White Paper

Arquitetura de segurança integrada de rede: Firewall de última geração com foco em ameaças

Por Jon Oltsik, analista sênior principal

Setembro de 2014

Este white paper do ESG foi autorizado pela Cisco Systems e é distribuído mediante licença do ESG.

Conteúdo

Resumo executivo

A maioria das empresas aborda a segurança de rede com um exército de ferramentas táticas como firewalls, gateways VPN, IDSs/IPSs, proxies de rede, sandboxes de malware, gateways da Web e e-mail etc. Essa matriz confusa de tecnologias independentes era adequada há dez anos, mas agora representa um número enorme de desafios operacionais, de aplicação de política e de monitoramento. Pior ainda, as defesas de segurança de rede são cada vez menos eficazes para bloquear ameaças direcionadas e sofisticadas e ataques avançados de malware.

Até que ponto as coisas pioraram e o que os CISOs devem fazer para lidar com esses problemas?

- **A segurança de rede está cada vez mais difícil.** Os profissionais de segurança enfrentam incontáveis desafios diários de segurança de rede com processos e controles sobrepostos, muitas ferramentas pontuais, processos manuais em demasia e falta de habilidades de segurança. Com todos esses problemas novos e históricos, a segurança de rede atual é incompatível com os requisitos empresariais.
- **Apenas as ferramentas de segurança de rede não são suficientes.** Muitas empresas adotam novas ferramentas de segurança de rede, como firewalls de última geração (NGFWs). Esses NGFWs podem aprimorar a segurança, mas com frequência, seu foco reside em controles de aplicativos limitados, não em fornecer uma proteção mais completa contra as ameaças à segurança cibernética. Além disso, ferramentas exclusivas como sandboxes de análise de malware permanecem táticas, pois não podem fornecer proteção, nem aprimorar a visibilidade de segurança na rede ou na nuvem.
- **Empresas de grande porte precisam de uma arquitetura de segurança de rede interoperável.** As empresas precisam de uma arquitetura de segurança de rede integrada que seja mais centralizada na ameaça, ofereça escalabilidade, automatize processos manuais e substitua ferramentas pontuais por serviços de segurança de rede interoperáveis. Uma arquitetura de segurança de rede deve incluir um comando e controle centrais, aplicação distribuída e inteligência acionável integrada.

