13 COISAS QUE SEU PRÓXIMO FIREWALL DEVE FAZER

A rápida evolução da TI mudou a cara do perímetro da rede. Os dados e usuários estão em toda parte. Os dispositivos estão proliferando mais rapidamente do que a maioria das organizações consegue acompanhar. Ao mesmo tempo, as equipes de TI estão adotando a nuvem, a análise de big data e a automação para acelerar a entrega de novos aplicativos para impulsionar o crescimento dos negócios. Enquanto isso, os aplicativos estão cada vez mais acessíveis. O resultado é uma rede incrivelmente complexa que apresenta um risco significativo para os negócios. As organizações devem minimizar esse risco sem diminuir o ritmo de seus negócios.

A segurança cibernética não está conseguindo acompanhar o ritmo, pois os ataques continuam a prejudicar os negócios. Gastar em segurança parece interminável, e a redução do risco não é clara. A implantação de ferramentas e tecnologias diferentes e não integradas deixa seus negócios expostos a ameaças. As ferramentas de segurança que não foram desenvolvidas para a automação exigem que os analistas agrupem manualmente insights de várias fontes dissociadas antes de tomar providências. Precisamos de outra abordagem.

Começa com uma plataforma de firewall de última geração como a base de uma estratégia de segurança de rede eficaz. Com uma arquitetura focada em prevenção, as equipes de segurança podem adotar facilmente as práticas recomendadas para evitar ataques bem-sucedidos, usar automação e análise para reduzir o esforço manual, substituir produtos pontuais desconectados e implantar inovações estreitamente integradas que fortalecem e simplificam a segurança.

Este documento descreve a evolução do firewall para "última geração" e destaca as treze principais ações que um firewall de última geração (NGFW) deve fazer para proteger sua rede e seus negócios.

Inicialmente, os firewalls de inspeção com informações de estado classificavam o tráfego observando apenas a porta de destino, como a porta TCP 80 para HTTP. À medida que surgiu a necessidade de conscientização do aplicativo, muitos fornecedores incluíram visibilidade de aplicativos e outros "blades" de software ou hardware em seus firewalls de inspeção com informações de estado, que eles venderam posteriormente como ofertas de gerenciamento unificado de ameaças (sigla em inglês: UTM). No entanto, como suas funções foram adaptadas (não nativamente integradas) os UTMs não melhoraram a segurança.

Ao contrário das ofertas de UTM, os NGFWs reconhecem os aplicativos e tomam decisões com base no aplicativo, no usuário e no conteúdo. O design integrado melhora a segurança e simplifica as operações. Dado o sucesso do modelo, o termo "NGFW" agora é sinônimo de "firewall".

Os critérios de seleção do NGFW normalmente se enquadram em três áreas: funções de segurança, operações e desempenho. As funções de segurança correspondem à eficácia dos controles de segurança e à capacidade de sua equipe de gerenciar o risco associado aos aplicativos que atravessam sua rede, sem diminuir ao ritmo dos negócios. Do ponto de vista operacional, a política de aplicativos deve ser acessível e simples de gerenciar, aplicando a automação para reduzir o esforço manual, para que as equipes de segurança possam se concentrar em atividades de alto valor. Os critérios de desempenho são simples: o firewall precisa fazer o que deve fazer no rendimento necessário para suas necessidades de negócios. Como parte disso, as últimas inovações devem ser estreitamente integradas e fáceis de serem adotadas. Embora os requisitos e prioridades variem dentro desses critérios, há treze coisas que seu próximo firewall deve fazer.

Até o final de 2019, 90% das conexões de Internet corporativa para a base instalada serão protegidas por firewalls de última geração.[1]

Requisitos do NGFW

1. Identifique aplicativos independentemente de porta, protocolo, táticas evasivas ou criptografia.
2. Identifique usuários, independentemente de dispositivo ou endereço IP.
3. Faça a decriptação do tráfego criptografado.
4. Proteja em tempo real contra ameaças conhecidas e desconhecidas incorporadas em aplicativos.
5. Entregue uma taxa de transferência em linha previsível e com vários gigabits.

