

Solução de problemas de caminho de dados do Firepower: Overview

Contents

[Introduction](#)

[Prerequisites](#)

[Visão geral da arquitetura do caminho de dados](#)

[Plataforma ASA com FirePOWER Services \(módulo SFR\)](#)

[Firepower Threat Defense no ASA500-X e na plataforma FTD virtual](#)

[FTD em plataformas SSP](#)

[Dispositivos Firepower 9300 e 4100](#)

[Dispositivos Firepower 2100](#)

[Processo recomendado para solução de problemas de caminho de dados do Firepower](#)

[Caminho real do pacote através do FTD](#)

[Caminho do pacote Snort](#)

[Entrada e saída do pacote](#)

[Camada DAQ Firepower](#)

[Inteligência de segurança](#)

[Política de controle de acesso](#)

[Política SSL](#)

[Autenticação Ativa](#)

[Política de invasão](#)

[Política de análise de rede](#)

[Informações Relacionadas](#)

Introduction

O objetivo deste guia é ajudar a identificar rapidamente se um dispositivo Firepower Threat Defense (FTD) ou Adaptive Security Appliance (ASA) com FirePOWER Services está causando um problema no tráfego de rede. Além disso, ele ajuda a reduzir quais componentes do Firepower devem ser investigados e quais dados devem ser coletados antes de entrar em contato com o Cisco Technical Assistance Center (TAC).

Lista de todos os artigos da série Firepower Data Path Troubleshooting.

Fase 1 da solução de problemas de caminho de dados do Firepower: Entrada de pacote

<https://www.cisco.com/c/en/us/support/docs/security/firepower-ngfw/214574-firepower-data-path-troubleshooting-phas.html>

Fase 2 da solução de problemas de caminho de dados do Firepower: Camada DAQ

<https://www.cisco.com/c/en/us/support/docs/security/firepower-ngfw/214575-firepower-data-path-troubleshooting-phas.html>

Fase 3 da solução de problemas de caminho de dados do Firepower: Inteligência de segurança

<https://www.cisco.com/c/en/us/support/docs/security/firepower-ngfw/214576-firepower-data-path-troubleshooting-phas.html>

Fase 4 de solução de problemas de caminho de dados do Firepower: Política de controle de acesso

<https://www.cisco.com/c/en/us/support/docs/security/firepower-ngfw/214577-firepower-data-path-troubleshooting-phas.html>

Fase 5 da solução de problemas de caminho de dados do Firepower: Política SSL

<https://www.cisco.com/c/en/us/support/docs/security/firepower-ngfw/214581-firepower-data-path-troubleshooting-phas.html>

Fase 6 da solução de problemas de caminho de dados do Firepower: Autenticação Ativa

<https://www.cisco.com/c/en/us/support/docs/security/firepower-ngfw-virtual/214608-firepower-data-path-troubleshooting-phas.html>

Fase 7 de solução de problemas de caminho de dados do Firepower: Política de invasão

<https://www.cisco.com/c/en/us/support/docs/security/firepower-ngfw/214609-firepower-data-path-troubleshooting-phas.html>

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

<https://www.cisco.com/c/en/us/support/docs/security/firepower-ngfw/214610-firepower-data-path-troubleshooting-phas.html>

Prerequisites

- Este artigo pressupõe que se tem uma compreensão básica das plataformas FTD e ASA.
- Recomenda-se o conhecimento do snort de código aberto, embora não seja obrigatório.

Para obter uma lista completa da documentação do Firepower, incluindo os Guias de instalação e configuração, visite a página [do roteiro da documentação](#).

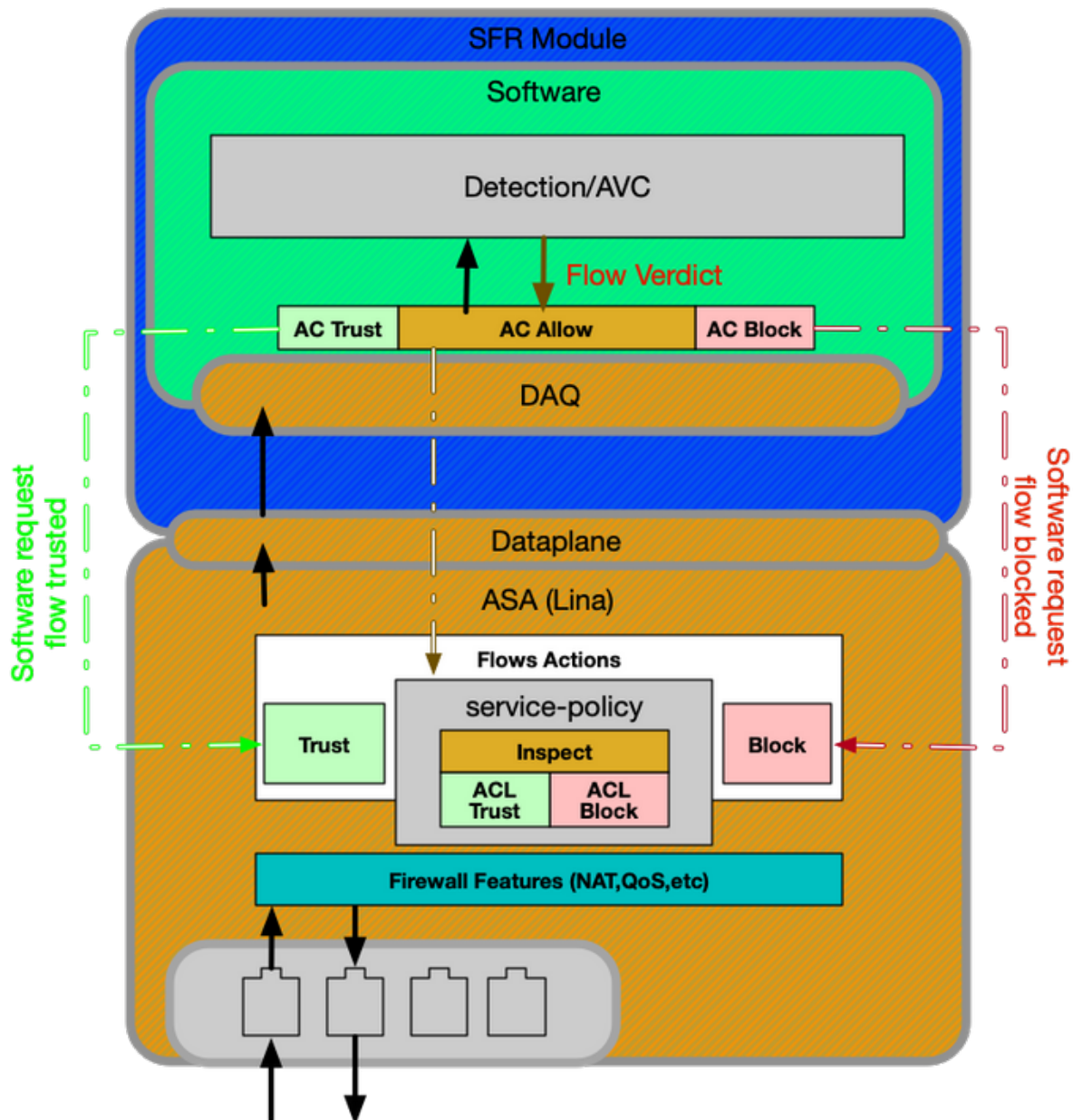
Visão geral da arquitetura do caminho de dados

A seção a seguir examina o caminho de dados arquitetônicos para várias plataformas Firepower. Com a arquitetura em mente, seguiremos para como determinar rapidamente se o dispositivo Firepower está ou não bloqueando o fluxo de tráfego.

Note: Este artigo não abrange os dispositivos antigos das séries Firepower 7000 e 8000, nem a plataforma virtual NGIPS (não FTD). Para obter informações sobre como solucionar problemas dessas plataformas, visite nossa página [TechNotes](#).

