RESUMO DA SOLUÇÃO

A Geração da Nuvem: Uma Combinação Problemática de Desafios de Segurança

Symantec™

Introdução

À medida que a adoção da nuvem fica mais rápida e nos acostumamos com a simplicidade, flexibilidade e vantagens de custo do modelo de nuvem, não devemos perder de vista um fato importante: A Segurança para a Geração da Nuvem não é nada simples.

O crescimento explosivo do número de usuários de dispositivos móveis, aplicativos na nuvem, escritórios remotos e requisitos de conformidade, combinados com uma série de ameaças de segurança emergentes, criou uma combinação extremamente complexa que está desafiando os limites das equipes de segurança e operações de rede.

A verdade é que os modelos de segurança legados não funcionam bem para a Geração da Nuvem. As abordagens tradicionais de backhauling para segurança de rede – que encaminham o tráfego da Internet de locais remotos e usuários de dispositivos móveis ao data center corporativo, onde as políticas de conformidade de dados e segurança são aplicadas – são desatualizadas, lentas e ineficientes.

O que você precisa é uma abordagem mais simples, otimizada e completa, focada em alguns conceitos principais:

Vá além das funções básicas de segurança de aplicativos na Web e na nuvem

Muitas organizações dependem de secure web gateways (SWGs) para executar as funções básicas de segurança na Web e na nuvem: filtragem de URLs, imposição de políticas de uso, fluxo seguro de dados para aplicativos da Web e na nuvem e varredura e orquestração de tráfego criptografado.

No entanto, a Geração da Nuvem exige muito mais funcionalidades de seus SWGs.

Ao analisar um SWG baseado na nuvem, procure um serviço que

- Inspecione de forma seletiva o tráfego criptografado com protocolo SSL/TLS para fazer uma varredura detalhada do conteúdo em busca de malware
- Use técnicas avançadas, como isolamento da Web, para bloquear ameaças e ataques de phishing direcionados aos navegadores da Web dos colaboradores
- Faça a varredura do conteúdo com serviços de prevenção de perda de dados (DLP) para evitar vazamentos de dados
- Proteja os aplicativos na nuvem através de controles CASB (Cloud Access Security Broker) para proteger os dados com interações em nuvens públicas
- Integre-se à proteção contra ameaças instalada em seus endpoints
- Direcione facilmente o tráfego remoto para a segurança na nuvem através de dispositivos SD-WAN opcionais e equipamentos similares

Symantec Web Security Service: Criado para a Geração da Nuvem

O Symantec Web Security Service oferece um amplo conjunto de recursos de segurança e proteção contra ameaças a partir da nuvem. Suportado por uma robusta infraestrutura na nuvem e pela força e alcance de nossa rede global de inteligência, o Symantec Web Security Service protege seus dados confidenciais, onde quer que estejam. A Symantec é líder em soluções da Geração da Nuvem e trabalha para garantir que seus aplicativos na Web e na nuvem sejam produtivos, seguros e em conformidade com as regulamentações.

Gerencie riscos e mantenha a conformidade à medida que suas operações mudam para a nuvem

A gestão de riscos regulatórios apresenta sérios desafios. Garantir a conformidade exige visibilidade e comando de dados confidenciais, onde quer que estejam. Isso é especialmente desafiador quando os documentos são facilmente compartilhados em aplicativos na nuvem, especialmente quando alguns desses aplicativos são adotados diretamente por funcionários que contornaram o processo de aprovação de TI.

Os recursos do CASB (Cloud Access Security Broker) oferecem visibilidade em todos os aplicativos na nuvem usados por seus colaboradores. Com essa visibilidade, você pode tomar ações para garantir que o uso de aplicativos na nuvem esteja em conformidade com as políticas da empresa e que os dados confidenciais sejam protegidos de forma adequada.

Ao analisar uma solução de CASB, busque uma que

- Identifique com precisão os aplicativos na nuvem usados por seus colaboradores
- Forneça ferramentas e dados para avaliar os riscos do uso desses aplicativos na nuvem
- Controle o acesso aos aplicativos na nuvem por usuário, grupo, local, etc.

Resolva o dilema de desempenho e custo

Multiprotocol Label Switching (MPLS) é uma técnica de transferência de dados para redes de alta velocidade. Os links MPLS oferecem desempenho que muitas vezes os tornam a opção preferencial para o backhauling do tráfego de Internet de outras unidades aos data centers corporativos principais, nos quais as políticas de segurança e proteção contra ameaças são aplicadas. No entanto, o backhauling de tráfego em links privados de MPLS, considerando o grande crescimento do tráfego de aplicativos na Web e na nuvem, é um custo que está ficando inviável.

Além disso, o backhauling adiciona latência significativa às transações de aplicativos na Web e na nuvem, resultando em velocidades lentas e uma experiência de usuário ruim para os colaboradores de outras unidades, além de uma experiência potencialmente pior para os trabalhadores que usam dispositivos móveis.

