TAILSCALE – VPN SOLUTION

RESUMO SOBRE SEGURANÇA DO TAILSCALE (TRADUZIDO DE https://tailscale.com/security/)

Itens relevantes:

1- Fornece criptografia de ponta a ponta entre dispositivos. O Tailscale não pode ler seu tráfego.

2- É construído em cima de WireGuard.COM (VPN extremamente simples, porém rápida e moderna. WireGuard foi revisado por criptografadores e o código auditado,)

3- O Tailscale não (e não pode) inspecionar seu tráfego. Privacidade é um direito humano fundamental, e projetamos o Tailscale de acordo. Nós não queremos seus dados.

4- Suas chaves de criptografia privadas dos dispositivos nunca saem de seus respectivos nós e nosso servidor de coordenação apenas coleta e troca chaves públicas. Os servidores DERP não registram seus dados;

5- O que Tailscale pode ver e capturar é criptografado.

6- Nunca vê informações sobre o tráfego público da Internet. Se você usa um nó de saída (no roteador), eles são seus nós de saída, não do TS, então ainda TS não pode ver o tráfego público da Internet. Se você gerar um IP exclusivo de um app gerador de ip, suas consultas públicas podem acabar passando por suas Proxy DNS local do TS dos dispositivos, mas não são registradas.

7- TS recebe metadados de seu nó particular com finalidade de ajudar a conectar-se

8- Sua rede permanece disponível mesmo que o Tailscale não esteja: conecta dispositivos ponto a ponto, mesmo que o servidor de coordenação do Tailscale está inoperante.

9- TS sempre prioriza conexão ponto a ponto, mas quando isso não é possível ele possui servidores DERPs distribuídos globalmente para ajudar a conexão.

10- TS usa o app Wireguard para implementar a estrutura VPN e são escritas em linguagem Go, ao qual fornece gerenciamento automático de memória, impedindo vulnerabilidades.

11- - TS fornece um único e imutável IP, mas você pode gerar o seu usando outros apps ou de listas de IPs públicos.

Recursos de segurança:

-Solução de login por SSO: funcionalidade de controle de acesso único a vários sistemas, ainda que independentes (login seguro de autenticação única: https://www.e-trust.com.br/o-que-e-sso-ou-single-sign-on/)

- MFA (Assinatura por multi fatores)

A Tailscale depende do seu provedor de identidade existente para autentique usuários com identidade de provedores, incluindo Google, Microsoft AD, GitHub, Okta e OneLogin.

Controles de acesso à rede (ACLs):

O Tailscale suporta regras de controle de acesso à rede permitem definir com precisão o que um usuário ou dispositivo específico é permitido acessar na sua rede Tailscale. vide: https://tailscale.com/kb/1018/acls/

Tailscale concluiu um SOC 2 Certificação tipo II, para atender aos serviços de confiança da AICPA critérios de segurança: https://tailscale.com/compliance

---

Algumas Perguntas frequentes:

O Tailscale pode descriptografar meu tráfego e ver meus dados?

Não. Os dispositivos que executam o Tailscale trocam apenas suas chaves públicas. Chaves particulares nunca saem do dispositivo. Todo o tráfego é criptografado de ponta a ponta, sempre.

Meu tráfego é roteado pelos seus servidores?

Não. Rotas de escala de cauda traficam o caminho mais curto possível. Na maioria dos casos, essa é uma conexão direta entre pares.

Nos casos em que uma conexão direta não possa ser estabelecida, os dispositivos se comunicarão saltando o tráfego de um ou mais distribuídos geograficamente Servidores de relé DERP. Seu tráfego permanece criptografado de ponta a ponta quando passa por um servidor de retransmissão e o Tailscale não pode descriptografá-lo.

Outros poderão acessar meu computador?

O Tailscale permite conectar seu computador a outros dispositivos conectados à mesma rede Tailscale. Somente dispositivos que têm permissão para acessar seu computador, conforme definido em ACLs pode iniciar conexões com o seu computador. Você também pode localmente bloquear conexões de entrada para o seu dispositivo. https://tailscale.com/kb/1072/client-preferences/#allow-incoming-connections

Posso optar por não fazer log?

O Tailscale coleta os metadados do cliente relacionados às tentativas de conexão, autenticação e roteamento para nos ajudar a monitorar e depurar redes.

Se você optar por não fazer log, o Tailscale poderá não ser capaz de fornecer suporte técnico. Para aprender a optar por não participar, consulte Optar por sair do log do cliente.

Você não pode limitar os logs do servidor de coordenação.

Quais dados o Tailscale coleta?

Para fornecer o serviço, o Tailscale coleta informações do dispositivo, incluindo SO, hardware, endereços IP públicos, informações de roteamento de rede, informações sobre o cliente Tailscale instalado e outras configurações do dispositivo. O Tailscale também usa informações da conta do usuário, como endereços de email, para autenticar os usuários em suas contas.

Veja nosso Política de Privacidade para mais detalhes sobre como coletamos e usamos informações pessoais.

O Tailscale criptografa meus dados?

Sim. O Tailscale criptografa os metadados do cliente no servidor de coordenação em repouso usando o AES de 256 bits e em trânsito usando o TLS. Os dados do cliente são criptografados em trânsito usando o WireGuard.

O Tailscale faz backup dos meus dados?

O Tailscale faz backup dos metadados do cliente no servidor de coordenação a cada hora e testa os backups pelo menos anualmente.

Sobre DNS: https://tailscale.com/kb/1054/dns/