

Fase 8 de Troubleshooting de Trayectoria de Datos de Firepower: Política de análisis de red

Contenido

[Introducción](#)

[Prerequisites](#)

[Solución de problemas de la función de política de análisis de red](#)

[Uso de la herramienta "trace" para encontrar caídas del preprocesador \(sólo FTD\)](#)

[Verificación de la Configuración NAP](#)

[Ver configuración NAP](#)

[Configuración de NAP que puede causar caídas silenciosas](#)

[Verificar la configuración del motor](#)

[Creación de un NAP dirigido](#)

[Análisis falso positivo](#)

[Pasos de mitigación](#)

[Datos que se deben proporcionar al TAC](#)

Introducción

Este artículo forma parte de una serie de artículos que explican cómo resolver sistemáticamente los problemas de la ruta de datos en sistemas Firepower para determinar si los componentes de Firepower pueden estar afectando al tráfico. Consulte el [artículo Descripción General](#) para obtener información sobre la arquitectura de las plataformas Firepower y los enlaces a los otros artículos de Troubleshooting de Trayectoria de Datos.

En este artículo se describe la octava etapa de la solución de problemas de la ruta de datos de Firepower, la función Política de análisis de red.



Prerequisites

- Este artículo se aplica a todas las plataformas Firepower
La función **trace** sólo está disponible en la versión de software 6.2.0 y posterior para la plataforma Firepower Threat Defense (FTD).
- El conocimiento de código abierto Snort es útil, aunque no es necesario Para obtener información sobre el Snort de código abierto, visite <https://www.snort.org/>

Solución de problemas de la función de política de análisis de red

La política de análisis de red (NAP) contiene la configuración del preprocesador de tubos que

realiza inspecciones del tráfico, en función de la aplicación identificada. Los preprocesadores tienen la capacidad de descartar tráfico, en función de la configuración. Este artículo trata sobre cómo verificar la configuración NAP y buscar caídas del preprocesador.

Nota: Las reglas del preprocesador tienen una ID de generador (GID) distinta de '1' o '3' (es decir, 129, 119, 124). Puede encontrar más información sobre el GID para las asignaciones de preprocesador en las [Guías de Configuración](#) de FMC.

Uso de la herramienta "trace" para encontrar caídas del preprocesador (sólo FTD)

La herramienta **de seguimiento de soporte del sistema** se puede utilizar para detectar caídas realizadas en el nivel del preprocesador.

