DECRIPTAÇÃO: POR QUE, ONDE E COMO

Por que: o caso para decriptação

O tráfego criptografado da Internet com protocolos Secure Sockets Layer ou Transport Layer Security, respectivamente SSL e TLD, está em franca ascensão. De acordo com o Google® Transparency Report: "Os usuários de desktops carregam mais da metade das páginas que são visualizadas através do HTTPS e gastam dois terços de seu tempo em páginas HTTPS. "[1]

Dados os benefícios básicos da criptografia, a troca privada e segura das informações pela internet, e a conformidade com certos regulamentos, como HIPAA (Health Insurance Portability and Accountability Act, PCI (Payment Card Industry) e DSS (Data Security Standard), espera-se que a tendência ascendente à adoção ao SSL cresça. A próxima grande melhoria do HTTP 1.1 é o HTTP/2, e embora o padrão não exija criptografia, a maioria dos clientes que o implementaram declararam que só vão suportar o HTTP/2 com TLS, o que torna a criptografia obrigatória na prática. Grandes navegadores como Chrome®, Firefox®, Safari® e Internet Explorer® estão marcando páginas HTTP como "não seguras" em vários graus.

A criptografia é um grande meio para a troca segura e confidencial de informações de negócios e é necessária para a conformidade. Contudo, o tráfego criptografado se resume, basicamente, a dados obscuros que impedem que as organizações enxerguem as ameaças à segurança neles contidas. Infelizmente, os criminosos aprenderam a explorar esta falta de visibilidade e identificação para se esconderem das inspeções de segurança dentro do tráfego criptografado e entregarem malwares. Até mesmo sites legítimos que usam SSL podem ser infectados com malwares. Além disso, os invasores usam cada vez mais aplicativos SaaS para entregar malware. Um invasor pode colocar um arquivo infectado em uma pasta compartilhada legítima no aplicativo de armazenamento de arquivos sancionados de uma organização, como Box ou Dropbox®, e, de lá, o arquivo infectado pode se disseminar facilmente entre os usuários que sincronizarem estes arquivos com a pasta.

Figura 1: Exemplos de malware transferido por tráfego criptografado com base na pesquisa de ameaças da Unit 42 da Palo Alto Networks

Sem a capacidade de fazer a decriptação, classificar, controlar e fazer a varredura do tráfego SSL criptografado, é impossível que uma organização proteja seus negócios e seus dados valiosos contra as ameaças modernas de forma apropriada. É então que a decriptação SSL (a capacidade de fazer a decriptação, inspecionar e codificar novamente o tráfego da internet antes que ele seja enviado para seu destino) entra em jogo. A decriptação, uma das "10 Coisas que a seu próximo Firewall deve fazer", é necessária para várias ações relacionadas à segurança, incluindo a prevenção de ameaças, prevenção avançada de malware, bloqueio de arquivos, filtragem de dados e bloqueio de páginas maliciosas da web.

Onde você deve fazer a decriptação? Opções

Muitas opções técnicas estão disponíveis para fazer a decriptação do tráfego na sua rede, incluindo proxies da web, controladores de entrega de aplicativos, dispositivos de visibilidade SSL e firewalls de última geração. O melhor lugar para fazer a decriptação do tráfego SSL depende de qual opção oferece a melhor proteção com o menor custo de gerenciamento, em outras palavras, o maior retorno de investimento em segurança.

Proxies da Web

Um proxy da web age como o "intermediário", decodificando e inspecionando o tráfego de saída antes de codificá-lo novamente e enviá-lo para o seu destino (veja a Figura 2). Contudo, os proxies da web estão limitados a inspecionar e proteger o tráfego da web, incluindo HTTP e HTTPS. Normalmente, eles são implantados em portas da web bem conhecidas, como a 80 e a 443. Se um aplicativo usa portas ou protocolos não-web, os proxies da web não podem visualizar o tráfego, frustrando a finalidade de ter completa visibilidade e controle do tráfego criptografado na sua rede. É como implementar segurança somente nos principais aeroportos, deixando os outros expostos. Os proxies também exigem que você mude as configurações de proxy dos navegadores ou use um arquivo de configuração automática do proxy, o que aumenta o custo do gerenciamento e de outra área para diagnosticar se os usuários não podem acessar a internet.

