

Fase 8 da solução de problemas de caminho de dados do Firepower: Política de análise de rede

Contents

[Introduction](#)

[Prerequisites](#)

[Solução de problemas do recurso de política de análise de rede](#)

[Usando a ferramenta "trace" para localizar quedas de pré-processador \(somente FTD\)](#)

[Verificar a configuração do NAP](#)

[Exibir configurações de NAP](#)

[Configurações de NAP que podem causar quedas silenciosas](#)

[Verifique a configuração de back-end](#)

[Criando um NAP direcionado](#)

[Análise Falsa Positiva](#)

[Etapas de mitigação](#)

[Dados a fornecer ao TAC](#)

Introduction

Este artigo faz parte de uma série de artigos que explicam como solucionar problemas sistematicamente no caminho de dados em sistemas Firepower para determinar se os componentes do Firepower podem estar afetando o tráfego. Consulte o [artigo Visão geral](#) para obter informações sobre a arquitetura das plataformas Firepower e links para outros artigos de Troubleshooting de Caminho de Dados.

Este artigo abrange o oitavo estágio da solução de problemas de caminho de dados do Firepower, o recurso Network Analysis Policy.



Prerequisites

- Este artigo se aplica a todas as plataformas Firepower
O recurso **trace** está disponível somente na versão de software 6.2.0 e superior para a plataforma Firepower Threat Defense (FTD).
- O conhecimento do Snort de código aberto é útil, mas não obrigatório Para obter informações sobre o Snort de código aberto, acesse <https://www.snort.org/>

Solução de problemas do recurso de política de análise de rede

O Network Analysis Policy (NAP) contém configurações de pré-processador de snort que realizam

inspeções no tráfego, com base no aplicativo identificado. Os pré-processadores têm a capacidade de descartar tráfego, com base na configuração. Este artigo trata de como verificar a configuração do NAP e verificar se há quedas no pré-processador.

Note: As regras do pré-processador têm um ID do gerador (GID) diferente de '1' ou '3' (ou seja, 129, 119, 124). Mais informações sobre o GID para os mapeamentos de pré-processador podem ser encontradas nos [Guias de Configuração](#) do FMC.

Usando a ferramenta "trace" para localizar quedas de pré-processador (somente FTD)

A ferramenta **de rastreamento de suporte do sistema** pode ser usada para detectar quedas executadas no nível do pré-processador.

No exemplo abaixo, o pré-processador de normalização TCP detectou uma anomalia. Como resultado, o tráfego é descartado pela regra **129:14**, que procura marcas de hora ausentes em um fluxo TCP.

```
> system support trace
[omitted for brevity...]
172.16.111.226-51174 - 50.19.123.95-443 6 Packet: TCP, ACK, seq 3849839667, ack 1666843207
172.16.111.226-51174 - 50.19.123.95-443 6 Stream: TCP normalization error in timestamp, window, seq, ack, fin, flags, or unexpected data, drop
172.16.111.226-51174 - 50.19.123.95-443 6 AppID: service unknown (0), application unknown (0)
172.16.111.226-51174 > 50.19.123.95-443 6 AS 4 | 0 Starting with minimum 3, 'block urls', and SrcZone first with zones -1 -> -1, geo 0 -> 0, vlan 0, inline sgt tag: untagged, ISE sgt id: 0, svc 0, payload 0, client 0, misc 0, user 9999997, icmpType 0, icmpCode 0
172.16.111.226-51174 > 50.19.123.95-443 6 Firewall: starting rule matching, zone -1 -> -1, geo 0 -> 0, vlan 0, sgt 65535, user 9999997, icmpType 0, icmpCode 0
172.16.111.226-51174 > 50.19.123.95-443 6 AS 4 | 0 pending rule order 3, 'block urls', URL
172.16.111.226-51174 > 50.19.123.95-443 6 Firewall: pending rule-matching, 'block urls', pending URL
172.16.111.226-51174 > 50.19.123.95-443 6 Snort: processed decoder alerts or actions queue, drop
172.16.111.226-51174 > 50.19.123.95-443 6 IPS Event: gid 129, sid 14, drop
172.16.111.226-51174 > 50.19.123.95-443 6 NAP id 1, IPS id 0, Verdict BLOCK
172.16.111.226-51174 > 50.19.123.95-443 6 ==> Blocked by Stream
```

