RESUMO DO RECURSO

FireCloud Total Access, a alternativa segura às VPNs

O desafio do usuário de VPNs

Por décadas, as redes privadas virtuais (VPNs) foram a solução ideal para permitir o acesso remoto de usuários. Elas criaram túneis criptografados na rede corporativa, oferecendo aos funcionários uma forma de se conectar a aplicativos e dados de qualquer lugar.

As VPNs foram originalmente projetadas para uma era diferente, quando os aplicativos eram hospedados em data centers, a maioria dos funcionários trabalhava no local e estar "dentro da rede" significava ser "confiável". Firewalls e VPNs normalmente têm endereços IP públicos na Internet, permitindo que usuários autorizados naveguem na web e encontrem pontos de entrada na rede. No entanto, esses access points também são visíveis para todos, incluindo criminosos cibernéticos que tentarão violá-los. Essa abordagem de ampla visibilidade e confiança aberta não é mais segura. O aumento do trabalho remoto, dos aplicativos em nuvem e dos ambientes de TI híbridos transformou as VPNs em um gargalo de desempenho e um risco significativo à segurança.

A alternativa de confiança zero FireCloud

A confiança zero desafio o modelo das VPNs ao assumir que nada é seguro: “nunca confie, sempre verifique” a cada sessão. Cada usuário, dispositivo e sessão é autenticado, autorizado e continuamente inspecionado, seja qual for a origem da conexão. Esse modelo garante que os trabalhadores remotos recebam o mesmo nível de proteção que os usuários locais e reduz drasticamente as superfícies de ataque disponíveis aos adversários. O FireCloud Total Access oferece esses princípios de confiança zero.

> Desafios e custos das VPNs

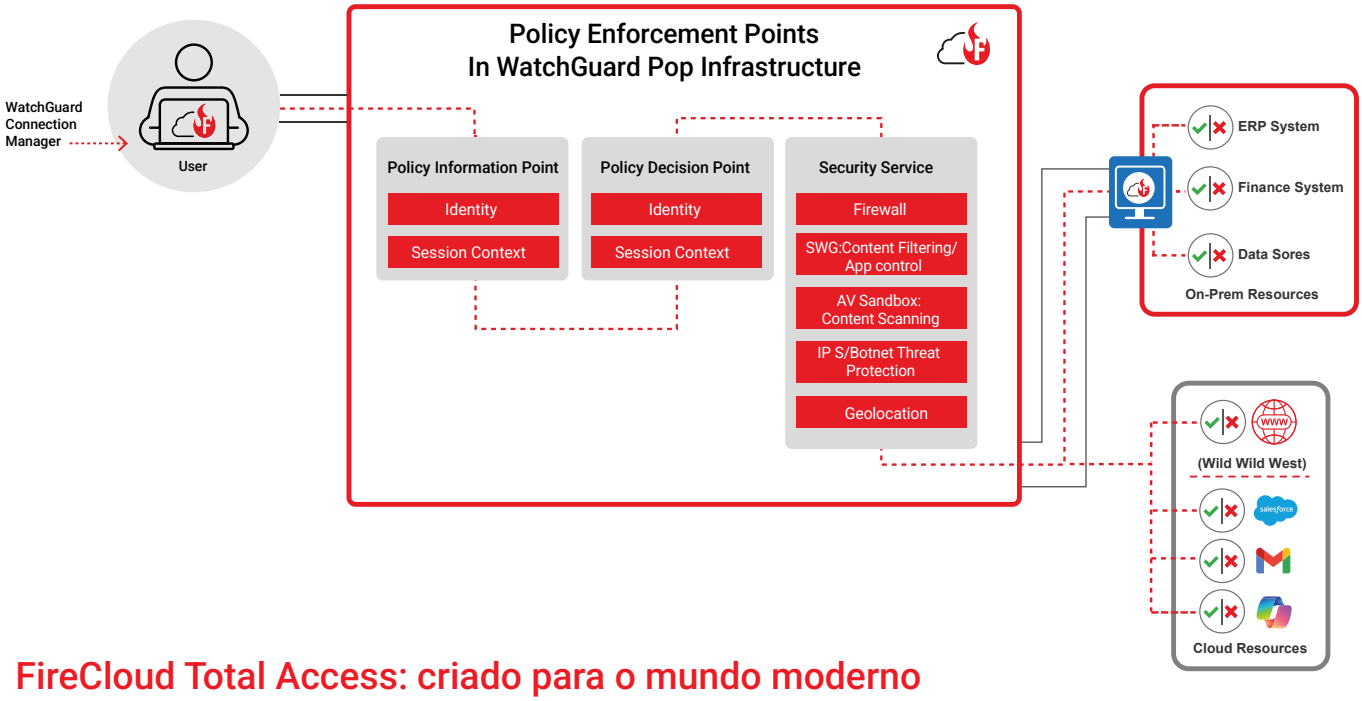
- **Modelo de confiança implícita falho**
  Após a conexão, os usuários têm amplo acesso, criando riscos de movimentação lateral.
- **Riscos de ataques cibernéticos**
  A visibilidade dos endereços IP e a complexidade dos códigos levaram a ataques de força bruta e baseados em vulnerabilidades.
- **Complexidade operacional**
  As equipes de TI devem gerenciar políticas de VPN, túneis e regras de firewall em um ambiente amplo.
- **Frustração do usuário**
  Latência das VPNs, sessões perdidas e baixo desempenho prejudicam a produtividade e aumentam os custos de suporte.
- **Custos operacionais ocultos**
  Manter túneis, certificados, regras de firewall e agentes de cliente cria custos significativos em horas-homem de gerenciamento.
- **Riscos de conformidade**
  As VPNs não fornecem visibilidade, segmentação ou controles de identidade que os reguladores exigem, o que leva a dificuldades de conformidade.

