White paper

Requisitos ao considerar um firewall de última geração

Resumo

A checklist deste documento detalha seis recursos que devem ser considerados durante a avaliação de um firewall de última geração (NGFW) para determinar se a solução pode garantir proteção abrangente para toda sua empresa.

Um NGFW deve ser capaz de:

- Integrar funções de segurança de modo a fornecer proteção eficaz contra malware e ameaças avançadas
- Fornecer indícios acionáveis de comprometimento para identificar a atividade de malware
- Oferecer visibilidade de rede abrangente
- Ajudar a reduzir os custos e a complexidade
- Integrar e criar interface de modo fácil e transparente com soluções de segurança de terceiros
- Oferecer proteção aos investimentos.

Histórico

Os sistemas de segurança cibernética que dependem apenas de defesas e técnicas pontuais não podem acompanhar os métodos de ataque sofisticados e em diversos vetores que estão atualmente em constante evolução. Na verdade, de acordo com o Relatório de Segurança Anual da Cisco de 2014, toda empresa deve pressupor que sofreu uma invasão.[1] Os pesquisadores de ameaças da Cisco descobriram que havia tráfego mal-intencionado visível em 100% das redes corporativas que observaram, o que significa que foram encontradas evidências de que competidores penetraram nessas redes e provavelmente operaram sem ser detectados por um longo período.[2]

As ameaças persistentes e em diversos vetores, os ambientes de TI fluidos e as velocidades de rede crescentes fazem com que mais empresas busquem uma solução NGFW que também possa fornecer proteção contra ameaças em camadas e defesa integrada contra ameaças com as melhores tecnologias de segurança que operam em conjunto e de modo transparente. No entanto, embora tenham surgido algumas soluções para tentar atender a essa necessidade, o NGFW descrito é raro.

Esta checklist e outras considerações de compra destacadas neste documento, podem ajudar você a provar que está investindo em uma solução NGFW realmente eficaz. O firewall deve oferecer uma visão holística da rede, analisar as ameaças em tempo real e o tráfego de rede efetivamente com escala, e ainda ajudar sua empresa a se defender contra ataques de malware direcionados e persistentes, inclusive ameaças emergentes.

[1] Relatório de Segurança Anual da Cisco de 2014: http://www.cisco.com/web/offers/lp/2014-annual-security-report/index.html.
[2] Ibid.

A base

Como uma primeira etapa na avaliação de soluções, considere a base do NGFW. Esse será o ponto de partida de sua decisão de compra. Para fornecer uma defesa integrada contra ameaças e proteção contra ameaças em diversas camadas, o NGFW deve ser desenvolvido a partir de uma base de firewall abrangente com informações de estado. Além disso, busque uma solução que tenha uma reputação de desempenho comprovado.

A base do NGFW deve ter um mecanismo de inspeção extensivo com informações de estado que ajude a proteger ativos críticos ao fornecer visibilidade abrangente das ameaças subjacentes. O NGFW também deve ser robusto o suficiente para fornecer proteção contra ameaças altamente eficaz em escala, até mesmo quando houver vários serviços ativados. Além disso, ele deve ser capaz de identificar não só as ameaças como também os usuários e dispositivos conectados à rede e monitorar as atividades deles para determinar anomalias.

A checklist de NGFW

Consulte esta checklist para garantir que a solução NGFW que você busca pode fornecer proteção, aplicar política, obter consistência e captar e compartilhar contexto ao mesmo tempo e em velocidade de cabo:

- **A solução integra funções de segurança de modo a fornecer proteção eficaz contra malware e ameaças avançadas.**

  Um NGFW deve ter camadas de segurança fortemente integradas que se comunicam. As novas formas de trabalho, como a computação em nuvem e a mobilidade, ampliam a área da superfície de ataque; a correlação de inteligência de ameaça entre todas as camadas de segurança pode identificar ataques que passam por brechas típicas na proteção e escapam da detecção. Esse nível de proteção requer coordenação contínua entre defesas na rede, endpoints e o console de gerenciamento central para ajudar as equipes de segurança a acompanhar ameaças e iniciar atividades de correção rapidamente.

  Procure um NGFW com foco nas ameaças que ofereça proteção avançada abrangente contra ameaças e malware, de modo a identificá-las e proteger contra elas. Os recursos de detecção de ameaças na solução NGFW devem ajudar as equipes de segurança não só a descobrir e parar malwares, como também a entendê-los.