Note: Embora o pré-processador **TCP Stream Configuration** descarte o tráfego, ele pode fazer isso porque o pré-processador **de normalização em linha** também está ativado. Para obter mais informações sobre a normalização em linha, leia este [artigo](#).

Verificar a configuração do NAP

Na IU do Firepower Management Center (FMC), o NAP pode ser visualizado em **Políticas > Controle de acesso > Intrusão**. Em seguida, clique na opção **Network Analysis Policy** na parte superior direita, depois disso você pode visualizar os NAPs, criar novos e editar os existentes.

Deploy System Help admin

Import/Export Intrusion Rules Access Control **Network Analysis Policy**

Policy Information

Name: My Custom NAP

Description:

Inline Mode

Inline Result | **Source IP** | **Destination IP** | **Source Port / ICMP Type** | **Destination Port / ICMP Code** | **Message**

Inline Result	Source IP	Destination IP	Source Port / ICMP Type	Destination Port / ICMP Code	Message
Dropped	172.16.111.226	50.19.123.95	51177 / tcp	443 (https) / tcp	STREAM5_NO_TIMESTAMP (129:14:2)
Dropped	172.16.111.226	50.19.123.95	51174 / tcp	443 (https) / tcp	STREAM5_NO_TIMESTAMP (129:14:2)

Annotations:
 - Edit or create a Network Analysis Policy (points to 'Network Analysis Policy')
 - Uncheck this box to disable Inline Mode (points to 'Inline Mode')
 - Inline Mode disabled = No Inline Result (points to empty 'Inline Result' cell)
 - Inline Mode enabled = "Dropped" Inline Result (points to 'Dropped' 'Inline Result' cell)

Como visto na ilustração acima, os NAPs contêm um recurso "Modo em linha", que é o equivalente à opção "Soltar quando em linha" na Política de intrusão. Uma rápida etapa de mitigação para impedir que o NAP descarte o tráfego seria desmarcar o **modo em linha**. Os Eventos de Intrusão gerados pelo NAP não exibem nada na guia **Resultado em Linha** com **Modo em Linha** desativado.

Exibir configurações de NAP

No NAP, você pode exibir as configurações atuais. Isso inclui o total de pré-processadores habilitados, seguido pelo comando

pré-processadores habilitados com configurações fora do padrão (aquelas que foram ajustadas manualmente) e aquelas que estão habilitadas com as configurações padrão, como mostrado na ilustração abaixo.

Edit Policy: My Custom NAP

Policy Information

Settings

- Back Office Detection
- DCE/RPC Configuration
- DNS Configuration
- FTP and Telnet Configurati
- GTP Command Channel Cc
- HTTP Configuration
- Inline Normalization
- IP Defragmentation
- Packet Decoding
- SIP Configuration
- SMTP Configuration
- SSH Configuration
- SSL Configuration
- Sun RPC Configuration
- TCP Stream Configuration
- UDP Stream Configuration

Policy Layers

- My Changes
 - Inline Normalization
 - TCP Stream Configurati
- Security Over Connectivity
 - Back Office Detection
 - Checksum Verification

Settings

Application Layer Preprocessors

- DCE/RPC Configuration: Enabled
- DNS Configuration: Enabled
- FTP and Telnet Configuration: Enabled
- HTTP Configuration: Enabled
- Sun RPC Configuration: Enabled
- SIP Configuration: Enabled
- GTP Command Channel Configuration: Enabled
- IMAP Configuration: Disabled
- POP Configuration: Disabled
- SMTP Configuration: Enabled
- SSH Configuration: Enabled
- SSL Configuration: Enabled

