Solucionar Problemas de Quedas de Pacotes FTD (tcp-not-syn) quando "Aplicativo Avançado e Detecção de URL" Está habilitado em interfaces em linha com fluxo de tráfego assimétrico

Contents

Problema

Os dispositivos Firewall Threat Defense (FTD) configurados com conjuntos de interface em linha descartam o tráfego de retorno TCP com o motivo de queda do Accelerated Security Path (ASP) tcp-not-syn. Isso ocorre imediatamente após o recurso TLS Server Identity Discovery (TSID) — especificamente a opção "Detecção de URL e aplicativo aprimorado" ser ativada. Em versões mais antigas do Firewall Management Center (FMC), a opção é chamada de "Detecção antecipada de aplicativos e categorização de URL". Os pacotes TCP SYN-ACK no caminho de retorno são descartados pelo mesmo dispositivo FTD que encaminhou o SYN original, impedindo que as sessões TCP sejam estabelecidas.

O problema se manifesta como falhas generalizadas de conectividade TCP e não está limitado ao tráfego TLS. Estes sintomas são observados quando o recurso é ativado:

- Os pacotes TCP SYN-ACK no caminho de retorno são descartados com o motivo de queda ASP tcp-not-syn.
- Novas sessões TCP não aparecem na tabela de conexão FTD.
- Os contadores de queda de ALTO ASP se acumulam rapidamente, como ilustrado por esta saída capturada aproximadamente 10 minutos após a ativação do recurso:

<#root>

```
device#
```

show asp drop

```
Frame drop:
 Flow is denied by configured rule (acl-drop)                                1

 First TCP packet not SYN (tcp-not-syn)                                  34802

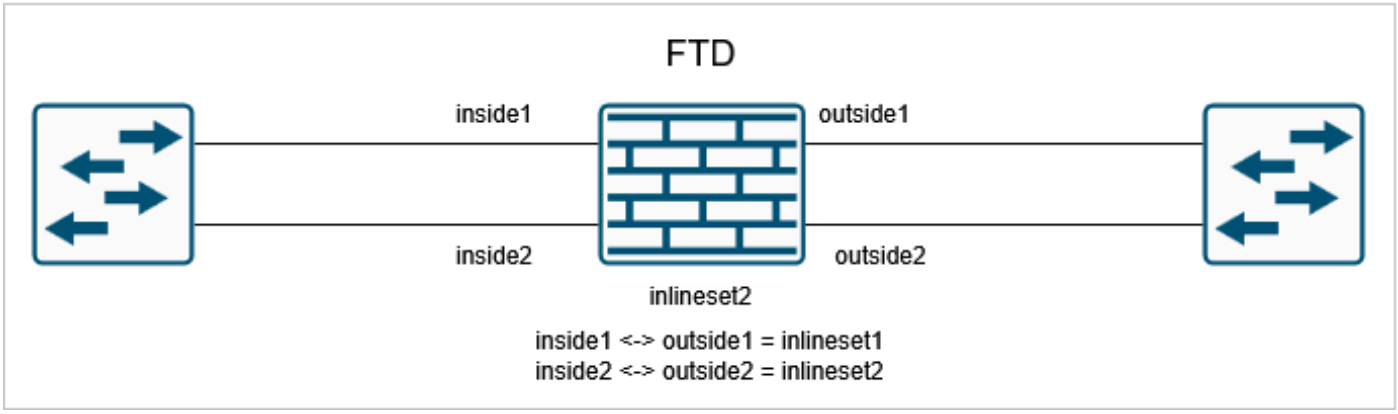

 TCP RST/FIN out of order (tcp-rstfin-ooo)                                   4
 Dst MAC L2 Lookup Failed (dst-l2_lookup-fail)                             995
 Dropped pending packets in a closed socket (np-socket-closed)               3
 TCP Proxy probe reset injected (tcp-proxy-probe-rst-injected)               1
 TCP Proxy probe receive drop (tcp-proxy-probe-tcp-probe-drop)               1
 Blocked or blacklisted by the reputation preprocessor (reputation)          1

Last clearing: 16:50:21 CEST Oct 24 2026 by enable_1
```

Ambiente

- Plataforma: Cisco Firepower 4115. Outras plataformas também podem ser afetadas.
- Versão do software FTD: 7.6.4. Outras versões de software também podem ser afetadas.
- Versão do software FMC: 10.1.0. Outras versões de software também podem ser afetadas.
- FTD com conjuntos de interface em linha.
- O FTD tem pelo menos dois pares de interface em linha: inlineset1 e inlineset2 (ou há dois FTDs diferentes com um inline-set cada).
- Fluxo de tráfego assimétrico presente no ambiente: O TCP SYN sai através da interface outside1 enquanto o TCP SYN-ACK correspondente retorna através da interface outside2 no mesmo dispositivo FTD.
- O recurso TSID está habilitado no FTD.

