

Cisco Secure Firewall para instituições financeiras



Transforme toda a rede em uma extensão da arquitetura de segurança

Com aplicações essenciais para os negócios que usam cada vez mais ambientes híbridos e multicloud e com funcionários que agora precisam de acesso seguro a recursos em qualquer lugar, a abordagem de firewall tradicional não funciona mais. O perímetro de rede individual evoluiu para vários micropérimetros. Para muitas instituições financeiras, a aplicação é o novo perímetro e as implantações tradicionais de firewall evoluíram para uma combinação de dispositivos físicos, virtuais e nativos da nuvem. Como resultado, as empresas estão com dificuldades para operacionalizar o suporte para ambientes modernos de aplicações. O desafio é manter a visibilidade constante, a aplicação de políticas e uma visibilidade uniforme de ameaças, sem gerar vulnerabilidades que expõem a empresa a riscos.

Na Cisco, estamos criando uma visão de segurança de rede, NetWORK, que permite uma abordagem mais ágil, automatizada e integrada para harmonizar políticas e execução em aplicações dinâmicas modernas e redes cada vez mais heterogêneas. O Cisco Secure Firewall oferece o conjunto mais profundo de integrações entre as principais funções de rede e a segurança da rede, oferecendo a arquitetura mais segura de todos os tempos. O resultado é um portfólio de segurança completo que protege as aplicações e os usuários em todos os lugares.

Benefícios

- Segurança unificada de rede e carga de trabalho em tempo real para controle integrado em ambientes de aplicações dinâmicas.
- Abordagem de plataforma para a segurança de rede, aproveitando e compartilhando informações de fontes importantes para detecção, resposta e correção mais rápidas. Proteja os funcionários remotos com acesso corporativo altamente seguro a qualquer hora, em qualquer lugar, em qualquer dispositivo, com recursos avançados de prevenção de ameaça que protegem a empresa, os funcionários e as aplicações essenciais.
- Qualificação para o SecureX™ incluída em cada Cisco® Secure Firewall para oferecer uma abordagem totalmente integrada à segurança, que permite a correlação de ameaças em todo o portfólio do Cisco Secure e acelera a resposta a incidentes.

Visibilidade e controle superiores

As ameaças se tornaram mais sofisticadas e as redes se tornaram mais complexas. Pouquíssimas instituições financeiras, se houver, têm os recursos para se dedicar a manter-se atualizado e evitar com sucesso essas ameaças em constante evolução.

À medida que as ameaças e as redes se tornam mais complexas, é essencial ter as ferramentas certas para proteger dados, aplicações e redes. Os Cisco Secure Firewalls têm a capacidade e a flexibilidade de que você precisa para estar um passo à frente das ameaças. Eles oferecem um aumento significativo 3x maior no desempenho em relação à geração anterior de dispositivos, além de recursos exclusivos de hardware para inspeção de tráfego criptografado em escala. Além disso, as regras legíveis para seres humanos do Snort 3 IPS ajudam a simplificar a segurança. A visibilidade e o controle dinâmicos das aplicações estão disponíveis por meio da integração do Cisco Secure Workload para oferecer proteção constante para as aplicações modernas da rede e da carga de trabalho.

[Encontre o firewall ideal para a sua empresa](#)

Gerenciamento de políticas simplificado e confiável

Com o portfólio Secure Firewall, você ganha uma postura de segurança mais forte, equipada com gerenciamento flexível e pronto para o futuro. A Cisco oferece uma variedade de opções de gerenciamento personalizadas para atender às suas necessidades comerciais.

- **Cisco Secure Firewall Device Manager:** gerencia um único firewall localmente; essa é uma solução de gerenciamento no dispositivo para o Firewall Threat Defense.
- **Cisco Secure Firewall Management Center:** gerencia uma implantação de firewall em grande escala. Está disponível em todos os formatos, por exemplo, local, nuvem privada, nuvem pública e Software como Serviço (SaaS).
- **Cisco Defense Orchestrator:** um gerenciador na nuvem que simplifica as políticas de segurança e o gerenciamento de dispositivos em vários produtos da Cisco, como Cisco Secure Firewall, Meraki® MX e Cisco IOS®.

A Cisco também oferece o Cisco Security Analytics and Logging para gerenciamento de logs escalável. Ele aprimora a detecção de ameaças e atende às exigências de conformidade em toda a empresa com mais recursos de retenção e análise comportamental.

[Caso de sucesso da Lake Trust Credit Union](#)

Razões para escolher a Cisco

O portfólio do Cisco Secure Firewall oferece mais proteção para a rede contra um conjunto de ameaças cada vez mais complexo e em evolução. Com a Cisco, você está investindo em uma base de segurança ágil e integrada, levando à postura de segurança mais forte disponível hoje e no futuro.

Do data center, das filiais, dos escritórios corporativos, dos ambientes de nuvem e de qualquer outro lugar, você pode aproveitar todo o potencial da Cisco para transformar a infraestrutura de rede atual em uma extensão da solução de firewall, resultando em controles de segurança de nível internacional em todos os locais que forem necessários.