SCADA Preprocessors

- Modbus Configuration: Disabled
- DNP3 Configuration: Disabled

Transport/Network Layer Preprocessors

- Checksum Verification: Disabled
- Inline Normalization: Enabled

Annotations:
 - View preprocessors (points to 'Settings')
 - Currently Enabled (points to 'Enabled' radio buttons)
 - Enabled with non-default settings (points to 'My Changes' and 'Security Over Connectivity')
 - Enabled with default settings (points to 'Back Office Detection' and 'Checksum Verification')

Configurações de NAP que podem causar quedas silenciosas

No exemplo mencionado na seção de rastreamento, a regra TCP Stream Configuration rule **129:14** está descartando tráfego. Isso é determinado pela saída **de rastreamento de suporte do sistema**. No entanto, se a referida regra não estiver ativada na respectiva política de intrusão, não serão enviados eventos de intrusão ao CVP.

O motivo disso acontecer é uma configuração no pré-processador **de normalização em linha** chamada **Bloquear anomalias de cabeçalho TCP não resolvíveis**. Essa opção basicamente permite que o Snort execute uma ação de bloqueio quando determinadas regras GID 129 detectam anomalias no fluxo TCP.

Se **Bloquear anomalias de cabeçalho TCP não resolvíveis** estiver ativado, é recomendável ativar as regras GID 129 de acordo com a ilustração abaixo.

The screenshot displays the 'Intrusion Policy' configuration page for GID: "129". It shows a list of 19 rules, with rule 129:14 (STREAMS_NO_TIMESTAMP) selected. A context menu is open over rule 129:14, showing options: 'Generate Events', 'Drop and Generate Events', and 'Disable'. The 'Drop and Generate Events' option is selected. On the right, the 'Policy Information' panel is open, showing the 'Inline Normalization' section. The 'Block Unresolvable TCP Header Anomalies' option is checked and highlighted with a red box. The 'Policy Layers' section is also visible, showing 'Network Analysis Policy'.

Rule ID	Rule Name	Selected
129 4	STREAMS_BAD_TIMESTAMP	<input checked="" type="checkbox"/>
129 5	STREAMS_BAD_SEGMENT	<input type="checkbox"/>
129 6	STREAMS_WINDOW_TOO_LARGE	<input checked="" type="checkbox"/>
129 7	STREAMS_EXCESSIVE_TCP_OVERLAPS	<input type="checkbox"/>
129 8	STREAMS_DATA_AFTER_RESET	<input checked="" type="checkbox"/>
129 9	STREAMS_SESSION_HIJACKED_CLIENT	<input type="checkbox"/>
129 10	STREAMS_SESSION_HIJACKED_SERVER	<input type="checkbox"/>
129 11	STREAMS_DATA_WITHOUT_FLAGS	<input checked="" type="checkbox"/>
129 12	STREAMS_SMALL_SEGMENT	<input type="checkbox"/>
129 13	STREAMS_4WAY_HANDSHAKE	<input type="checkbox"/>
129 14	STREAMS_NO_TIMESTAMP	<input checked="" type="checkbox"/>
129 15	STREAMS_BAD_RST	<input checked="" type="checkbox"/>
129 16	STREAMS_BAD_FIN	<input checked="" type="checkbox"/>
129 17	STREAMS_BAD_ACK	<input checked="" type="checkbox"/>
129 18	STREAMS_DATA_AFTER_RST_RCVD	<input checked="" type="checkbox"/>
129 19	STREAMS_WINDOW_SLAM	<input checked="" type="checkbox"/>

A ativação das regras GID 129 faz com que os Eventos de Intrusão sejam enviados ao FMC quando tomam medidas no tráfego. No entanto, enquanto **Bloquear Anomalias de Cabeçalho TCP Não Resolível** estiver ativado, ele ainda poderá descartar tráfego mesmo se o **Estado da Regra** na Política de Intrusão estiver definido como somente **Gerar Eventos**. Esse comportamento é explicado nos Guias de Configuração do FMC.