Plataforma ASA com FirePOWER Services (módulo SFR)

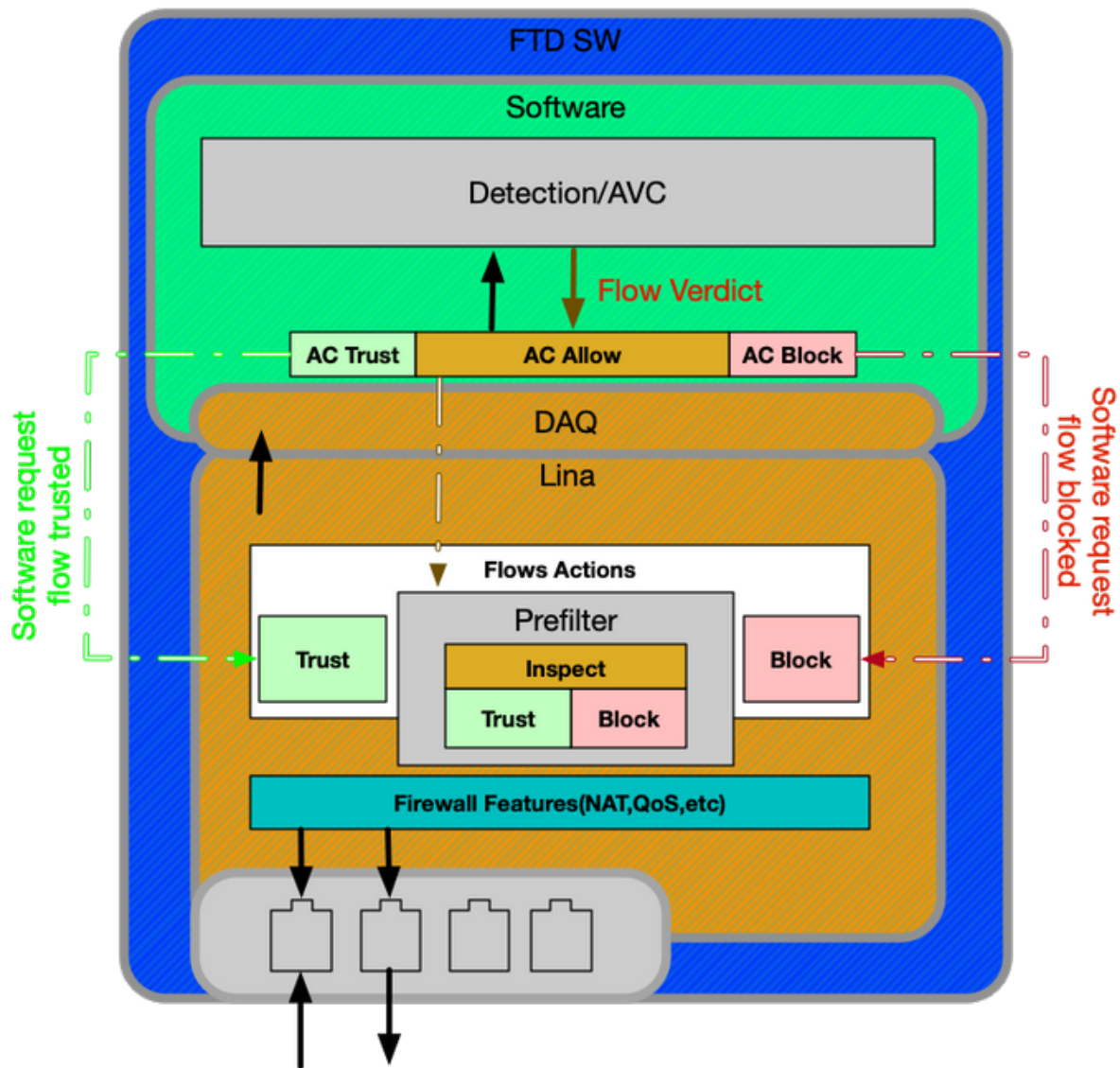
A plataforma FirePOWER Services também é conhecida como módulo SFR. Basicamente, essa é uma máquina virtual executada em plataformas 5500-X ASA.



A política de serviço no ASA determina qual tráfego está sendo enviado ao módulo SFR. Há uma camada de painel de dados usada para se comunicar com o mecanismo de aquisição de dados (DAQ) do Firepower, que é usado para converter pacotes de uma forma que o snort possa entender.

Firepower Threat Defense no ASA500-X e na plataforma FTD virtual

A plataforma FTD consiste em uma única imagem contendo o código Lina (ASA) e Firepower. Uma grande diferença entre isso e a plataforma do módulo ASA com SFR é que há comunicações mais eficientes entre Lina e snort.

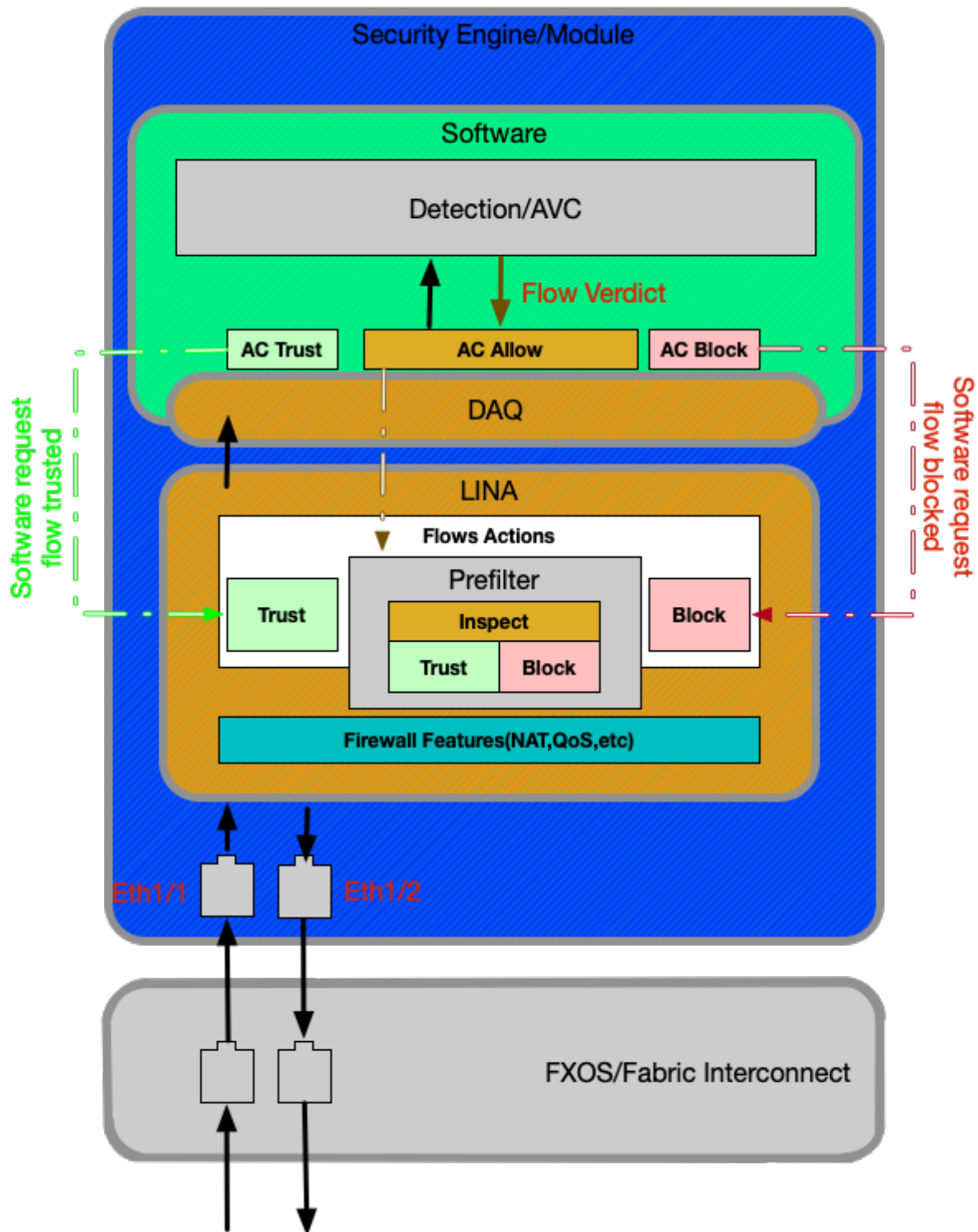


FTD em plataformas SSP

Nos modelos de plataformas de serviço de segurança (SSP), o software FTD é executado sobre a plataforma do sistema operacional Firepower eXtensible (FXOS), que é um sistema operacional (OS) subjacente usado para gerenciar o hardware do chassi e hospedar vários aplicativos conhecidos como dispositivos lógicos.