Hoje, investir em um dispositivo Secure Firewall oferece proteção sólida até mesmo contra as ameaças mais sofisticadas, sem comprometer o desempenho ao inspecionar o tráfego criptografado. Além disso, as integrações com outras soluções da Cisco e de terceiros oferecem um portfólio amplo e detalhado de produtos de segurança, todos trabalhando juntos para correlacionar eventos anteriormente desconectados, eliminar ruídos e interromper ameaças mais rapidamente.

Recursos avançados do Cisco Secure Firewall

Recurso avançado	Detalhes
Integração do Cisco Secure Workload	<ul style="list-style-type: none"> A integração do Cisco Secure Workload (antigo Tetration) permite visibilidade abrangente e aplicação de políticas para aplicações modernas distribuídas e dinâmicas em toda a rede e carga de trabalho para implementação constante de forma escalável.
Cisco Secure Firewall Cloud Native	<ul style="list-style-type: none"> Desenvolvido com o Kubernetes e disponível pela primeira vez no AWS, o Secure Firewall Cloud Native é uma solução de acesso a aplicações fácil para o desenvolvedor para criar uma infraestrutura altamente flexível e nativa da nuvem.
Suporte a políticas dinâmicas	<ul style="list-style-type: none"> Os atributos dinâmicos são compatíveis com as tags VMware, AWS e Azure para situações em que os endereços IP estáticos não estão disponíveis. A Cisco foi pioneira em políticas de marcas com o suporte a atributos do Security Group Tags (SGTs) e do Cisco Identity Services Engine (ISE).
Sistema de prevenção contra invasão do Snort 3	<ul style="list-style-type: none"> O próximo passo na proteção contra ameaças com o Snort 3 de código aberto líder do setor ajuda a melhorar a detecção, simplificar a personalização e melhorar o desempenho.
Identidade e descoberta do servidor TLS (Transport Layer Security)	<ul style="list-style-type: none"> Permite manter políticas de camada 7 no tráfego TLS 1.3 criptografado. Mantenha visibilidade e controle em um mundo criptografado, em que não é plausível descriptografar e inspecionar cada fluxo de tráfego. Os firewalls da concorrência violam as políticas de camada 7 com tráfego TLS 1.3 criptografado.
Cisco Secure Firewall Management Center	<ul style="list-style-type: none"> Oferece gerenciamento unificado de firewalls, controle de aplicações, prevenção contra invasão, filtragem de URL e políticas de defesa contra malware. A integração com o Cisco Secure Workload (antigo Tetration) permite visibilidade constante e aplicação de políticas para aplicações dinâmicas em toda a rede e carga de trabalho.
Cisco Defense Orchestrator	<ul style="list-style-type: none"> Gerenciamento de firewall na nuvem que ajuda a gerenciar de forma constante e confiável as políticas em todos os firewalls Cisco Secure.
Cisco Security Analytics and Logging	<ul style="list-style-type: none"> Gerenciamento de logs de firewall altamente escalável no local e na nuvem, com análise comportamental para detecção de ameaças em tempo real e tempos de resposta mais rápidos. Além da análise contínua para aperfeiçoar ainda mais a postura de segurança para obter melhor defesa contra futuros esforços. Atenda às suas necessidades de conformidade com a agregação de logs em todos os Cisco Secure Firewalls. Forte integração com os gerenciadores de firewall para aprimorar o registro e a análise, além de agregar dados de log de firewall em uma única visualização intuitiva.
Cisco SecureX	<ul style="list-style-type: none"> Aproveite a plataforma SecureX para acelerar a detecção e a correção de ameaças. Cada Secure Firewall inclui a qualificação para o Cisco SecureX. A nova faixa de opções do SecureX no Firewall Management Center permite que o SecOps mude instantaneamente para a plataforma aberta do SecureX, acelerando a resposta a incidentes.
Inteligência de ameaças do Cisco Talos®	<ul style="list-style-type: none"> O Cisco Talos Intelligence Group é uma das maiores equipes de inteligência de ameaças comerciais do mundo. Ele cria inteligência de ameaças precisa, rápida e prática para os clientes, produtos e serviços da Cisco. O Talos mantém os conjuntos de regras oficiais do Snort.org, ClamAV e SpamCop.

Próximas etapas

Saiba mais sobre o [Cisco Secure Firewall](#) ou, para ver mais soluções de segurança para serviços financeiros, acesse o [gerenciador de portfólios](#). Fale com um [representante de vendas da Cisco](#) ou [veja as opções de compra](#).

Sede - América
Cisco Systems, Inc.
San Jose, CA

Sede - Ásia e Pacífico
Cisco Systems (USA) Pte 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.

Cisco e o logotipo da Cisco são marcas comerciais ou marcas comerciais registradas da Cisco e/ou de suas afiliadas nos EUA e em outros países. Para ver uma lista de marcas registradas da Cisco, consulte [www.cisco.com/go/trademarks](#). Hauptgeschäftsstelle Nord und Südamerika Hauptgeschäftsstelle Asien/Pazifik Raum Hauptgeschäftsstelle Europa "parceiro" não implica uma relação de sociedade entre a Cisco e qualquer outra empresa. (1110R)

Cisco Systems, Inc.
Impresso nos EUA
San Jose, CA

Cisco Systems (USA) Pte. Ltd.
Singapur

Cisco Systems International BV Amsterdam,
C45-3380706-00 02/23
Niederlande