SOPHOS
Cybersecurity evolved.

A criptografia tornou o seu firewall irrelevante?

Cinco recursos da inspeção TLS de que você precisa no seu próximo firewall

Documento técnico Sophos. Junho, 2021

Cinco recursos da inspeção TLS de que você precisa no seu próximo firewall

O rápido aumento no tráfego de rede criptografado, acompanhado da incapacidade da maioria dos firewalls Next Gen de inspecionar esse tráfego, deu vez a um imenso rebuliço na segurança, com consequências devastadoras.

Mais de 90% do tráfego na maioria das redes é criptografado e passa através de um firewall mediano sem nenhum filtro. Isso certamente não é falta de vontade de inspecioná-lo. Pelo contrário, isso se deve à falta de capacidade da maioria dos firewalls para fazer o trabalho. Mesmo que o firewall possa inspecionar o tráfego criptografado, muito comumente a solução de inspeção TLS é mal-implementada, quebrando a conexão de websites e propiciando uma experiência insatisfatória ao usuário.

Não surpreende que os hackers estejam se agarrando com todo afinco a esse ponto cego na segurança organizacional. Eles estão começando a se aproveitar dessa fraqueza para infiltrar ameaças nas redes e ali mantê-las.

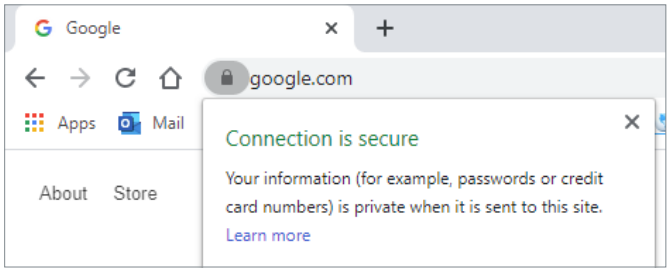
Leia este documento para saber como a criptografia tornou a maioria dos firewalls Next Gen irrelevante, os desafios da inspeção TLS e as cinco capacidades de inspeção SSL de que você precisa para fechar essa lacuna na segurança.

Criptografia oferece privacidade, não segurança

As pessoas frequentemente acreditam que as conexões criptografadas da Internet são "seguras". Mas "seguras" contra o quê, exatamente?

O protocolo TLS (Transport Layer Security, segurança de camada de transporte) é o padrão de criptografia usado na Internet hoje em dia. Os termos SSL e TLS são geralmente utilizados de modo intercambiável. De fato, SSL é um antigo padrão que foi obscurecido pelo TLS, contudo, SSL se mantém o termo mais comum. Quando dizem SSL, as pessoas estão se referindo a TLS, na maioria das vezes.

TLS foi criado para oferecer confidencialidade e autenticidade com a criptografia das comunicações entre duas partes e verificar se o servidor é quem diz ser com base em seu certificado e em quem o emitiu.



O símbolo de cadeado no seu navegador indica que a conexão está criptografada, para a sua privacidade.

O que a criptografia TLS NÃO faz é proteger, ou seja, oferecer segurança ao conteúdo da página da Web. Cargas de malware hospedadas em um site apresentam criptografia perfeitamente válida e conexão "segura".

Quando alguém diz que tem uma conexão segura a um servidor da Web, o que está realmente querendo dizer é que a conexão está protegida contra interceptação (ainda que talvez nem mesmo esse seja o caso). Por isso é tão importante inspecionar o tráfego criptografado.

A inspeção TLS não é fácil

O desafio na inspeção TLS é que o protocolo TLS é bastante complexo. Deve haver a troca de diferentes certificados e os pacotes de códigos a serem usados precisam ser negociados para poder determinar como a conexão deverá ser criptografada. Para complicar ainda mais a situação, existem várias versões TLS, e muitos dos aplicativos e serviços Web operam de modo diferente.