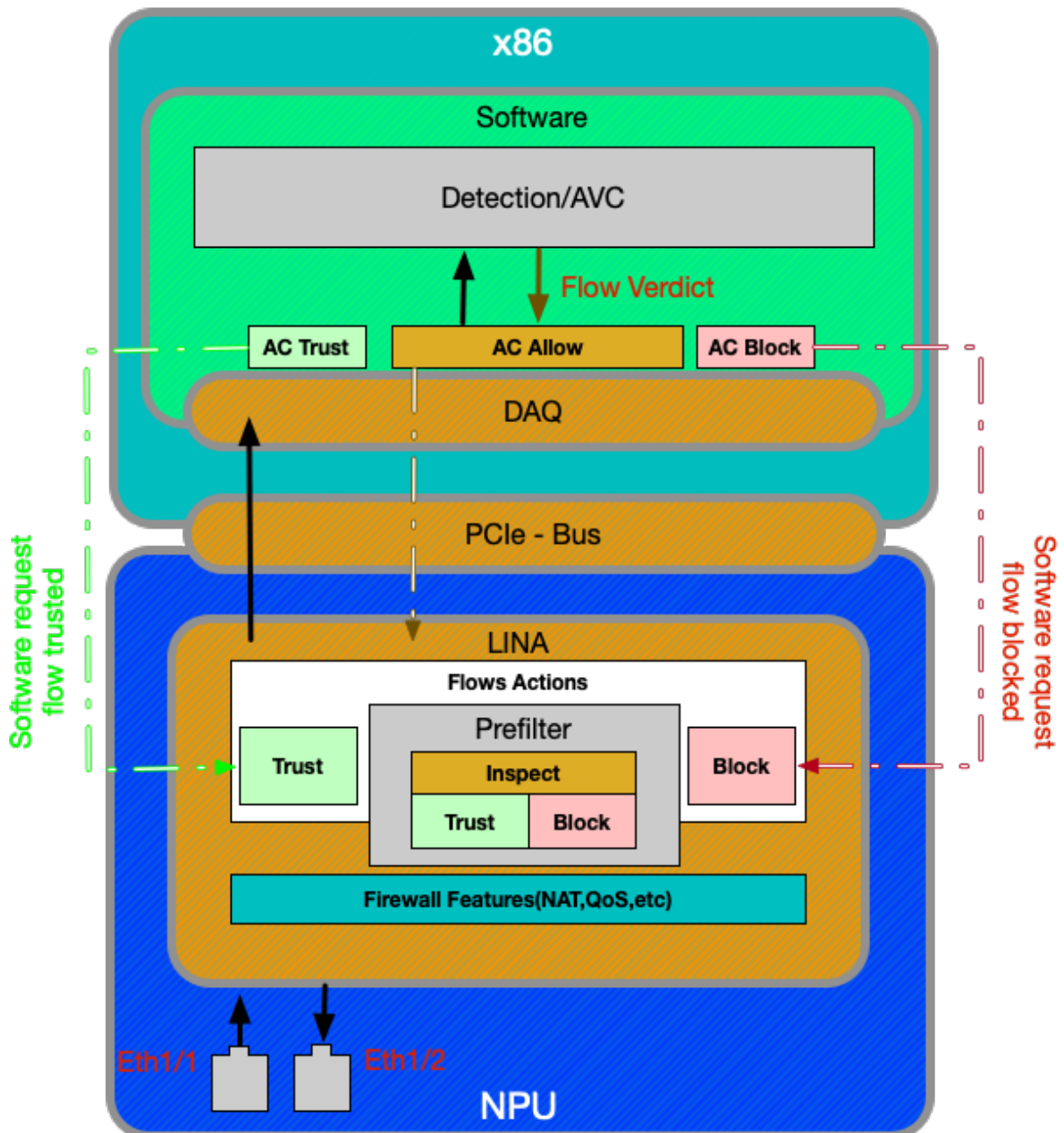
Na plataforma SSP, há algumas diferenças entre os modelos, como visto nos diagramas e descrições abaixo.

Dispositivos Firepower 9300 e 4100



Nas plataformas Firepower 9300 e 4100, os pacotes de entrada e saída são tratados por um switch alimentado pelo firmware FXOS (Fabric Interconnect). Os pacotes são enviados às interfaces atribuídas ao dispositivo lógico (neste caso, FTD). Depois disso, o processamento de pacotes é o mesmo que está nas plataformas FTD não SSP.

Dispositivos Firepower 2100



O dispositivo Firepower 2100 funciona de forma semelhante às plataformas FTD que não são SSP. Ele não contém a camada de interconexão de estrutura presente nos modelos 9300 e 4100. No entanto, há uma grande diferença nos dispositivos da série 2100 em relação aos outros dispositivos, que é a presença do circuito integrado específico de aplicativos (ASIC). Todos os recursos tradicionais do ASA (Lina) são executados no ASIC e todos os recursos do firewall de próxima geração (NGFW) (snort, filtragem de URL, etc.) são executados na arquitetura x86 tradicional. A forma como Lina e Snort se comunicam nesta plataforma é através de uma PCIe (Peripheral Component Interconnect Express) através de uma fila de pacotes, ao contrário de outras plataformas que usam DMA (Direct Memory Access, Acesso Direto de Memória) para enfileirar pacotes para snort.

Note: Os mesmos métodos para a solução de problemas das plataformas FTD não SSP serão seguidos na plataforma FPR-2100.

Processo recomendado para solução de problemas de caminho de dados do Firepower

Agora que abordamos como identificar o tráfego único, bem como a arquitetura básica do caminho de dados nas plataformas Firepower, agora observamos os locais específicos nos quais os pacotes podem ser descartados. Há oito componentes básicos que são abordados nos artigos de Caminho de dados, que podem sistematicamente solucionar problemas para determinar possíveis descartes de pacotes. Eles incluem:

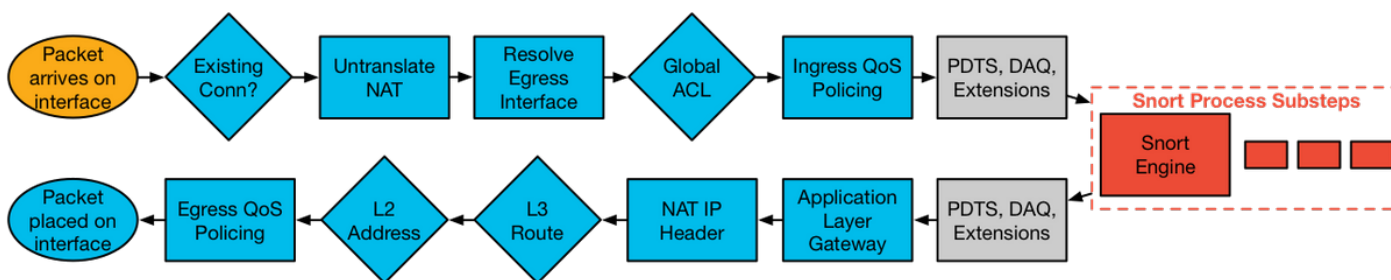
1. Entrada de pacote
2. Camada DAQ Firepower
3. Inteligência de segurança
4. Política de controle de acesso
5. Política SSL
6. Recursos de autenticação ativa
7. Política de intrusão (regras IPS)
8. Política de análise de rede (configurações de pré-processador de snort)



Note: Esses componentes não estão listados na ordem exata das operações no processamento do Firepower, mas são solicitados de acordo com nosso fluxo de trabalho de solução de problemas recomendado. Veja a ilustração abaixo para o caminho real do diagrama de pacotes.