1. Identificar usuários e permitir um acesso adequado

O problema

Funcionários, clientes e parceiros conectam-se a diferentes repositórios de informações dentro de sua rede, bem como da Internet. Essas pessoas e seus diversos dispositivos representam os usuários da sua rede. É importante para a postura de risco da sua organização identificar seus usuários além do endereço IP, bem como compreender os riscos inerentes que eles trazem com base nos dispositivos que estão usando, especialmente quando as políticas de segurança foram contornadas ou novas ameaças foram introduzidas à sua rede. Além disso, os usuários estão constantemente mudando para diferentes locais

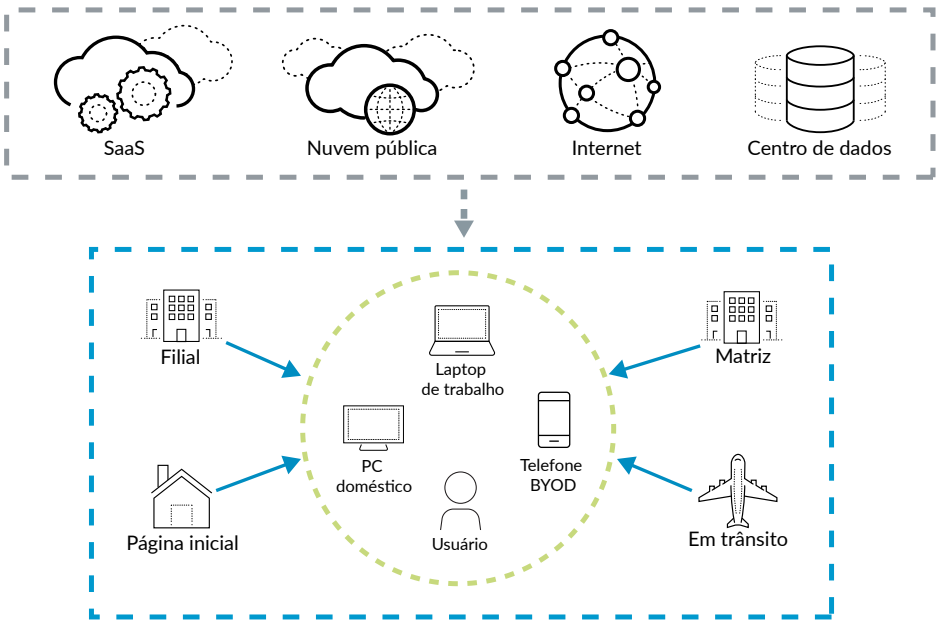

Figura 1: Os usuários acessam dados de diferentes dispositivos e locais

1. Adam Hils, Jeremy d'Hoinne, Rajpreet Kaur, "Quadrante mágico para firewalls de rede corporativa", Gartner, 10 de julho de 2017.

físicos e usando vários dispositivos, sistemas operacionais e versões de aplicativos para acessar os dados que precisam. As sub-redes de endereços IP são mapeadas apenas para locais físicos, não para usuários individuais, o que significa que, se os usuários mudarem de lugar, mesmo dentro do escritório, a política não os seguirá.

Abordando o problema

As informações sobre usuários e grupos devem estar diretamente integradas às plataformas de tecnologia que protegem as organizações modernas. Seu próximo firewall deve ser capaz de extrair a identidade do usuário de várias fontes, incluindo VPN, controladores de acesso à WLAN, servidores de diretório, servidores de e-mail e portais cativos. Saber quem está usando os aplicativos em sua rede e quem está transmitindo uma ameaça ou transferindo arquivos fortalece as políticas de segurança e melhora os tempos de resposta a incidentes. O firewall deve permitir que as políticas habilitem com segurança aplicativos baseados em usuários ou grupos de usuários, de saída ou de entrada, por exemplo, permitindo que apenas o departamento de TI use ferramentas como SSH, telnet e FTP. As políticas baseadas no usuário seguem os usuários, em qualquer lugar (na sede, nos escritórios remotos ou em casa) e em qualquer dispositivo que usem. No entanto, o problema de identidade do usuário vai além da classificação de usuários para relatórios de políticas.

2. Impedir roubo e abuso de credenciais corporativas

O problema

Os usuários e suas credenciais estão entre os links mais fracos da infraestrutura de segurança de uma organização. De acordo com o relatório sobre investigações de violação de dados de 2017 da Verizon, no período de doze meses abordado no relatório, 81% das violações relacionadas a hackers se aproveitaram de senhas roubadas e/ou fracas.[2] Com credenciais roubadas como parte de seu conjunto de ferramentas, aumentam as chances de violação bem-sucedida por invasores e o risco de eles serem pegos diminui. Para evitar o roubo de credenciais, a maioria das organizações depende da educação dos funcionários, que é suscetível a erros humanos por natureza. Os produtos de tecnologia geralmente dependem da identificação de sites de phishing conhecidos e da filtragem de e-mails.

