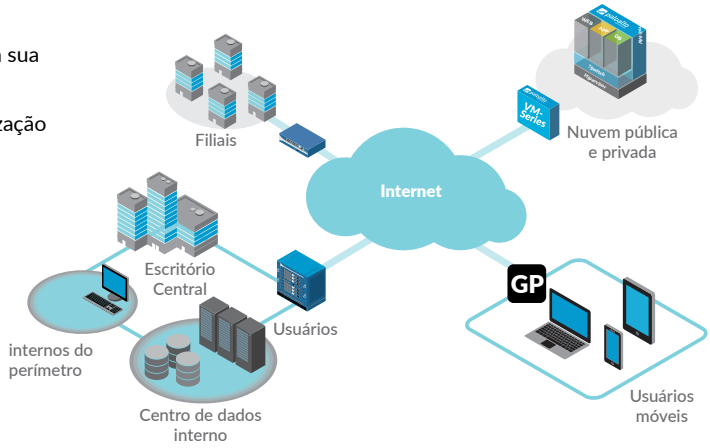

Figura 1: Implante políticas de ativação segura em toda a empresa

Uso da segurança para potencializar seus negócios

Nossa plataforma de segurança de última geração permite que você potencialize seus negócios com políticas que girem em torno de aplicativos, usuários e conteúdo. Ela usa um modelo de controle positivo, um design exclusivo de nossa plataforma que permite que você ative funções ou aplicativos específicos e bloqueie todo o resto (implícita ou explicitamente). O firewall de última geração executa uma inspeção de passagem única e total de todo o tráfego em todas as portas, fornecendo assim contexto completo do aplicativo, conteúdo associado e identidade do usuário como base para as suas decisões sobre a política de segurança.

- Classifique todo o tráfego, em todas as portas, o tempo todo. Hoje, aplicativos e seu conteúdo associado podem facilmente evitar um firewall baseado em porta mediante o uso de várias técnicas. Nossa plataforma de segurança de última geração aplica nativamente vários mecanismos de classificação ao fluxo do tráfego para identificar aplicativos, ameaças e malware. Todo tráfego é classificado, independentemente da porta, criptografia (SSL ou SSH) ou técnicas evasivas utilizadas. Os aplicativos não identificados – geralmente uma pequena porcentagem do tráfego, mas elevada em risco potencial – são automaticamente classificados para gerenciamento sistemático.
- Reduza a área de ameaça, evite ataques cibernéticos. Quando o tráfego for totalmente classificado, você pode reduzir a área de ameaça de rede ao permitir aplicativos específicos e negar todos os outros. A prevenção coordenada de ataques cibernéticos pode então ser aplicada para bloquear sites conhecidos de malware e evitar explorações de vulnerabilidade, vírus, spyware e consultas maliciosas de DNS. Qualquer malware personalizado ou desconhecido é analisado e identificado através da execução de arquivos e observação direta de seu comportamento malicioso em um ambiente virtualizado de área restrita. Quando o novo malware é descoberto, uma assinatura para o arquivo infeccioso e o tráfego relacionado ao malware é automaticamente gerado e entregue a você.
- Mapeie o tráfego do aplicativo e ameaças associadas para usuários e dispositivos. Para melhorar a sua postura de segurança e reduzir os tempos de resposta ao incidente, é essencial mapear o uso do aplicativo para usuário e tipo de dispositivo, e ser capaz de aplicar esse contexto às suas políticas de segurança. A integração com uma vasta gama de repositórios de usuários corporativos fornece a identidade do usuário e do dispositivo do Microsoft® Windows®, Mac® OS X®, Linux®, Android® ou iOS que está