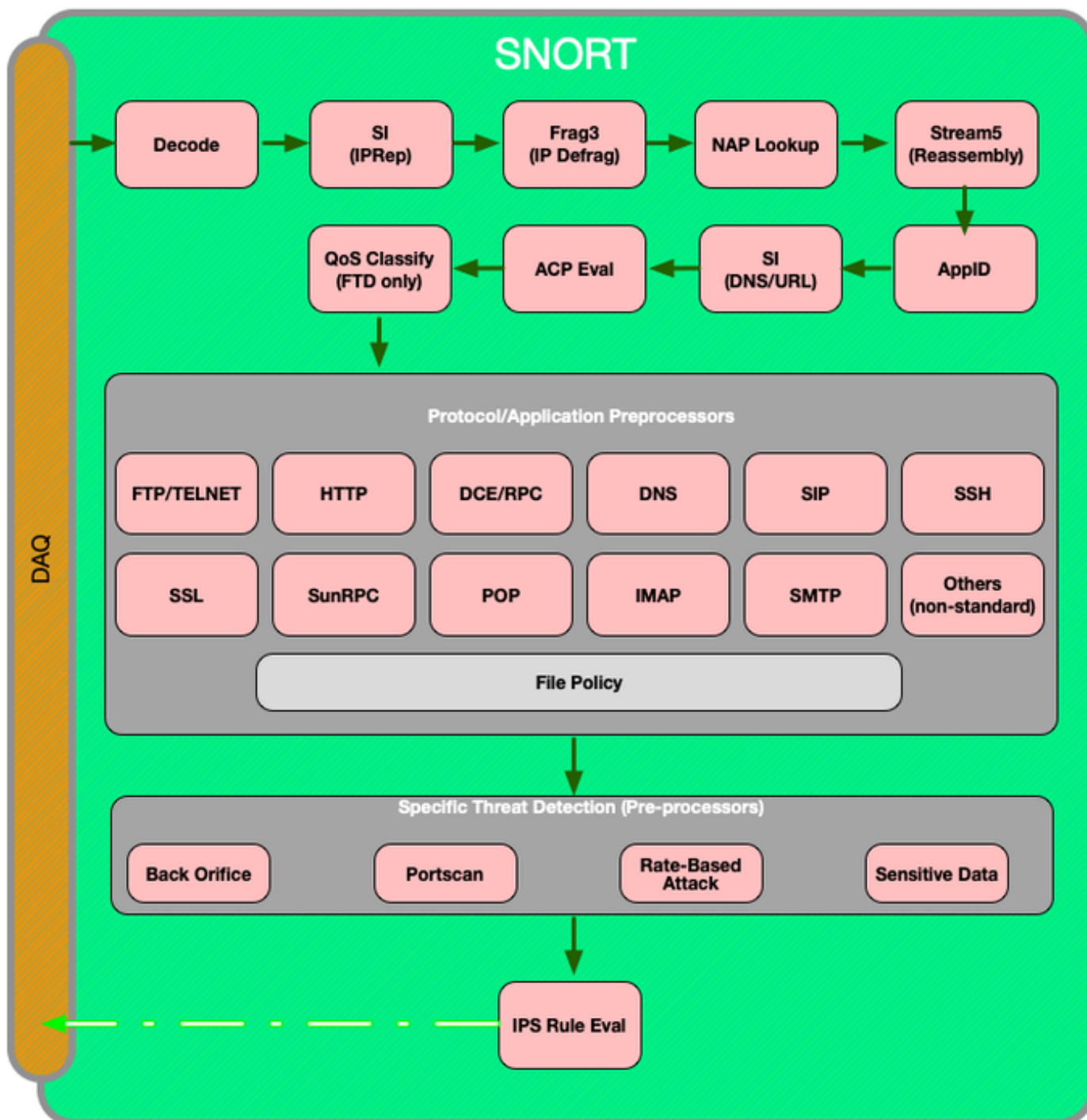
Caminho real do pacote através do FTD

A ilustração abaixo mostra o caminho real do pacote enquanto ele atravessa o FTD.



Caminho do pacote Snort

A ilustração abaixo mostra o caminho do pacote através do mecanismo Snort.



Entrada e saída do pacote

A primeira etapa da solução de problemas do caminho de dados é garantir que não ocorram quedas no estágio de entrada ou saída do processamento de pacotes. Se um pacote estiver ingressando, mas não egressando, você pode ter certeza de que o pacote está sendo descartado pelo dispositivo em algum lugar no caminho de dados.

Este [artigo](#) mostra como solucionar problemas de entrada e saída de pacotes em sistemas Firepower.

Camada DAQ Firepower

Se for determinado que o pacote está ingressando mas não egressando, a próxima etapa na solução de problemas de caminho de dados deve estar na camada DAQ (Aquisição de Dados) do Firepower para garantir que o tráfego em questão esteja sendo enviado ao Firepower para inspeção e, em caso afirmativo, se está sendo descartado ou modificado.

Este [artigo](#) analisa como solucionar problemas do tratamento inicial do tráfego pelo Firepower, bem como o caminho que ele está tomando em todo o dispositivo.

Ele também aborda como o dispositivo Firepower pode ser ignorado completamente para determinar se um componente Firepower é responsável pelo problema de tráfego.

Inteligência de segurança

A inteligência de segurança é o primeiro componente do Firepower a inspecionar o tráfego. Os blocos neste nível são muito fáceis de determinar, desde que o registro esteja ativado. Isso pode ser determinado na GUI do FMC navegando para **Políticas > Controle de acesso > Política de controle de acesso**. Depois de clicar no ícone de edição ao lado da política em questão, navegue até a guia **Security Intelligence**.

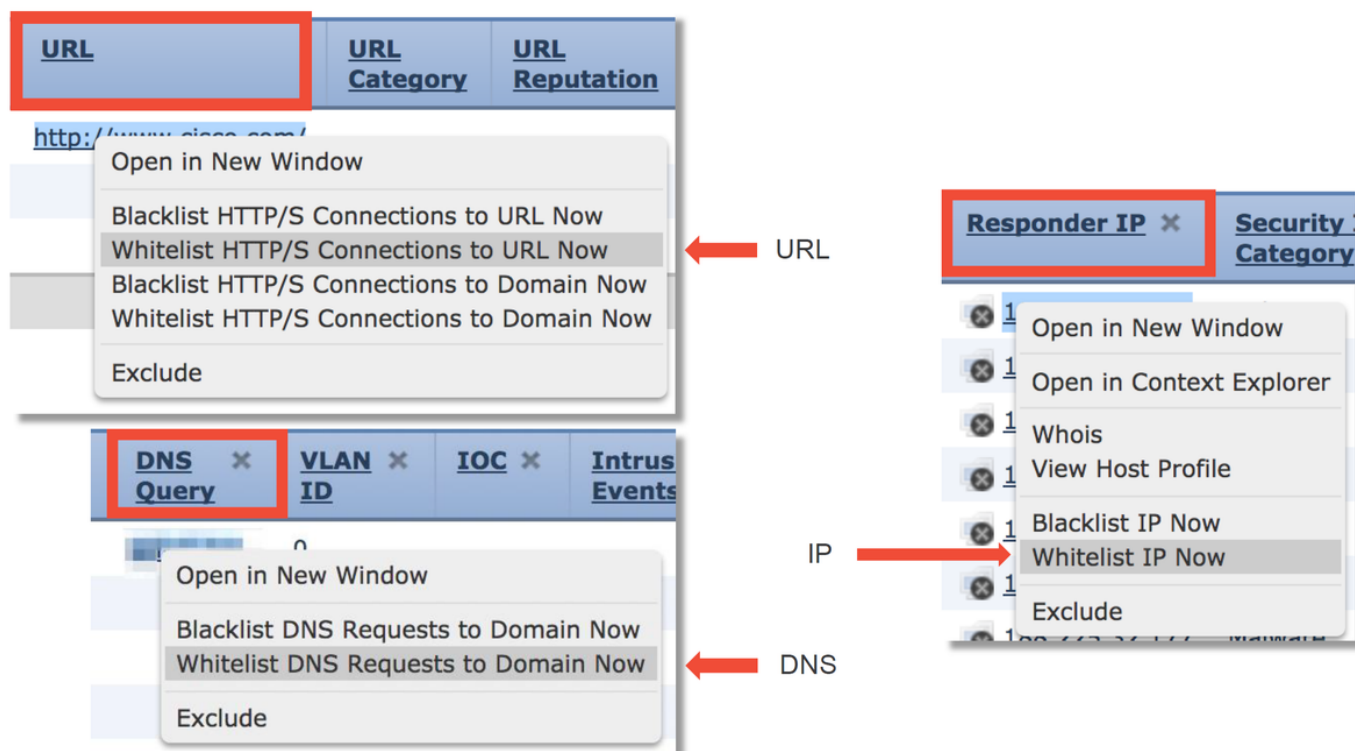
The screenshot shows the Firepower Security Intelligence configuration interface. The 'Security Intelligence' tab is selected. The 'Blacklist (30)' section is expanded, showing a list of categories. The 'Networks' category is highlighted with a red box and an arrow pointing to it, with the text 'Logging enabled' next to it. The 'URLs' category is also highlighted with a red box and an arrow pointing to it, with the text 'Logging disabled' next to it. A red box highlights the edit icon in the top right corner of the interface.

Category	Logging Status
Networks	Logging enabled
Attackers (Any Zone)	Logging disabled
Bogon (Any Zone)	Logging disabled
Bots (Any Zone)	Logging disabled
CnC (Any Zone)	Logging disabled
Dga (Any Zone)	Logging disabled
Exploitkit (Any Zone)	Logging disabled
Malware (Any Zone)	Logging disabled
Open_proxy (Any Zone)	Logging disabled
Phishing (Any Zone)	Logging disabled
Response (Any Zone)	Logging disabled
Spam (Any Zone)	Logging disabled
Suspicious (Any Zone)	Logging disabled
Tor_exit_node (Any Zone)	Logging disabled
Global Blacklist (Any Zone)	Logging disabled
URLs	Logging disabled
my_custom_url (Any Zone)	Logging disabled
Global Blacklist for URL (Any Zone)	Logging disabled
URL Attackers (Any Zone)	Logging disabled
URL Bogon (Any Zone)	Logging disabled
URL Bots (Any Zone)	Logging disabled
URL CnC (Any Zone)	Logging disabled
URL Dga (Any Zone)	Logging disabled
URL Exploitkit (Any Zone)	Logging disabled
URL Malware (Any Zone)	Logging disabled
URL Open_proxy (Any Zone)	Logging disabled
URL Open_relay (Any Zone)	Logging disabled
URL Phishing (Any Zone)	Logging disabled
URL Response (Any Zone)	Logging disabled
URL Spam (Any Zone)	Logging disabled
URL Suspicious (Any Zone)	Logging disabled
URL Tor_exit_node (Any Zone)	Logging disabled

Quando o registro estiver ativado, você poderá visualizar os Eventos de Inteligência de Segurança em **Analysis > Connections > Security Intelligence Events**. Deve ficar claro por que o tráfego está sendo bloqueado.