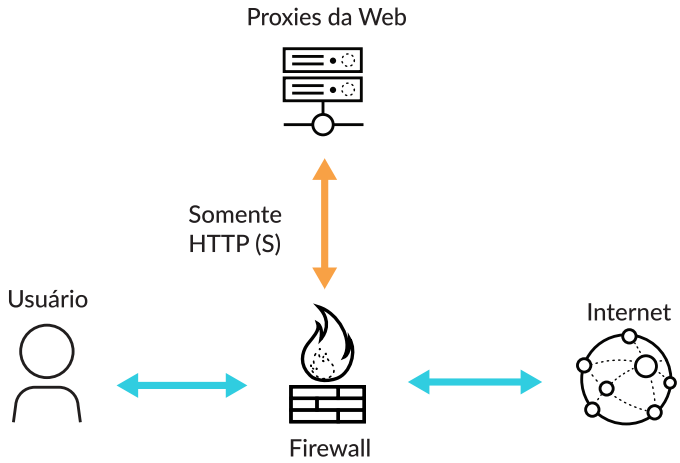

Figura 2: Decriptação e nova criptografia por um proxy da web

Controladores de entrega de aplicativo (sigla em inglês: ADC)

Descarregar o SSL é uma das funções realizadas pelos controladores de entrega de aplicativo. Uma implantação ADC geralmente exige duas

1. https://transparencyreport.google.com/https/overview?hl=en

caixas separadas: uma para decriptação do tráfego, outra para criptografá-lo novamente.

O problema das implantações ADC é que o tráfego viaja sem criptografia entre os dispositivos ADC, o que significa que pessoas não autorizadas de TI ou qualquer pessoa com acesso à rede física que esteja conectando os dispositivos tenha acesso fácil aos dados. Um inimigo pode fazer o espelhamento de porta e executar uma interceptação de pacote de dados para extrair dados sigilosos de textos limpos. Isso compromete a promessa de confidencialidade total, que é um dos propósitos fundamentais da criptografia, além de violar leis de conformidade em alguns setores e geografias.

Dispositivos de visibilidade SSL

Os dispositivos de visibilidade SSL decodificam o tráfego e o disponibilizam para todas as outras funções de segurança da rede que precisam inspecioná-lo, como proxies da web, sistemas de prevenção de perda de dados e antivírus (veja a Figura 3).

O problema é que estes dispositivos aumentam o capex e o opex. Além do custo único, um dispositivo de visibilidade SSL também se torna mais um dispositivo na rede que precisa de gerenciamento, manutenção e atualização, com configurações e base de regras totalmente diferente de outros dispositivos de segurança. Se, em vez disso, for usado um único dispositivo para decriptação e intermediação do tráfego em todos os dispositivos complementares, não haverá necessidade de incluir dispositivos de visibilidade SSL.