Segurança centrada na identidade
O acesso é concedido com base na identidade e no contexto verificados, não na localização da rede.

Acesso com privilégios mínimos
Os usuários acessam apenas os aplicativos e recursos específicos para os quais estão autorizados, eliminando exposição desnecessária.

Validação contínua As verificações de segurança não param no login. O tráfego é inspecionado em tempo real em busca de ameaças, configurações incorretas ou anomalias.

Controle de política unificado As equipes de TI podem aplicar políticas centralmente para todos os usuários e dispositivos, eliminando a complexidade e lacunas na cobertura.



FireCloud Total Access: criado para o mundo moderno

O FireCloud Total Access combina firewall como serviço (FWaaS), gateway seguro da web (SWG), e acesso a redes com confiança zero (ZTNA) em uma única plataforma nativa da nuvem que oferece:

- **Confiança zero:** cada sessão tem sua identidade verificada e privilégios mínimos aplicados
- **Implementação de políticas centralizadas e nativas da nuve**m em todos os usuários e dispositivos
- **Roteamento otimizado** com pontos de presença na nuvem para desempenho mais rápido
- **Inspeção contínua do tráfego** para SaaS, aplicativos privados e acesso à Internet
- Criado especificamente para **acesso híbrido e remoto seguro** em um mundo que prioriza a nuvem

A realidade: uma VPN não é gratuita. É um centro de custos oculto e uma responsabilidade de segurança.

As VPNs foram criadas para redes antigas. Atualmente, os ambientes híbridos, distribuídos e com uso intenso de SaaS exigem uma nova abordagem que pressuponha que nada é confiável por padrão, imponha verificação contínua e ofereça segurança na ponta. O FireCloud Total Access é mais do que um substituto para as VPNs. É uma plataforma de acesso baseada em confiança zero que reduz riscos, melhora a experiência do usuário e cria uma oportunidade de serviço previsível e de alta margem.

Sobre a WatchGuard

A WatchGuard® Technologies, Inc. é líder global em segurança cibernética unificada. A abordagem da nossa Unified Security Platform® foi projetada exclusivamente para que provedores de serviços gerenciados forneçam segurança de classe mundial que aumenta a escala e a velocidade dos negócios e melhora a eficiência operacional. Com a confiança de mais de 17.000 revendedores de segurança e provedores de serviços para proteger mais de 250.000 clientes, os produtos e serviços premiados da empresa abrangem segurança e inteligência de rede, proteção avançada de terminais, autenticação multifator e Wi-Fi seguro. Juntos, eles oferecem cinco elementos essenciais de uma plataforma de segurança: segurança abrangente, conhecimento compartilhado, clareza e controle, alinhamento operacional e automação. A empresa tem sede em Seattle, Washington, com escritórios na América do Norte, Europa, Ásia-Pacífico e América Latina. Para saber mais, acesse WatchGuard.com

VENDAS NO BRASIL (41) 3073-1663 Curitiba / (11) 3164-3031 São Paulo WEB www.secureone.com.br WatchGuard Technologies, Inc.