Figura 2: Conclusões da Verizon 2017 DBIR sobre senhas comprometidas

No entanto, esses métodos, às vezes, podem ser contornados; a verificação de sites conhecidos maliciosos não leva em conta os recém-criados, e os invasores podem evadir a tecnologia de filtragem de e-mail enviando links por meio das mídias sociais. Os invasores podem facilmente roubar credenciais por meio de phishing, malware, engenharia social ou força bruta, e podem até comprá-las no mercado negro. Os invasores usam essas credenciais para obter acesso a uma rede, movimentar-se lateralmente e escalar seus privilégios para acesso não autorizado a aplicativos e dados.

Abordando o problema

As organizações devem procurar um firewall com análise baseada em aprendizado de máquina para identificar sites que roubam credenciais. Se a análise identificar um site como malicioso, o firewall deverá ser atualizado e bloqueará o site. Ainda assim, sempre haverá sites de phishing novos, nunca vistos antes, que são tratados como "desconhecidos". Seu próximo firewall deve permitir que você bloqueie o envio de credenciais corporativas para sites desconhecidos. O firewall também deve permitir que você proteja dados e aplicativos confidenciais aplicando a autenticação multifatorial (sigla em inglês: MFA) para impedir que invasores abusem de credenciais roubadas. Ao integrar fornecedores comuns de MFA, seu firewall pode proteger seus aplicativos que contêm dados confidenciais, incluindo aplicativos antigos.

3. Ativar com segurança todos os aplicativos e funções de controle

O problema

Mais e mais aplicativos, como aplicativos de mensagens instantâneas, compartilhamento de arquivos ponto a ponto ou VoIP, são capazes de operar em portas não padrão ou em portas em hopping. Além disso, os usuários estão acessando diversos tipos de aplicativos, incluindo aplicativos de software com um serviço (sigla em inglês: SaaS), de vários dispositivos e locais. Alguns desses aplicativos são autorizados, alguns são tolerados e outros não são autorizados, e os usuários são cada vez mais experientes para forçar a execução de aplicativos em portas fora do padrão por meio de protocolos como RDP e SSH. Além disso, os novos aplicativos fornecem aos usuários conjuntos ricos de funções que ajudam a garantir a fidelidade do usuário, mas podem representar diferentes perfis de risco. Por exemplo, o WebEx® é uma ferramenta de negócios valiosa, mas usar o compartilhamento de área de trabalho WebEx para assumir o controle da área de trabalho de um funcionário de uma fonte externa pode ser uma violação de conformidade interna ou regulamentar. O Gmail® e o Google Drive são outro bom exemplo. Depois que os usuários fizerem login no Gmail, o que pode ser permitido pela política, eles poderão alternar facilmente para o YouTube® ou o Google Photos, o que pode não ser permitido. Os administradores de segurança desejam ter controle total sobre o uso desses aplicativos e definir políticas para permitir ou controlar determinados tipos de aplicativos e funções de aplicativos, ao mesmo tempo que negam a outros.

2. "Relatório sobre investigações de violação de dados de 2017", Verizon, 2017, www.knowbe4.com/hubfs/rp_DBIR_2017_Report_execsummary_en_xg.pdf.

Abordando o problema

Seu próximo firewall deve classificar o tráfego por aplicativo em todas as portas, o tempo todo, por padrão, e não deve sobrecarregá-lo com a pesquisa de portas comuns usadas por cada aplicativo. O firewall deve fornecer visibilidade completa do uso do aplicativo junto com os recursos para entender e controlar seu uso (consulte a Figura 3). Por exemplo, ele deve entender o uso de funções do aplicativo, como transmissão de áudio, acesso remoto e publicação de documentos, e ser capaz de aplicar controles granulares sobre esse uso, como permissões de download e de upload, transferência de arquivos

Figura 3: Controlar o uso de aplicativos em política

e chat, e assim por diante. Isso deve ser feito continuamente. O conceito de classificação de tráfego "one-and-done" não é uma opção, pois ignora o fato de que esses aplicativos comumente usados compartilham sessões e suportam múltiplas funções. Se uma função ou um recurso diferente for introduzido na sessão, o firewall deverá executar uma verificação de política novamente. Seu próximo firewall deve ter rastreamento de estado contínuo para entender as funções que cada aplicativo pode suportar (e os diferentes riscos associados).