- **O NGFW fornece indicações acionáveis de comprometimento para identificar atividade de malware.**

  As indicações de comprometimento, ou IoCs, são “identificadores” em um host que indicam a provável ocorrência de uma infecção. Os IoCs correlacionam a inteligência de segurança de rede e endpoint. Eles podem identificar atividade de malware em hosts e endpoints e fornecem visibilidade altamente precisa de comportamentos suspeitos e mal-intencionados.

  Uma solução NGFW com esses recursos leva a processos mais rápidos de identificação, contenção e correção.

- **O NGFW oferece visibilidade de rede abrangente.**

  Um NGFW deve fornecer reconhecimento contextual completo com uma visão holística e clara do que acontece na rede o tempo todo: usuários e dispositivos, comunicação entre máquinas virtuais, ameaças e vulnerabilidades, aplicativos e acessos a sites, transferências de arquivos e muito mais.

A visibilidade de rede abrangente deve envolver um monitoramento contínuo e passivo de todos os ativos na sua rede. Essas informações podem ser usadas, por meio da automação, para otimizar a eficácia da segurança com controles dinâmicos que respondem em tempo real a mudanças no ambiente de TI ou no cenário de ameaças. A solução deve fornecer informações em tempo real para ajudar as equipes de segurança na identificação e abordagem de brechas de segurança, ajuste fino da política de segurança e, por fim, redução do número de eventos significativos.

O NGFW também deve ser capaz de automatizar a resposta de defesa depois de um ataque, inclusive definição de escopo e contenção da infecção, para reduzir ainda mais a carga nas equipes de segurança.

- **O NGFW ajuda a reduzir a complexidade e os custos.**

  Um NGFW que seja eficaz contra ameaças avançadas unifica a segurança nas camadas de defesa. Uma abordagem integrada e em diversas camadas pode proporcionar mais visibilidade para as ameaças e, consequentemente, melhor proteção. A consolidação de várias caixas em uma única plataforma também elimina a complexidade e o custo da compra e do gerenciamento de várias soluções.

  Procure um NGFW que também ofereça:

- **Alta escalabilidade:** um NGFW com proteção de ameaças em diversas camadas permitirá que os administradores de segurança forneçam segurança consistente e robusta em escala a pequenos escritórios de filiais, sites de borda da Internet e até grandes data centers tanto em ambientes físicos quanto virtuais.
- **Automação das tarefas de segurança de rotina:** a solução NGFW deve automatizar estas atividades:
  - **Avaliação de impacto:** a correlação automática de ameaças contra inteligência de vulnerabilidade de host, topologia de rede e contexto de ataque ajuda os analistas de segurança a voltar sua atenção apenas para os eventos de invasão que garantem o monitoramento e uma resposta precisa.
  - **Ajuste de política:** a automação do provisionamento, o ajuste e a aplicação consistente de políticas de segurança em toda a empresa ajudam as equipes de segurança na otimização da eficácia de segurança e na resposta em tempo real para as condições em constante mudança e novos ataques. A automação do gerenciamento de políticas de segurança é especialmente importante para departamentos de TI com recursos limitados.
  - **Identificação do usuário:** o NGFW deve ter a capacidade de atribuir facilmente identidades de usuário a eventos de segurança. Isso poupa tempo dos analistas de segurança e os ajuda a conter e corrigir ameaças com mais rapidez.
- **O NGFW integra e cria uma interface de modo fácil e transparente com soluções de segurança de terceiros.**

Uma solução NGFW pode ajudar a aprimorar seu custo total de propriedade (TCO) e reduzir a complexidade para manter a segurança efetiva do seu ambiente de outra forma: com a integração e interface fáceis com tecnologias de terceiros. Isso inclui verificadores de vulnerabilidade, soluções de gerenciamento de software, sistemas de tíquetes de problemas e plataformas de informações de segurança e gerenciamento de eventos (SIEM) que você já implantou ou precisa implementar.

A integração com soluções de terceiros aprofunda a proteção em diversas camadas que uma solução NGFW fornece ao combinar camadas de segurança essenciais em uma plataforma. Essa abordagem simplifica a implantação de segurança e as atividades operacionais contínuas ao apoiar as tecnologias de segurança existentes e compartilhar inteligência para coordenar e simplificar respostas.