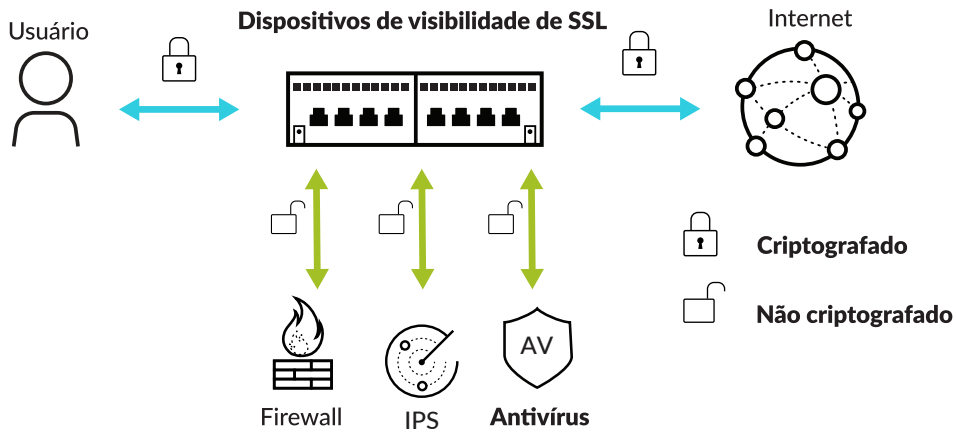

Figura 3: Decriptação através de um dispositivo de visibilidade de SSL

Onde você deve fazer a decriptação? Recomendação

As organizações estão substituindo rapidamente firewalls antigos, ou tradicionais, por firewalls de última geração. Na verdade, de acordo com a Gartner, agora o "firewall empresarial" é sinônimo de NGFW[2]. Os NGFWs incluem funções de segurança, como controle de aplicativos e usuários, sistemas de prevenção de intrusão, filtragem de URL, antivírus de rede e análise avançada de malware. Os clientes estão usando as oportunidades de atualização de firewall para consolidar vários dispositivos de segurança em um NGFW, para se beneficiarem com a economia, melhora na segurança e facilidade de gerenciamento de um único dispositivo. Além disso, reduzir o número de dispositivos e consolidar as funções de segurança reduz drasticamente a complexidade e o tempo gasto para a solução de problemas, já que a topologia da rede é muito mais simples.

Firewalls de última geração com e sem decriptação		
Casos de usos suportados	**Com decriptação**	**Sem decriptação**
Identificar o tamanho da carga útil, largura de banda	✓	✓
Identificar a fonte do tráfego - quem e quando dentro da empresa	✓	✓
Identificar o endereço de IP, a porta e o protocolo da fonte e do destino	✓	✓
Identificar o aplicativo usado	✓	—
Identificar o tipo de dados enviados	✓	—
Identificar se houve violação das políticas de uso da empresa	✓	—
Parar a transferência de tipos específicos de arquivos (como por exemplo .EXE, .RAR)	✓	—
Acabar com a perda de dados sigilosos	✓	—
Identificar e parar ameaças dentro de um túnel criptografado	✓	—

Figura 4: NGFWs com e sem decriptação

2. "Quadrante Mágico para Firewalls de Rede Empresarial", 10 de julho de 2017 por Adam Hils, Jeremy D'Hoinne, Rajpreet Kaur.

Os NGFWs são os dispositivos mais adequados para a decriptação de tráfego, e oferecem várias vantagens:

1. O tráfego decodificado é armazenado em memória e não é enviado para outros dispositivos. Isso preserva a promessa de confidencialidade do SSL e atende os regulamentos de conformidade.
2. Os NGFWs podem ver e fazer a decriptação do tráfego de todas as portas, oferecendo visibilidade de todos os aplicativos, usuários, conteúdos e ameaças.
3. Ao consolidar várias funções em um único dispositivo, um NGFW oferece melhorias na segurança. Por exemplo, ele pode bloquear ameaças conhecidas usando a proteção contra vulnerabilidade, antivírus e assinatura anti-spyware, e bloquear sites maliciosos. Ele também pode enviar novas possíveis ameaças para o ambiente de análise avançada de malwares. Se as ameaças forem identificadas, as novas proteções podem ser entregues e distribuídas mundialmente em alguns minutos.
4. Um NGFW pode intermediar o tráfego decodificado para outros dispositivos complementares conforme adequado, como para retenções de longo prazo dos logs em dispositivos forenses.
5. Os NGFWs oferecem interfaces de gerenciamento fáceis de usar, reduzindo a complexidade e opex. Você pode, por exemplo, combinar aplicativos, usuários, conteúdos, URLs, a prevenção de ameaças e a análise avançada de malwares em uma única regra.

Critério de compra do NGFW para suas necessidades de decriptação

Nem todos os NGFWs são iguais, e infelizmente pode ser difícil distinguir entre firewalls com argumentos similares. É importante ter diretrizes claras para avaliar um NGFW antes de comprá-lo. Isso garante que o firewall pode suportar uma estratégia abrangente de prevenção a brechas, incluindo a decriptação SSL.

Consulte o "Guia do comprador de firewall" para obter uma lista com todos os requisitos empresariais que o seu próximo firewall deve atender, além de conselhos sobre como criar um RFP e um plano de testes funcionais para ajudar o fornecedor e o processo de seleção do produto.

Veja alguns critérios para comparar os recursos de decriptação SSL dos NGFWs:

