Resumo

Benefícios

- **Centralize e unifique o controle de acesso altamente seguro** com base na função empresarial para oferecer uma política coerente de acesso à rede para usuários finais, estejam eles conectados por meio de uma rede com fio ou sem fio ou por VPN.
- **Obtenha maior visibilidade e identificação mais precisa de dispositivos** com o serviço de criação de perfis de dispositivos Cisco® Identity Services Engine (ISE) e o feed de perfis de dispositivos que, juntos, reduzem o número de endpoints desconhecidos.
- **Simplifique as experiências de convidados** para facilitar o acesso e a administração por meio de portais de convidados móveis e de desktops de marcas conhecidas, totalmente personalizáveis, criados em minutos com fluxos de trabalho visuais e dinâmicos, que permitem gerenciar facilmente a experiência dos convidados.

Cisco Identity Services Engine

A rede corporativa já não se limita a quatro paredes seguras. Ela se estende até onde os funcionários e os dados vão. Hoje, mais do que nunca, os funcionários querem ter acesso a recursos de trabalho de mais dispositivos e através de redes não empresariais. A mobilidade e a Internet de Todas as Coisas (IoE) estão mudando a maneira como vivemos e trabalhamos. As empresas são desafiadas a oferecer suporte a uma proliferação de novos dispositivos na rede, à medida que uma infinidade de ameaças à segurança e violações de dados com alta divulgação demonstram claramente a importância de se garantir acesso à rede corporativa em constante evolução.

Conforme a rede moderna se expande, a complexidade da organização de recursos, do gerenciamento de soluções de segurança distintas e do controle de risco também cresce. Some-se a isso a conectividade onipresente da IoE com recursos de TI já restritos, e o possível impacto da falha na identificação e correção de ameaças à segurança torna-se realmente muito grande.

É necessária uma abordagem diferente para possibilitar o gerenciamento e a segurança da empresa móvel em evolução. Ela se chama Cisco® Identity Services Engine (ISE).

Reduza a exposição e o risco

Esteja à frente das ameaças por meio de visibilidade e controle. Para isso, é necessário ter profunda visibilidade dos usuários e dispositivos que acessam a rede, além de controle dinâmico, para assegurar que apenas as pessoas certas, com os dispositivos corretos, obtenham o acesso adequado aos serviços corporativos.

O ISE 2.0 reprojetado simplifica ainda mais a disponibilização do controle de acesso seguro constante em redes de vários fornecedores com e sem fio e conexões de VPN remotas. Com o sensor inteligente de longo alcance e os recursos de criação de perfis, o Cisco ISE pode analisar profundamente a rede para oferecer visibilidade superior de quem e de qual dispositivo estão acessando os recursos. Através do compartilhamento de dados contextuais fundamentais com as integrações do parceiro do ecossistema e a implementação da política Cisco TrustSec para segmentação definida por software, o Cisco ISE transforma a rede de um simples canal de dados em um aplicador de segurança que acelera o tempo de detecção e o tempo de resolução das ameaças à rede.

- **Acelere a consumerização de TI (BYOD) e a mobilidade corporativa** com configuração fácil e pronta para uso, integração e gerenciamento de dispositivos por autoatendimento, gerenciamento de certificados de dispositivos internos e software de parceiro de gerenciamento de mobilidade corporativa (EMM) integrado, para integrar dispositivos dentro e fora das instalações.
- **Construa uma política de segmentação definida por software para conter ameaças à rede** usando a tecnologia Cisco TrustSec® para aplicar o controle de acesso por função na camada de roteamento e switching. Segmente dinamicamente o acesso sem a complexidade de várias VLANs nem a necessidade de refazer o projeto da rede.
- **Compartilhe dados contextuais avançados com soluções de rede e segurança de parceiros** para aperfeiçoar a eficiência geral, além de acelerar o tempo de detecção (TTD) e o tempo de resolução (TTR) das ameaças à rede.
- **Contenha ameaças automaticamente** pela integração com o Cisco Firepower Management Center, pois o ISE pode conter endpoints infectados para correção, observação ou remoção.

As atualizações e melhorias do ISE 2.0 incluem:

- Integração com o Cisco Mobility Services Engine (MSE), que oferece dados de localização para criar e aplicar o acesso a uma localização específica. Dessa forma, por exemplo, profissionais da área médica só podem acessar prontuários médicos na sala de emergência.
- Melhoria de nossa arquitetura aberta para determinados parceiros do ecossistema do ISE, de forma que os clientes possam usar as soluções de segurança de que dispõem para trabalhar com o ISE na identificação de ameaças na rede para rápida contenção e correção.
- Compatibilidade com dispositivos de acesso à rede de terceiros (NADs) e endpoints IPv6 para aumentar o alcance e o escopo do ISE, a fim de oferecer conformidade de endpoint em uma variedade de redes maior.
- Gerenciamento de políticas otimizado, incluindo administração simplificada de dispositivos de autenticação, autorização e contabilização (AAA) com os recursos de acesso TACACS+ e RADIUS, para facilitar ainda mais a implantação da política de controle de acesso seguro para redes com fio.
- O Cisco AnyConnect 4.2 acompanha o novo módulo de visibilidade de rede (NVM), que oferece um nível de detalhe dos fluxos de tráfego de aplicativos anteriormente indisponível em endpoints externos.

Além disso, o ISE utiliza a tecnologia Cisco Platform Exchange Grid (pxGrid) para compartilhar dados contextuais avançados com soluções de ecossistema de parceiros integradas. Essa tecnologia acelera suas habilidades para identificar, minimizar e corrigir ameaças à segurança na rede estendida. No geral, o controle de acesso seguro é centralizado e simplificado para disponibilizar serviços empresariais fundamentais com segurança, melhorar a segurança da infraestrutura, aplicar a conformidade e otimizar as operações de serviço.

O ISE, por meio de integrações com as principais soluções de informações de segurança e gerenciamento de eventos (SIEM) e de defesa contra ameaças (TD), visibilidade de rede profunda e recursos de controle de acesso seguro, desempenha papel fundamental nas soluções Cisco Cyber Threat Defense, Network-as-a-Sensor e Network-as-an-Enforcer Em última análise, o ISE oferece a visibilidade, o contexto e o controle dinâmico necessários para as empresas implementarem de modo eficaz a segurança direcionada a todo o ciclo do ataque, gerenciando o acesso à rede antes do ataque, oferecendo visibilidade e contenção de ameaças durante o ataque e melhorando o tempo de detecção (TTD) e o tempo de resolução (TTR) após o ataque.

Próximas etapas

Para obter mais informações sobre o Cisco ISE, acesse http://www.cisco.com/go/ise ou entre em contato com o representante de contas local.

C45-654884-13 10/15