En el siguiente ejemplo, el preprocesador de normalización TCP detectó una anomalía. Como resultado, el tráfico se descarta por la regla **129:14**, que busca marcas de tiempo faltantes dentro de una secuencia 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 I 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 I 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
```

Nota: Aunque el preprocesador **TCP Stream Configuration** descarta el tráfico, puede hacerlo porque el preprocesador **Inline Normalization** también está habilitado. Para obtener más información sobre la Normalización en línea, puede leer este [artículo](#).

Verificación de la Configuración NAP

En la interfaz de usuario de Firepower Management Center (FMC), el NAP se puede ver en **Políticas > Control de acceso > Intrusión**. A continuación, haga clic en la opción **Network Analysis Policy** en la parte superior derecha, después de lo cual podrá ver los NAPs, crear otros nuevos y editar los existentes.

Inline Result	Source IP	Destination IP	Source Port / ICMP Type	Destination Port / ICMP Code	Message
<input type="checkbox"/>	172.16.111.226	50.19.123.95	51177 / tcp	443 (https) / tcp	STREAM5_NO_TIMESTAMP (129:14:2)
<input checked="" type="checkbox"/>	172.16.111.226	50.19.123.95	51174 / tcp	443 (https) / tcp	STREAM5_NO_TIMESTAMP (129:14:2)

Inline Mode disabled = No Inline Result

Inline Mode enabled = "Dropped" Inline Result

Como se puede ver en la ilustración anterior, los NAP contienen una función "Modo en línea", que equivale a la opción "Descartar cuando en línea" de la política de intrusiones. Un paso de mitigación rápido para evitar que el NAP descarte tráfico sería desmarcar el **modo en línea**. Los eventos de intrusión generados por el NAP no muestran nada en la pestaña **Resultados en línea** con **Modo en línea** desactivado.

Ver configuración NAP

En el NAP, puede ver la configuración actual. Esto incluye el total de preprocesadores habilitados, seguido por el

preprocesadores habilitados con configuraciones no predeterminadas (que se modificaron manualmente) y que están habilitados con configuraciones predeterminadas, como se muestra en la ilustración siguiente.

Configuración de NAP que puede causar caídas silenciosas

En el ejemplo mencionado en la sección de seguimiento, la regla TCP Stream Configuration **129:14** está descartando tráfico. Esto se determina observando el resultado **del seguimiento de soporte del sistema**. Sin embargo, si la regla mencionada no está habilitada dentro de la política de intrusiones respectiva, no se envía ningún evento de intrusión al FMC.

La razón por la que esto sucede se debe a una configuración dentro del preprocesador de **normalización en línea** llamado **Bloqueo de Anomalías de Encabezado TCP Inresolubles**. Esta opción básicamente permite a Snort realizar una acción de bloqueo cuando ciertas reglas GID 129 detectan anomalías en la secuencia TCP.

Si **Block Unresolvable TCP Header Anomalies** está habilitado, se recomienda activar las reglas GID 129 por la ilustración siguiente.

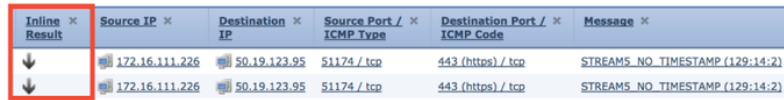
The screenshot displays the 'Intrusion Policy' configuration page. The filter is set to 'GID:"129"'. A table lists 19 rules, with 12 selected. A context menu is open over rule 129, showing options: 'Generate Events', 'Drop and Generate Events', and 'Disable'. The 'Policy Information' sidebar is open, showing the 'Inline Normalization' section. The 'Block Unresolvable TCP Header Anomalies' option is checked and highlighted with a red box.

Rule ID	Action	Rule Name
129 4	<input checked="" type="checkbox"/>	STREAM5_BAD_TIMESTAMP
129 5	<input type="checkbox"/>	STREAM5_BAD_SEGMENT
129 6	<input checked="" type="checkbox"/>	STREAM5_WINDOW_TOO_LARGE
129 7	<input type="checkbox"/>	STREAM5_EXCESSIVE_TCP_OVERLAPS
