

Fehlerbehebung für FirePOWER-Datenpfade

Phase 8: Richtlinie für Netzwerkanalysen

Inhalt

[Einführung](#)

[Voraussetzungen](#)

[Fehlerbehebung: Network Analysis Policy-Funktion](#)

[Verwendung des "trace"-Tools zum Suchen von Preprocessor Drops \(nur FTD\)](#)

[NAP-Konfiguration überprüfen](#)

[NAP-Einstellungen anzeigen](#)

[NAP-Einstellungen, die stille Verluste verursachen können](#)

[Überprüfen der Backend-Konfiguration](#)

[Erstellen eines zielgerichteten NAP](#)

[Fehlalarme Analyse](#)

[Schritte zur Risikominimierung](#)

[Daten für TAC](#)

Einführung

Dieser Artikel ist Teil einer Reihe von Artikeln, in denen erläutert wird, wie der Datenpfad auf FirePOWER-Systemen systematisch behoben wird, um festzustellen, ob Komponenten von FirePOWER den Datenverkehr beeinträchtigen können. Weitere Informationen zur Architektur von FirePOWER-Plattformen und Links zu anderen Artikeln zur Fehlerbehebung für Datenpfade finden Sie im [Overview-Artikel](#).

Dieser Artikel behandelt die achte Phase der Fehlerbehebung für den FirePOWER-Datenpfad, die Funktion Network Analysis Policy (Netzwerkanalyserichtlinie).



Voraussetzungen

- Dieser Artikel gilt für alle Firepower-Plattformen
Die **Ablaufverfolgungsfunktion** ist nur in der Softwareversion 6.2.0 und höher für die Firepower Threat Defense (FTD)-Plattform verfügbar.
- Kenntnisse von Open-Source-Snort sind hilfreich, aber nicht erforderlich Informationen zu Open-Source-Snort finden Sie unter <https://www.snort.org/>

Fehlerbehebung: Network Analysis Policy-Funktion

Die Network Analysis Policy (NAP) enthält Präprozessoreinstellungen, die

Datenverkehrskontrollen anhand der identifizierten Anwendung durchführen. Die Präprozessoren können Datenverkehr je nach Konfiguration verwerfen. In diesem Artikel wird beschrieben, wie Sie die NAP-Konfiguration überprüfen und nach Verwerfen von Präprozessoren suchen.

Hinweis: Präprozessorregeln haben eine andere Generator-ID (GID) als '1' oder '3' (d. h. 129, 119, 124). Weitere Informationen zu GID-Präprozessorzusammenordnungen finden Sie in den FMC-[Konfigurationsanleitungen](#).

Verwendung des "trace"-Tools zum Suchen von Preprocessor Drops (nur FTD)

Das Trace-Tool für die Systemunterstützung kann verwendet werden, um auf Präprozessorebene durchgeführte Verwerfungen zu erkennen.

Im folgenden Beispiel hat der TCP-Normalisierungspräprozessor eine Anomalie erkannt. Daher wird der Datenverkehr durch Regel **129:14** unterbrochen, die nach fehlenden Zeitstempeln innerhalb eines TCP-Streams sucht.

```
> 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
```

Hinweis: Obwohl der Vorprozessor TCP-Stream-Konfiguration den Datenverkehr verwirft, ist dies möglich, da der Inline-Normalisierungs-Präprozessor ebenfalls aktiviert ist. Weitere Informationen zur Inline-Normalisierung finden Sie in diesem [Artikel](#).

NAP-Konfiguration überprüfen

Auf der FirePOWER Management Center (FMC)-Benutzeroberfläche kann das NAP unter **Richtlinien > Zugriffskontrolle > Zugriffskontrolle** angezeigt werden. Klicken Sie dann oben rechts auf die Option **Network Analysis Policy** (Netzwerkanalyserichtlinie), um die NAPs anzuzeigen, neue zu erstellen und vorhandene zu bearbeiten.