4. Preencher lacunas perigosas de políticas

O problema

Os firewalls antigos permitem e bloqueiam o tráfego com base em portas e endereços IP. Essa abordagem é inadequada, pois as regras baseadas em porta permitem aplicativos bons e ruins por meio do firewall. Os aplicativos podem passar facilmente por um firewall baseado em porta, alternando entre portas, usando SSL e SSH, ou usando portas abertas conhecidas, como 80 e 443. Com o tempo, os clientes acumulam milhares de regras baseadas em porta em seus firewalls e geralmente migram essas regras como estão para os firewalls de última geração. Essas regras deixam lacunas perigosas na política. Os clientes percebem que precisam migrar para regras baseadas em aplicativos para obter segurança eficaz, mas isso exige um esforço manual significativo; e, devido à escassez de habilidades em segurança cibernética, a maioria das organizações não possui os recursos. Isso se torna um alto risco de segurança que pode causar uma interrupção nos negócios. De fato, de acordo com o Gartner, até 2023, 99% das violações de firewall serão causadas por erros de configuração do firewall, não por falhas no firewall.[3]

Abordando o problema

Ao avaliar seu próximo firewall, procure um que reduza a complexidade do gerenciamento de regras e políticas. Isso começa com mostrar a você quais aplicativos estão sendo executados em sua rede, mapeando-os para as regras antigas e ajudando a substituir essas regras. Um NGFW deve ajudar sua equipe de segurança a substituir facilmente as regras antigas por políticas intuitivas e baseadas em aplicativos. Como as regras baseadas em ID de aplicativo são fáceis de criar, entender e modificar à medida que as necessidades de negócios evoluem, elas minimizam os erros de configuração que o deixam vulnerável a violações de dados. Essas políticas fortalecem a segurança e levam significativamente menos tempo para gerenciar.

Figura 4: Conclusões do Google 2019 sobre tráfego criptografado[4]

5. Proteger o tráfego criptografado

O problema

A maior parte do tráfego da web corporativa agora é criptografada e os invasores exploram a criptografia para ocultar ameaças de dispositivos de segurança. Isso significa que mesmo empresas com medidas de segurança abrangentes e maduras

3. Rajpreet Kaur, Adam Hils, John Watts, "Insight de tecnologia para gerenciamento de política de segurança de rede", Gartner, 21 de fevereiro de 2019,www.gartner.com/doc/3902564/technology-insight-network-security-policy.
4. "Relatório de transparência do Google: criptografia HTTPS na Web", Google, acessado em 8 de março de 2019, transparencyreport.google.com/https/overview?hl=en.

podem ser violadas se não estiverem monitorando o tráfego criptografado. Além disso, o SSH é usado quase que universalmente, e os usuários finais podem configurá-lo facilmente para esconder atividades não relacionadas ao trabalho.

Abordando o problema

A capacidade de fazer a decriptação SSL e SSH é uma função básica de segurança. Os principais elementos a serem procurados incluem reconhecimento e decriptação em qualquer porta, entrada ou saída; controle de políticas sobre decriptação; e os elementos de hardware e software necessários para executar a decriptação em dezenas de milhares de conexões SSL simultâneas com desempenho previsível. No entanto, seu próximo firewall deve ser flexível o suficiente para fazer a decriptação com facilidade de determinados tipos de tráfego criptografado (como HTTPS de sites não classificados) por meio de políticas, enquanto outros tipos, como tráfego da Web de organizações de serviços financeiros conhecidas, são deixados em paz em conformidade com os padrões de privacidade. Um firewall de última geração deve aplicar segurança e balanceamento de carga a fluxos decriptografados em várias pilhas de dispositivos de segurança para aplicação adicional. Isso elimina os descarregadores de SSL dedicados, reduzindo a complexidade da rede e simplificando a operação de decriptação. Leia **Decriptação: Por que, onde e como** para obter uma visão geral detalhada deste importante recurso.