Desafios de segurança de rede

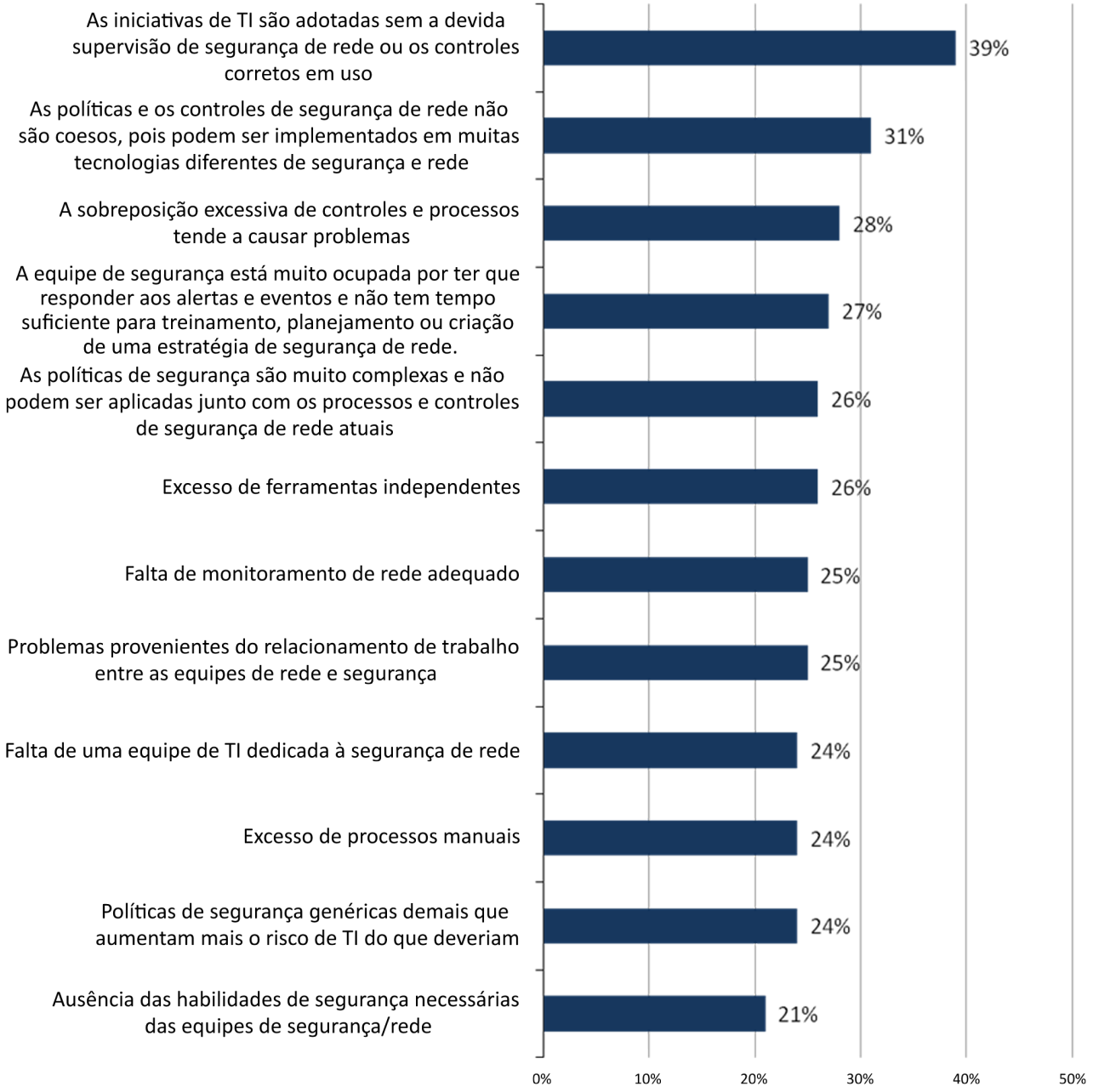
Rapidamente, as empresas grandes transformam suas infraestruturas de TI antigas com a inclusão de novas iniciativas, como computação em nuvem, análises de Big Data, mobilidade e aplicativos da Internet das Coisas (IoT). Todas essas mudanças representam alguns desafios de segurança de rede para as empresas (consulte a figura 1).[1] Com frequência, os CISOs têm dificuldades com a segurança de rede devido aos seguintes fatores:

- **Excesso de soluções diferentes e silos de tecnologia.** Aproximadamente um terço (31%) das empresas enfrentam o desafio da falta de coesão nas políticas e controles de segurança de rede, 28% têm problemas com o excesso de políticas e controles sobrepostos e 26% têm dificuldade com muitas ferramentas independentes. Essa confusão de soluções diferentes e silos de tecnologia dificulta a prevenção, a detecção ou a correção de incidentes de segurança.
- **Grande quantidade de processos manuais.** Os dados do ESG indicam que a equipe de segurança apaga incêndios com frequência, em vez de abordar a segurança de rede com políticas ou procedimentos mais proativos. Além disso, 24% das empresas afirmam que precisam enfrentar o desafio de lidar com muitos processos manuais. Combinar o combate a incêndios com processos manuais não é suficiente para atender aos requisitos atuais de gerenciamento de risco e resposta a emergências da segurança de rede.
- **Carência de habilidades de segurança de rede.** Os dados do ESG também indicam que 24% das empresas enfrentam a falta de equipe dedicada à segurança de rede, enquanto 21% delas afirmam que carecem das habilidades de segurança de rede certas. Dada a carência global de habilidades de segurança cibernética, essa é uma receita para o desastre.