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)

Annotations: A red box around the first row's checkbox is linked to the text 'Inline Mode disabled = No Inline Result'. A red box around the second row's checkbox is linked to the text 'Inline Mode enabled = "Dropped" Inline Result'.

Wie in der Abbildung oben gezeigt, enthalten die NAPs eine Funktion für den "Inline-Modus", die der Option "Drop When Inline" in der Intrusion Policy entspricht. Um zu verhindern, dass das NAP Datenverkehr verwirft, können Sie die Option **Inline Mode (Inline-Modus)** deaktivieren. Die vom NAP generierten Intrusion Events (Intrusion Events) zeigen auf der Registerkarte **Inline Result (Inline-Ergebnis)** keine Ereignisse an, bei denen der **Inline-Modus** deaktiviert ist.

NAP-Einstellungen anzeigen

Im NAP können Sie die aktuellen Einstellungen anzeigen. Dazu gehören die insgesamt aktivierten Vorprozessoren, gefolgt von

Voreinstellungen, die mit nicht standardmäßigen Einstellungen aktiviert wurden (solche, die manuell angepasst wurden) und solche, die mit Standardeinstellungen aktiviert sind, wie in der Abbildung unten gezeigt.

NAP-Einstellungen, die stille Verluste verursachen können

Im Beispiel, das im Ablaufverfolgungsabschnitt erwähnt wird, verwirft die Regel TCP Stream Configuration Rule **129:14** den Datenverkehr. Dies wird durch die **Trace**-Ausgabe der **Systemunterstützung** bestimmt. Wenn die genannte Regel jedoch nicht in der entsprechenden Intrusion Policy aktiviert ist, werden keine Intrusion Events an das FMC gesendet.

Der Grund dafür liegt in einer Einstellung innerhalb des Präprozessors **Inline-Normalisierung**, die als **Unauflösbare TCP-Header-Anomalien** bezeichnet wird. Mit dieser Option kann Snort eine Blockaktion ausführen, wenn bestimmte GID 129-Regeln Anomalien im TCP-Stream erkennen.

Wenn **Blockieren nicht auflösbarer TCP-Header-Anomalien** aktiviert ist, wird empfohlen, die GID 129-Regeln entsprechend der unten stehenden Abbildung zu aktivieren.

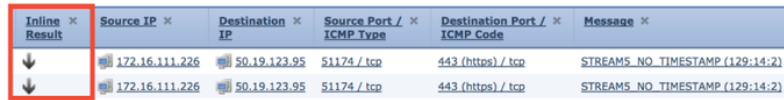
The screenshot displays the 'Intrusion Policy' configuration page with a filter set to 'GID:129'. It shows a list of 19 rules, with 12 selected. A context menu is open over rule 129:19, showing options: 'Generate Events', 'Drop and Generate Events', and 'Disable'. The 'Policy Layers' section is expanded to 'Inline Normalization', which is further expanded to show various settings. The 'Block Unresolvable TCP Header Anomalies' checkbox 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"/>

Durch das Aktivieren der GID 129-Regeln werden Intrusion Events an das FMC gesendet, wenn diese Aktionen für den Datenverkehr ausführen. Solange jedoch die **Unauflösbare TCP-Header-Anomalien blockiert** sind, kann der Datenverkehr trotzdem verworfen werden, selbst wenn der **Regelstatus** in der Intrusion Policy auf **Ereignisse** festgelegt ist. Dieses Verhalten wird in den FMC-Konfigurationsanleitungen erläutert.

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.

Die obige Dokumentation finden Sie in diesem [Artikel](#) (für Version 6.4, die neueste Version zum Zeitpunkt der Veröffentlichung dieses Artikels).

Überprüfen der Backend-Konfiguration

Eine weitere Ebene der Komplexität wird dem Verhalten des Präprozessors hinzugefügt, da bestimmte Einstellungen am Backend aktiviert werden können, ohne dass sie im FMC übernommen werden. Dies sind einige mögliche Gründe.