Procure um NGFW que apoie um “ecossistema” de soluções completo por meio de APIs abertas para tecnologias de terceiros, incluindo:

- Sistemas de gerenciamento de vulnerabilidades
- Virtualização de rede e sistemas SIEM
- Controle de acesso de rede (NAC, Network Access Control)
- Análise de rede
- Fluxo de trabalho de resposta a eventos

OUTRAS CONSIDERAÇÕES DE COMPRA: SERVIÇOS DE MIGRAÇÃO E SUPORTE TÉCNICO

A migração para um NGFW é um empreendimento importante. Ao migrar para um NGFW e se afastar dos firewalls de terceiros ou tradicionais, procure um fornecedor que ofereça serviços que ajudem na migração. Serviços de migração profissional no local e fornecidos remotamente podem ajudar a simplificar e acelerar o processo. Qualquer fornecedor de NGFW, ou seus parceiros certificados, deve ser capaz de oferecer uma experiência profunda, conhecimentos, práticas líderes e ferramentas para reduzir a interrupção e apoiar a continuidade dos negócios durante a migração e fazer isso de modo econômico.

O nível e a qualidade do suporte técnico que um fornecedor de NGFW oferecerá à sua empresa durante e depois da migração também deverão ser incluídos na sua avaliação técnica. Os serviços de gerenciamento remoto, por exemplo, podem ajudar a reduzir o TCO com o monitoramento e o gerenciamento contínuos de segurança de rede e a liberação de seus talentos de TI para que possam se concentrar nas principais prioridades do negócio. Além disso, os serviços que fornecem um exame contínuo da postura de segurança, políticas e eficiência da sua infraestrutura de segurança o ajudam a evoluir e aprimorar seu programa de segurança.

A assistência técnica após a instalação da solução NGFW também é uma consideração importante. O fornecedor de segurança disponibilizará à sua equipe de TI acesso a qualquer momento (24 horas, 365 dias por ano) a engenheiros especializados? Ele oferece cobertura flexível de hardware, diagnóstico proativo de dispositivo, recursos de autoatendimento, ferramentas ou treinamento online? Os serviços e o suporte estão disponíveis em todo o mundo? Um excelente suporte técnico ajuda a reduzir o tempo de inatividade da rede e mantém sua empresa funcionando.

- A solução NGFW protege o investimento.

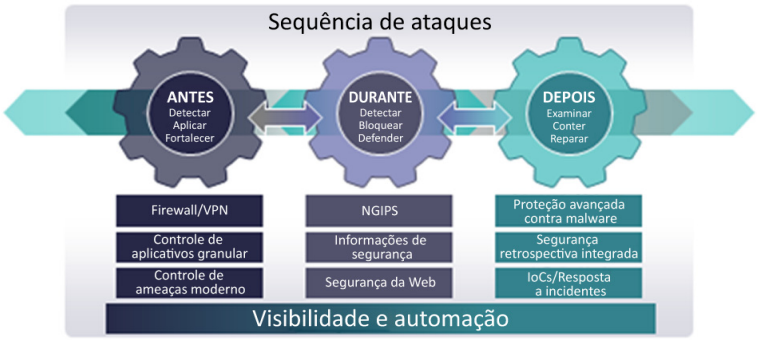
Ao se preparar para investir em uma solução de segurança de última geração que possa fornecer proteção abrangente para toda sua empresa, talvez você deva considerar alternativas além de uma compra direta. Procure um fornecedor de NGFW que ofereça opções de compra diferentes e dê à sua empresa as oportunidades de:

- Diminuir os custos e aprimorar a produtividade por meio de ciclos de vida de TI mais curtos e gerenciamento proativo
- Renovar ativos de tecnologia em linha tanto com sua estratégia de negócios atual quanto com sua visão futura e manter orçamentos previsíveis
- Acessar soluções de financiamento de ponta a ponta e acessíveis que incluem hardware, software e equipamentos complementares de terceiros

Um NGFW que atende aos requisitos da checklist: Cisco ASA com Serviços FirePOWER

O Cisco ASA com Serviços FirePOWER atende aos critérios destacados na checklist acima. Na verdade, essa é a única solução NGFW corporativa que fornece defesa integrada contra ameaças durante todo o ciclo de um ataque: antes, durante e depois de um ataque (consulte a figura 1).