First Packet	Last Packet	Action	Reason	Initiator IP	Responder IP	Security Intelligence Category
2017-05-16 17:00:16		Domain Not Found	DNS Block	192.168.1.95		DNS Response
2017-05-16 16:57:50	2017-05-16 16:57:50	Block	URL Block	192.168.1.95	10.83.48.40	my_custom_url
2017-05-16 16:50:05		Block	IP Block	192.168.1.95		Malware

Como uma rápida etapa de mitigação, você pode clicar com o botão direito do mouse na Consulta IP, URL ou DNS sendo bloqueada pelo recurso Security Intelligence e escolher uma opção de lista branca.



Se você suspeitar que algo foi colocado incorretamente na lista negra, ou se quiser solicitar que você altere a reputação, poderá abrir um tíquete diretamente com o Cisco Talos no link a seguir:

https://www.talosintelligence.com/reputation_center/support

Você também pode fornecer os dados ao TAC para informar o que está sendo bloqueado e talvez tenha uma entrada removida de uma lista negra.

Para obter uma solução de problemas detalhada do componente Security Intelligence, consulte o [artigo](#) relevante sobre solução de problemas de caminho de dados.

Política de controle de acesso

Se for determinado que o recurso de inteligência de segurança não está bloqueando o tráfego, a próxima etapa recomendada é solucionar problemas das regras de política de controle de acesso para ver se uma regra com ação 'Bloquear' está descartando o tráfego.

Recomenda-se começar a usar o comando "firewall-engine-debug" ou a captura com rastreamento. Geralmente, essas ferramentas podem dar a resposta imediatamente e dizer a você qual regra o tráfego está atingindo e por quais motivos.

- Execute a depuração na CLI do Firepower para ver qual regra está bloqueando o tráfego (insira o máximo de parâmetros possível) por meio do seguinte comando: **> system support firewall-engine-debug**
- A saída de depuração pode ser fornecida ao TAC para análise

Abaixo está um exemplo de saída, mostrando a avaliação de regras para o tráfego que corresponde a uma regra de Controle de Acesso com a ação de 'Permitir':

```
SHLL
> system support firewall-engine-debug
Please specify an IP protocol: tcp
Please specify a client IP address: 192.168.62.51
Please specify a client port:
Please specify a server IP address:
Please specify a server port:
Monitoring firewall engine debug messages

192.168.62.51-51216 > 173.37.145.84-80 6 AS 1 I 0 New session
192.168.62.51-51216 > 173.37.145.84-80 6 AS 1 I 0 Starting with minimum 3, 'block urls', and SrcZone
first with zones 1 -> 2, 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
192.168.62.51-51216 > 173.37.145.84-80 6 AS 1 I 0 pending rule order 3, 'block urls', URL
192.168.62.51-51216 > 173.37.145.84-80 6 AS 1 I 0 Starting with minimum 3, 'block urls', and SrcZone
first with zones 1 -> 2, geo 0(0) -> 0, vlan 0, inline sgt tag: untagged, ISE sgt id: 0, svc 676,
payload 2655, client 638, misc 0, user 9999997, url http://www.cisco.com/, xff
192.168.62.51-51216 > 173.37.145.84-80 6 AS 1 I 0: DataMessaging_GetURLData: Returning URL_BCTYPE
for www.cisco.com
192.168.62.51-51216 > 173.37.145.84-80 6 AS 1 I 0 rule order 3, 'block urls', URL Lookup Success:
http://www.cisco.com/ waited: 0ms
192.168.62.51-51216 > 173.37.145.84-80 6 AS 1 I 0 no match rule order 3, 'block urls',
url=(http://www.cisco.com/) c=4 r=96
192.168.62.51-51216 > 173.37.145.84-80 6 AS 1 I 0 match rule order 4, 'inspect it all', action Allow
192.168.62.51-51216 > 173.37.145.84-80 6 AS 1 I 0 allow action
192.168.62.51-51216 > 173.37.145.84-80 6 AS 1 I 0 File policy verdict is Type, Malware, and Capture
```

Se você não puder determinar qual regra de controle de acesso (AC) está sendo correspondida ou se não puder determinar se a política AC é o problema usando as ferramentas acima, abaixo estão algumas etapas básicas para solucionar problemas da política de controle de acesso (observe que essas opções não são a primeira opção porque exigem alterações/implantações de política):

- Habilitar registro para quaisquer regras com uma ação 'Bloquear'
- Se você ainda não vir eventos de conexão para o tráfego e ele estiver sendo bloqueado, crie uma regra de Confiança para o tráfego em questão como uma etapa de mitigação
- Se a regra de confiança para o tráfego ainda não resolver o problema, mas você ainda suspeitar que a política de CA está com defeito, em seguida, crie uma nova política de controle de acesso em branco, se possível, usando uma ação padrão diferente de 'Bloquear todo o tráfego'

Check logging for block rules

#	Name	Sou... Zon...	Dest Zon...	Sou... Net...	Dest Net...	VLA...	Use...	App...	Sou...	Des...	URLs	ISE... Attr...	Acti...						
▼ Mandatory - My AC Policy (1-2)																			
1	block with logging	any	any	any	any	any	any	YouTube	any	any	any	any	Block						
2	block no logging	any	any	any	any	any	any		any	any	any	Gam	Block						

↓ Add trust rule

1	Trust traffic	any	any	192.	any	any	any		any	any	any	any	Trust						
2	block with logging	any	any	any	any	any	any	YouTube	any	any	any	any	Block						
3	block no logging	any	any	any	any	any	any		any	any	any	Gam	Block						

↓ Create blank AC policy

#	Name	Sour... Zones	Dest Zones	Sour... Netw...	Dest Netw...	VLAN...	Users	Appli...	Sour...	Dest ...	URLs	ISE/... Attr...	Action						
▼ Mandatory - Test - No rules (-)																			
There are no rules in this section. Add Rule or Add Category																			
▼ Default - Test - No rules (-)																			
There are no rules in this section. Add Rule or Add Category																			
Default Action												Intrusion Prevention: Balanced Security and Connectivity							

Para obter uma solução de problemas detalhada da política de controle de acesso, consulte o [artigo](#) relevante sobre solução de problemas de caminho de dados.

Política SSL

Se a Política SSL estiver sendo usada, é possível que ela esteja bloqueando o tráfego. Abaixo estão algumas etapas básicas para a solução de problemas da política SSL:

- Habilitar registro para todas as regras, incluindo a 'Ação padrão'

#	Name	Sour... Zones	Dest Zones	Source Netw...	Dest Netw...	VLA...	Us...	Appli...	Sour...	Dest ...	Categories	SSL	Action						
Administrator Rules																			
This category is empty																			
Standard Rules																			
1	DnD banking	any	any	any	any	any	any	any	any	any	Financial Services (Any Reputatio	any	Do not decrypt						
2	decrypt outbound suspicious	inside	outside	any	any	any	any	any	any	any	Any (Reputations 1-2)	any	Decrypt - Resign						

Editing Rule - DnD banking

Name: DnD banking Enabled [Move](#)

Action: Do not decrypt

Zones Networks VLAN Tags Users Applications Ports **Category** Certificate DN Cert Status Cipher Suite Version **Logging**

Log at End of Connection **Enable Logging**

Send Connection Events to:

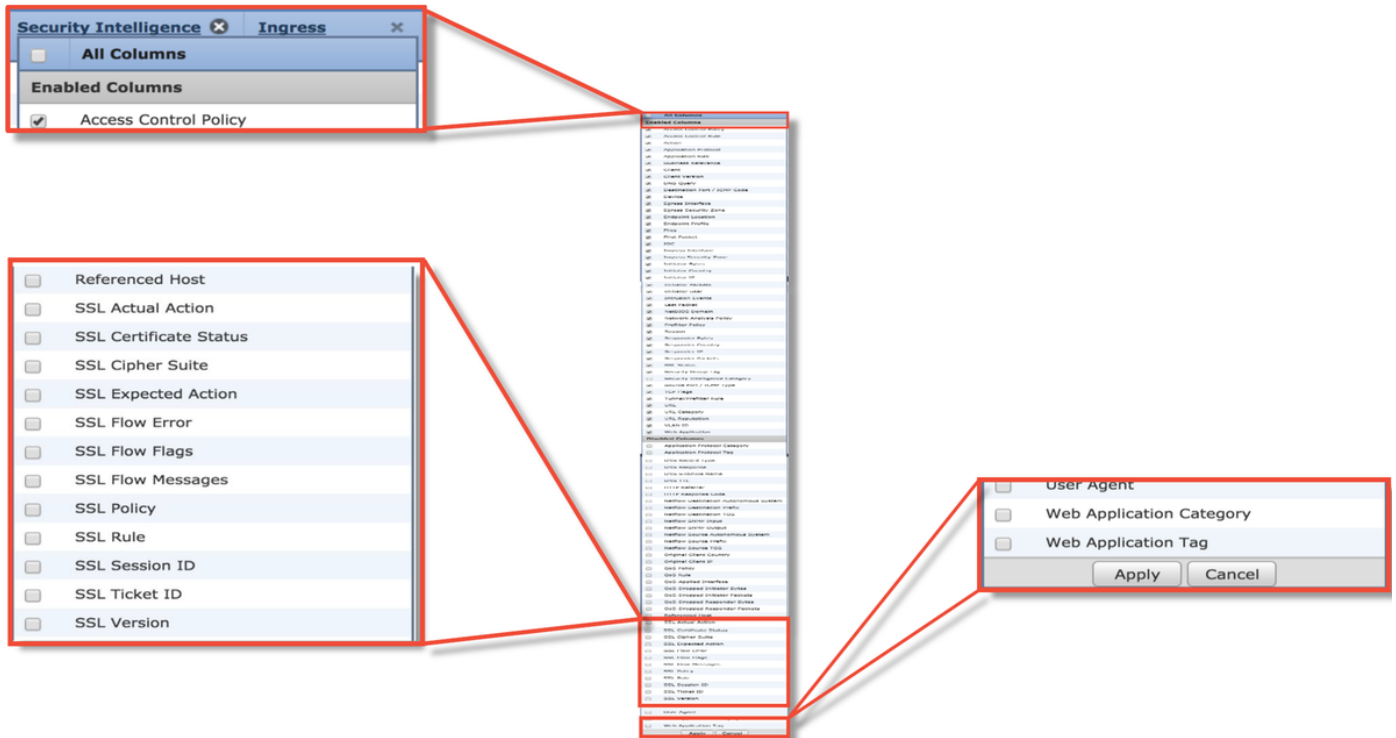
Event Viewer

Syslog [Select a Syslog Alert Configuration...](#)

SNMP Trap [Select an SNMP Alert Configuration...](#)

[Save](#) [Cancel](#)

- Verifique a guia Ações não descriptografáveis para ver se uma opção está definida para bloquear o tráfego
- Na seção Eventos do Connection, verifique todos os campos com 'SSL' no nome. A maioria é desabilitada por padrão e precisa ser habilitada no visualizador Eventos de Conexão clicando na cruz ao lado de qualquer nome de coluna



Connection Events (switch workflow)
 Connections with Application Details > **Table View of Connection Events**
 Search Constraints (Edit Search Save Search)

SSL Blocking flow

First Packet	Last Packet	Action	Reason	Initiator IP	Initiator Country	Responder IP	Responder Country
2017-05-30 13:09:23	2017-05-30 13:09:24	Block	SSL Block	192.168.1.200		216.58.217.138	USA
2017-05-30 13:08:53	2017-05-30 13:08:54	Block	SSL Block	192.168.1.200		216.58.217.138	USA
2017-05-30 13:08:23	2017-05-30 13:08:24	Block	SSL Block	192.168.1.200		216.58.217.138	USA
2017-05-30 13:08:19	2017-05-30 13:08:20	Block	SSL Block	192.168.1.200		216.58.217.138	USA
2017-05-30 13:07:53	2017-05-30 13:07:54	Block	SSL Block	192.168.1.200		216.58.217.138	USA
2017-05-30 13:07:23	2017-05-30 13:07:24	Block	SSL Block	192.168.1.200		216.58.217.138	USA

Cause of the SSL failure

SSL Status	SSL Flow Error	SSL Actual Action	SSL Expected Action	SSL Certificate Status	SSL Version
Decrypt (Resign)	PUB_CRYPTO_OPENSSL_RSA_OP_FAILURE (0xb7000a20)	Decrypt (Resign)	Decrypt (Resign)	Valid	TLSv1.2
Decrypt (Resign)	PUB_CRYPTO_OPENSSL_RSA_OP_FAILURE (0xb7000a20)	Decrypt (Resign)	Decrypt (Resign)	Valid	TLSv1.2
Decrypt (Resign)	PUB_CRYPTO_OPENSSL_RSA_OP_FAILURE (0xb7000a20)	Decrypt (Resign)	Decrypt (Resign)	Valid	TLSv1.2
Decrypt (Resign)	PUB_CRYPTO_OPENSSL_RSA_OP_FAILURE (0xb7000a20)	Decrypt (Resign)	Decrypt (Resign)	Valid	TLSv1.2
Decrypt (Resign)	PUB_CRYPTO_OPENSSL_RSA_OP_FAILURE (0xb7000a20)	Decrypt (Resign)	Decrypt (Resign)	Valid	TLSv1.2
Decrypt (Resign)	PUB_CRYPTO_OPENSSL_RSA_OP_FAILURE (0xb7000a20)	Decrypt (Resign)	Decrypt (Resign)	Valid	TLSv1.2

SSL flow flags for what happened with flow

SSL Rule	SSL Session ID	SSL Ticket ID	SSL Flow Flags	SSL Flow Messages
MITM	0x0	0x0	VALID, INITIALIZED, SSL_DETECTED, CERTIFICATE_DECODED, FULL_HANDSHAKE, CLIENT_HELLO_SSESSTKT, SERVER_HELLO_SSESSTKT, CH_PROCESSED, SH_PROCESSED, CH_CIPHERS_MODIFIED, ...	CLIENT_HELLO, SERVER_HELLO, SERVER_CERTIFICATE
MITM	0x0	0x0	VALID, INITIALIZED, SSL_DETECTED, CERTIFICATE_DECODED, FULL_HANDSHAKE, CLIENT_HELLO_SSESSTKT, SERVER_HELLO_SSESSTKT, CH_PROCESSED, SH_PROCESSED, CH_CIPHERS_MODIFIED, ...	CLIENT_HELLO, SERVER_HELLO, SERVER_CERTIFICATE
MITM	0x0	0x0	VALID, INITIALIZED, SSL_DETECTED, CERTIFICATE_DECODED, FULL_HANDSHAKE, CLIENT_HELLO_SSESSTKT, SERVER_HELLO_SSESSTKT, CH_PROCESSED, SH_PROCESSED, CH_CIPHERS_MODIFIED, ...	CLIENT_HELLO, SERVER_HELLO, SERVER_CERTIFICATE
MITM	0x0	0x0	VALID, INITIALIZED, SSL_DETECTED, CERTIFICATE_DECODED, FULL_HANDSHAKE, CLIENT_HELLO_SSESSTKT, SERVER_HELLO_SSESSTKT, CH_PROCESSED, SH_PROCESSED, CH_CIPHERS_MODIFIED, ...	CLIENT_HELLO, SERVER_HELLO, SERVER_CERTIFICATE
MITM	0x0	0x0	VALID, INITIALIZED, SSL_DETECTED, CERTIFICATE_DECODED, FULL_HANDSHAKE, CLIENT_HELLO_SSESSTKT, SERVER_HELLO_SSESSTKT, CH_PROCESSED, SH_PROCESSED, CH_CIPHERS_MODIFIED, ...	CLIENT_HELLO, SERVER_HELLO, SERVER_CERTIFICATE
MITM	0x0	0x0	VALID, INITIALIZED, SSL_DETECTED, CERTIFICATE_DECODED, FULL_HANDSHAKE, CLIENT_HELLO_SSESSTKT, SERVER_HELLO_SSESSTKT, CH_PROCESSED, SH_PROCESSED, CH_CIPHERS_MODIFIED, ...	CLIENT_HELLO, SERVER_HELLO, SERVER_CERTIFICATE

- Criar uma política SSL em branco com Não descriptografar como ação padrão como etapa de mitigação
 - Remova a política SSL da política de controle de acesso como etapa de mitigação
- Isso é definido na guia Avançado

A Política SSL suspeita de descartar tráfego, os eventos de conexão juntamente com a configuração de política podem ser enviados ao TAC.