1. **Escolher o que decriptar:** as preocupações com privacidade e regulamentos exigem que o seu NGFW possa fazer a decriptação do tráfego seletivamente com base em critérios flexíveis o suficiente para se adequarem às suas necessidades. Esses critérios podem incluir usuários, URLs, categorias de URL, como finanças ou saúde, listas de URLs hospedados externamente para estarem de acordo com os regulamentos, origens e destinos baseados em endereço IP; portas; e protocolos. Para capturar um possível malware, o firewall também deve permitir que você exclua aplicativos da decriptação quando eles estiverem sendo executados em suas portas padrão mas continuem a fazer a decriptação dos mesmos aplicativos quando eles forem detectados em portas não padrão.
2. **Excluir aplicativos que possam parar com a decriptação:** os fornecedores de aplicativos podem usar HTTP Public Key Pinning, também conhecido como pinning de certificado, para combater a falsificação pelos invasores que usem certificados emitidos erroneamente ou que sejam fraudulentos. Quando esta técnica é empregada, os dispositivos de segurança da rede podem parar alguns aplicativos com a decriptação. Seu NGFW deve permitir a exclusão com facilidade de tal tráfego usando o nome do host do website ou do aplicativo na regra de exclusão. Se o NGFW forçar a definição de exclusões com base em nomes distintos e comuns dos certificados, ele será muito complexo. Para facilitar ainda mais, o NGFW deve fazer os envios com exclusões pré-definidas para aplicativos bem conhecidos que parem com a decriptação.
3. **Aplicar status dos certificados:** pode ser que você queira diminuir o tráfego do certificado SSL que expirou, do emissor do certificado do servidor que não é confiável ou do certificado que foi revogado. O seu NGFW deve permitir que você aceite ou recuse o tráfego que estiver de acordo com qualquer combinação destes critérios.
4. **Aplicar conjuntos de cifras:** os pacotes de criptografia incluem os principais algoritmos de troca, como RSA, DHE e ECDHE; algoritmos de criptografia, como 3DES, RC4 e variáveis do AES e algoritmos de autenticação, como MD5 e variáveis do SHA. O NGFW deve suportar vários conjuntos de cifras e permitir que você aplique aqueles que atendam seus requisitos de segurança. Você deve poder escolher se quer permitir ou bloquear o tráfego que não atende aos conjuntos de cifras especificados.
5. **Aplicar a versão do protocolo:** pode ser preciso aplicar o uso de versões específicas do SSL/TLS, como TLS 1.2. O NGFW deve oferecer flexibilidade para a aplicação de versões específicas do protocolo e bloquear o tráfego que usa qualquer versão mais fraca.
6. **Integração com os módulos de segurança de hardware (sigla em inglês HSM):** um HSM é um dispositivo físico que gerencia as chaves digitais, incluindo a geração e o armazenamento seguro. Ele oferece proteção lógica e física desses materiais contra o uso não autorizado e potenciais inimigos. O seu NGFW deve poder se integrar com o HSM para armazenar as chaves secretas e as chaves mestre. Mesmo que a sua empresa não exija que essas chaves sejam armazenadas no HSM atualmente, essa funcionalidade pode ser necessária no futuro.
7. **Permitir que os usuários escolham não usar a decriptação SSL:** em alguns casos, pode ser preciso alertar os usuários que o NGFW está decodificando determinado tráfego da web e permitir que as sessões que eles não querem que sejam inspecionadas sejam finalizadas. O seu NGFW deve permitir que o usuário escolha não usar o SSL, então o usuário será notificado de que a decriptação da sessão será feita e ele pode escolher entre continuar ou finalizar a sessão.
8. **Fazer a decriptação do tráfego de entrada e de saída:** o NGFW deve poder fazer a decriptação do tráfego em ambas as direções para que você tenha a flexibilidade de implementá-la perante os usuários ou seus servidores da web para fazer a decriptação

do tráfego de saída ou o de entrada, respectivamente.

9. **Decriptação SSH:** a maioria do tráfego da internet é criptografado por SSL/TLS. Contudo, o Secure Shell, ou SSH, também pode ser usado para criptografar o tráfego e colocá-lo em túnel dentro da sua rede. Por exemplo, alguns aplicativos internos de centros de dados podem usar SSH, o que é permitido pela política. Para impedir que os usuários usem o SSH para contornar seu uso aceitável ou as políticas de prevenção de ameaças, o seu NGFW deve suportar a decriptação do tráfego SSH que atenda seus critérios.
10. **Usar hardware de aceleração de criptografia:** a decriptação SSL faz uso intenso de recursos. O seu NGFW deve usar um hardware para aceleração da criptografia para manter o alto desempenho enquanto decodifica o tráfego.
11. **Compartilhar a inteligência de ameaças e parar ameaças em todos os lugares com base na inteligência de ameaças compartilhada:** há casos em que o tráfego não é decodificado no NGFW devido às preocupações com a privacidade ou pinning dos certificados, por exemplo. Nesses casos, se o NGFW for parte de uma plataforma que atua com a inteligência de ameaças coletadas da rede, endpoints e da nuvem, você ainda poderá parar as ameaças, mesmo que o tráfego não seja decodificado na rede. Digamos que uma ameaça passou pela rede sem ser detectada no tráfego criptografado e chega no endpoint. A plataforma compartilha a inteligência de ameaças entre a rede, o endpoint e a nuvem, e a proteção avançada de endpoint com base nesta inteligência compartilhada vai bloquear a ameaça antes que aconteçam novos ataques. Além disso, as informações sobre essa ameaça são compartilhadas com toda a plataforma para deixar a segurança da rede e da nuvem mais inteligente. Essa é uma vantagem inconfundível que um NGFW agindo sozinho pode oferecer.

