Esclareça o impacto no desempenho e as práticas recomendadas para descriptografia SSL/TLS em FTD

Contents

Problema

Um usuário planeja habilitar a decodificação SSL/TLS em um dispositivo FTD (Firewall Threat Defense, defesa contra ameaças de firewall) e precisa entender o impacto potencial no desempenho do dispositivo antes da implementação. As principais preocupações incluem:

- Impacto na taxa de transferência do firewall, latência e desempenho geral de processamento de tráfego.
- Aumento esperado da utilização da CPU e da memória após habilitar a descriptografia.
- Diretrizes de dimensionamento e parâmetros de desempenho para modelos específicos de FTD.
- Limites recomendados em sessões descriptografadas simultâneas.
- Práticas recomendadas e pré-requisitos para a implantação da produção.

Ambiente

- Firepower 4115. Outras plataformas de hardware também podem ser afetadas.
- FTD Versão 7.4.2 (Build 172). Outras versões de software também podem ser afetadas.
- Consideração do recurso de descriptografia de SSL/TLS.
- Planejamento de implantação do ambiente de produção.

Resolução

A descriptografia SSL/TLS adiciona sobrecarga de processamento ao Firepower 4115, mas o impacto real depende muito da quantidade de tráfego descriptografado e da inspeção aplicada após a descriptografia.

Análise do impacto no desempenho

Os impactos da descriptografia SSL/TLS incluem:

- Throughput efetivo mais baixo.
- Maior latência.
- Aumento do uso de CPU de Snort/Inspection.
- Aumento da CPU e da memória que não pode ser previsto com precisão como uma porcentagem fixa sem a análise do perfil de tráfego real.

Benchmarks de desempenho do FPR 4115

Especificações de benchmark do Firepower 4115 publicadas da Cisco:

- Taxa de transferência de descriptografia de hardware TLS: 6.5 Gbps.
- Rendimento de FW + AVC: 33 Gbps.
- Máximo de sessões simultâneas com AVC: 15 milhões.
- Máximo de novas conexões por segundo com AVC: 210 mil.

Observação importante sobre dimensionamento: O benchmark de descriptografia de hardware TLS de 6,5 Gbps é baseado em condições específicas de teste. A produtividade de produção pode ser menor se você descriptografar uma grande porcentagem do tráfego, inspecionar o tráfego descriptografado com políticas de intrusão/arquivo/malware ou processar muitas sessões

TLS de curta duração.

A Cisco não publica um número separado de "máximo de sessões descriptografadas simultâneas" para o Firepower 4115 no FTD 7.4.2. Na prática, a capacidade é validada usando combinação de tráfego, sessões simultâneas, taxa de conexão, pacotes de codificação e carga de política de inspeção.

Abordagem recomendada de implantação de produção

Passo 1: Comece com um piloto limitado

- Não ative regras amplas de "descriptografar tudo" inicialmente.
- Comece com os usuários, sub-redes ou categorias de destino selecionados.
- Mantenha o tratamento padrão conservador com Não descriptografar para o tráfego que não requer inspeção.

Passo 2: Excluir o tráfego que geralmente é interrompido com descriptografia

- Sites bancários/financeiros.
- Portais de saúde.
- Aplicativos com certificados fixados.
- Alguns aplicativos de software como serviço (SaaS) e segurança de endpoint/nuvem.
- Aplicativos essenciais aos negócios confidenciais, a menos que sejam testados explicitamente.

Passo 3: Mantenha as regras de SSL simples e ordenadas cuidadosamente

- Coloque as exclusões do tipo Não descriptografar específicas acima das regras de descriptografia mais amplas.
- Evite correspondências excessivamente amplas ou complexas sempre que possível.
- Não use a versão TLS ou as condições do conjunto de cifras para regras de decodificação-

demissão/chave conhecida, pois a Cisco documenta que isso pode causar um comportamento imprevisível.

Passo 4: Validar prontidão do certificado

- Para Decrypt-Resign de saída, o certificado de CA de assinatura deve ser confiável para pontos de extremidade do cliente.
- Para descriptografia de chave conhecida de entrada, o firewall deve ter o material de certificado/chave privada do servidor correto.

Passo 5: Monitorar durante a implementação

- Rastreie a utilização geral da CPU e, mais importante, Snort/inspection CPU.
- Rastreie conexões simultâneas e novas conexões por segundo.
- Revisar erros de handshake/status de fluxo SSL em eventos de conexão.
- Aguarde indicadores de excesso de assinaturas TLS e falhas específicas de aplicativos.

Para obter mais informações sobre como monitorar a verificação da CPU:

- https://www.ciscolive.com/c/dam/r/ciscolive/emea/docs/2026/pdf/BRKSEC-2362.pdf
- Pense como um engenheiro do TAC: Um guia para os pontos problemáticos mais comuns do Cisco Secure Firewall

Para conexões de rastreamento e novas conexões por segundo, verifique:

- Melhores práticas de registo

Para rastrear erros de status/handshake de fluxo SSL na verificação de eventos de conexão e nos indicadores de excesso de assinaturas TLS, verifique:

- Solucionar problemas de assinatura excedente de TLS/SSL

Passo 6: Reverta ou restrinja o escopo se você vir:

- Inspeção sustentada da saturação da CPU.

- Aumento da latência visível ao usuário.
- Falhas de handshake TLS.
- Falha nos aplicativos comerciais após a descriptografia.
- Excesso de assinaturas ou excesso de erros de SSL.

Passo 7: Considere o impacto do TLS 1.3

A adoção do TLS 1.3 pode afetar a visibilidade e o comportamento, já que certas características de handshake e inspeção diferem do TLS 1.2.

Causa

A descriptografia SSL/TLS requer recursos computacionais adicionais para descriptografar, inspecionar e criptografar novamente os fluxos de tráfego. O impacto no desempenho varia significativamente com base nos padrões de tráfego, nas políticas de inspeção aplicadas ao tráfego descriptografado e na configuração de implantação específica. Sem um planejamento adequado e uma implementação gradual, as empresas podem sofrer uma degradação inesperada do desempenho em ambientes de produção.

Conteúdo relacionado

- Guia de configuração de dispositivos do Cisco Secure Firewall Management Center - Regras de descriptografia
- Diretrizes da política de descriptografia do Cisco Secure Firewall
- Prática recomendada para ordem de regra de política de descriptografia
- Simplificando a descriptografia com o Secure Firewall 7.7 da Cisco
- Práticas recomendadas de regras de descriptografia
- Data Sheet do Cisco Firepower 4100 Series
- Suporte técnico e downloads da Cisco

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.