DEMONSTRAÇÃO DE SOLUÇÕES

A Cisco apresenta uma plataforma avançada de firewall de próxima geração

Data: Fevereiro de 2016 **Autor:** Jon Oltsik, analista sênior principal

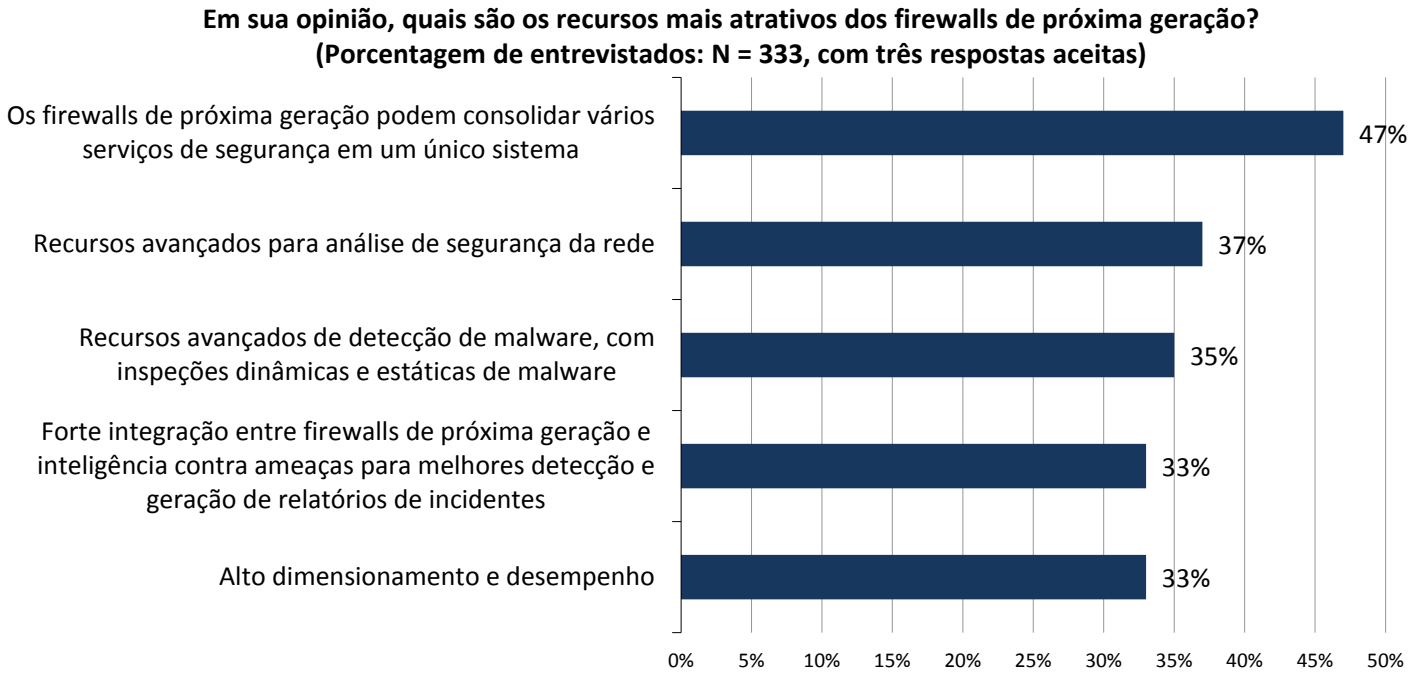
Resumo: Quando surgiram pela primeira vez, os firewalls de próxima geração foram comercializados como um remédio para todos os males, pois consolidariam a proteção de rede e de aplicativos em dispositivos de rede exclusivos. É claro que os NGFWs foram uma evolução, mas muitas ofertas ainda pecavam em integração de software, recursos de gerenciamento de ameaças, alto desempenho e gerenciamento de sistemas como um todo. O ESG acredita que essas deficiências serão mitigadas com a introdução de plataformas de firewall de próxima geração, criadas para extensibilidade, alta produtividade, gerenciamento abrangente de ameaças e comando e controle centrais. O anúncio do NGFW Firepower da Cisco trata deste tipo de plataforma, que deve chamar a atenção dos CISOs das empresas que estejam em busca da redução do risco, do aprimoramento do gerenciamento de ameaças e da racionalização das operações de segurança.