[1] Fonte: ESG Research Report, *Network Security Trends in the Era of Cloud and Mobile Computing*, agosto de 2014.

Figura 1. Desafios de segurança de rede

Quais das opções a seguir você consideraria como sendo os maiores desafios de segurança de rede da sua empresa? (Porcentagem de entrevistados, N=397, cinco respostas aceitas)



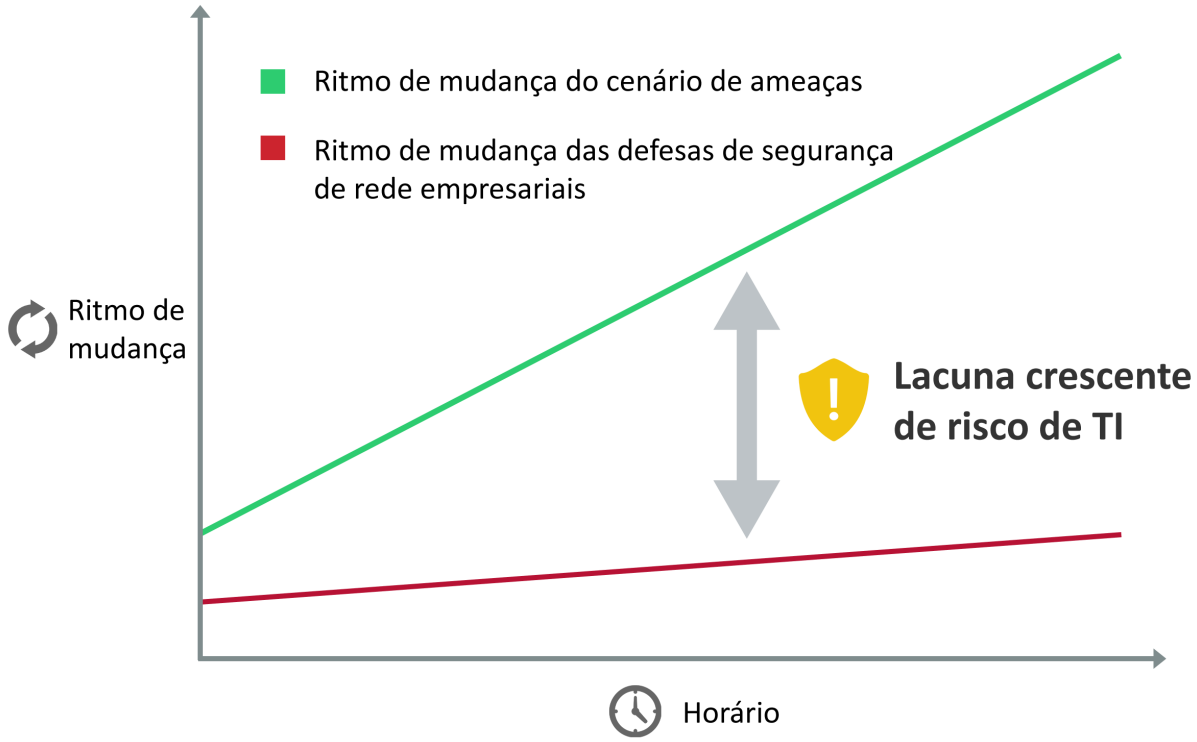
Fonte: Enterprise Strategy Group, 2014.