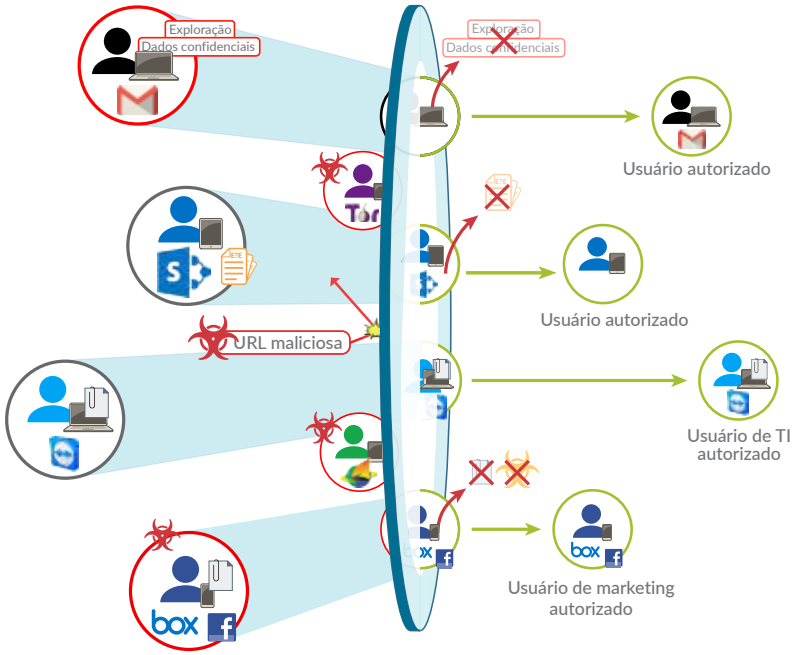

Figura 2: Aplicativos, conteúdo, usuários e dispositivos – todos sob o seu controle

Figura 3: Visualize a atividade do aplicativo em um formato claro, fácil de ler. Inclua e remova filtros para saber mais sobre o aplicativo, suas funções e quem o está usando

acessando o aplicativo. A combinação da visibilidade e do controle sobre usuários e dispositivos significa que você pode ativar com segurança o uso de qualquer aplicativo que passa por sua rede, independentemente de onde o usuário estiver ou do tipo de dispositivo que estiver sendo usado.

Definir o contexto de aplicativos específicos em uso, o conteúdo ou a ameaça que podem conter e o usuário ou dispositivo associado ajuda a simplificar o gerenciamento de políticas, melhorar sua postura de segurança e acelerar a investigação de incidentes.

Ter o contexto completo resulta em políticas de segurança mais rígidas

As melhores práticas de segurança ditam que as decisões que você toma em relação às políticas, a sua capacidade de elaborar um relatório sobre a atividade de rede e sua capacidade de análise forense dependem do contexto. O contexto do aplicativo em uso, do site visitado, da carga útil associada e do usuário são todos pontos de dados valiosos no seu esforço para proteger a sua rede. Quando você sabe exatamente quais aplicativos estão passando por seu gateway de Internet, operando dentro do seu centro de dados ou ambiente de nuvem ou ainda sendo usados por usuários remotos, você pode aplicar políticas específicas para esses aplicativos, completas com proteção contra ameaças coordenadas. O conhecimento de quem é o usuário, não apenas o seu endereço de IP, acrescenta outro elemento contextual que permite que você seja mais granular em sua atribuição de políticas.

Um rico conjunto de ferramentas altamente interativas para a filtragem de registros e visualizações interativas fornece o contexto da atividade do aplicativo, do conteúdo ou da ameaça associada, de quem é o usuário e do tipo de dispositivo. Esses pontos de dados, por si sós, dão a você uma visão parcial da sua rede, mas quando o contexto completo é levado em conta, eles fornecem uma visão completa do potencial risco de segurança, o que permite que você tome decisões mais substanciadas sobre as políticas. Todo tráfego é classificado continuamente. Conforme o estado muda, as alterações são registradas para análise, os resumos gráficos são atualizados dinamicamente e as informações são fornecidas em uma interface fácil de usar e baseada na Web.

- No gateway da Internet, você pode investigar aplicativos novos ou desconhecidos para rapidamente visualizar uma descrição do aplicativo, as suas características comportamentais e quem os está usando. A visibilidade adicional em categorias de URL, ameaças e padrões de dados fornece um quadro mais completo do tráfego de rede que passa pelo gateway.
- Todos os arquivos analisados pelo WildFire™ em busca de malware desconhecido são registrados com acesso total aos detalhes, incluindo o aplicativo, o usuário, o tipo de arquivo, o sistema operacional de destino utilizados e os comportamentos maliciosos observados.
- Dentro do centro de dados, verifique todos os aplicativos em uso e garanta que eles estejam sendo usados apenas por usuários autorizados. A visibilidade agregada à atividade do centro de dados pode confirmar que não há aplicativos mal configurados ou usos não autorizados de SSH ou RDP.
- Os fluxos de trabalho para análise de ameaça, investigação forense e busca são acelerados com o serviço de inteligência de ameaças do AutoFocus™, que fornece dados exclusivos sobre a ameaça contextual do dispositivo diretamente no PAN-OS®.
- Nos ambientes de nuvem pública ou privada, aplique a política e proteja os aplicativos com a plataforma de segurança de última geração, enquanto acompanha o ritmo de criação e movimentação de seus servidores virtuais.
- Em todos os cenários de implantação, aplicativos desconhecidos – normalmente uma pequena porcentagem em todas as redes – podem ser categorizados para análise e gestão sistemática.