Visão geral

De acordo com uma pesquisa do ESG, no ano de 2014, 30% das empresas relataram ter implantado firewalls de próxima geração, enquanto 33% estavam em processo de implantação de um NGFW.[1] Por que esses dispositivos são tão populares? A pesquisa do ESG revelou que os profissionais de segurança julgavam certos recursos do NGFW especialmente atrativos, como a consolidação do serviço de segurança, as funções de análise de segurança de rede avançada e os atributos de detecção avançada de malware (veja a Figura 1).[2]

[1] Fonte: Relatório de pesquisa do ESG, *Network Security Trends in the Era of Cloud and Mobile Computing*, agosto de 2014.
[2] Fonte: Ibid.

FIGURA 1. Os cinco recursos mais atrativos dos firewalls de próxima geração



Fonte: Enterprise Strategy Group, 2016.

A realidade do NGFW

Os firewalls de próxima geração prometeram recursos, como controles de aplicativos e de rede e funções de gerenciamento de ameaças, em um único sistema unificado. Infelizmente, essa história é geralmente muito boa para ser verdade. Os profissionais de segurança digital se queixam com frequência sobre as deficiências do NGFW, como:

- Problemas de desempenho. É comum que os firewalls de próxima geração venham com uma miscelânea de serviços, criando a ilusão de que um equipamento pode substituir vários outros. Na verdade, o desempenho do NGFW pode tornar-se excessivamente lento se muitos serviços forem usados em um único equipamento.Os planos de consolidação são, por vezes, impedidos quando testes de prova de conceito descobrem problemas de desempenho e de rendimento que poderiam congestionar as redes e interromper aplicativos e serviços corporativos essenciais.

- Falta de integração da camada da aplicação. Em alguns casos, serviços de firewall, como a inspeção profunda de pacotes, o IDS/IPS, e os recursos contra malware, são integrados de forma frágil no melhor dos casos.Isso acaba fazendo com que esses NGFWs sejam, na verdade, apenas uma melhoria em relação aos dispositivos de gerenciamento unificado de ameaças (UTM, do inglês), em vez de uma tecnologia revolucionária de segurança digital.

- Gerenciamento básico de ameaças. Com os primeiros firewalls de próxima geração, o gerenciamento de ameaças estava mais próximo de serviços prosaicos, como antivírus de rede, detecção de intrusão por assinatura e proteção simplificada contra ameaças da Web. Alguns NGFWs adicionaram recursos para sandbox de malware, mas esses sistemas estão caminhando muito mais em direção à integração tática das defesas contra ameaças do que a uma cobertura de gerenciamento de ameaças que abarque o perímetro de rede, a rede interna e as cargas de trabalho em nuvem.

- **Uma arquitetura fechada.** Por causa de sua herança, alguns NGFWs vêm com uma variedade de recursos projetados para dispositivos de hardware patenteados. Esses sistemas podem abrir APIs ou se conectar a um número limitado de outras ferramentas de segurança, mas isso simplesmente não é o suficiente para a infraestrutura de TI atual definida por software, que oferece processos de DevOps e ferramentas para automação/orquestração self-service.

- **Desafios de gerenciamento.** Os NGFWs baseados em serviços de segurança que apresentam frágil integração tendem a acompanhar sistemas de gerenciamento com a mesma frágil integração, que tratam como atividades isoladas o gerenciamento de configurações, políticas e mudanças e a emissão de relatórios. Isso pode adicionar complexidade e sobrecarga às operações de segurança.