É melhor que o seu fornecedor do NGFW tenha planos de suporte para as próximas tendências progressivas, que provavelmente se tornarão essenciais:

- **HTTP/2:** esta é uma grande revisão do protocolo de rede HTTP usado pela World Wide Web. Ele foi desenvolvido a partir do protocolo SPDY anterior, que era experimental e que foi desenvolvido originalmente pela Google. Embora o padrão não exija criptografia, a maioria dos clientes que o implementaram declararam que só vão suportar o HTTP/2 com TLS, o que torna a criptografia obrigatória na prática.
- **TLS 1.3:** depois de ser aprovado pela Internet Engineering Task Force, o TLS 1.3 deve fazer as conexões seguras da internet mais seguras e rápidas. Os destaques do TLS 1.3 incluem a entrega mais rápida dos dados, eliminando a criptografia não-AEAD e a troca de chaves não-PFS, e descartando a renegociação.

O impacto na segurança da intercepção do HTTPS

A University of Michigan, University of Illinois Urbana-Champaign e outras publicaram um estudo em 2017 chamado "The Security Impact of HTTPS Interception" (O impacto na segurança da intercepção do HTTPS), que examina a preponderância e o impacto da intercepção do HTTPS pelos dispositivos de segurança da rede. As descobertas indicam que quase todas as intercepções reduzem a segurança da conexão, e muitas delas apresentam graves vulnerabilidades.

Isso é de interesse dos administradores de segurança de rede porque a intenção por trás da intercepção e decriptação do tráfego HTTPS é obter visibilidade e controle. Este estudo indica vários motivos do porquê as intercepções reduzem a segurança das conexões:

- A configuração padrão de vários desses dispositivos de segurança de rede enfraquece a segurança, por exemplo, ao usar criptografia baseada em RC4.
- Vários dispositivos quebraram a validação do certificado.
- O processo de instalação de vários dispositivos é convoluto e propenso a falhas.
- A configuração do dispositivo é confusa.

Portanto, é muito importante garantir que o seu NGFW:

- Não habilite a criptografia baseada em RC4 por padrão. As melhores práticas da política de segurança recomendada devem evitar algoritmos fracos, como MD5, RC4, SHA1 e 3DES.
- Bloqueie certificados inválidos por padrão, incluindo sessões com certificados expirados, certificados com emissores não confiáveis e certificados com status desconhecidos.
- Bloqueie sessões com versões não suportadas. As melhores práticas da política de segurança recomendada devem bloquear o uso de versões vulneráveis do SSL/TLS, incluindo TLS 1.0 e SSLv3.
- Use o protocolo de status do certificado online (sigla em inglês: OSCP) e /ou as listas de certificados revogados (sigla em inglês: CRL) para verificar o status de revogação dos certificados.
- Não armazene tráfego decrepitado em disco. As informações devem ser armazenadas somente em memória, atendendo aos requisitos regulatórios e de segurança.

Em suma, a decriptação do tráfego sozinha pode enfraquecer a segurança. Contudo, dada a devida diligência ao se comprar um NGFW, e se você seguir as melhores práticas, a decriptação vai oferecer a visibilidade necessária em todo o tráfego e também vai protegê-lo de inimigos que escondem ameaças em túneis criptografados.