Still drops after setting to generate



Inline Result	Source IP	Destination IP	Source Port / ICMP Type	Destination Port / ICMP Code	Message
↓	172.16.111.226	50.19.123.95	51174 / tcp	443 (https) / tcp	STREAMS_NO_TIMESTAMP (129:14:2)
↓	172.16.111.226	50.19.123.95	51174 / tcp	443 (https) / tcp	STREAMS_NO_TIMESTAMP (129:14:2)

Check configuration guide for relative protocols/preprocessors:

Block Unresolvable TCP Header Anomalies

When you enable this option, the system blocks anomalous TCP packets that, if normalized, would be invalid and likely would be blocked by the receiving host. For example, the system blocks any SYN packet transmitted subsequent to an established session.

The system also drops any packet that matches any of the following TCP stream preprocessor rules, regardless of whether the rules are enabled:

- 129:1
- 129:3
- 129:4
- 129:6
- 129:8
- 129:11
- 129:14 through 129:19

The Total Blocked Packets performance graph tracks the number of packets blocked in inline deployments and, in passive deployments and inline deployments in tap mode, the number that would have been blocked in an inline deployment.

A documentação acima pode ser encontrada neste [artigo](#) (para a versão 6.4, que é a versão mais recente no momento da publicação deste artigo).

Verifique a configuração de back-end

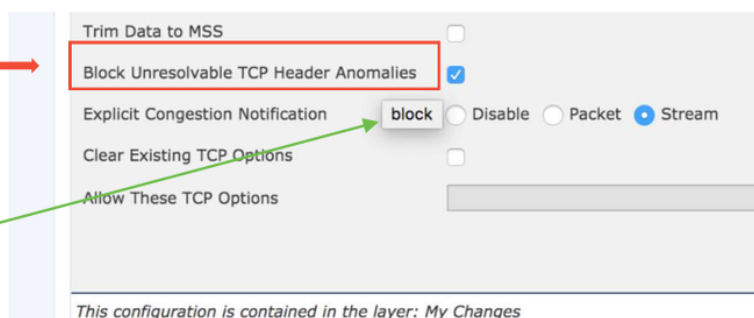
Outra camada de complexidade é adicionada ao comportamento do pré-processador, na medida em que determinadas configurações podem ser ativadas no back-end, sem serem refletidas no FMC. Estas são algumas razões possíveis.

- Outros recursos habilitados têm a capacidade de forçar as configurações de pré-processador de ativação (o principal é a Política de arquivo)
- Algumas regras da política de intrusão exigem determinadas opções de pré-processador para executar a detecção
- Um defeito pode causar o comportamento Vimos uma instância disso: [CSCuz50295](#) - "A política de arquivos com bloco de malware permite a normalização do TCP com flag de bloqueio"

Antes de examinar a configuração de back-end, observe que as palavras-chave Snort, que são usadas nos arquivos de configuração do Snort de back-end, podem ser vistas passando o mouse sobre uma configuração específica dentro do NAP. Consulte a ilustração abaixo.

Hover over option to see backend snort configuration keyword

Snort config keyword is "block"