A lacuna de segurança de rede

Os CEOs e diretores corporativos precisam entender que os desafios de segurança de rede fazem parte de um problema muito maior relacionado ao gerenciamento de riscos de segurança cibernética. A segurança de rede antiga, baseada em silos de tecnologia e processos manuais, e que exigia habilidades avançadas de segurança, não pode ser ampliada para lidar com o volume, a variedade e a sofisticação das ameaças cibernéticas atuais. Soluções desconectadas têm pontos cegos que os ataques sofisticados exploram. Esse é um dos motivos pelos quais muitas empresas sofrem violações de segurança: os hackers simplesmente aproveitam essas fraquezas da segurança de rede, passam despercebidos ao contornar os controles de segurança de rede e comprometer os ativos de TI. Depois que os hackers conquistam o "primeiro território", frequentemente ficam invisíveis por meses conforme navegam pela rede, acessam sistemas críticos de negócios e, por fim, roubam dados confidenciais.

Antigamente, os CISOs tendiam a abordar ameaças à segurança cibernética com tecnologias de segurança de rede, processos e equipes cada vez mais numerosos, mas essa não é mais uma estratégia apropriada. As ameaças cibernéticas crescem de modo exponencial em função das novas tecnologias e avanços nas técnicas de exploração. Alternativamente, os investimentos crescentes na segurança de rede proporcionam um aumento insignificante na proteção de segurança, especialmente diante dos desafios operacionais discutidos antes. Essa situação cria uma lacuna de segurança de rede na qual o risco para TI cresce diariamente (consulte a figura 2).

Figura 2. A segurança de rede tática cria uma lacuna de risco crescente para TI



Fonte: Enterprise Strategy Group, 2014.

As empresas precisam de uma arquitetura de segurança de rede integrada com foco nas ameaças

As grandes empresas enfrentam um enigma cada vez mais complexo: as redes empresariais devem estar disponíveis e ser escaláveis, dinâmicas e abertas para ancoragem dos processos atuais de TI e negócios, mas esse modelo levou a um aumento alarmante no risco para a segurança cibernética. Os controles de segurança de rede antigos não são adequados para esse ambiente de TI fluido e cenário de ameaças em constante mudança.

Então, o que é necessário? O ESG acredita que os requisitos de segurança de rede demandam uma nova abordagem para a segurança de rede. Os CISOs precisam pensar na segurança de rede em termos de um novo modelo arquitetônico completo, que vá da borda da rede para o núcleo e até a nuvem. O ESG define uma arquitetura de segurança de rede integrada como:

Um sistema integrado de hardware e software de segurança de rede, onde um serviço de segurança pode ser aplicado em um ponto em uma rede interna ou estendida como um formato físico ou virtual. Uma arquitetura de segurança de rede também permite comunicações subjacentes para que todos os serviços e componentes de segurança possam compartilhar e reagir às informações em tempo real, de modo a ajustar os controles de segurança, detectar eventos de segurança e corrigir sistemas comprometidos.

Uma arquitetura de segurança de rede integrada com foco nas ameaças se baseia nos mesmos tipos de firewalls (firewalls de última geração e firewalls padrão), IDSs/IPSs e outras tecnologias de segurança em uso hoje. No entanto, a principal diferença é que os dispositivos individuais interoperam e cooperam de modo mais fluido na rede e compartilham sua inteligência de telemetria e, quando fazem isso, se informam o tempo todo e atuam melhor em harmonia. Além disso, as funções de segurança de rede como firewalls ou IDS/IPS podem ser pensadas como serviços e aplicadas de modo consistente na LAN, data center corporativo ou provedor de nuvem externo onde e quando forem necessárias.

Para realmente permitir a integração, a cobertura abrangente e a interoperabilidade, uma arquitetura de segurança de rede integrada com foco nas ameaças deve se basear em três itens:

1. **Comando e controle centrais.**
2. **Aplicação distribuída.**
3. **Inteligência acionável integrada.**

Comando e controle centrais

Um dos principais desafios associados à tecnologia de segurança de rede antiga está relacionado ao gerenciamento e às operações. Cada dispositivo de segurança de rede tem seu próprio mecanismo de política, provisionamento, configuração e relatório, o que causa alguns grandes problemas associados à sobrecarga operacional e às tarefas redundantes. Além disso, é difícil ou talvez impossível identificar o status da segurança empresarial ao examinar vários relatórios táticos.