Um novo modelo para firewalls de próxima geração

Os firewalls de próxima geração pareciam promissores quando surgiram, mas todas as questões descritas fizeram com que as equipes de segurança ficassem em uma situação apenas um pouco melhor do que estavam antes da implantação dos NGFWs. Então, o que é necessário? Para atender às necessidades, o ESG acredita que as empresas devem adotar uma plataforma de firewall de próxima geração projetada para (consulte a Tabela 1):

- **Dimensionamento, desempenho e flexibilidade**. Os firewalls de próxima geração precisam de alta potência para executar vários serviços de rede e de segurança em um único sistema de forma a atender às necessidades de consolidação da empresa. Isso exige a combinação certa de processadores de alta qualidade, componentes de hardware especializados e um sistema operacional multi-threaded moderno. Além disso, os NGFWs devem ser projetados de forma flexível para que as cargas de trabalho e os serviços de segurança possam ser coordenados por diversos dispositivos de hardware, VMs e ambientes em nuvem, quando necessário.

- **Integração.** Os NGFWs devem permitir a integração total de uma ampla variedade de ferramentas de segurança, ao comportar padrões comuns e fornecer APIs documentadas que interoperem com tecnologias de parceiros do ecossistema. Esses tipos de opções de integração constituem a diferença entre os antigos dispositivos de firewall de próxima geração e uma verdadeira plataforma extensível.

- **Gerenciamento de ameaças ponta a ponta.** Em vez de fixar-se em medidas de segurança básicas, uma plataforma endpoint de próxima geração deve ser rigorosamente integrada a um amplo espectro de segurança digital, que inclui sandboxing, inteligência de ameaças, indicadores de comprometimento da rede e do endpoint e alertas IDS/IPS. Isso transforma uma plataforma NGFW em uma conexão entre compartilhamento de ameaças, enriquecimento de dados, correlação de eventos e correção automatizada em redes e endpoints.

- **Recursos abrangentes de gerenciamento.** O gerenciamento de firewalls deve se alinhar às necessidades empresariais no que diz respeito à prevenção, detecção e resposta.Isso exige o gerenciamento intuitivo de políticas de ponta a ponta em todos os serviços de segurança, a centralização de relatórios e a capacidade de automatizar, modificar ou aplicar políticas de acordo com mudanças em tempo real relativas a ameaças, vulnerabilidades ou necessidades de administração interna.

TABELA 1. Aspectos de uma plataforma de firewall de próxima geração

Requisitos	Descrição	Lógica
Dimensionamento, desempenho e flexibilidade	Hardware e software de alto desempenho. Capacidade para executar serviços de segurança em todos os dispositivos e implantá-los como VM.	As empresas precisam de sistemas com alto desempenho e produtividade para consolidar as funções de segurança sem comprometer aplicativos e serviços. Há também a necessidade de conseguir distribuir serviços de segurança para acomodar mudanças na infraestrutura de TI, nas redes definidas por software e na computação em nuvem
Integração	APIs documentadas abertas, ecossistemas de parceiros e adoção de padrões.	As empresas precisam ser capazes de obter mais valor das ferramentas atuais e integrar as novas com facilidade. Há uma necessidade adicional de interoperar funções de segurança como as cadeias de serviço em fluxos de trabalho de gerenciamento de riscos e de resposta a incidentes.
Gerenciamento de ameaças ponta a ponta	Serviços de gerenciamento de ameaças fortemente integrados, incluindo sandbox de malware, IDS/IPS, inteligência de ameaças e computação forense de endpoint/rede.	As empresas precisam de uma coordenação estreita entre as ferramentas de gerenciamento de ameaças para reduzir a superfície de ataque, detectar ataques digitais em andamento e acelerar as tarefas de resposta a incidentes.

Fonte: Enterprise Strategy Group, 2016.