Figura 1. Defesa integrada contra ameaças à sequência de ataque



O Cisco ASA com Serviços FirePOWER é o primeiro NGFW adaptável, com foco nas ameaças projetado para uma nova era de proteção avançada contra malware e ameaças. Seus controles dinâmicos permitem uma visibilidade e proteção sem precedentes contra ameaças em tempo real. A solução NGFW combina os recursos de segurança comprovados de:

- **Cisco Adaptive Security Appliance (ASA)**, o firewall com informações de estado de nível corporativo mais implantado do mundo com VPN de acesso remoto e clustering avançado para acesso de alto desempenho, altamente seguro e de alta disponibilidade para ajudar a assegurar a continuidade dos negócios.
- **Serviços FirePOWER**, a proteção avançada líder do setor contra ameaças e malware da Sourcefire® que fornece a maior eficácia contra ameaças segundo avaliação de um teste independente do NSS Labs.[3]

Cisco ASA com Serviços FirePOWER: Proteção contra ameaças em diversas camadas e defesas integrada contra ameaças em uma única plataforma

Conforme mostrado na figura 2, o Cisco ASA com Serviços FirePOWER fornece os seguintes recursos em uma plataforma:

- **Proteção superior contra ameaça em diversas camadas** tanto de ameaças conhecidas quanto desconhecidas, inclusive ataques de malware direcionados e persistentes.
- **Proteção avançada contra malware** (AMP) que fornece a melhor detecção de violação do setor, um baixo TCO e valor de proteção superior. Ela usa Big Data para detectar, entender e bloquear ataques avançados de malware. O AMP fornece a visibilidade e o controle necessários para deter ameaças que foram ignoradas por outras camadas de segurança.

[3] "Mapa de valor de segurança do NSS Labs para sistemas de detecção de violação: a Proteção avançada contra malware da Sourcefire é líder na eficácia de segurança e TCO", Sourcefire.com: https://info.sourcefire.com/NSSBreachDetectionReportSEM.html?gclid=Cj0KEQjw7b-gBRC45uLY_avSrdgBEiQAD3Olx8BtffrsQkNYs3AtCojRqyy42V1yLfGyh78OMov3iUAaAlNc8P8HAQ.

- **IOCs acionáveis:** o Cisco ASA com Serviços FirePOWER fornece IoCs holísticos e acionáveis que correlacionam informações detalhadas de rede e endpoint, o que fornece às equipes de segurança uma visibilidade ainda maior das infecções por malware. A solução NGFW também pode correlacionar todos os eventos de invasão e realizar automaticamente uma avaliação de impacto de um ataque contra o alvo.
- **Visibilidade e controle de rede abrangentes:** o Cisco ASA com Serviços FirePOWER é gerenciado pelo Cisco FireSIGHT™ Management Center. Ele fornece visibilidade de rede sem precedentes e a automação necessária para responder às condições em constante mudança e novos ataques. Com o FireSIGHT Management Center, as equipes de segurança podem verificar o que acontece na rede o tempo todo: usuários, dispositivos, comunicações entre máquinas virtuais, vulnerabilidades, ameaças, aplicativos do lado do cliente, arquivos e sites.

O sistema de prevenção contra invasões (NGIPS) Cisco ASA com Serviços FirePOWER (NGIPS) de última geração lidera o setor com prevenção de ameaças altamente eficaz e um reconhecimento contextual completo de usuários, infraestrutura, aplicativos e conteúdo para detectar ameaças multivetoriais e automatizar a resposta de defesa. O reconhecimento de conteúdo com trajetória de arquivo de malware auxilia na definição do escopo da infecção e determinação da causa para acelerar a correção.

Os administradores podem gerenciar centenas de dispositivos centralmente com o FireSIGHT Management Center. E com o Application Visibility and Control (AVC) granular fornecido pelo Cisco ASA com Serviços FirePOWER, eles podem otimizar a eficácia de segurança com 3000 controles da camada de aplicativo e baseados em risco que podem executar políticas de detecção de ameaças IPS personalizadas.

- **Automação — para reduzir o custo e a complexidade:** o Cisco FireSIGHT Management Center também ajuda os administradores a simplificar as operações para correlacionar ameaças, avaliar seu impacto, ajustar automaticamente a política de segurança e atribuir facilmente identidades de usuário a eventos de segurança. Ele monitora continuamente como a rede muda com o tempo e avalia as ameaças automaticamente para determinar quais delas exigem ação imediata. Com esse insight, as equipes de segurança podem concentrar seus esforços de resposta na correção e adaptar as defesas de rede.
- **Integração de terceiros:** o Cisco ASA com Serviços FirePOWER pode ter uma interface perfeita e transparente com soluções de terceiros, inclusive verificadores de gerenciamento de vulnerabilidade, gerenciamento de software e sistemas de tíquetes de problemas, para aprimorar o TCO. Você recebe os benefícios de um sistema aberto que tem interface com os recursos do Cisco OpenSource. O OpenAppID, uma linguagem de detecção com foco no aplicativo e módulo de processamento do Snort®, o IPS e o sistema de detecção de invasões (IPS/IDS) desenvolvidos pela Sourcefire, que permite que as equipes de TI criem, compartilhem e implementem detecção de aplicativos.