Para obter uma solução de problemas mais detalhada da Política SSL, consulte o [artigo](#) relevante sobre solução de problemas de caminho de dados.

Autenticação Ativa

Quando usada em uma política de identidade, a autenticação ativa tem a capacidade de descartar tráfego que deve ser permitido se algo der errado. O próprio recurso de autenticação ativa pode afetar diretamente todo o tráfego HTTP/HTTPS porque, se for determinado que precisamos autenticar um usuário, tudo isso acontece somente através do protocolo HTTP. Isso significa que a autenticação ativa não deve afetar outros serviços de rede (como DNS, ICMP, etc.), a menos que você tenha regras específicas de controle de acesso que bloqueiem com base no usuário e que os usuários não possam se autenticar através dos serviços de autenticação ativa no FTD. No entanto, isso não seria um problema direto do recurso de autenticação ativa, mas um resultado de os usuários não poderem autenticar e terem uma política que bloqueia usuários não autenticados.

Uma etapa de mitigação rápida seria desativar qualquer regra na Política de identidade com a ação de "Autenticação ativa".

Além disso, certifique-se de que as regras com a ação 'Autenticação passiva' não tenham a opção 'Usar autenticação ativa se a autenticação passiva não puder identificar o usuário' marcada.

Editing Rule - Passive

Name: Passive Enabled Move

Action: Passive Authentication Realm: my-realm Authentication Type: HTTP Basic

Zones Networks VLAN Tags Ports Realm & Settings

Realm * my-realm Use active authentication if passive authentication cannot identify user

* Required Field

Save Cancel

Make sure passive auth rules don't fall back to active auth

Remove or disable active auth rules

Or remove identity from Advanced tab of ACP

Action	Auth Type	
Active Authentication	NTLM	<input type="checkbox"/> <input type="checkbox"/>
Active Authentication	Kerberos	<input type="checkbox"/> <input type="checkbox"/>
Active Authentication	HTTP Negotiate	<input type="checkbox"/> <input type="checkbox"/>
Active Authentication	HTTP Response Paq	<input type="checkbox"/> <input type="checkbox"/>
Active Authentication	HTTP Basic	<input type="checkbox"/> <input type="checkbox"/>
Passive Authenticatio	none	<input type="checkbox"/> <input type="checkbox"/>

Identity Policy Settings

Identity Policy None

Solução de problemas mais detalhada da Autenticação Ativa, consulte o [artigo](#) relevante sobre solução de problemas de caminho de dados.

Política de invasão

Uma política de intrusão pode estar descartando tráfego ou causando latência de rede. Uma política de intrusão pode ser usada em um dos três locais a seguir na política de controle de acesso:

- Em uma regra de controle de acesso, na guia "Inspeção"
- Na ação padrão
- Na guia Avançado, na seção **Análise de Rede e Políticas de Intrusão > Política de Intrusão usada antes que a regra de Controle de Acesso seja determinada**

Para ver se uma regra de política de intrusão está bloqueando o tráfego, navegue até a página **Analysis > Intrusions > Events** no FMC. A exibição **Tabela de Eventos de Intrusão** fornece informações sobre os hosts envolvidos nos eventos. Consulte o artigo relevante sobre solução de problemas de caminho de dados sobre informações relacionadas à análise de eventos.

A primeira etapa recomendada para determinar se um IPS (Intrusion Policy Signature, Assinatura de Política de Invasão) está bloqueando o tráfego seria utilizar o recurso de **rastreamento de suporte do sistema** do CLI do FTD. Esse comando debug funciona de forma semelhante ao `firewall-engine-debug`, e também oferece a opção de ativar o `firewall-engine-debug` ao lado do `trace`.

A ilustração abaixo mostra um exemplo de uso da ferramenta de rastreamento de suporte do sistema, na qual o resultado mostrou que um pacote foi bloqueado devido a uma regra de intrusão. Isso fornece todos os detalhes, como GID (Group Identifier), SID (Signature Identifier), NAP (Network Analysis Policy) e ID de IPS para que você possa ver exatamente qual política/regra está bloqueando esse tráfego.

```
SHELL
> system support trace

Please specify an IP protocol: tcp
Please specify a client IP address: 192.168.62.69
Please specify a client port:
Please specify a server IP address:
Please specify a server port:
Enable firewall-engine-debug too? [n]: y
Monitoring packet tracer debug messages

[... output omitted for brevity]

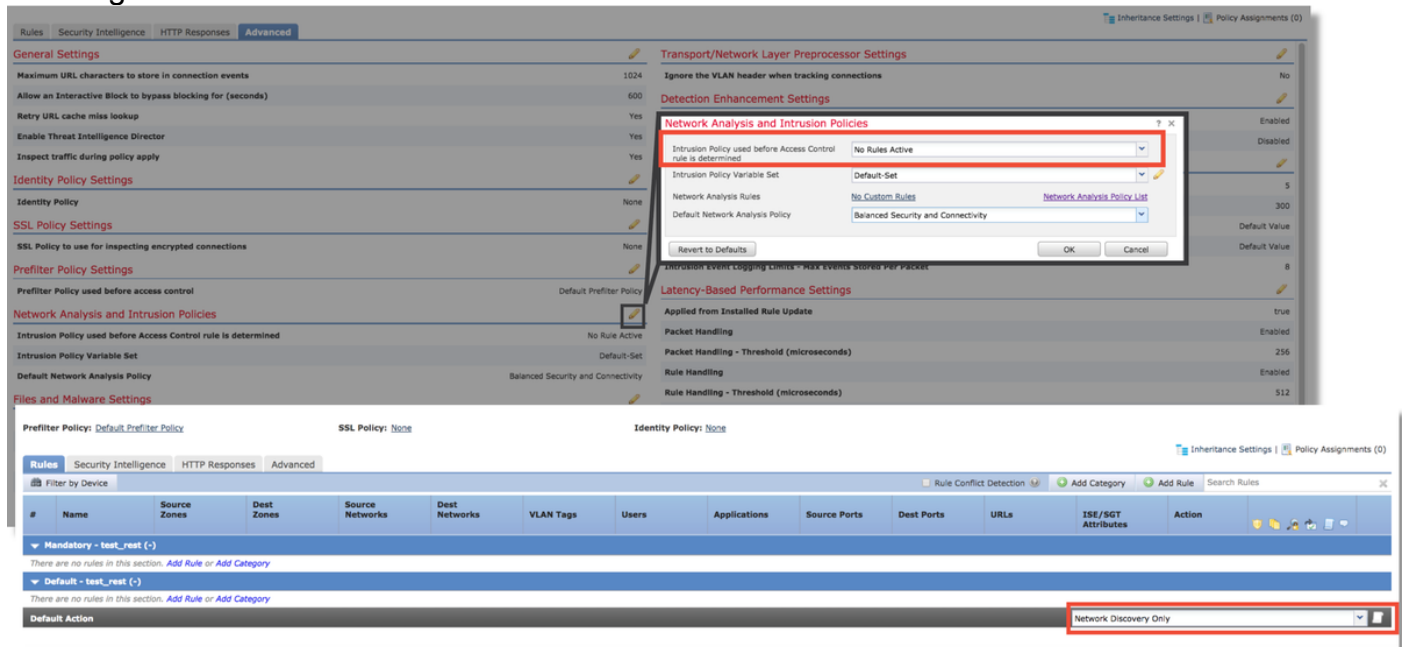
173.37.145.84-80 - 192.168.62.69-38488 6 Packet: TCP, ACK, seq 3594105349, ack 3856774965
173.37.145.84-80 - 192.168.62.69-38488 6 AppID: service HTTP (676), application Cisco (2655)
192.168.62.69-38488 > 173.37.145.84-80 6 AS 1 I 0 URL SI: ShmDBLookupURL("http://www.cisco.com/<?php")
returned 0
...
192.168.62.69-38488 > 173.37.145.84-80 6 AS 1 I 0 match rule order 5, 'inspect it all', action Allow
192.168.62.69-38488 > 173.37.145.84-80 6 AS 1 I 0 allow action
192.168.62.69-38488 > 173.37.145.84-80 6 Firewall: allow rule, 'inspect it all', allow
192.168.62.69-38488 > 173.37.145.84-80 6 IPS Event: gid 1, sid 23111, drop
192.168.62.69-38488 > 173.37.145.84-80 6 Snort detect_drop: gid 1, sid 23111, drop
192.168.62.69-38488 > 173.37.145.84-80 6 AS 1 I 0 Deleting session
192.168.62.69-38488 > 173.37.145.84-80 6 NAP id 1, IPS id 0, Verdict BLACKLIST
192.168.62.69-38488 > 173.37.145.84-80 6 -> Blocked by IPS
Verdict reason is sent to DAQ's PDTS
```

Se você não puder determinar que o IPS está bloqueando a saída de rastreamento, mas suspeitar que o IPS está sendo descartado devido a uma política de intrusão personalizada, substitua a política de intrusão por uma política de "segurança e conectividade equilibradas" ou uma política de "conectividade sobre segurança". Essas são as políticas de intrusão fornecidas pela Cisco. Se fizer essa alteração, resolverá o problema e a Política de intrusão personalizada usada anteriormente poderá ser solucionada pelo TAC. Se uma política padrão da Cisco já for usada, você pode tentar alterar o padrão para um padrão menos seguro, pois eles têm menos regras, portanto, isso pode ajudar a restringir o escopo. Por exemplo, se o tráfego for bloqueado e você estiver usando uma política equilibrada, então você mudará para a conectividade em relação à política de segurança e o problema desaparecerá, é provável que haja uma regra na política equilibrada que elimine o tráfego que não está definido para cair na conectividade em relação à política de segurança.