Plataforma NGFW da Cisco

A Cisco Systems tem uma longa história em segurança de rede que abrange várias mudanças na tecnologia de firewalls, incluindo filtragem de pacotes, inspeção stateful, inspeção profunda de pacotes (Deep Packet Inspection ou DPI) e firewalls de próxima geração. A Cisco está indo mais além com seu novo NGFW Firepower. O NGFW Firepower combina vários serviços de segurança da Cisco e da Sourcefire em uma plataforma comum que abarca a prevenção, a detecção e a resposta a incidentes. Em particular, este anúncio de produto da Cisco inclui:

- A introdução ao NGFW Firepower. Este anúncio marca a verdadeira integração por software entre o Cisco ASA Firewall, o IPS de próxima geração da Sourcefire, a proteção contra malware avançado (AMP) e outros itens de segurança da Cisco.A Cisco qualifica essa plataforma como "o primeiro firewall de próxima geração totalmente integrado e com foco em ameaças do setor" e acredita que pode oferecer melhores proteção e gerenciamento, além de racionalizar as operações de segurança.

- Uma série de novos dispositivos. A Cisco apresenta os dispositivos FirePower 4100 Series, uma linha de dispositivos de baixa latência/alto rendimento que oferece um mecanismo integrado de inspeção para firewall, IPS de próxima geração, filtragem de URL e prevenção/detecção avançada de malware em um projeto com uma unidade de rack (1 RU) otimizado para densidade.

- Firepower Management Center 6.0. Para complementar sua nova plataforma NGFW, a Cisco também anunciou um novo sistema de gerenciamento de segurança projetado para disponibilizar ao pessoal de TI e às equipes de SOC opções para gerenciamento de políticas, encadeamento de serviços e análises de segurança de forma granular. Com o Firepower Management Center 6.0, a Cisco pretende simplificar as operações de segurança e oferecer às equipes de segurança digital um conjunto de ferramentas mais eficiente e robusto.

A plataforma NGFW Firepower tem como foco casos de uso específicos, como ambientes da borda da Internet, mas não é para todos. Por exemplo, o software NGFW Firepower não oferecerá elementos como VPN, clusters ou compatibilidade para multiusuários na versão inicial. No entanto, a Cisco ainda pode atender a esses clientes com outros softwares e produtos, como seus firewalls ASA (disponíveis para execução como software nos novos dispositivos) com FirePOWER Services. A Cisco planeja continuar a prestar suporte aos sistemas atuais, enquanto aprimora os NGFWs Firepower ao longo do tempo.

Com a introdução do NGFW Firepower, a Cisco está realizando a transição dos dispositivos de firewall para uma plataforma NGFW mais moderna. Essa mudança é do extremo interesse dos CISOs das empresas que estejam em busca de reduzir o risco, melhorar o gerenciamento de ameaças e racionalizar as operações de segurança.

A grande verdade

Os profissionais de segurança digital vêm procurando pela solução definitiva que possa ser implantada na rede de forma rápida e que ofereça otimizações consideráveis em termos de prevenção, detecção e resposta. Infelizmente, tal solução não existe. CISOs sagazes sabem que uma segurança digital robusta depende de processos formais, políticas certas, comando e controle centrais, aplicação de política distribuída e visibilidade abrangente em tempo real. A tecnologia de firewall evoluiu para ser a principal engrenagem da máquina que é a segurança digital, mas ainda é uma das várias peças necessárias.

Uma plataforma de firewall de próxima geração é projetada tendo essa situação em mente, ampliando e integrando os recursos de firewall para melhorar a prevenção, a detecção e a correção de ameaças. As plataformas NGFW interoperam com outras ferramentas de segurança, alinhando-se ao antigo ditado “o todo é maior do que a soma de suas partes”. Por fim, uma plataforma de firewall de próxima geração é idealizada pensando em gerenciamento, com o objetivo de aumentar a produtividade das equipes de segurança digital, assoberbadas de trabalho e com carência de pessoal.

A Cisco vem sendo participante ativa na evolução da segurança da rede, e seu mais recente anúncio vem corroborar esse compromisso. A introdução de novos dispositivos NGFW, de uma nova plataforma e de uma solução mais completa para o gerenciamento de segurança constitui apenas o mais novo capítulo de sua história em segurança da rede.