Figura 2. Cisco ASA com FirePOWER Services

Cisco ASA com Serviços FirePOWER: considerações de compra adicionais

Quando você selecionar o Cisco ASA com Serviços FirePOWER como sua solução NGFW, você terá acesso ao seguinte:

- **Proteção do investimento:** o financiamento da Cisco Capital® está disponível com condições que atendem aos requisitos da sua empresa e do seu orçamento. Com um arrendamento em valor de mercado razoável da Cisco Capital, você pode pagar pelo uso do equipamento, não sua propriedade. Você tem a flexibilidade de atualizar seu equipamento conforme necessário, ao mesmo tempo em que elimina a obsolescência da tecnologia.
- **Serviços e suporte técnico:** a Cisco obteve a certificação do J.D. Power Certified Technology Service and Support Program por cinco anos seguidos e oito anos no total.[4] Os serviços e as ofertas de suporte da Cisco para o Cisco ASA com Serviços FirePOWER incluem:
  - O **Cisco Migration Services para Firewalls**, fornecido pelos engenheiros de segurança da Cisco ou Parceiros da Cisco especializados em segurança, ajuda as empresas na migração perfeita para o Cisco ASA com Serviços FirePOWER. A Cisco disponibiliza orientação e suporte especializados para ajudar a manter a segurança durante uma migração, bem como para melhorar a precisão e a integridade do processo.
  - Os **Cisco Remote Management Services** ajudam a reduzir mais ainda o TCO com o gerenciamento contínuo das redes de segurança e a liberação dos seus recursos de TI para se concentrar em outras prioridades empresariais de agregação de valor.
  - Os **Cisco Network Optimization Services** têm ferramentas analíticas inteligentes com uma interface gráfica intuitiva para fornecer insight inigualável ao desempenho da rede, para que os clientes possam reduzir a complexidade de rede, aprimorar a excelência operacional, monitorar a conformidade com políticas, atenuar riscos e detectar e prevenir, de modo proativo, possíveis interrupções de rede. O serviço melhora radicalmente o retorno sobre o investimento e chega a superar 120% segundo um estudo da Forrester Research.[5]
  - O **Cisco SMARTnet ® Service** ajuda a reduzir o tempo de inatividade da rede e outros problemas críticos de rede com acesso a suporte técnico especializado, 24 horas por dia, 365 dias por ano, e com uma cobertura de hardware flexível e diagnóstico proativo de dispositivos.

Para baixar o software

Acesse o Cisco Software Center para fazer download do software Cisco ASA com Serviços FirePOWER.

[4] "A Cisco foi reconhecida pela excelência no Programa de Serviço e Suporte de Tecnologia Certificada por cinco anos seguidos e oito anos no total", release para imprensa da J.D. Power, 21 de julho de 2014: http://www.jdpower.com/press-releases/certified-technology-service-and-support-program#sthash.7oyGxBUo.dpuf.

[5] *The Total Economic Impact™ of Cisco SP Network Optimization Service and Focused Technical Support*, relatório preparado para a Cisco pela Forrester Research, novembro de 2009: http://www.cisco.com/en/US/services/ps6889/TEI_of_SP_NOS_FTS_Forrester.pdf.

Para obter mais informações

Para obter mais informações, acesse:

- www.cisco.com/go/asafps para obter mais informações sobre o Cisco ASA com Serviços FirePOWER
- www.cisco.com/go/asa para obter mais informações sobre os firewalls de próxima geração Cisco ASA 5500-X Series
- www.cisco.com/go/services/security para obter mais informações sobre o Cisco Migration Services para Firewalls
- www.cisco.com/go/smartnet para obter mais informações sobre o Cisco SMARTnet Service
- www.ciscocapital.com para obter mais informações e links para representantes locais da Cisco Capital

Sede - América
Cisco Systems. Inc
San Jose. CA

Sede - Ásia e Pacífico
Cisco Systems (USA) Pad Ltd.
Cingapura

Sede - Europa
Cisco Systems International BV Amsterdam,
Países Baixos

A Cisco possui mais de 200 escritórios no mundo todo. Os endereços, números de telefones e fax estão disponíveis no site **www.cisco.com/go/offices**.

Impresso nos EUA C11-733098-00 10/14