Em muitos casos, você pode não estar plenamente consciente de quais aplicativos estão em uso, a frequência com que são utilizados ou por quem. A visibilidade total dos aspectos relevantes aos negócios do seu tráfego de rede – o aplicativo, o conteúdo e o usuário – é o primeiro passo em direção a um controle mais substanciado da política.

Figura 4: O editor de política unificada permite a criação e a implantação rápida de políticas que controlam aplicativos, usuários e conteúdo

Redução do risco ao habilitar aplicativos

Tradicionalmente, o processo para reduzir riscos significava que você precisava limitar o acesso aos serviços de rede e possivelmente prejudicar os seus negócios. Hoje, a redução de riscos significa habilitar aplicativos de maneira segura usando uma abordagem voltada aos negócios que ajuda a manter o equilíbrio entre a abordagem tradicional de negar tudo e a abordagem de permitir tudo.

- Use grupos de aplicativos e decriptação SSL para limitar webmail e mensagens instantâneas para algumas variantes de aplicativos específicos; inspecione-os no que diz respeito às ameadas e carregue arquivos suspeitos desconhecidos (arquivos EXE, DLL, ZIP, documentos PDF, documentos do Office, Java® e Android® APK) no WildFire para que sejam analisados e a assinatura desenvolvida.
- Controle a navegação na Web para todos os usuários, ao permitir e varrer o tráfego para sites relacionados com os negócios e bloquear o acesso a sites obviamente não relacionados ao trabalho; "oriente" sobre o acesso a sites questionáveis através de páginas de bloqueio personalizadas.
- Bloqueie explicitamente aplicativos de transferência direta de arquivo de funcionário para funcionário para todos os usuários que estão usando filtros dinâmicos de aplicativo.
- Compreenda o uso de aplicativo SaaS em sua organização, estabeleça acesso granular e controles de uso para cada aplicativo e impeça a distribuição de malware por meio desses aplicativos.
- Adote dispositivos móveis ao ampliar suas políticas de gateway de Internet e capacidades de prevenção de ameaças para usuários remotos com o serviço de segurança móvel GlobalProtect™.

No centro de dados, use o contexto para confirmar se os aplicativos do seu centro de dados estão sendo executados em suas portas padrão, encontre aplicativos maliciosos, valide os usuários, isole os dados e proteja dados críticos para os negócios contra as ameaças. Os exemplos podem incluir:

- Mediante o uso de zonas de segurança, isole o repositório de números de cartão de crédito baseado em Oracle®, forçando o tráfego do Oracle em todas as suas portas padrão, ao mesmo tempo que inspeciona o tráfego de ameaças de entrada e limita o acesso apenas ao grupo financeiro.
- Crie um grupo de aplicativos de gerenciamento remoto (por exemplo, SSH, RDP, Telnet) para que apenas o departamento de TI o use dentro do centro de dados.
- No seu centro de dados virtual, use objetos dinâmicos para ajudar a automatizar a criação da política de segurança conforme as máquinas virtuais SharePoint® sejam estabelecidas, retiradas ou passem por todo seu ambiente virtual.

Proteção de aplicativos habilitados e conteúdo

Quando você aplica políticas de prevenção de ameaças e de varredura de conteúdo, o contexto do aplicativo e do usuário passam a ser partes integrantes de sua política de segurança. O contexto completo dentro das suas políticas de prevenção de ameaças neutraliza as táticas de evasão, tais como alternância de porta e encapsulamento. Reduza a área de superfície de destino da ameaça ao habilitar um conjunto selecionado de aplicativos e, então, aplique políticas de prevenção de ameaças e verificação de conteúdo a esse tráfego.