O resultado disso é que, apesar dos padrões rigorosos, muito provavelmente haverá incompatibilidade. Isso apresenta imensos desafios para qualquer solução de segurança que tente se injetar no processo a fim de inspecionar e proteger o conteúdo da troca.

A importância do TLS 1.3 e alguns mitos esclarecidos

A boa-nova é que o último padrão TLS, o TLS 1.3, oferece várias vantagens sobre seus predecessores nos quesitos desempenho, privacidade e tratamento de vulnerabilidades.

A adoção do TLS 1.3 para servidores ainda está engatinhando, mas todos os grandes navegadores já aceitam esse padrão. Contudo, devido às complexidades e aos esforços de P&D exigidos para implementá-lo, muitos firewalls com inspeção TLS disponíveis atualmente no mercado não são totalmente compatíveis com a versão 1.3 e, assim, forçam o downgrade para o TLS 1.2. Isso abre as conexões para serem exploradas e atacadas devido às vulnerabilidades legadas.

Como acontece com muitas tecnologias novas, existem alguns mitos ou mal-entendidos sobre a inspeção TLS 1.3. Há aqueles que afirmam taxativamente que o TLS 1.3 não pode ser inspecionado. Essa declaração é falsa. Ainda que seja verdade que a inspeção TLS passiva, que ocorria nas linhas laterais, não seja mais possível, com a participação de um endpoint colaborativo – como aqueles em uma rede corporativa – a inspeção continua inteiramente possível.

Outros afirmam que ao inspecionar fluxos de tráfego criptografado você os está deixando ainda menos seguros. Isso é verdade, se você fizer o downgrade da conexão TLS 1.3 para a TLS 1.2, como fazem muitas das soluções atuais de inspeção TLS. As vulnerabilidades em TLS 1.2 abrem as portas para uma possível exploração por um ataque man-in-the-middle (MITM) malicioso. O TLS 1.3 foi projetado para tratar dessas vulnerabilidades de modo que a inspeção do tráfego sem o downgrade da conexão não crie um risco.

Para finalizar, há ainda aqueles que afirmam que o certificate pinning impossibilita a inspeção TLS. Ainda que isso seja verdade para alguns aplicativos com certificados embutidos no código, a maioria dos aplicativos usa a abordagem de certificate pinning que respeita o resigning certificate e continuará a funcionar com soluções de inspeção SSL.

A importância da validação de certificado

A validação de certificado é um componente fundamental do TLS, pois permite que o cliente (ou dispositivo de inspeção como o seu firewall) prove a identidade do servidor de onde a comunicação está vindo.

Porém, para a validação de certificado funcionar, ela precisa ser implementada adequadamente. Caso contrário, os firewalls, e os endpoints a que eles estão conectados, podem ser levados a pensar que estão se comunicando com um servidor que não estão, abrindo as portas para um ataque MITM malicioso.

Equilibrando desempenho, privacidade e proteção

Além de todas as complexidades técnicas com os fluxos de tráfego criptografado TLS, existem restrições regulatórias e políticas que também precisam ser consideradas e respeitadas. Além disso, streaming de mídia e o tráfego de aplicativos corporativos podem consumir uma grande parte do tráfego de TLS criptografado que talvez não precise de inspeção.

A conclusão é que nem todo tráfego criptografado pode ou deveria ser tratado do mesmo jeito. Trata-se de uma questão de equilíbrio: você precisa equilibrar privacidade, segurança, conformidade e desempenho. Algumas jurisdições podem ditar esse equilíbrio, enquanto outras deixam que os seus próprios dispositivos encontrem um equilíbrio adequado para a sua organização.