129 8	<input checked="" type="checkbox"/>	STREAM5_DATA_AFTER_RESET
129 9	<input type="checkbox"/>	STREAM5_SESSION_HIJACKED_CLIENT
129 10	<input type="checkbox"/>	STREAM5_SESSION_HIJACKED_SERVER
129 11	<input checked="" type="checkbox"/>	STREAM5_DATA_WITHOUT_FLAGS
129 12	<input type="checkbox"/>	STREAM5_SMALL_SEGMENT
129 13	<input type="checkbox"/>	STREAM5_4WAY_HANDSHAKE
129 14	<input checked="" type="checkbox"/>	STREAM5_NO_TIMESTAMP
129 15	<input checked="" type="checkbox"/>	STREAM5_BAD_RST
129 16	<input checked="" type="checkbox"/>	STREAM5_BAD_FIN
129 17	<input checked="" type="checkbox"/>	STREAM5_BAD_ACK
129 18	<input checked="" type="checkbox"/>	STREAM5_DATA_AFTER_RST_RCVD
129 19	<input checked="" type="checkbox"/>	STREAM5_WINDOW_SLAM

Setting	Status
Normalize IPv4	<input type="checkbox"/>
Normalize Don't Fragment Bit	<input type="checkbox"/>
Normalize Reserved Bit	<input type="checkbox"/>
Normalize TOS Bit	<input type="checkbox"/>
Normalize Excess Payload	<input type="checkbox"/>
Normalize IPv6	<input type="checkbox"/>
Normalize ICMPv4	<input type="checkbox"/>
Normalize ICMPv6	<input type="checkbox"/>
Normalize/Clear Reserved Bits	<input checked="" type="checkbox"/>
Normalize/Clear Option Padding Bytes	<input checked="" type="checkbox"/>
Clear Urgent Pointer if URG=0	<input checked="" type="checkbox"/>
Clear Urgent Pointer/URG on Empty Payload	<input checked="" type="checkbox"/>
Clear URG if Urgent Pointer Is Not Set	<input checked="" type="checkbox"/>
Normalize Urgent Pointer	<input type="checkbox"/>
Normalize TCP Payload	<input checked="" type="checkbox"/>
Remove Data on SYN	<input type="checkbox"/>
Remove Data on RST	<input type="checkbox"/>
Trim Data to Window	<input type="checkbox"/>
Trim Data to MSS	<input type="checkbox"/>
Block Unresolvable TCP Header Anomalies	<input checked="" type="checkbox"/>

Al activar las reglas GID 129, los eventos de intrusión se envían al FMC cuando realizan acciones sobre el tráfico. Sin embargo, siempre y cuando se habilite **Block Unresolvable TCP Header Anomalies**, todavía puede descartar el tráfico incluso si el **Estado de regla** en la política de intrusiones está configurado como **Generate Events**. Este comportamiento se explica en las Guías de configuración de 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.

La documentación anterior puede encontrarse en este [artículo](#) (para la versión 6.4, que es la versión más reciente en el momento de la publicación de este artículo).

Verificar la configuración del motor

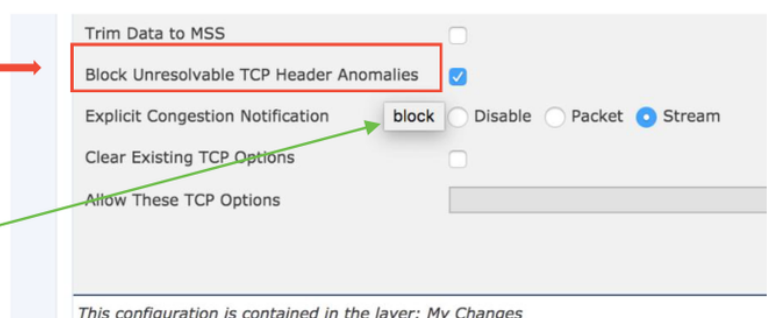
Se agrega otra capa de complejidad al comportamiento del preprocesador en el sentido de que ciertos ajustes se pueden habilitar en el motor, sin reflejarse en el FMC. Estas son algunas de las razones posibles.

- Otras funciones habilitadas pueden forzar la activación de la configuración del preprocesador (la principal es la política de archivos)
- Algunas reglas de la política de intrusiones requieren ciertas opciones del preprocesador para realizar la detección
- Un defecto puede provocar el comportamiento Hemos visto un ejemplo de esto: [CSCuz50295](#) - "La política de archivos con bloqueo de malware habilita la normalización de TCP con indicador de bloqueo"

Antes de observar la configuración del motor, observe que las palabras clave Snort, que se utilizan en los archivos de configuración del motor Snort, se pueden ver pasando el cursor sobre una configuración específica dentro del NAP. Consulte la ilustración siguiente.

Hover over option to see backend snort configuration keyword

Snort config keyword is "block"



La opción **Block Unresolvable TCP Header Anomalies** en la ficha NAP se traduce a la palabra clave **block** en el motor. Con esa información en mente, la configuración del motor se puede verificar desde el shell de expertos.