A opção **Bloquear Anomalias de Cabeçalho TCP Não Resolvíveis** na guia NAP converte para a palavra-chave **de bloco** no back-end. Com essas informações em mente, a configuração de back-end pode ser verificada no shell do especialista.

```
root@ciscoasa:~# de_info.pl
-----
DE Name      : Primary Detection Engine (c9ef19d6-e187-11e6-ba76-99617d53da68)
DE Type      : ids
DE Description : Primary detection engine for device c9ef19d6-e187-11e6-ba76-99617d53da68
DE Resources  : 1
DE UUID      : 0d82120c-e188-11e6-8606-a4827d53da68
-----

root@ciscoasa:~# cd /var/sf/detection_engines/0d82120c-e188-11e6-8606-a4827d53da68/network_analysis/
root@ciscoasa: network_analysis# ls
b50f27b0-e31a-11e6-b866-dd9e65c01d56 object_b50f27b0-e31a-11e6-b866-dd9e65c01d56 snort.conf.b50f27b0-e31a-11e6-b866-
dd9e65c01d56 snort.conf.b50f27b0-e31a-11e6-b866-dd9e65c01d56.default
root@ciscoasa: network_analysis# cat b50f27b0-e31a-11e6-b866-dd9e65c01d56/normalize.conf
#
# generated from My Changes
#
preprocessor normalize_tcp: ips, rsv, pad, req_urg, req_pay, req_urp, block
```

“block” option is enabled in normalize.conf

Criando um NAP direcionado

Se determinados hosts estiverem acionando eventos de pré-processador, um NAP personalizado pode ser usado para inspecionar o tráfego de ou para esses hosts. No NAP personalizado, as configurações que estão causando problemas podem ser desativadas.

Estas são as etapas para implementar um NAP direcionado.

1. Crie o NAP de acordo com as instruções mencionadas na seção **Verificar a configuração do NAP** deste artigo.
2. Na guia **Avançado** da Política de controle de acesso, navegue até a seção **Análise de rede e Políticas de intrusão**. Clique em **Adicionar regra** e crie uma regra, usando os hosts de destino e escolha o NAP recém-criado na seção **Política de análise de rede**.

Network Analysis and Intrusion Policies

#	Source Zo...	Dest Zones	Source Networ...	Dest Networks	VLAN T...	Network Analysis ...
1	Any	Any	62_network	Any	Any	My Custom NAP

Análise Falsa Positiva

A verificação de falsos positivos em Eventos de Intrusão para regras de pré-processador é bem diferente da das regras de Snort usadas para avaliação de regras (que contêm uma GID de 1 e 3).

Para executar uma análise positiva falsa para eventos de regra de pré-processador, uma captura de sessão completa é necessária para procurar anomalias no fluxo TCP.

No exemplo abaixo, a análise de falsos positivos está sendo executada na regra **129:14**, que mostra que está deixando o tráfego cair nos exemplos acima. Como **129:14** está procurando fluxos TCP nos quais os timestamps estão ausentes, você pode ver claramente por que a regra foi disparada de acordo com a análise de captura de pacotes ilustrada abaixo.

Full session pcap

Packet that triggered event

SYN packet has TCP Timestamps

No TCP Timestamps in event packet (violates RFC)

