White paper

Cinco etapas para proteger o Data Center: por que a segurança tradicional pode não funcionar?

Resumo

Os administradores do data center enfrentam um desafio significativo: eles precisam proteger o data center sem comprometer o desempenho e a funcionalidade proporcionados pelos novos ambientes. A maioria procura proteger o data center usando soluções projetadas para a borda da Internet, mas essas soluções não são suficientes. O data center tem requisitos específicos relacionados ao provisionamento, ao desempenho, à virtualização, às aplicações e ao tráfego. E os dispositivos de borda da Internet simplesmente não foram feitos para abordar esses itens.

Para proteger o data center, é necessário uma solução que possa:

- Oferecer visibilidade e controle de aplicativos personalizados do data center
- Lidar com fluxos de tráfego assimétricos e transações de aplicativos entre os dispositivos e os data centers
- Adaptar-se à medida que os data centers evoluem: para virtualização, redes definidas por software (SDN), virtualização das funções de rede (NFV), Infraestrutura centrada em aplicativos da Cisco (ACIs) e muito mais.
- Lidar com o ciclo de ataque completo: antes, durante e depois de um ataque
- Integrar-se com a segurança implantada em toda a rede
- Comportar implantações e tráfego entre DC dispersado, incluindo ambientes privados, públicos e ambientes da nuvem

Principal alvo para o comprometimento: o data center

Muitas campanhas modernas de crime cibernético são desenvolvidas especificamente para ajudar os adversários a atingirem o data center, que abriga dados de alto valor, incluindo dados pessoais do cliente, informações financeiras e propriedade intelectual corporativa.[1] Entretanto, a proteção do data center é um desafio. Tráfego assimétrico, aplicativos personalizados, altos volumes de tráfego que precisam ser roteados para fora da camada do computador até o perímetro do data center para inspeção, virtualização em vários hipervisores e data centers geograficamente diferentes dificultam a proteção do data center para soluções de segurança que não foram projetadas para esses propósitos. Isso resulta em lacunas no alcance da segurança, impactos graves no desempenho do data center, necessidade de comprometer a funcionalidade do data center para acomodar limitações de segurança; além de provisionamento complexo de soluções de segurança que prejudicam a capacidade do data center de oferecer recursos de modo dinâmico e sob demanda.

Ao mesmo tempo, o data center está evoluindo, migrando de físico para virtual em ambientes de próxima geração, como SDN e ACI. O tráfego do data center já está crescendo exponencialmente, na maior parte devido ao aumento da utilização da nuvem e do ambiente emergente de Internet das Coisas (IoT), em que a Internet e as redes se expandem para locais como áreas de produção, redes de energia, instalações na área de saúde e transporte.

[1] Relatório de segurança anual da Cisco de 2014: http://www.cisco.com/web/offers/lp/2014-annual-security-report/index.html?keycode=000350063.

A Cisco prevê que até 2017, 76% do tráfego de data center permanecerá dentro do data center e será gerado, em grande parte, pelos dados de armazenamento, produção e desenvolvimento em um ambiente virtualizado.[2] O Gartner projeta um aumento de 3.000% nas conexões de data center por segundo até o final de 2015.[3]

Os data centers modernos já oferecem um host de aplicativos, serviços e soluções para o comércio. Muitas empresas contam com os serviços implantados em data centers espalhados pelo mundo para o suporte das necessidades cada vez maiores de computação em nuvem e tráfego. Elas também precisam abordar iniciativas estratégicas, como análise de Big Data e gestão de continuidade comercial, que fazem do data center uma parte ainda mais essencial da empresa. Mas isso também solidifica o data center como alvo principal de agentes mal-intencionados que desenvolvem ameaças cada vez mais sofisticadas, com o objetivo de burlar a detecção e acessar os recursos de data center. Tudo o que foi descrito acima significa que as equipes de segurança terão mais dificuldade para monitorar e proteger o data center.