Para atenuar esses problemas, uma arquitetura de segurança de rede integrada precisa começar com comandos e controles centrais para:

- **Gerenciamento de serviços.** O provisionamento, a configuração e a alteração dos serviços de segurança de rede devem ser gerenciados centralmente, com o suporte de uma GUI intuitiva e um mecanismo de fluxo de trabalho e interoperar com outras ferramentas operacionais de TI. Por exemplo, os profissionais de segurança de rede devem ter a capacidade de provisionar e configurar regras de firewall, VLANs e ACLs de roteador/switch de uma única GUI. Só isso deve ser suficiente para simplificar os controles de segurança de rede, aprimorar a proteção e simplificar as operações de segurança de rede.

- **Interoperabilidade com virtualização de servidor e orquestração em nuvem.** Ferramentas de nível superior para a configuração de cargas de trabalho virtuais para VMware, Hyper-V, OpenStack ou AWS precisam ter o suporte dos controles de segurança apropriados. Com comandos e controles centrais, uma arquitetura de segurança de rede deve oferecer as APIs apropriadas para alinhar os benefícios da nuvem, como provisionamento rápido e autoatendimento, com as camadas apropriadas de proteção de segurança de rede**.**
- **Monitoramento e geração de relatórios.** Além das funções de gerenciamento e operações, uma arquitetura de segurança de rede integrada também deve oferecer monitoramento central e geração de relatórios alinhados com atividades como o gerenciamento de eventos. Os analistas de segurança devem ter a capacidade de passar de um relatório para outro ou correlacionar vários relatórios rapidamente para uma visão mais precisa e oportuna do status de segurança de rede. Para aliviar os pontos cegos, o monitoramento central e a geração de relatórios também devem monitorar controles virtuais e baseados na nuvem junto com dispositivos de segurança de rede físicos.
- **Visibilidade avançada.** Além do monitoramento, os analistas de segurança precisam ter visibilidade profunda de seus ambientes, para identificar ameaças multivetoriais e verificar quais usuários, aplicativos, conteúdo e dispositivos estão na rede e o que fazem para implementar uma política de segurança efetiva a fim de acelerar a detecção de ameaças e a resposta a elas.

Aplicação distribuída

Com os comandos e controles centrais, os CISOs podem criar políticas globais de segurança, mas essas políticas ainda terão que ser aplicadas por vários serviços de segurança residentes na rede. Uma arquitetura de segurança de rede integrada também atende a esse requisito com:

- **Apoio para qualquer formato em qualquer local.** Os serviços de segurança de rede devem estar disponíveis em qualquer local, em qualquer formato e em qualquer combinação. Assim, a equipe de segurança pode aplicar políticas de segurança de rede granulares aos segmentos de rede, fluxos, aplicativos ou grupos específicos de usuários. Por exemplo, empresas de varejo podem usar um conjunto de controles de segurança de rede física e virtual para assegurar que os sistemas de POS só possam se conectar a determinados endereços IP por meio de uma combinação de firewalls, IDSs/IPSs e ferramentas avançadas de detecção de malware. Ou os usuários na LAN corporativa podem receber políticas de acesso diferentes daqueles que trabalham em casa, em redes públicas.
- **Um portfólio de serviços de segurança de rede.** Uma arquitetura de segurança de rede precisa executar tarefas L2-7 e dar respaldo a todos os tipos de filtragem de pacotes em qualquer ponto na LAN, WAN ou nuvem. A filtragem de pacotes é uma categoria ampla aqui e inclui a procura de ameaças como vírus, worms, ataques DDoS, SPAM, phishing, ameaças da Web, vazamentos de conteúdo e ataques de camada de aplicativo. Com a combinação de vários formatos e diversos serviços, as empresas criam ataques de segurança em camadas superiores que podem ser personalizados para diferentes fluxos de rede, grupos de usuários e requisitos de mobilidade ou ajustados rapidamente para abordar novos tipos de ameaças.
- **Integração de segurança de rede e endpoint.** Antigamente, a segurança de rede e endpoint era gerenciada quase sempre por grupos de segurança diferentes com o uso de processos e ferramentas distintos, porém, dado o atual panorama de ameaças insidiosas, isso não faz mais sentido. Para preencher essa laguna, uma arquitetura de segurança de rede deve oferecer integração firme entre os controles de rede e endpoint e a análise de detecção. Por exemplo, os controles de aplicativos devem ser consistentes entre os NGFWs e endpoints para proteger ativos confidenciais quando os usuários se conectam à rede via LAN corporativa ou de redes públicas remotas em todo o mundo. Para melhorar a detecção de incidentes, as sandboxes de análise devem interoperar com agentes de endpoint para correlacionar o tráfego de rede suspeito anômalo às atividades anômalas do sistema.