Os elementos de proteção contra ameaça e verificação de conteúdo disponíveis dentro das suas políticas incluem:

- **Prevenção de ameaças conhecidas usando IPS e antivírus/anti-spyware de rede.** A proteção contra uma gama de ameaças conhecidas é realizada com a inspeção de passagem única, usando um formato uniforme de assinatura e um mecanismo de varredura baseado em fluxo. Os recursos do sistema de prevenção de intrusão (IPS) bloqueiam as explorações de vulnerabilidade da rede e da camada do aplicativo, transbordamentos de dados/estouros de buffer, ataques DoS e varreduras de portas. A proteção antivírus/anti-spyware bloqueia milhões de variantes de malware, incluindo aqueles escondidos em arquivos compactados ou no tráfego da Web (HTTP/HTTPS compactado), bem como vírus de PDF conhecidos. Para tráfego criptografado com SSL, você pode aplicar seletivamente decriptação baseada em política e, em seguida, inspecionar o tráfego quanto a ameaças, independentemente da porta.
- **Bloqueie malware direcionado ou desconhecido com o WildFire.** Malware direcionado ou desconhecido (por exemplo, ameaças avançadas persistentes) escondido em arquivos pode ser identificado e analisado pelo WildFire em todos os diversos sistemas operacionais e versões do aplicativo, que observam e executam diretamente arquivos desconhecidos em um ambiente de área limitada virtualizada na nuvem ou no aparelho WF-500. O WildFire monitora mais de 420 comportamentos maliciosos e,

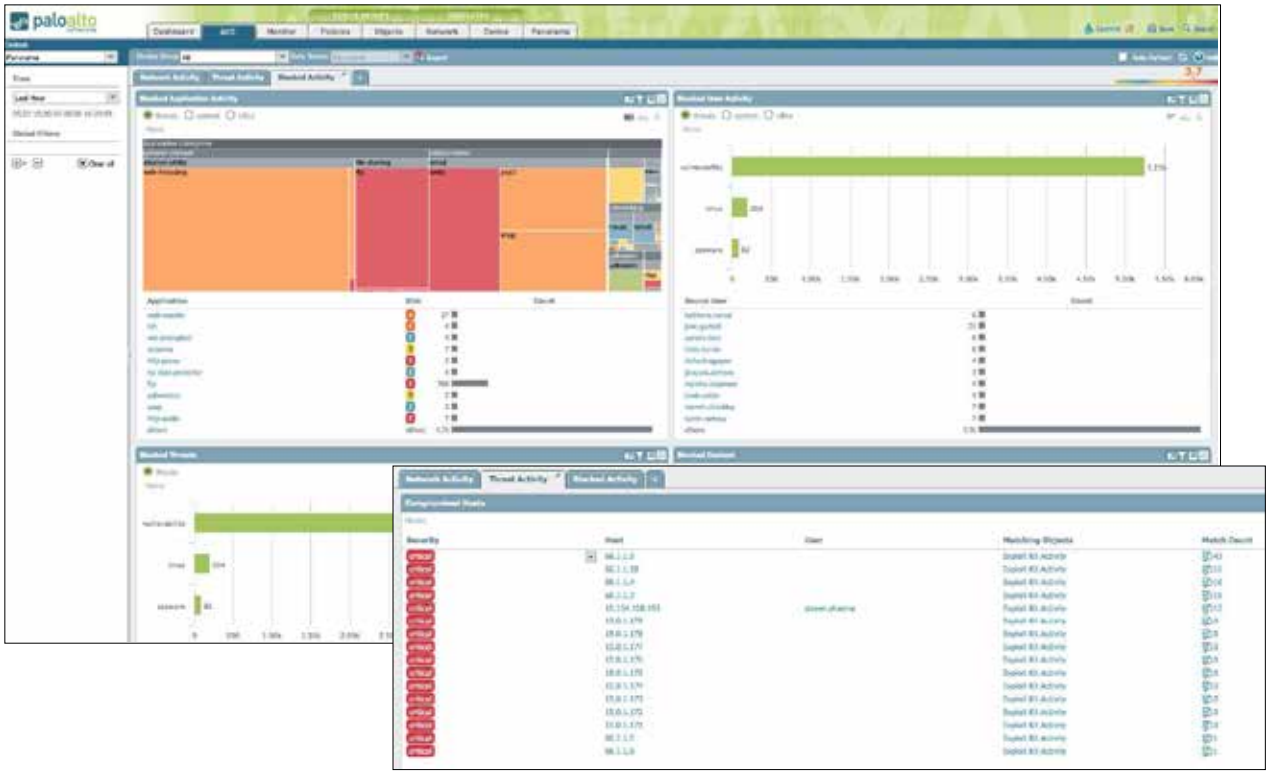

Figura 5: Visibilidade de conteúdo e ameaça – visualize a atividade de URL, as ameaças e a transferência de arquivo/dados, bem como os hosts comprometidos em um formato claro e fácil de ler que é altamente personalizável. Inclua e remova filtros para saber mais sobre os elementos individuais