Outra complicação para os administradores do data center e suas equipes: as limitações de provisionamento e desempenho impactam bastante o modo pelo qual as soluções de segurança, como firewalls de próxima geração, são implantadas e quais tráfegos podem ser inspecionados. A segurança não pode prejudicar o desempenho do data center. No data center moderno, o provisionamento de segurança deve ocorrer em minutos, não dias ou semanas. O desempenho deve ser dinamicamente escalado para lidar com picos de alto volume de tráfego.

Cinco etapas para proteção do data center

A segurança abrangente do data center requer uma abordagem de defesa detalhada que pode ser aplicada em cinco áreas principais. A solução deve:

1. **Oferecer visibilidade e controle de aplicativos personalizados do data center.** Os administradores do data center precisam de visibilidade e controle dos aplicativos do data center personalizados, não somente dos aplicativos Web tradicionais (por exemplo, Facebook e Twitter) e microaplicativos relacionados inspecionados pelos dispositivos de segurança de borda da Internet. Os firewalls de próxima geração são projetados para inspecionar o tipo de tráfego que flui pela borda da Internet, e não protegem esses aplicativos de data center personalizados.
2. **Como lidar com fluxos de tráfego assimétricos e transações de aplicativos entre os dispositivos ou os data centers.** A segurança deve ser integrada à malha do data center, não somente à borda. As soluções na borda não podem inspecionar os fluxos de tráfego de norte-sul (entrada-saída) e leste-oeste (entre aplicativos), sendo que o segundo fluxo representa a maior parte do tráfego de data center atual. Se o tráfego do aplicativo tiver que ser enviado ao perímetro do data center para inspeção em um firewall de próxima geração e, em seguida, roteado de volta à camada do computador (hairpinned), a solução prejudica o fluxo de tráfego dinâmico necessário para os data centers modernos.

   Muitos firewalls de próxima geração não podem proteger o tráfego assimétrico. No roteamento assimétrico, normal para os data centers, um pacote se deslocará em um caminho diferente ao retornar à sua origem. Isso se torna um problema para muitos firewalls de próxima geração, pois são projetados para rastrear, inspecionar e gerenciar fluxos de tráfego ao longo de um caminho único e previsível.

   As soluções de segurança do data center também devem poder lidar com transações de aplicativos entre os data centers ou dispositivos, incluindo os dispositivos virtuais. Os dispositivos virtuais são tão vulneráveis quanto os físicos, mas a segurança do data center também deve lidar com os desafios próprios dos ambientes virtuais, como a criação constante de carga de trabalho, limpeza e migração.

[2] Índice de nuvem global da Cisco: previsão e metodologia, 2012-2017: http://www.cisco.com/2012–2017/c/en/us/solutions/collateral/service-provider/global-cloud-index-gci/Cloud_Index_White_Paper.html.
[3] Semana da segurança: http://www.securityweek.com/data-centered-focusing-security-combat-rise-data-center-attacks

3. **Adaptar-se de acordo com a expansão do data center.** À medida que os ambientes de data center migram de modelos SDN, ACI e NFV físicos para virtuais e para os de próxima geração, as soluções de segurança devem ser capazes de escalar dinamicamente e oferecer proteção uniforme que funcione de modo perfeito entre os ambientes em evolução e de data center híbrido. Nesses novos modelos de data center, em que os dispositivos físicos e virtuais estão sendo oferecidos de maneira rápida, as regras de segurança podem aumentar sem controle. O gerenciamento da lista de controle de acesso (ACL) já é um desafio para muitas equipes de TI.

   A aplicação automática é necessária, pois novos dispositivos são oferecidos para que as implantações possam ser reduzidas de dias para minutos, sem que haja preocupação com as consequências ligadas à segurança. Da mesma forma, a capacidade de implantar uma única solução de segurança entre os data centers híbridos, muitos com vários hipervisores (monitores de máquina de virtualização), permite que as equipes de TI se concentrem na funcionalidade do data center, sem se sobrecarregarem pela complexidade da segurança administrativa.