Inteligência acionável integrada

Embora as tecnologias de segurança de rede como dispositivos de ameaça da Web, IDSs/IPSs e gateways antivírus dependam de assinatura e atualizações de inteligência da nuvem, muitas outras tecnologias de segurança de rede são contingenciais para alterações de configuração pelo pessoal de segurança ou criação de novas regras para o bloqueio de conexões de rede. Como alternativa, uma arquitetura de segurança de rede integrada pode ser criada do zero para ser "voltada para inteligência" do jeito que está:

- **Com base no número de fontes de dados diversas.** Embora os sistemas SIEM geralmente executem a análise de segurança com base nos eventos de log, uma arquitetura de segurança de rede oferece uma ampla variedade de outros tipos de dados para análise. Isso inclui recursos de rede como o NetFlow e a captura de pacote completo, além de dados detalhados sobre análise e criação de perfis de endpoint, padrões de acesso de usuário/dispositivo e auditoria de aplicativo em nuvem. Quando combinados, correlacionados e analisados corretamente, esses novos dados podem ajudar as empresas a melhorar o gerenciamento de risco e acelerar a detecção/resposta a incidentes.
- **Integração com a inteligência de ameaças baseada na nuvem.** Uma arquitetura de segurança de rede deve se estender à inteligência de ameaças baseada em nuvem e detalhar itens como vulnerabilidades de software, endereços IP inválidos, URLs falsas, canais de C&C conhecidos, arquivos maliciosos, indicadores de comprometimento (IoCs) e padrões de ataque que mudam rapidamente.
- **Criada para automação.** Por fim, uma arquitetura de segurança de rede aproveita a inteligência de segurança interna e externa para ajudar as empresas na automatização de suas defesas de segurança de rede. Por exemplo, tráfego anômalo no data center pode acionar uma regra de firewall automatizada que termina os fluxos com base em uma combinação de fatores como IP de origem, porta, protocolo e atividades de DNS. Ou, quando o malware for detectado, a rede poderá analisar downloads de arquivos e descobrir retroativamente e corrigir endpoints que fizeram download de arquivos suspeitos de URLs específicas. Atividades de correção automatizadas como essas podem levar ao aprimoramento contínuo nos controles de segurança de rede e ajudar a sistematizar investigações de segurança para proporcionar uma resposta mais rápida.

Em conjunto, uma arquitetura de segurança de rede não só pode abordar os desafios existentes, como também fornecer benefícios de negócios, TI e segurança (consulte a tabela 1).