Topologia



Resolução

A resolução recomendada para parar os descartes de tcp-not-syn e restaurar a conectividade TCP através das interfaces FTD em linha é desabilitar a opção "Detecção Avançada de Aplicativos e URL" dentro do TSID. Isso permite que o desvio de estado TCP permaneça ativo nos conjuntos de interface em linha, o que é necessário para acomodar fluxos de tráfego assimétricos no ambiente.

Desabilitar "Detecção Avançada de Aplicativos e URL" no FMC

Navegue até: Políticas > Controle de Acesso > [Sua Política de Controle de Acesso] > Avançado > Descoberta de Identidade de Servidor TLS. Desmarque ou desative a caixa de seleção "Detecção aprimorada de aplicativos e URL" e implante a política nos dispositivos FTD afetados.

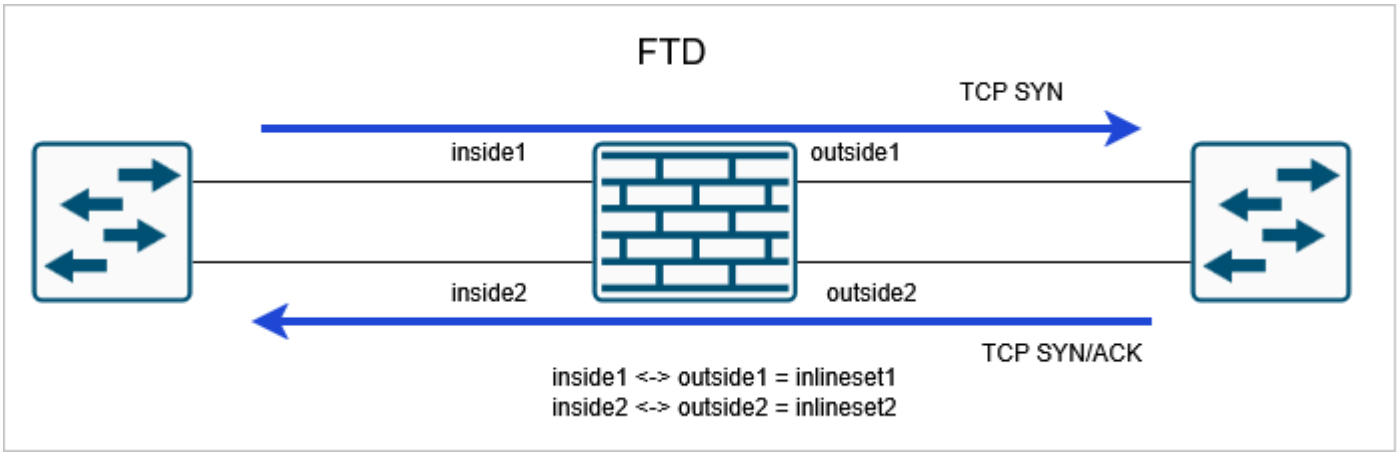
Após desativar o recurso, novas sessões são exibidas na tabela de conexão, confirmando que as conexões TCP estão concluindo o handshake triplo com êxito.

Note: Com o TSID desabilitado, o FTD não pode mais ver o certificado do servidor em sessões TLS 1.3. As regras de aplicativo e URL correspondem o tráfego menos precisamente no tráfego criptografado.

Causa

A causa raiz dos descartes de tcp-not-syn é uma incompatibilidade entre o recurso Descoberta de identidade do servidor TLS e Desvio de estado TCP nos conjuntos de interface embutida no FTD.