4. **Lidar com o ciclo de ataque completo, antes, durante e depois de um ataque.** As abordagens de segurança tradicionais apresentam informações e visibilidade limitadas sobre as ameaças em um ambiente do data center, e se concentram principalmente no bloqueio na altura do perímetro. Cobrir todo o ciclo do ataque requer o monitoramento de uma ampla variedade de vetores de ataque com soluções que operam em todos os lugares em que a ameaça possa se manifestar: na rede, em endpoints, em dispositivos móveis e em ambientes virtuais. Uma abordagem holística voltada para a ameaça, com o objetivo de proteger o data center e que inclui a proteção antes, durante e depois de um ataque, é necessária para proteger o data center moderno e o seu tráfego especializado.

   Os firewalls tradicionais de próxima geração não oferecem praticamente nenhuma solução para identificar e mitigar ataques furtivos que pretendem ultrapassar as defesas, não conseguem oferecer remediação e análise após a interrupção de um ataque e não são capazes de rastrear e proteger o tipo de tráfego assimétrico que os data centers geram. Eles podem ser considerados ferramentas defensivas, mas não conseguem se defender contra ameaças emergentes e desconhecidas que se voltam para servidores vulneráveis, aplicativos específicos e dados importantes.

5. **Proteger toda a rede.** Qualquer solução de segurança do data center deve considerar a necessidade do usuário remoto de se conectar diretamente a recursos essenciais do data center. Ela precisa oferecer transparência entre o usuário remoto e o recurso do data center e ao mesmo tempo ser parte de um ambiente de rede complexo que se estende a filiais, passa pelo núcleo, entra no data center e sai para a nuvem. A solução de segurança deve fazer parte da arquitetura do data center, bem como de uma solução mais ampla, que pode detectar as ameaças na Internet e os ataques direcionados ao data center, ao mesmo tempo que oferece uma proteção eficiente durante todo o caminho dos dados.

A segurança do data center é diferente. Para proteger verdadeiramente o data center moderno e os novos modelos de data center que surgem atualmente, as empresas não podem contar somente com um firewall de próxima geração. Elas precisam de uma estratégia de segurança abrangente e integrada e uma arquitetura que ofereça uma proteção uniforme e inteligente em toda a rede distribuída, da borda da rede, para o data center e até a nuvem, sem prejudicar o desempenho.

Como proteger o data center moderno

A Cisco oferece ferramentas potentes para defender os ambientes de data center em evolução e não apenas a borda de rede do data center. As soluções inovadoras Cisco® Adaptive Security Appliances (ASA) para a segurança do data center foram projetadas para proteger ambientes físicos e virtuais e capacitar empresas a realizar a migração dos data centers tradicionais para os de próxima geração sem dificuldades. Dessa forma, é possível realizar testes de implantações com antecedência, proteger o investimento e obter proteção abrangente. As novas adições à plataforma Cisco ASA incluem:

- **Cisco Adaptive Security Virtual Appliance (ASAv):** o Cisco ASAv é uma versão virtual do conjunto de recursos completo de firewall da Cisco ASA, combinada com uma escalabilidade dinâmica e provisionamento simplificado para ambientes virtuais. Ele é projetado para ser executado em uma variedade de hipervisores e não depende da tecnologia VMware vSwitch. Isso torna o Cisco ASAv uma solução que atende a todos os ambientes de data centers, tanto da Cisco como de outras empresas, e híbridos. A arquitetura flexível do Cisco ASAv faz com que ele possa ser implantado como um gateway de segurança tradicional e como um recurso de segurança para ambientes inteligentes SDN e ACI que podem ser conectados diretamente às cadeias de serviço de aplicativos.
- **Cisco ASA 5585-X com serviços FirePOWER:** como um dispositivo de segurança de data center com finalidade específica que é totalmente compatível a ambientes de data center tradicionais, SDN e ACI, o Cisco ASA 5585-X Adaptive Security Appliance com serviços FirePOWER inclui firewall moderno e funcionalidade de segurança IPS de próxima geração e capacidade de detectar e inspecionar os aplicativos de data center personalizados, em conjunto com o desempenho avançado e recursos de provisionamento. Ele oferece recursos de agrupamento avançados para até 16 nós, fornecendo 640 Gbps de desempenho do data center que pode ser implantado em vários data centers. As soluções agrupadas podem ser gerenciadas como um único dispositivo para reduzir significativamente a complexidade administrativa. Como o ASAv, o 5585-X também foi projetado para funcionar em ambientes de data center tradicionais e de próxima geração, como SDN, NFV e ACI, oferecendo segurança estável em todos os ambientes híbridos e proteção eficiente durante as migrações de data centers.
- **IPS de próxima geração do Cisco FirePOWER:** o FirePOWER é o NGIPS líder de mercado, disponível como soluções físicas ou virtuais, que identifica e avalia as conexões aos recursos do data center e monitora atividades suspeitas na rede. A atividade do arquivo é monitorada e controlada quase que em tempo real e determinados arquivos (especialmente os arquivos desconhecidos que poderiam ser malware) são analisados com mais detalhes via sandboxing (análise isolada de exercício e comportamento do arquivo) ou pesquisas na nuvem (verificação da inteligência da comunidade geral em relação à reputação). Tal abordagem permite uma análise detalhada e a resposta ao tráfego crítico do data center.