6. Interromper as ameaças avançadas para impedir ataques cibernéticos bem-sucedidos

O problema

A maioria dos malwares modernos (incluindo variantes de ransomware) usa técnicas avançadas, como encapsular cargas maliciosas em arquivos legítimos ou compactar arquivos para evitar a detecção, para transportar ataques ou explorações por meio de dispositivos e ferramentas de segurança de rede. À medida que as organizações implantam cada vez mais áreas limitadas de proteção virtuais para análises dinâmicas, os invasores evoluíram para se concentrar em maneiras de evadi-las. Eles empregam técnicas que fazem varredura de atividades válidas do usuário, configurações do sistema ou indicadores de tecnologias de virtualização específicas. Com o crescimento do submundo do crime cibernético, qualquer invasor, novato ou avançado, pode adquirir ameaças plug-and-play criadas para identificar e evitar ambientes de análise de malware.

Abordando o problema

Seu firewall, usando serviços de segurança integrados, deve bloquear automaticamente as ameaças conhecidas. As ameaças

Figura 5: Interrupção em todas as etapas para impedir ataques bem-sucedidos

desconhecidas também precisam ser analisadas e combatidas automaticamente. Sua organização precisa de um serviço que procure ameaças em todos os pontos do ciclo de vida do ataque cibernético, e não apenas quando as ameaças entrarem pela primeira vez na rede. Bloquear tipos de arquivos conhecidos e arriscados ou acessar URLs maliciosos, antes que eles comprometam sua rede, reduz a exposição a ameaças. Seu firewall deve protegê-lo contra explorações de vulnerabilidades, malware e atividades de comando e controle (C2) conhecidas, sem exigir que você gerencie ou mantenha vários dispositivos de função única. As assinaturas devem ser atualizadas automaticamente assim que um novo malware for encontrado, mantendo você protegido, ao mesmo tempo em que permite que as equipes de segurança e resposta a incidentes se concentrem nas coisas importantes.

Um firewall de última geração que utiliza vários métodos de análise para detectar ameaças desconhecidas, incluindo análise estática com aprendizado de máquina, análise dinâmica e análise bare-metal, é capaz de descoberta de alta fidelidade e resistente à evasão. Em vez de usar assinaturas baseadas em atributos específicos, os firewalls devem usar assinaturas baseadas em conteúdo para detectar variantes, malware polimórfico ou atividade C2. Além disso, as assinaturas C2 baseadas na análise de padrões de comunicação de saída são medidas protetivas muito mais eficazes que podem ser dimensionadas na velocidade da máquina quando criadas automaticamente. Finalmente, a infraestrutura de segurança entregue na nuvem é fundamental para a aplicação da segurança. Ela oferece suporte à detecção e à prevenção de ameaças em grande escala em toda a sua rede, endpoints e nuvens, além de permitir que você explore um ecossistema aberto de inovadores confiáveis.

7. Interromper ataques que usam DNS

O problema

O DNS é um canal massivo, muitas vezes negligenciado, que pode ser usado para a entrega de malware, C2 e transferência não autorizada de dados. Os adversários aproveitam a natureza difundida do DNS para abusar dele em vários pontos de um

ataque. De acordo com a equipe de pesquisa de ameaças, a Unit 51 da Palo Alto Networks, quase 80% dos malwares usam o DNS como forma de estabelecer comunicação com um servidor C2. Os invasores estabelecem canais confiáveis de comando que são difíceis de derrubar ou identificar, já que o DNS é uma forma confiável de manter uma conexão com os servidores DNS. Depois que uma conexão for estabelecida, os invasores podem usar o tráfego de DNS para entregar malware em uma rede ou fazer o encapsulamento de dados. Além disso, os invasores desenvolvem algoritmos de geração de domínio (sigla em inglês: DGAs), que criam automaticamente milhares de domínios maliciosos que podem ser usados para o C2. À medida que os adversários automatizam cada vez mais seus ataques, torna-se quase impossível identificar e bloquear essas ameaças.

Abordando o problema

Sua organização não pode simplesmente colocar na lista negra os ataques que usam o DNS, pois essa tática geralmente depende de feeds de ameaça relativamente estáticos que funcionam em domínios maliciosos conhecidos. Sem a análise, é impossível prever domínios maliciosos altamente dinâmicos. A interrupção de ataques que usam DNS exige um firewall de última geração que possa aplicar análise preditiva e aprendizado de máquina para identificar domínios maliciosos desconhecidos dinamicamente.