se um malware for encontrado, uma assinatura é automaticamente desenvolvida e entregue a você em 5 minutos. Todos os principais tipos de arquivos são suportados pelo WildFire, incluindo: arquivos PE; .doc, .xls e .ppt do Microsoft Office; PDF (Portable Document Format); Java Applet (jar e class); e APK (Android Application Package). Além disso, o WildFire analisa links em e-mails para interromper ataques de phishing.

- **Identifique hosts infectados por robôs e interrompa a atividade de rede que vem do malware.** A classificação completa e contextual de todos os aplicativos, em todas as portas, incluindo qualquer tráfego desconhecido, pode muitas vezes expor sua rede a anomalias ou ameaças. Use o App-ID™ de comando e controle, relatório de botnet comportamental, envio de resolução errada e/ou caminho alternativo para DNS e DNS passivo para correlacionar rapidamente o tráfego desconhecido, DNS suspeito e consultas URL com hosts infectados. Aplique a inteligência global para interceptar e permitir que o firewall dê informações falsas para consultas de DNS para domínios maliciosos.
- **Limite a transferência de arquivos e dados não autorizados.** Os recursos de filtragem de dados permitem que seus administradores implantem políticas que reduzirão os riscos associados às transferências de arquivos e dados não autorizadas. As transferências de arquivos podem ser controladas quando não se olha apenas a extensão do arquivo, mas sim o que há dentro dele, para determinar se a ação de transferência deve ser permitida ou não. Os arquivos executáveis, geralmente encontrados em downloads que acontecem sem o conhecimento do usuário, podem ser bloqueados, protegendo, assim, sua rede de propagação de malware invisível. Os recursos de filtragem de dados podem detectar e controlar o fluxo de padrões de dados confidenciais (números de cartão de crédito, CPF, bem como padrões personalizados).
- **Controle da navegação na Web.** Um mecanismo de filtragem de URL totalmente integrado e personalizável permite que seus administradores apliquem políticas granulares de navegação na Web, complementando a visibilidade do aplicativo e das políticas de controle que protegem a empresa contra uma gama completa de riscos regulatórios legais e de produtividade.
- **Política baseada em dispositivo para acesso ao aplicativo.** Usando o GlobalProtect, uma empresa pode definir políticas específicas para controlar quais dispositivos podem acessar aplicativos e recursos específicos da rede. Por exemplo, garanta que laptops estejam em conformidade com a imagem corporativa antes de dar acesso ao centro de dados. Verifique se o dispositivo móvel está atualizado, se é propriedade da empresa e se todos os patches foram aplicados antes que acesse dados confidenciais.
- **Confirme automaticamente hosts comprometidos.** Um mecanismo de correlação automatizado procura por indicadores predefinidos de comprometimento de toda a rede, correlaciona correspondências e destaca automaticamente hosts comprometidos, reduzindo a necessidade de pesquisa manual de dados.

Gerenciamento de segurança de rede

A plataforma de segurança de última geração pode ser gerenciada individualmente por meio da interface de linha de comando ou de uma interface completa com recursos baseados em navegador. Para implantações de grande escala, você pode usar o Panorama™ para distribuir globalmente os recursos de visibilidade, edição de política, elaboração de relatórios e recursos de registro de log para todos os seus hardwares e firewalls de dispositivos virtuais. O Panorama™ oferece o mesmo nível de controle contextual sobre a implantação global que você tem sobre um único dispositivo.