Por padrão, para o tráfego que passa por interfaces em linha no FTD, o desvio de estado TCP está habilitado. O desvio de estado de TCP é projetado para permitir que o tráfego assimétrico — onde os caminhos de encaminhamento e de retorno de uma conexão TCP podem atravessar diferentes interfaces ou até mesmo diferentes dispositivos — passe sem que o FTD imponha o rastreamento de estado de TCP estrito. Este é um comportamento necessário em ambientes onde a assimetria de roteamento está presente:

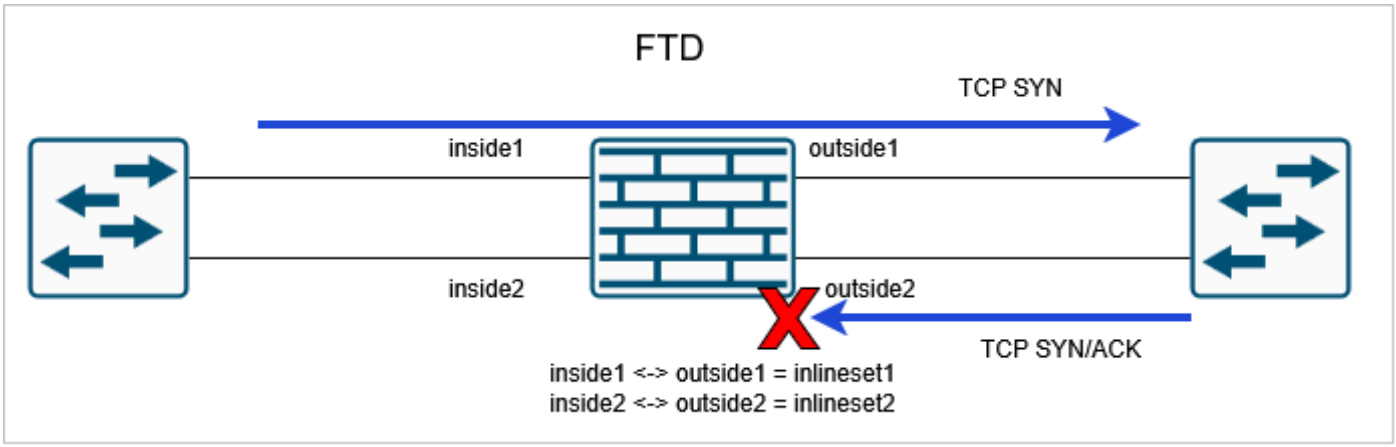


Fluxo TCP assimétrico através de conjuntos em linha FTD quando TSID está desabilitado.

No entanto, quando qualquer um desses recursos estiver habilitado, o sistema FTD substituirá o desvio de estado TCP e começará a executar verificações completas de estado TCP no tráfego da interface em linha:

- A opção "Detecção aprimorada de aplicativos e URL" em Descoberta de identidade do servidor TLS.
- Qualquer política de descriptografia TLS/SSL ativa.

Quando as verificações de estado do TCP são aplicadas, o FTD rastreia a sequência completa de handshake do TCP. Em ambientes com roteamento assimétrico — onde, por exemplo, o pacote TCP SYN sai pela interface outside1, mas o TCP SYN-ACK correspondente retorna pela interface outside no mesmo dispositivo — o FTD não reconhece o SYN-ACK como pertencente a uma sessão TCP rastreada conhecida. Como o SYN-ACK chega em uma interface diferente do esperado e nenhum SYN correspondente foi visto nessa interface, o FTD o classifica como um pacote não-SYN para uma conexão desconhecida e o descarta com o motivo de queda ASP tcp-not-syn.



Fluxo TCP assimétrico através de conjuntos em linha FTD quando TSID está habilitado.

Conteúdo relacionado

- ID de bug Cisco CSCwp84746 — Documentação: Incompatibilidade da Descoberta de Identidade do Servidor TLS com Desvio de Estado TCP em interfaces do conjunto em linha
- ID de bug Cisco CSCwx42897 — DOC: A Descoberta de Identidade do Servidor TLS substitui o Desvio de Estado TCP em interfaces do conjunto em linha, fazendo com que o tráfego TCP seja descartado (tcp-not-syn)
- ID de bug Cisco CSCwx42901 — Adicione um aviso ao ativar "Detecção antecipada de aplicativos e categorização de URL" (TSID) que desativa o desvio de estado TCP em interfaces de conjunto em linha
- Documentação da Cisco — Diretrizes para desvio de estado TCP (inclui restrição de descoberta de identidade de servidor TLS)
- Estudo de caso - Tráfego assimétrico através de conjuntos em linha
- Nota técnica da Cisco — Como gerar pacotes de solução de problemas de FTD e FMC
- 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.