```
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

Creación de un NAP dirigido

Si ciertos hosts están activando eventos del preprocesador, se puede utilizar un NAP personalizado para inspeccionar el tráfico hacia o desde dichos hosts. Dentro del NAP personalizado, las configuraciones que están causando problemas pueden desactivarse.

Estos son los pasos para implementar un PAN específico.

1. Cree el NAP según las instrucciones mencionadas en la sección Verificación de la configuración NAP de este artículo.
2. En la ficha **Avanzadas** de la política de control de acceso, vaya a la sección **Análisis de red y Políticas de intrusión**. Haga clic en **Agregar regla** y cree una regla, utilizando los hosts objetivo y elija el NAP recién creado en la sección **Política de análisis de red**.

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

Análisis falso positivo

La comprobación de falsos positivos en eventos de intrusión para las reglas del preprocesador es muy diferente a la de las reglas de Snort utilizadas para la evaluación de reglas (que contienen una GID de 1 y 3).

Para realizar un análisis falso positivo para los eventos de regla del preprocesador, es necesaria una captura de sesión completa para buscar anomalías dentro del flujo TCP.

En el ejemplo siguiente, se está realizando un análisis de falsos positivos sobre la regla **129:14**, que se muestra que está descartando el tráfico en los ejemplos anteriores. Dado que **129:14** busca secuencias TCP en las que faltan marcas de tiempo, puede ver claramente por qué se activó la regla según el análisis de captura de paquetes que se muestra a continuación.

Full session pcap

Packet 1: SYN packet has TCP Timestamps

```
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
```

Packet 2: Packet that triggered event

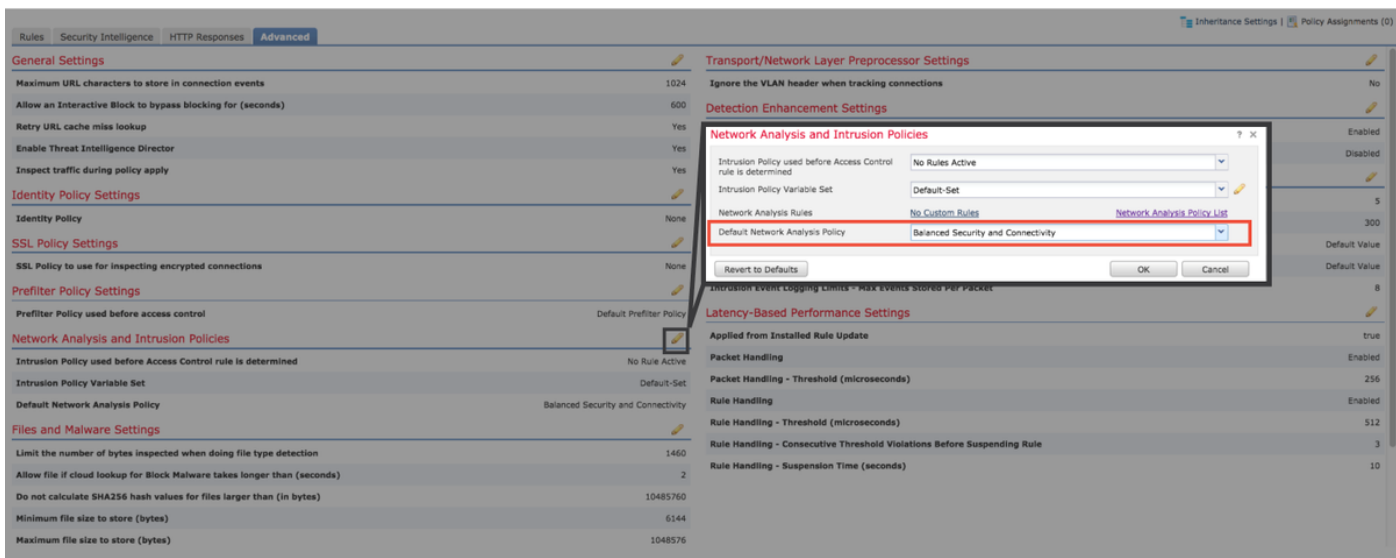
```
Internet Protocol Version 4, Src: 172.16.111.226, Dst: 50.19.123.95
Transmission Control Protocol, Src Port: 51174, Dst Port: 443, Seq: 3849839667, Ack: 1666843207, Len: 0
  Source Port: 51174
  Destination Port: 443
  [Stream index: 0]
  [TCP Segment Len: 0]
  Sequence number: 3849839667
  Acknowledgment 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
```

No TCP Timestamps in event packet (violates RFC)