Tabela 1. Características das arquiteturas de segurança de rede

Propriedade da arquitetura de segurança de rede	Detalhes	Funcionalidades	Benefícios
Comando e controle centrais	Gerenciamento de serviços, interoperabilidade de orquestração da virtualização de nuvem/servidor, monitoramento central e relatórios	Centraliza o gerenciamento de política, provisionamento, gerenciamento de configuração, gerenciamento de alterações, gerenciamento de eventos etc.	Operações de segurança simplificadas, facilidade de uso, controle central e visibilidade em todos os elementos de segurança de rede, independentemente do local ou formato
Aplicação distribuída	Qualquer serviço de segurança de rede, qualquer local, qualquer formato, integração entre segurança de rede e endpoint	Coordenação entre serviços de rede, extensão da aplicação da política de segurança para a nuvem	A segurança em camadas personalizada para vários casos de uso para proteger usuários, dispositivos e aplicativos pode ser facilmente aprimorada ou modificada para novos tipos de ameaças
Inteligência acionável integrada	Diversas fontes de dados, inclusive inteligência de ameaças baseada na nuvem	Informa detalhes granulares sobre o tráfego de aplicativos, o tráfego de rede, as atividades de endpoint e novas ameaças à solta	Permite que a equipe de segurança tome decisões com base em inteligência em tempo real e fornece automação de processos de correção

Fonte: Enterprise Strategy Group, 2014.

Arquitetura de segurança de rede da Cisco: Firewall de última geração com foco em ameaças

Embora a Cisco Systems sempre tenha sido reconhecida por seus produtos de segurança de rede, a empresa teve que evoluir sua visão de tecnologia para acompanhar os crescentes requisitos empresariais e o cenário de ameaças cada vez mais perigoso. Na busca desse objetivo, a Cisco fez um grande movimento em 2013 com a aquisição da Sourcefire.

A fusão Cisco/Sourcefire uniu dois gigantes da segurança de rede, mas ainda havia muito trabalho a ser feito para integrar as tecnologias para formar o tipo de arquitetura de segurança de rede de nível empresarial descrita antes. Agora, esse esforço começa a dar frutos com o anúncio do Cisco ASA com Serviços Firepower. Com a combinação do firewall Cisco ASA, IPS da Sourcefire de última geração e proteção avançada contra malware em um único dispositivo, agora a Cisco oferece um conjunto abrangente de serviços de segurança de rede para:

- **Visibilidade e controle de aplicativos granulares.** Assim como outros NGFWs, a Cisco pode detectar e relatar sobre conexões de aplicativo e aplicar políticas de controle granulares com base nos usuários, grupos, dispositivos etc. Agora, com o FirePOWER, a Cisco provavelmente ampliará sua visibilidade e controle de aplicativos em toda a rede e integrará esses recursos com outros ativos da empresa, como TrustSec e seu Identity Services Engine (ISE).

- **Proteção centralizada em ameaças em toda a rede e endpoints.** A arquitetura de segurança de rede da Cisco inclui proteção abrangente contra ameaças e funções avançadas de detecção/prevenção de malware com o uso do FirePOWER para proteção de rede e FireAMP para cobertura de segurança de endpoint. A detecção/prevenção de ameaças fica ainda melhor com o FirePOWER NGIPS, a filtragem de URLs com base na reputação e na categoria e sua inteligência de ameaças de amplo alcance. O FireAMP também pode acompanhar a atividade de endpoint para análise histórica. Quando um novo arquivo de malware é descoberto, o FireAMP pode aplicar políticas de segurança retrospectivas para identificar e corrigir endpoints que encontraram o arquivo antes. Por fim, a Cisco combina eventos de IPS, inteligência de ameaças e eventos de malware para fornecer IoCs detalhados que podem ajudar a equipe de segurança a aprimorar ou automatizar investigações de segurança e processos de correção.
- **Vários serviços de segurança com visibilidade de ponta a ponta.** Agora, a Cisco tem um portfólio completo de serviços de segurança física e virtual para firewalls, controle de aplicativos, IDS/IPS, filtragem de URLs, detecção/prevenção avançada de malwares etc. Com isso, as empresas podem personalizar sua proteção em camadas para os usuários, aplicativos, segmentos de rede e fluxos de rede com o uso de vários formatos e cobertura de todos os locais de rede. A Cisco também fornece monitoramento e visibilidade em todos esses serviços/locais para eliminar pontos cegos.
- **Avaliação do impacto.** A arquitetura de segurança de rede da Cisco foi projetada para correlacionar eventos de invasão ao possível impacto que um ataque pode ter em um determinado alvo. A Cisco exibe essa correlação por meio de uma série de cinco diferentes “sinalizadores de impacto”. Um sinalizador de impacto classificado como número um indica um evento que corresponde a uma vulnerabilidade mapeada para um determinado host que requer atenção imediata, enquanto outros sinalizadores de impacto têm prioridades mais baixas. Dessa forma, a Cisco pode ajudar os profissionais de segurança que já estão sobrecarregados a determinar onde aplicar seus escassos recursos, aprimorando a proteção de segurança e a eficiência operacional.