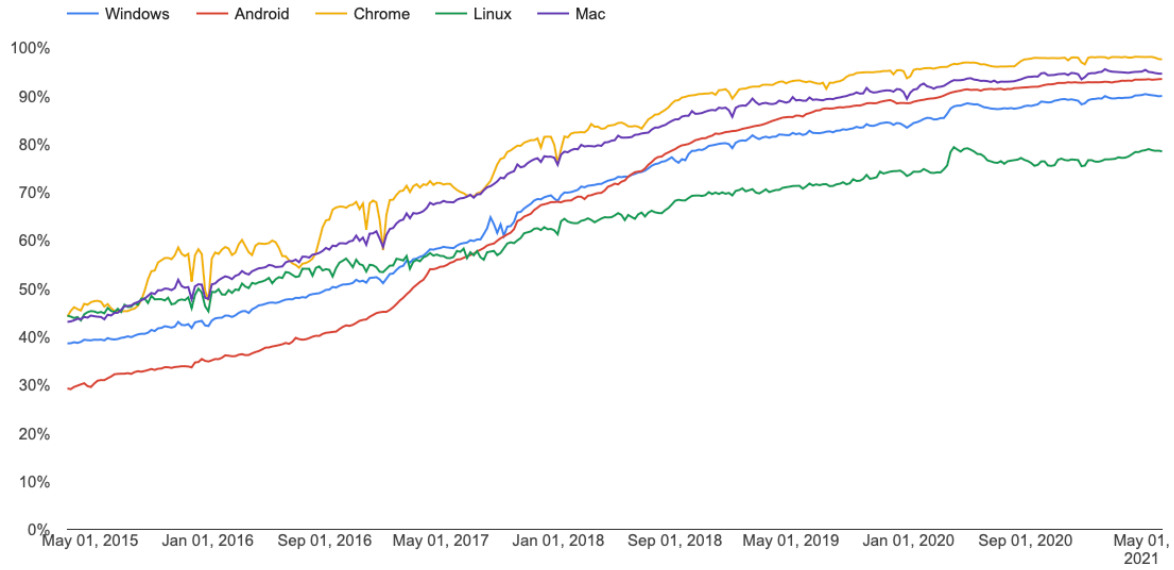
Infelizmente, as limitações nas soluções de inspeção TLS na maioria dos firewalls disponíveis hoje no mercado forçam as organizações a adotarem uma abordagem bastante desbalanceada: as necessidades de segurança e conformidade são sacrificadas no esforço para oferecer desempenho e interoperabilidade essenciais.

O volume do tráfego criptografado está chegando a 100%

A maioria das conexões de Internet já são totalmente criptografadas. De fato, e de acordo com o Google Transparency Report, mais de 90% das sessões da Web já são criptografadas, um aumento drástico dos cerca de 60% de dois anos atrás.

Google Transparency Report

Percentage of pages loaded over HTTPS in Chrome by platform



O volume do tráfego criptografado subiu drasticamente nos últimos dois anos, se encaminhando para os 100%.

A criptografia tornou o seu firewall irrelevante?

Esse crescimento drástico no tráfego criptografado criou um imenso ponto cego na segurança para a maioria das organizações. Os firewalls atuais simplesmente não conseguem inspecionar todo esse volume de sessões criptografadas. Na verdade, a criptografia TLS tornou a maioria dos firewalls irrelevante, já que não têm mais informações sobre grande parte do tráfego que passa através da rede.

O verdadeiro perigo está nas ameaças ocultas no tráfego criptografado

Com o crescimento explosivo em criptografia TLS nos últimos anos, não surpreende que hackers e agentes de ataque estejam seguindo essa tendência para ajudar a inserir malwares na sua rede sem serem notados – e ali mantê-los.