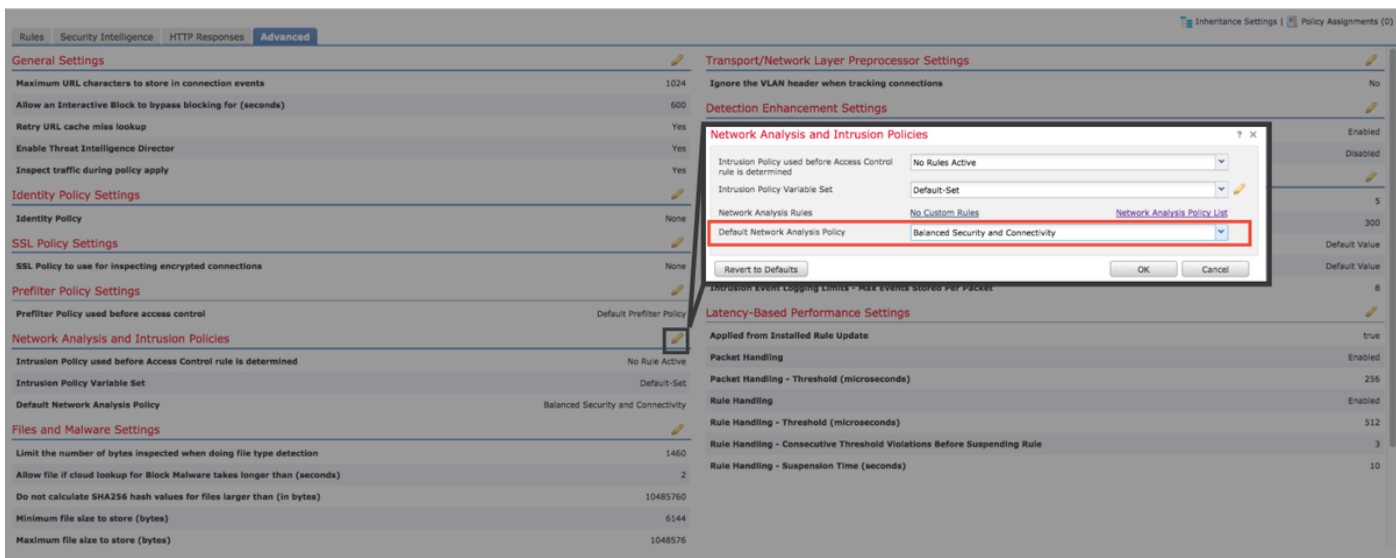
```
Internet Protocol Version 4, Src: 172.16.111.226, Dst: 50.19.123.95
Transmission Control Protocol, Src Port: 51174, Dst Port: 443, Seq: 3849839666, Len: 0
  Source Port: 51174
  Destination Port: 443
  [Stream index: 2]
  [TCP Segment Len: 0]
  Sequence number: 3849839666
  Acknowledgment number: 0
  Header Length: 40 bytes
  Flags: 0x002 (SYN)
  Window size value: 8192
  [Calculated window size: 8192]
  Checksum: 0x70ba [correct]
  [Checksum Status: Good]
  [Calculated Checksum: 0x70ba]
  Urgent pointer: 0
  Options: 20 bytes, Maximum segment size, No-Operation (NOP), Window scale, SACK permitted, Timestamps
    Maximum segment size: 1380 bytes
    No-Operation (NOP)
    Window scale: 8 (multiply by 256)
    TCP SACK Permitted Option: True
    Timestamps: TSval 2054852, TSecr 0

Internet Protocol Version 4, Src: 172.16.111.226, Dst: 50.19.123.95
Transmission Control Protocol, Src Port: 51174, Dst Port: 443, Seq: 3849839667, Ack: 1666843207, Len: 0
  Source Port: 51174
  Destination Port: 443
  [Stream index: 0]
  [TCP Segment Len: 0]
  Sequence number: 3849839667
  Acknowledgment number: 1666843207
  Header Length: 20 bytes
  Flags: 0x010 (ACK)
  Window size value: 57
  [Calculated window size: 57]
  [Window size scaling factor: -1 (unknown)]
  Checksum: 0xed47 [correct]
  [Checksum Status: Good]
  [Calculated Checksum: 0xed47]
  Urgent pointer: 0
```