A Cisco acredita que a combinação do ASA e FirePOWER pode melhorar a segurança na sequência de ataques antes, durante e depois de um ataque de segurança. Na fase “antes”, a arquitetura de segurança de rede da Cisco pode ser usada para descobrir ativos de rede, aplicar políticas de segurança e fortalecer controles para proteção aprimorada. Na fase “durante”, o ASA e o FirePOWER podem ser usados para detectar atividades mal-intencionadas/suspeitas (nas redes e endpoints), bloquear conexões de rede e assim defender a rede como um todo. Por fim, a arquitetura de segurança de rede da Cisco pode agregar valor no período “depois” ao ajudar os analistas de segurança a na identificação do impacto de uma violação, modificação dos controles de contingência e aproveitamento de dados de análise para acelerar os processos de correção.

A Cisco sabe que ainda há trabalho a fazer e tem muitos recursos de arquitetura adicionais em seu roteiro de 12 a 18 meses. A Cisco também sabe que muitos CISOs vão precisar de ajuda para avaliar suas defesas de segurança de rede atuais e criar um plano para desenvolver uma arquitetura de segurança de rede. Alguns serviços específicos são oferecidos pela Cisco para ajudar as empresas nessas áreas.

A grande verdade

Alguns fatos sobre segurança digital amplamente difundidos:

1. A TI está cada vez mais complexa, acionada pela virtualização, mobilidade e computação em nuvem.
2. O cenário de ameaças é cada vez mais perigoso e os ataques direcionados são particularmente difíceis de prevenir, detectar e corrigir.
3. As defesas de segurança de rede antigas são menos eficazes do que eram antes.
4. Muitas empresas carecem de habilidades de segurança de rede em uma ou mais áreas.

Em geral, isso representa um panorama assustador no qual o risco para a segurança cibernética aumenta diariamente.

Como Albert Einstein disse certa vez, “A definição de insanidade é fazer a mesma coisa várias vezes e esperar resultados diferentes”. Sábias palavras, mas isso é exatamente o que muitos CISOs fazem quando se trata da segurança de rede. É hora de os líderes de negócios, TI e segurança perceberem que estão em uma batalha perdida. Os criminosos cibernéticos usam novos tipos de armas e táticas ofensivas, para que as empresas tenham que combater essa ofensiva com novos tipos de defesa que possam ajudá-las a aprimorar a proteção, a detecção e a resposta.

O ESG acredita que esses aprimoramentos não virão de alterações táticas incrementais para defesas de segurança de rede antigas. Em vez disso, as empresas precisam avançar com uma mudança mais estratégica: uma arquitetura integrada de segurança de rede de ponta a ponta. A combinação de recursos da Cisco e da Sourcefire ofereceu possibilidades interessantes com a fusão em 2013. Agora que a Cisco integrou o melhor do firewall ASA, FirePOWER NGIPS, proteção avançada contra malware e sua inteligência contra ameaças coletiva, a Cisco pode estabelecer um novo patamar de liderança com sua arquitetura integrada de segurança de rede.