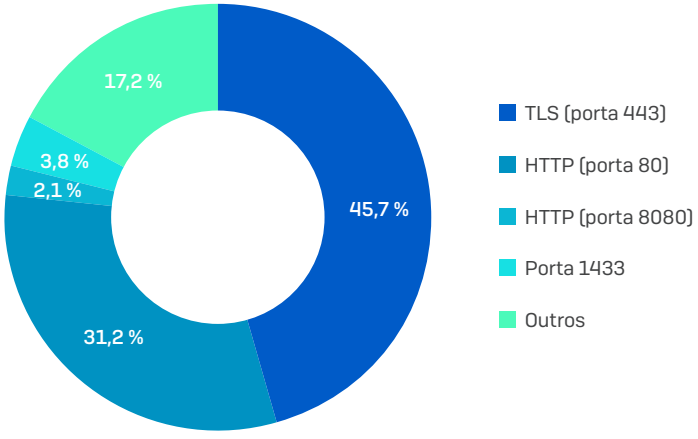
Em particular, vimos um aumento no uso de TLS em ataques de ransomware no decorrer do último ano, especialmente em ransomwares implantados manualmente — em parte devido ao uso por invasores de ferramentas modulares que se aproveitam da criptografia. Mas a maioria do tráfego TLS malicioso se origina de um malware de comprometimento inicial: loaders, droppers e instaladores baseados em documentos voltam às páginas da Web seguras para restaurar seus pacotes de instalação.

Praticamente todas as ameaças agora entram na rede através de conexões criptografadas.

Uma vez que a ameaça chegar à rede, ela se utilizará de todos as artimanhas possíveis para não ser detectada. O uso de TLS permite que os comandos enviados ao cliente a partir de servidores de controle permaneçam sem detecção e, ao mesmo tempo, ocultem a informação coletada da rede e também outras cargas baixadas para o host comprometido.

Não surpreende que houve um aumento drástico no último ano em malwares usando TLS para ocultar essas comunicações. Em 2020, 23% dos malwares que detectamos se comunicando pela Internet usavam TLS; hoje, esse valor chega a quase 46%.

Comunicações de C2 de Malware, TLS x Outros, T1 2021

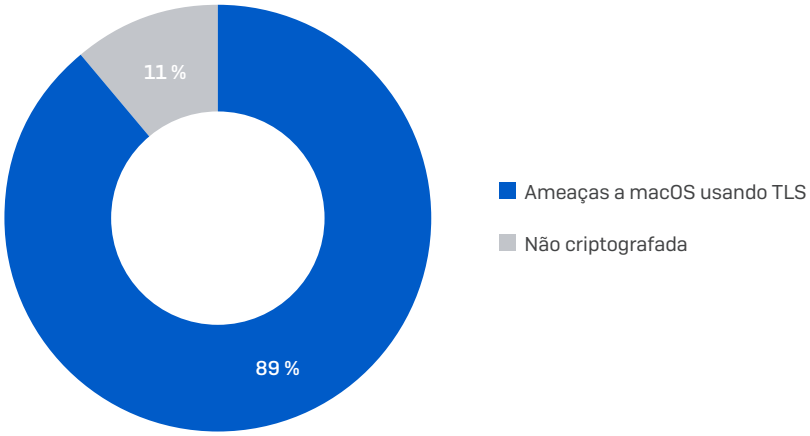


Detalhamento das comunicações de saída de malware

Há também uma proporção significativa de comunicações TLS que usam uma porta de protocolo IP diferente da 443 — como um malware usando um proxy SOCKS ou Tor através de um número de porta fora do padrão.

Os hackers também estão começando a hospedar conteúdo malicioso em serviços de compartilhamento legítimos, como Discord, Github e Google Cloud, que utilizam a criptografia TLS para assegurar a privacidade de conteúdo. Isso oferece a perfeita ofuscação para malwares, permitindo que as ameaças entrem na maioria das redes sem serem notadas.

Não são apenas as ameaças que estão utilizando a criptografia para se manterem ocultas: os aplicativos potencialmente indesejados, como spywares, adwares e barras de ferramentas de navegador, além de clientes de compartilhamento de arquivos ponto a ponto e ferramentas de impedimento de proxy, também usam a criptografia para escapar da detecção pelo firewall. Isso se aplica especialmente à plataforma macOS, em que 89% das ameaças a macOS, como comunicações C2, usaram TLS para fazer o call home ou recuperar código nocivo adicional.



A maioria das organizações não tem poder de ação

Como observamos, a inspeção TLS é complexa e apresenta uso intensivo de recursos. Além disso, com mais de 90% do tráfego de rede agora criptografado, poucos firewalls estão preparados para o trabalho.