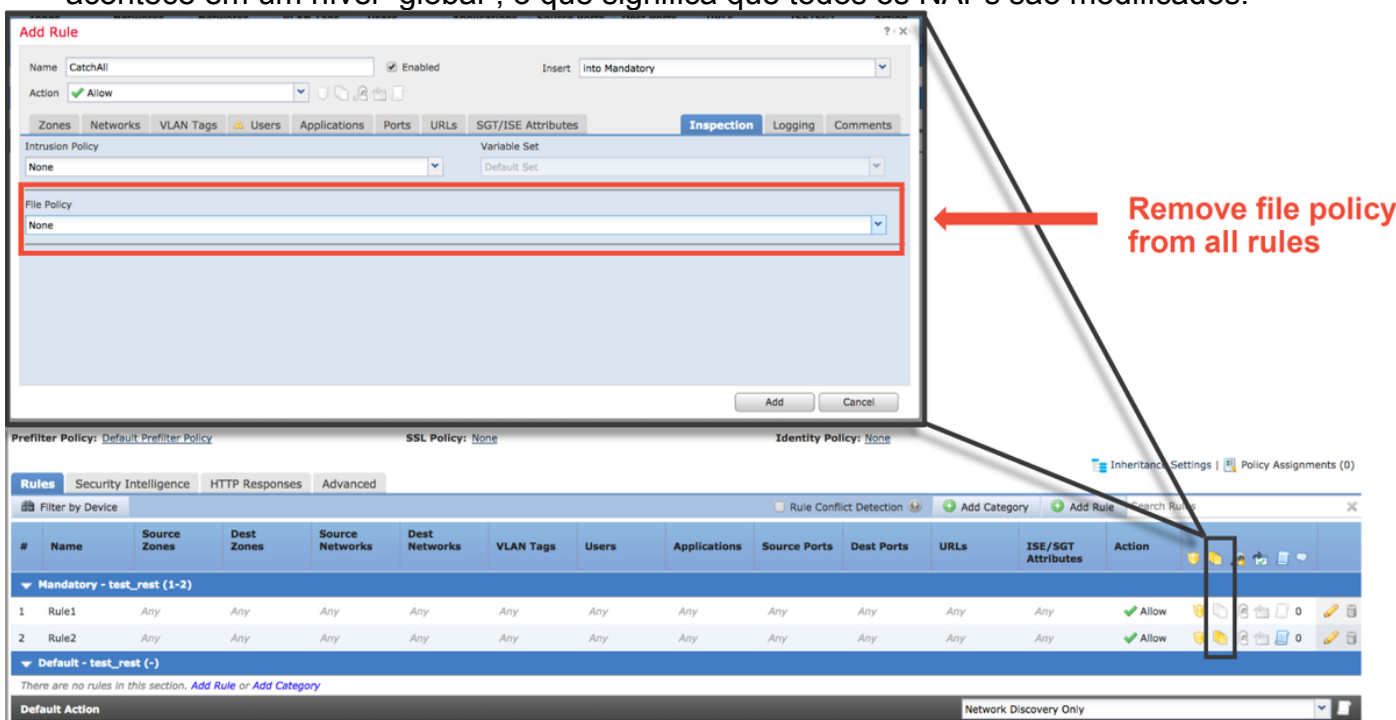
Etapas de mitigação

Para atenuar rapidamente possíveis problemas com o NAP, as etapas a seguir podem ser executadas.

- Se um NAP personalizado estiver sendo usado e você não tiver certeza de que uma configuração de NAP está descartando o tráfego, mas suspeitar que sim, você pode tentar substituí-lo por uma política de "segurança e conectividade equilibradas" ou "conectividade sobre segurança".



- Se alguma "Regras personalizadas" estiver sendo usada, certifique-se de definir o NAP como um dos padrões mencionados acima
- Se alguma regra de controle de acesso usar uma política de arquivo, talvez seja necessário tentar removê-la temporariamente, pois uma política de arquivo pode habilitar as configurações de pré-processador no backend que não são refletidas no FMC, e isso acontece em um nível "global", o que significa que todos os NAPs são modificados.



Cada protocolo tem um pré-processador diferente e a solução de problemas pode ser muito específica ao pré-processador. Este artigo não abrange todas as configurações do pré-processador e métodos de solução de problemas para cada um.

Você pode verificar a documentação de cada pré-processador para ter uma ideia melhor do que cada opção faz, o que é útil na solução de problemas de um pré-processador específico.

Dados a fornecer ao TAC

Dados Instruções

Solucione
problemas
de
arquivos
do
dispositivo
Firepower
Captura
de pacote
de sessão
completa
do
dispositivo
Firepower

<http://www.cisco.com/c/en/us/support/docs/security/sourcefire-defense-center/117663-technot>

<http://www.cisco.com/c/en/us/support/docs/security/sourcefire-firepower-8000-series-applianc>