8. Proteja sua evolutiva força de trabalho móvel

O problema

A força de trabalho móvel continua a crescer, juntamente com o uso de dispositivos móveis para se conectar a aplicativos de negócios, muitas vezes por meio de redes públicas e dispositivos que estão abertos a ameaças avançadas. Isso aumenta o risco quando os usuários estão fora das instalações porque não há firewall de rede para interromper os ataques, e o problema se torna ainda mais complexo ao considerar os efeitos das práticas de nuvem e BYOD. Além disso, os locais remotos e as pequenas filiais geralmente não têm segurança consistente, pois é operacionalmente ineficiente e dispendioso enviar firewalls para eles ou o tráfego de backhaul para a sede.

Cobertura holística para todos os sistemas operacionais

Dada a investida das iniciativas de BYOD e uma força de trabalho cada vez mais móvel, a cobertura holística em ambientes e cargas de trabalho do Windows®, macOS®, Android® e Linux é essencial. A cobertura holística permite que as organizações bloqueiem com segurança malware conhecido e desconhecido, independentemente de quais sistemas operacionais seus usuários preferem.

Abordando o problema

A força de trabalho móvel e os locais remotos precisam acessar aplicativos de lugares muito além da sua rede. Eles também precisam de proteção contra ataques cibernéticos direcionados, aplicativos e sites mal-intencionados, phishing, tráfego C2 e outras ameaças desconhecidas. Isso requer segurança consistente. Seu próximo firewall deve habilitar os níveis necessários de visibilidade, prevenção de ameaças e aplicação de políticas de segurança para proteger seus usuários e locais distribuídos, oferecendo recursos de firewall de última geração a partir da nuvem, protegendo-os sem a necessidade de implantar hardware físico.

9. Amplie a segurança para seus ambientes de nuvem em evolução

O problema

Os dados e aplicativos residem em todos os lugares: na sua rede e na nuvem. De acordo com o RightScale 2018 State of the Cloud™, 81% das empresas usam várias nuvens públicas, privadas e/ou híbridas: cinco nuvens diferentes em média.[5] Ampliadas com ambientes SaaS, as organizações agora precisam proteger dados confidenciais na rede e uma série de ambientes de nuvem. Além disso, as ferramentas e técnicas de segurança antigas projetadas para redes estáticas não funcionam com ferramentas ou recursos nativos da nuvem. Além disso, os serviços de segurança nativos dos próprios provedores de nuvem, como o Google Cloud Platform (GCP), o Amazon Web Services (AWS®) e o Microsoft Azure®, geralmente fornecem apenas proteções de Camada 4 e são específicas desse provedor de nuvem.

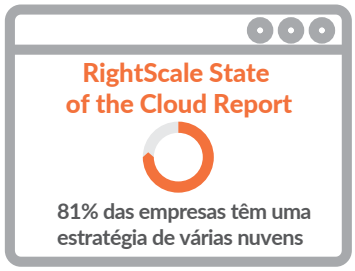

Figura 6: Conclusões da RightScale sobre estratégia de várias nuvens

Abordando o problema

Para ter sucesso, sua organização precisa de segurança na nuvem que estenda a política de forma consistente da rede para a nuvem, impeça que o malware acesse e se movimente lateralmente (Leste-Oeste) na nuvem, simplifique o gerenciamento e minimize a defasagem de política de segurança à medida que as cargas de trabalho virtuais mudam. Seu próximo firewall deve proteger os aplicativos e dados residentes com a mesma postura de segurança que você pode ter estabelecido em sua rede física. Para proteger implantações com várias nuvens, o firewall deve suportar uma série de ambientes de nuvem e virtualização, incluindo todos os principais provedores de nuvem pública e nuvens privadas virtualizadas. O firewall deve se integrar aos serviços nativos da nuvem, como o Amazon Lambda e o Azure, e às ferramentas de automação, como Ansible® e Terraform®, para integrar segurança em seus projetos de desenvolvimento primordialmente em nuvem.

5. "Relatório 2018 sobre o estado da nuvem", RightScale, 2018, www.suse.com/media/report/rightscale_2018_state_of_the_cloud_report.pdf.