As seguintes alterações podem ser feitas na política de controle de acesso para eliminar todas as possibilidades de bloqueio de inspeção da política de intrusão (recomenda-se fazer o menor número possível de alterações para não alterar a sua eficácia de segurança, por isso recomenda-

se a elaboração de regras de CA direcionadas para o tráfego em questão, em vez de desativar o IPS em toda a política):

- Em todas as regras de controle de acesso (ou apenas nas regras que o tráfego específico está correspondendo e que sofre impacto), remova a política de intrusão da guia Inspeção
- Na guia Avançado, na seção **Análise de Rede e Políticas de Intrusão > Política de Intrusão usada antes que a regra de Controle de Acesso seja determinada**, escolha a política "Sem Regras Ativas".



Se isso ainda não resolver o problema, avance para a solução de problemas da política de análise de rede.

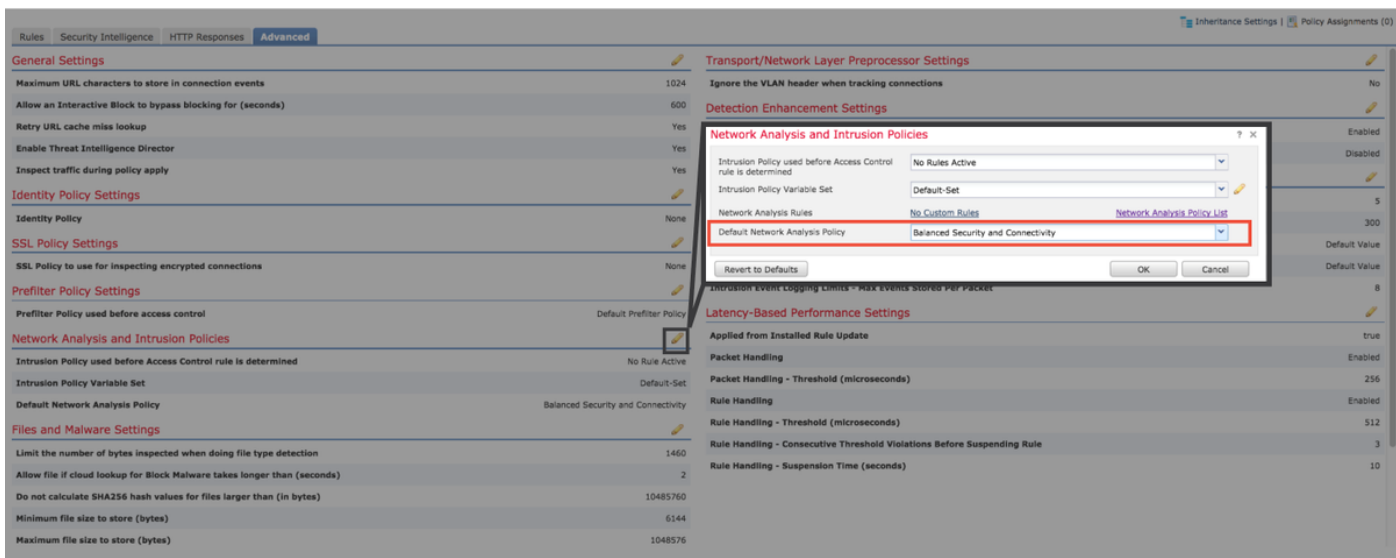
Solução de problemas mais detalhada do recurso de política de intrusão, reveja o [artigo](#) relevante de solução de problemas de caminho de dados.

Política de análise de rede

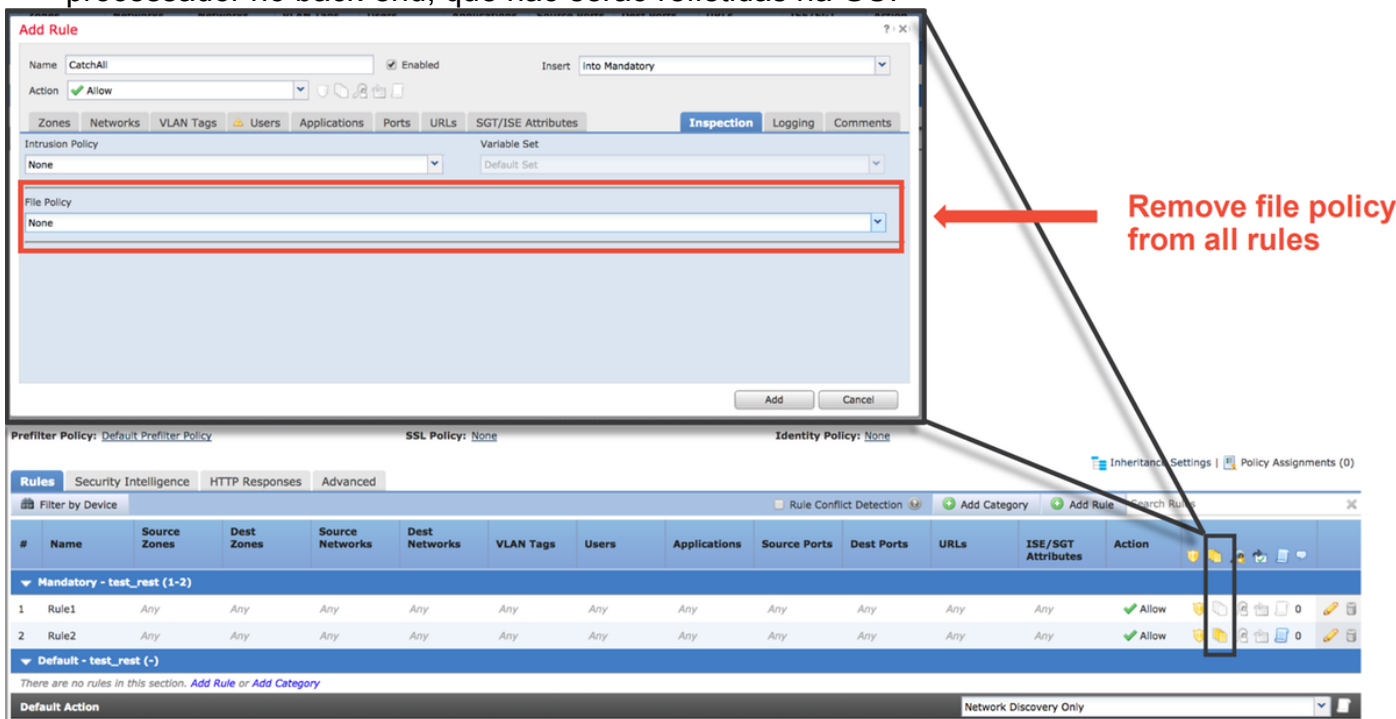
O NAP (Network Analysis Policy, Política de análise de rede) contém configurações de pré-processador do Firepower, algumas das quais podem descartar tráfego. A primeira etapa recomendada para a solução de problemas é a mesma que para a solução de problemas de IPS, que é usar a ferramenta > **system support trace** para tentar descobrir o que no snort está bloqueando o tráfego. Consulte a seção "Política de intrusão" acima para obter mais informações sobre esta ferramenta e sobre o uso de exemplos.

Para atenuar rapidamente possíveis problemas com o NAP, as seguintes etapas podem ser executadas:

- Se um NAP personalizado estiver sendo usado, substitua-o 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, remova-a temporariamente como uma política de arquivo pode ativar as configurações de pré-processador no back-end, que não serão refletidas na GUI



Uma solução de problemas mais detalhada do recurso Network Analysis Policy pode ser revisada neste [artigo](#).

Informações Relacionadas

Links para a documentação do Firepower

<https://www.cisco.com/c/en/us/td/docs/security/firepower/roadmap/firepower-roadmap.html>