Outras soluções disponíveis na Cisco que ajudam a oferecer uma segurança ampla ao data center incluem:

- **Cisco Identity Services Engine e TrustSec:** as equipes de TI podem criar, compartilhar e implementar as políticas de segurança de forma dinâmica, à medida que novos dispositivos ou usuários são adicionados ao ambiente do data center por meio do diretor de UCS. O ISE pode, em seguida, anexar tags de grupo de segurança que incluem política de segurança e regras de execução diretamente em pacotes individuais. Além disso, essas tags de segurança permitem que os data centers sejam segmentados com base na função do usuário e do dispositivo, sem as complicações e complexidades associadas a VLANs e ACLs.

- **Tecnologia Cisco OpenAppID para Snort:** com a tecnologia Cisco OpenAppID, as equipes de TI podem criar, compartilhar e implementar a detecção de aplicativo, além de desenvolver regras personalizadas para aplicativos personalizados no data center. É um módulo aberto de processamento e linguagem de detecção centrada no aplicativo para Snort™, o sistema de prevenção de intrusão (IPS) e o sistema de detecção de intrusão (IDS), desenvolvido pelo Sourcefire, que agora faz parte da Cisco. O Cisco OpenAppID está totalmente integrado ao framework do Snort, oferecendo aos administradores um conhecimento mais aprofundado dos aplicativos nas suas redes.

  Os usuários do Snort podem utilizar os detectores do Cisco OpenAppID para localizar e identificar, e relatar o uso de aplicativos. O Cisco OpenAppID oferece contexto na camada do aplicativo com eventos relacionados à segurança e ajuda a aprimorar a análise e a velocidade de remediação. Ele permite que o Snort bloqueie ou avise sobre a detecção de determinados aplicativos, o que ajuda a reduzir os riscos ao gerenciar toda a área de ameaça.
- **Soluções Cisco FireAMP™ e FireSIGHT™:** análise e proteção contra malware avançadas são necessárias para oferecer uma abordagem holística e com foco na ameaça para proteger o data center moderno, antes, durante e após um ataque. Os produtos Cisco FireAMP, da Sourcefire, utilizam Big Data para detectar, compreender e bloquear ataques de malware avançados. É a única solução que permite a visibilidade e o controle necessários para deter ameaças que não foram vistas por outras camadas de segurança. Além disso, ao combinar os produtos Cisco FireAMP com o Cisco ASA, os usuários podem oferecer inspeção e proteção mais aprofundadas para o tráfego de data center assimétrico.

  O Cisco FireSIGHT, também do Sourcefire, oferece a visibilidade de rede, o contexto e a automação necessários para responder às condições em constante mudança e aos novos ataques. Os administradores podem gerenciar centenas de dispositivos centralmente com o Cisco FireSIGHT Management Center.

Para obter mais informações

Para obter mais informações sobre os produtos de segurança da Cisco, como o firewall Cisco ASAvl, o dispositivo Cisco ASA 5585-X, a solução Cisco Secure Data Center e as soluções de segurança Sourcefire, acesse www.cisco.com/c/en/us/products/security/index.html.

Para saber mais sobre Snort e Cisco OpenAppID, acesse www.snort.org.

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 C11-732259-00 07/14