Pessoas	**Várias equipes precisam trabalhar juntas:** • A equipe jurídica/de conformidade deve decidir quais tipos de tráfego podem ser decrepitados. • A equipe de recursos humanos deve informar o impacto da decriptação para todos que usam sua rede, incluindo os colaboradores, visitantes e fornecedores. Além disso, as políticas de uso do computador, concessão de registro para visitantes e as políticas de uso para fornecedores devem ser todas atualizadas para continuarem conformes. • A equipe de governança de segurança deve gerenciar a infraestrutura da chave pública (sigla em inglês: PKI). • A equipe de TI deve instalar os certificados nos endpoints, além de gerenciar os projetos e o dimensionamento. • A equipe de servidores deve garantir a decriptação do tráfego de entrada destinado a servidores da web.
Proces-so	**Habilitar a decriptação SSL envolve vários processos, como:** • Análise de desempenho para projetos e dimensionamento. • Teste de impacto na experiência dos usuários e problemas de implantações, além de cenários como certificados expirados e exclusão de usuário. • Suporte das operações para tratar de possíveis problemas relacionados com a decriptação. • Troca de controle e implantação gradual da decriptação.
Ferra-mentas	**O sucesso da implantação e a análise dos resultados exige ferramentas para várias funções, incluindo:** • Gerenciamento de certificado. • Análise de desempenho da rede. • NGFW para criação de política de decriptação, exclusões, registros e relatórios.

Como habilitar a decriptação SSL: pessoas, processos e ferramentas

Habilitar a decriptação SSL não se trata apenas de ter a tecnologia certa. O trio: pessoas, processos e ferramentas também deve estar alinhado e trabalhar em conjunto, visando o mesmo objetivo.

Como habilitar a decriptação SSL: melhores práticas

Com um acordo entre as equipes e com os processos e ferramentas adequados, você pode começar a decriptação do tráfego. Siga estas melhores práticas para melhorar os resultados e evitar as armadilhas comuns:

1. **Defina o tráfego sigiloso que não deve ser decrepitado:** as melhores práticas dizem que você deve fazer a decriptação de todo o tráfego, exceto o que pertence às categorias sigilosas, como saúde, finanças, governo, exército e compras.
2. **Inclua as exclusões que devem evitar a decriptação em casos especiais:** você vai precisar evitar a decriptação em alguns casos, como o tráfego que para com a decriptação, usuários específicos que precisam evitar a decriptação por motivos legais ou websites parceiros que possam ter permissão para evitar verificações rigorosas de certificados. Certifique-se de criar tais exclusões apenas quando for garantido e crie o menor número possível.
3. **Defina as verificações do status de revogação do certificado:** para verificar o status da revogação dos certificados, o NGFW usa OCSP e/ou CRLs. Certifique-se de que os certificados apresentados durante a decriptação SSL são válidos ao configurar o firewall para realizar as verificações CRL/OCSP.
4. **Configure conjuntos de cifras mais fortes e versões do protocolo SSL:** consulte a sua equipe de governança de segurança para saber quais conjuntos de cifras devem ser aplicados e defina a versão mínima aceitável do protocolo SSL/TLS. Por exemplo, sua equipe de segurança pode querer usar os algoritmos de troca de chave DHE ou ECDHE para habilitar o sigilo encaminhado perfeito (sigla em inglês: PFS), junto com o protocolo TLS 1.2. A equipe também pode querer bloquear o uso de versões vulneráveis de SSL/TLS, como o TLS 1.0 e SSLv3, e evitar algoritmos fracos, como MD5, RC4, SHA1 e 3DES. Aplique as recomendações de sua equipe de segurança no seu NGFW.
5. **Implemente o certificado de decriptação da autoridade de certificado raiz da sua empresa:** implemente este certificado no seu NGFW para que os usuários finais não vejam mensagens de aviso do certificado SSL.
6. **Decriptação SSH além de SSL:** o SSH é necessário para alguns aplicativos, mas pode ser usado impropriamente, conforme mencionado anteriormente. Por este motivo, recomenda-se que você permita que o SSH seja usado somente por aplicativos e usuários que precisam dele, além de habilitar a decriptação SSH.

Para saber mais, veja nossos outros recursos:

- ✓ **Página da web da decriptação SSL**
- ✓ **Avaliação de melhores práticas:** esta avaliação complementar ajudará a maximizar a capacidade do seu NGFW, como a decriptação SSL, para bloquear ataques cibernéticos bem-sucedidos.

3000 Tannery Way
Santa Clara, CA 95054

Principal: +1.408.753.4000
Vendas: +1.866.320.4788
Suporte: +1.866.898.9087

www.paloaltonetworks.com

decryption-why-where-and-how-wp-091918