E o backhauling não é o único fator que contribui para o fraco desempenho da rede. A inspeção SSL, exigida para tarefas como o bloqueio de malware oculto no tráfego criptografado, também adiciona latência. A interceptação e decodificação exigem muito da CPU e, quando executadas de forma ineficiente com um dispositivo inadequado (pense em um firewall de próxima geração), impacta negativamente o desempenho em até 80% (segundo a **pesquisa do NSS Labs**).

Para concluir, a Geração da Nuvem também apresenta um conjunto exclusivo de problemas de desempenho nos endpoints. À medida que usuários acessam cada vez mais conteúdo de locais remotos com laptops e smartphones, são necessários mais agentes para ampliar a segurança de cada dispositivo conectado. Cada agente quer uma fatia da memória do dispositivo; isso acaba se acumulando, prejudicando o desempenho e reduzindo a velocidade de conectividade que já não era ideal.

É muito arriscado conceder aos usuários acesso direto à Web e à nuvem, ignorar a necessidade de segurança da informação e inspeção para prevenção de ameaças. No entanto, a maneira antiga – backhauling do tráfego e uso excessivo da capacidade de agentes – é cara, lenta e não é sustentável.

A nuvem criou uma combinação problemática de desafios. Ainda bem que a nuvem também é o local onde você pode encontrar as respostas para suas preocupações de desempenho.

Veja como os serviços de segurança fornecidos na nuvem melhoram o desempenho:

- Os serviços de segurança fornecidos na nuvem eliminam a necessidade de backhaul de tráfego para aplicação de políticas de segurança; esses serviços podem ser acessados diretamente por seus colaboradores remotos, portanto, as políticas são aplicadas à medida que o tráfego é transmitido aos aplicativos na Web e na nuvem.
- Os serviços de segurança na nuvem oferecem recursos pré-integrados, como prevenção contra perda de dados, sandbox, isolamento e CASB, sendo projetados para trocar dados com facilidade entre si; uma transferência de dados eficiente com "handoffs" otimizados significa menor latência e melhor experiência do usuário.
- Da mesma forma, alguns serviços de segurança na nuvem são projetados para inspecionar com rapidez e eficiência o tráfego criptografado com protocolo SSL, fornecendo a proteção que você precisa com o desempenho que seus usuários exigem.

Nem todos os serviços de segurança fornecidos na nuvem melhoram o desempenho com a mesma eficiência. Ao avaliar serviços, procure aqueles hospedados em uma infraestrutura na nuvem projetada para escalabilidade e alto desempenho. Certifique-se que os serviços usem recursos como peering de conteúdo para melhorar a latência com o Office 365, por exemplo, e otimização da janela TCP para incrementar o desempenho ao transmitir arquivos grandes com o Box e outros aplicativos de armazenamento na nuvem.

Gerencie suas políticas de segurança com eficiência

Para finalizar, à medida que os requisitos regulatórios e exigências corporativas evoluem rapidamente, vale a pena ter uma estrutura flexível que permita definir e implementar rapidamente políticas de segurança. Certifique-se que você pode migrar de forma simples suas políticas existentes nas instalações locais para sua nova segurança fornecida na nuvem. Se você possui um ambiente de segurança híbrido, local e na nuvem, busque um gerenciamento unificado de políticas para definir políticas somente uma vez e enviá-las para todos os seus gateways de segurança, onde quer que estejam.

Confie na sua solução de gerenciamento de políticas para

- Simplificar a transição da sua organização para uma segurança baseada na nuvem
- Criar e gerenciar políticas consistentes em todos os gateways
- Maximizar seu investimento existente na criação de políticas

Sobre a Symantec

A Symantec Corporation (NASDAQ: SYMC) é líder mundial em soluções de cibersegurança e ajuda organizações, governos e indivíduos a proteger seus dados mais importantes onde quer que estejam. Organizações em todo o mundo buscam a Symantec para soluções estratégicas e integradas para se defender contra ataques sofisticados em endpoints, nuvem e infraestrutura. Da mesma forma, uma comunidade global de mais de 50 milhões de pessoas e famílias dependem da suíte de produtos Norton e LifeLock da Symantec para proteger suas vidas digitais em casa e todos seus dispositivos. A Symantec opera uma das maiores redes civis de ciberinteligência do mundo, possibilitando a proteção contra as ameaças mais avançadas. Para mais informações, visite **www.symantec.com** ou conecte-se conosco no **Facebook**, **Twitter** e **LinkedIn**.

Symantec™

350 Ellis St., Mountain View, CA 94043 USA | +1 (650) 527 8000 | +1 (800) 721 3934 | www.symantec.com

19B176756_SB_CLOUD_GEN_PERFECT_STORM_EN