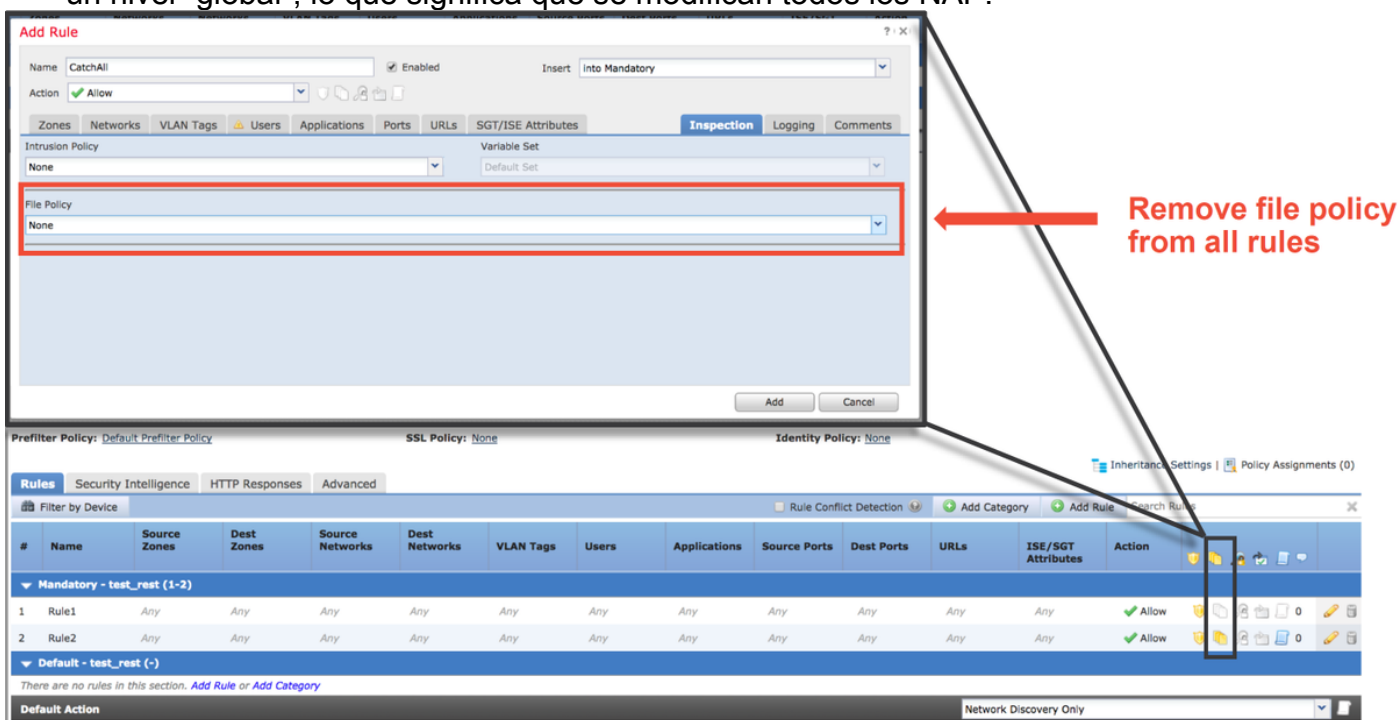
Pasos de mitigación

Para mitigar rápidamente los posibles problemas con el NAP, se pueden realizar los siguientes pasos.

- Si se está utilizando un NAP personalizado y no está seguro de si una configuración NAP está descartando tráfico pero sospecha que podría serlo, puede intentar sustituirlo por una política de "Seguridad y conectividad equilibradas" o "Conectividad sobre seguridad".



- Si se está utilizando alguna "Reglas personalizadas", asegúrese de establecer el NAP en uno de los valores predeterminados mencionados anteriormente
- Si alguna regla de control de acceso utiliza una política de archivos, es posible que tenga que intentar eliminarla temporalmente, ya que una política de archivos puede habilitar la configuración previa al procesador en el motor que no se refleja en el FMC, y esto sucede a un nivel "global", lo que significa que se modifican todos los NAP.



Cada protocolo tiene un preprocesador diferente y la resolución de problemas puede ser muy específica para el preprocesador. Este artículo no cubre todos los parámetros del preprocesador ni los métodos de resolución de problemas para cada uno.

Puede comprobar la documentación de cada preprocesador para obtener una mejor idea de lo que hace cada opción, lo que resulta útil a la hora de resolver problemas de un preprocesador específico.

Datos que se deben proporcionar al TAC

Datos Instrucciones

Solución

de

problemas

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

desde el

dispositivo

Firepower

Captura

de

paquetes

de sesión

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

desde el

dispositivo

Firepower