A realidade é que a maioria dos firewalls atuais não oferece as capacidades de inspeção TLS necessárias. Eles não são capazes de determinar de modo inteligente o que deve ou não ser inspecionado, não sendo capaz de lidar com a enorme carga necessária para descriptografar tudo. Além disso, os mecanismos de processamento de pacotes e inspeção profunda de pacotes (DPI) não foram criados para lidar eficientemente com a inspeção TLS. Somando-se a isso, as implementações de inspeção que não suportam os padrões mais recentes resultarão na redução da segurança, deixando as organizações abertas a vulnerabilidades e criando condições bastante insatisfatórias para o usuário.

O rápido aumento no tráfego de rede criptografado, acompanhado da incapacidade da maioria dos firewalls Next Gen de inspecionar esse tráfego, deu vez a um imenso rebuliço na segurança de redes.

Cinco características que seu próximo firewall deve ter

Para minimizar o risco de tráfego de rede criptografado, assegure-se de que o seu próximo firewall inclua estas cinco funcionalidades de Inspeção TLS:

1. Um mecanismo de streaming moderno e de alto desempenho que suporte os mais recentes padrões, como TLS 1.3, e funcione de maneira eficaz entre todas as portas/protocolos para identificar ameaças e tráfego arriscado.
2. Listas de exclusões inteligentes predefinidas que sejam atualizadas dinamicamente para evitar quebrar o link da Internet de sites e serviços que não suportam ou não exigem descriptografia.
3. Visibilidade no painel dos seus fluxos de tráfego criptografado e possíveis controvérsias com sites e serviços incompatíveis, permitindo que você adicione excepções dinamicamente antes que se tornem um problema.
4. Validação de certificado robusta capaz de lidar com certificados inválidos, autoassinados, revogados ou não confiáveis e evitar possíveis ataques man-in-the-middle (MITM) maliciosos.
5. Ferramentas de política que permitam analisar a privacidade de usuários, a segurança organizacional e o desempenho para encontrar o equilíbrio perfeito das suas necessidades.

Sophos Firewall – Projetado para a Internet criptografada moderna

A arquitetura Xstream totalmente nova e os dispositivos Série XGS do Sophos Firewall oferecem a melhor solução de inspeção TLS disponível em um firewall, permitindo eliminar o ponto cego da sua criptografia TLS sem causar impacto no desempenho. Você recebe:

- Alto desempenho – um mecanismo leve e reformulado com alta capacidade de conexão
- Visibilidade incomparável dos seus fluxos de tráfego criptografado e erros com a opção de adicionar exclusões com apenas dois cliques
- Segurança superior, com suporte a TLS 1.3 e todos os pacotes de codificação modernos com validação de certificado robusta
- Inspeção de todo o tráfego, independentemente de aplicativo e porta
- Uma extensa lista de exclusões incorporada para assegurar desempenho ideal e excelente experiência do usuário com incrível interoperabilidade para evitar a quebra do link com a Internet
- Ferramentas avançadas de política, que oferecem o equilíbrio perfeito entre desempenho, privacidade e proteção

Para saber mais, leia o Resumo da solução XG Firewall ou inicie uma demonstração instantânea online em www.sophos.com/firewall.

Experimente agora gratuitamente

Experimente o Sophos Firewall online gratuitamente
sophos.com/demo

Vendas na América Latina
E-mail: latamsales@sophos.com

Vendas no Brasil
E-mail: brasil@sophos.com

© Copyright 2020-21. Sophos Ltd. Todos os direitos reservados.
Empresa registrada na Inglaterra e País de Gales sob o nº. 2096520, The Pentagon, Abingdon Science Park, Abingdon, OX14 3YP, Reino Unido
A Sophos é marca registrada da Sophos Ltd. Todos os outros nomes de produtos e empresas mencionados são marcas comerciais ou marcas registradas de seus respectivos proprietários.

21-06-17 PTBR (DD)