10. Usar uma estratégia de Confiança Zero

O problema

Os modelos convencionais de segurança operam na suposição desatualizada de que você pode confiar em tudo na sua rede. No entanto, devido à crescente sofisticação de ataques e ameaças internas, você precisa de novas medidas de segurança para impedir que elas se espalhem quando estiverem dentro. Como os modelos tradicionais de segurança são projetados para proteger seu perímetro, as ameaças que entram em sua rede são invisíveis para eles e não são inspecionadas, livres para se transformar e movimentar para onde quiserem para extrair dados comerciais confidenciais. No mundo digital, a confiança é simplesmente uma vulnerabilidade.

Abordando o problema

Ao avaliar um firewall de última geração, considere um firewall que possa atuar como um gateway de segmentação para ativar uma arquitetura de Confiança Zero. A Confiança Zero é uma estratégia projetada em torno do conceito de que usuários, aplicativos e dados nunca podem ser confiados, que suas ações devem sempre ser verificadas em um ambiente. O principal objetivo do modelo Confiança Zero é eliminar a confiança em um sistema e impedir que invasores explorem vulnerabilidades escondidas em aplicativos confiáveis. A abordagem envolve limitar o escopo de um ataque e bloquear a movimentação lateral, aproveitando a microssegmentação com base em usuários, dados e localização. Uma plataforma de firewall de última geração deve ajudar nessas etapas, incluindo a habilitação do acesso seguro a todos os usuários, independentemente da localização, a inspeção de todo o tráfego, a aplicação de políticas para controle de acesso menos privilegiado e a detecção e prevenção de ameaças avançadas. Isso reduz significativamente os caminhos para os adversários acessarem seus aplicativos e dados mais importantes, quer eles estejam dentro ou fora da sua organização. Assista a este webinar para obter informações sobre como implementar efetivamente a Confiança Zero.

11. Manter uma política consistente entre nuvens e redes locais, remotas e móveis

O problema

Os produtos isolados de segurança normalmente vêm com seus próprios aplicativos de gerenciamento. Para configurar a segurança para cada um, os operadores de segurança devem trabalhar com diferentes dispositivos de gerenciamento. De acordo com o relatório sobre serviços de TI dos EUA de 2017 da ResearchCorp, quase 72% das organizações usam produtos de três ou mais fornecedores separados para proteger sua infraestrutura de rede.[5] Esses produtos são desconectados e não podem compartilhar insights. As organizações também acham difícil dimensionar a integração do firewall, manter políticas de segurança consistentes e implantar alterações de emergência em milhares de firewalls. Isso torna a segurança complexa e exige que as equipes de TI trabalhem à exaustão.

Abordando o problema

Você deve ser capaz de operacionalizar a implantação de políticas de segurança centralizadas e consistentes em dezenas de milhares de firewalls abrangendo implantações locais e na nuvem (incluindo locais remotos, usuários móveis e aplicativos SaaS) por meio de gerenciamento centralizado, principais tarefas de segurança consolidadas e recursos simplificados. Por exemplo, você deve ser capaz de usar um único console para visualizar todo o tráfego da rede, gerenciar a configuração, enviar políticas globais e gerar relatórios sobre padrões de tráfego ou incidentes de segurança. Seus recursos de geração de relatórios devem permitir que sua equipe de segurança explore a rede, o aplicativo e o comportamento do usuário em relação ao contexto necessário para tomar decisões embasadas.

Quando esses recursos são entregues a partir da nuvem, suas equipes podem criar a arquitetura de segurança correta para evitar ameaças conhecidas e desconhecidas em cada canto da sua rede estendida. No atual cenário evolutivo de ameaças, usar um único fornecedor de segurança para lidar com o amplo espectro de suas necessidades de segurança e negócios nem sempre é prático. Nesse caso, a capacidade de se integrar e consumir insight e inovação de terceiros é fundamental. Ao avaliar futuros fornecedores de segurança, certifique-se de avaliar a extensibilidade e a programação do que eles oferecem.

12. Automatizar tarefas de rotina e se concentrar nas ameaças que importam

O problema

Uma pesquisa do Enterprise Strategy Group descobriu que 51% dos profissionais de segurança cibernética acham que sua organização tem um problemático déficit de qualificação em segurança cibernética.[6] Isso é agravado pela dependência de muitos processos manuais para operações rotineiras de segurança, como perseguir dados, investigar alertas falsos positivos e gerenciar correção. Analisar e correlacionar manualmente o grande número de eventos de segurança diminui a mitigação, aumenta a chance de erro e é difícil de dimensionar. As equipes de segurança podem facilmente se perder no volume de alertas e perder as ações críticas e acionáveis. Isso é exacerbado por uma iminente escassez de profissionais qualificados em segurança cibernética. Embora a análise de big data descubra padrões ocultos, correlações e outros insights para fornecer inteligência às equipes de segurança, você ainda precisa dos dados corretos. Esses dados devem ser originados em todos os lugares (redes, endpoints, aplicativos SaaS, nuvens públicas, nuvens privadas, data centers, etc.) e estar prontos para análises.