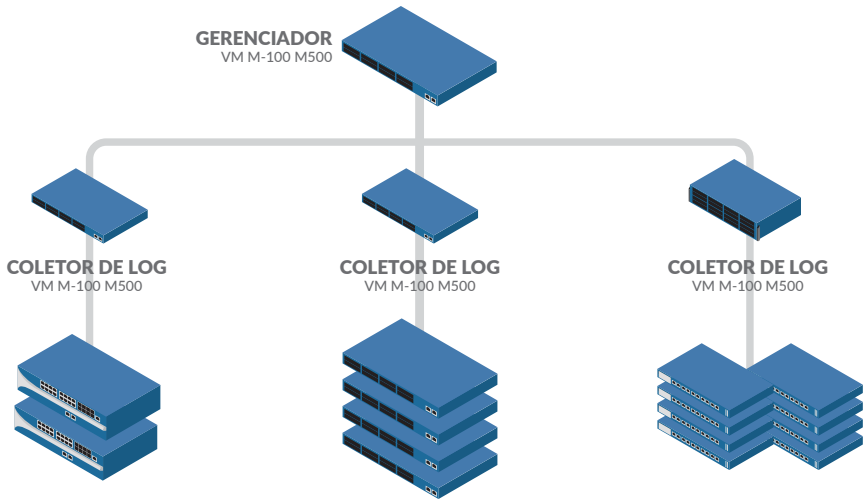

Figura 6: O Panorama™ pode ser implantado em um dispositivo dedicado ou de modo distribuído para maximizar a escalabilidade

A administração baseada em função, combinada com pré e pós-regras, permite que você estabeleça o equilíbrio entre o controle centralizado com a necessidade de edição da política local e a flexibilidade na configuração do dispositivo. Seja usando a interface da web do dispositivo ou o Panorama, a aparência da interface é idêntica, garantindo que não haja nenhuma curva de aprendizagem quando houver mudança de uma para a outra. Os seus administradores podem usar qualquer uma das interfaces fornecidas para fazer mudanças a qualquer momento, sem precisarem se preocupar com problemas de sincronização. O suporte adicional para ferramentas baseadas em padrões, como SNMP e APIs baseados em REST, permite a integração com ferramentas de gerenciamento de terceiros.

Elaboração de relatórios e registros de log

Melhores práticas de segurança significam encontrar um equilíbrio entre os esforços de gerenciamento em curso e ser reativo, o que pode envolver a investigação e análise de incidentes de segurança ou a elaboração de relatórios diários.

- **Elaboração de relatórios:** Relatórios predefinidos podem ser usados como estão, personalizados ou agrupados como um único relatório, a fim de atender às necessidades específicas. Todos os relatórios podem ser exportados para o formato CSV ou PDF e podem ser executados e enviados por e-mail de forma programada.
- **Registro de log:** A filtragem de logs em tempo real facilita a investigação forense rápida em cada sessão que passar por sua rede. O contexto completo do aplicativo, o conteúdo – incluindo malware detectado pelo WildFire – e o usuário podem ser usados como critérios de filtragem, e os resultados podem ser exportados para um arquivo CSV ou enviados para um servidor syslog para arquivamento offline ou análise adicional. Os registros de log que foram agregados pelo Panorama também podem ser enviados para um servidor syslog para fins de arquivo ou análise adicional.
- **Busca de ameaça:** A inteligência de ameaça do serviço do AutoFocus é disponibilizada diretamente no PAN-OS, agilizando os fluxos de trabalho de análise e procura de ameaça, sem recursos especializados adicionais. Quando for necessária análise adicional, os usuários podem escolher entre o AutoFocus e o PAN-OS, com pesquisas previamente preenchidas para os dois sistemas.

Além dos recursos de elaboração de relatórios e registro de log fornecidos pela plataforma de segurança de última geração da Palo Alto Networks, a integração está disponível com ferramentas SIEM de terceiros, como Splunk® da Palo Alto Networks. Essas ferramentas fornecem mais recursos para a elaboração de relatórios e a visualização de dados, e permitem que você correlacione eventos de segurança em vários sistemas na sua empresa.

Hardware especificamente desenvolvido ou plataformas virtualizadas

Nosso firewall de última geração está disponível em uma plataforma de hardware especificamente desenvolvida, que é escalável a partir de uma filial da empresa para um centro de dados de alta velocidade ou em um fator de forma virtualizada para dar suporte às suas iniciativas de computação baseadas em nuvem. Nós damos suporte para a mais vasta gama de plataformas virtuais para darmos cobertura às suas necessidades distintas de centro de dados virtualizado e de nuvem pública e privada. A plataforma de firewall do VM-Series está disponível para VMware® ESXi™, NSX™, Citrix® SDX™, Microsoft Hyper-V®, Amazon® Web Services (AWS), Microsoft Azure™ e hipervisores KVM. Ao implantar nossas plataformas, seja em hardware ou fatores de forma virtuais, você pode usar o Panorama para o gerenciamento centralizado.

4401 Great America Parkway
Santa Clara, CA 95054

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

www.paloaltonetworks.com