Ao usar uma análise precisa para direcionar a automação, você pode operar facilmente as práticas recomendadas de

6. "Relatório sobre serviços de TI dos EUA de 2017", ResearchCorp.org, 2017, www.fidelus.com/wp-content/uploads/2017/12/researchcorp-fidelus_us_it_servicesreport_full_report.pdf.

segurança, como a Confiança Zero, acelerar as tarefas rotineiras e focar nas prioridades de negócios, seja agilizando a entrega de aplicativos, melhorando processos ou caçando ameaças. Há três maneiras de pensar sobre automação:

- **Automação de fluxo de trabalho:** o firewall deve expor APIs padrão para que ele possa ser programado a partir de outras ferramentas e scripts que você possa estar usando. Na nuvem, ele deve se integrar a ferramentas como Ansible e Terraform. Além disso, o firewall deve ser capaz de iniciar fluxos de trabalho em outros dispositivos no ecossistema de segurança, usando suas APIs, sem intervenção manual.
- **Automação de políticas:** o firewall deve ser capaz de adaptar políticas a quaisquer alterações em seu ambiente, como a movimentação de aplicativos em máquinas virtuais. Ele também deve ser capaz de absorver inteligência de ameaças de fontes de terceiros e agir automaticamente com essa inteligência.
- **Automação de segurança:** seu ambiente deve ser capaz de descobrir ameaças desconhecidas e entregar proteções para o firewall para que novas ameaças sejam bloqueadas automaticamente.

Figura 7: Conclusões da ResearchCorp 2018 sobre vários fornecedores para segurança de rede

Algumas ameaças ficam escondidas em dados. Ao analisar mais profundamente esses dados nos locais e tipos de implantação, você pode encontrar ameaças que podem estar escondidas. Com a automação, você pode identificar ameaças com precisão, habilitar a prevenção rápida, melhorar a eficiência, aproveitar melhor o talento de sua equipe especializada e melhorar a postura de segurança de sua organização.

Figura 8: Conclusões da Cybersecurity Ventures sobre empregos de segurança cibernética

13. Consumir inovações de segurança facilmente

O problema

Consumir inovação em segurança cibernética é difícil. As organizações perdem tempo implantando hardware ou software adicional toda vez que querem aproveitar uma nova tecnologia de segurança. Elas investem mais recursos gerenciando sua infraestrutura de segurança em constante expansão, em vez de melhorar seus controles de segurança para ficar à frente dos invasores e bloquear ameaças.

Abordando o problema

À medida que aumenta o número de funções de segurança necessárias, há duas opções: adicionar mais produtos pontuais independentes ou usar um dispositivo existente para suportar novos recursos. Se o seu firewall puder atuar como um sensor e um ponto de aplicação para a tecnologia de terceiros, você poderá adotar rapidamente as últimas inovações de segurança sem implantar ou gerenciar novos e infindáveis dispositivos. Seu próximo firewall deve permitir que as equipes descubram, avaliem e usem novas tecnologias de segurança rapidamente. As equipes de segurança devem ser capazes de colaborar entre diferentes aplicativos, compartilhar inteligência e contexto de ameaças, e direcionar resposta e aplicação automatizadas com aplicativos profundamente integrados. Dessa forma, elas podem resolver os casos de uso de segurança mais desafiadores com a melhor tecnologia disponível, e podem fazer isso sem o custo ou a carga operacional de implantar nova infraestrutura para cada nova função. Assista a este vídeo para saber como uma plataforma de segurança contínua, aberta e integrada, baseada em inteligência artificial, pode ajudar você a descobrir novos aplicativos e recursos inovadores.

Você está pronto para avaliar seu próximo firewall? Faça um **Ultimate Test Drive**.

3000 Tannery Way
Santa Clara, CA 95054

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

www.paloaltonetworks.com