- Andere aktivierte Funktionen können die Aktivierung von Präprozessoreinstellungen erzwingen (die Haupteinstellung ist Dateirichtlinie).
- Einige Intrusion Policy-Regeln erfordern bestimmte Präprozessoroptionen, um die Erkennung durchzuführen
- Ein Fehler kann das Verhalten verursachen. Ein Beispiel hierfür ist [CSCuz50295](#) - "File policy with Malware block enable TCP normalization with block flag" (Dateirichtlinie mit Malware-Block aktiviert TCP-Normalisierung mit Blockflag).

Bevor Sie sich die Backend-Konfiguration ansehen, beachten Sie, dass die Snort-Schlüsselwörter, die in den Snort-Konfigurationsdateien für das Backend verwendet werden, sichtbar sind, indem Sie den Mauszeiger über eine bestimmte Einstellung im NAP bewegen. Weitere Informationen finden Sie in der Abbildung unten.

Hover over option to see backend snort configuration keyword

Snort config keyword is "block"

The screenshot shows a configuration panel with several options. A red box highlights the option 'Block Unresolvable TCP Header Anomalies', which is checked. A red arrow points from the text 'Hover over option to see backend snort configuration keyword' to this option. Below it, the 'Explicit Congestion Notification' option is set to 'block', with a green arrow pointing from the text 'Snort config keyword is "block"' to this value. Other options include 'Trim Data to MSS', 'Clear Existing TCP Options', and 'Allow These TCP Options'. The bottom of the panel indicates 'This configuration is contained in the layer: My Changes'.

Die Option **Unauflösbare TCP-Header-Anomalien** auf der Registerkarte NAP **blockieren** wird in das **Block**-Schlüsselwort auf dem Backend übersetzt. Unter Berücksichtigung dieser Informationen kann die Backend-Konfiguration über die Expert Shell überprüft werden.

```
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

Erstellen eines zielgerichteten NAP

Wenn bestimmte Hosts Präprozessorereignisse auslösen, kann ein benutzerdefiniertes NAP verwendet werden, um den Datenverkehr zu oder von diesen Hosts zu überprüfen. Innerhalb des benutzerdefinierten NAP können die Einstellungen, die Probleme verursachen, deaktiviert werden.

Dies sind die Schritte zur Implementierung eines zielgerichteten NAP.

1. Erstellen Sie den NAP gemäß den Anweisungen, die im Abschnitt "NAP-Konfiguration überprüfen" in diesem Artikel erwähnt werden.
2. Navigieren Sie auf der Registerkarte **Erweitert** der Zugriffskontrollrichtlinie zum Abschnitt **Netzwerkanalyse und Zugriffsrichtlinien**. Klicken Sie auf **Regel hinzufügen**, erstellen Sie eine Regel, verwenden Sie die Zielhosts, und wählen Sie im Abschnitt **Network Analysis Policy (Netzwerkanalyse-richtlinie)** den neu erstellten NAP aus.

Network Analysis and Intrusion Policies

Intrusion Policy used before Access Control rule is determined	My Intrusion Policy
Intrusion Policy Variable Set	Default-Set
Default Network Analysis Policy	Security Over Connectivity

Click to expand NA Rules

Add rule(s) to target traffic with certain NAP

Fehlalarme Analyse

Das Überprüfen auf Fehlalarme in Intrusion Events für Präprozessorregeln unterscheidet sich stark von den Snort-Regeln, die für die Regelauswertung verwendet werden (die eine GID von 1 und 3 enthalten).

Um eine falsch positive Analyse für Präprozessorregelereignisse durchzuführen, ist eine vollständige Sitzungserfassung erforderlich, um nach Anomalien im TCP-Stream zu suchen.

Im folgenden Beispiel wird eine Fehlalarme-Analyse für Regel **129:14** durchgeführt, die in den obigen Beispielen nachweislich den Datenverkehr verwirft. Da **129:14** nach TCP-Streams sucht, in denen Zeitstempel fehlen, können Sie deutlich erkennen, warum die Regel gemäß der unten abgebildeten Paketerfassungsanalyse ausgelöst wurde.

Full session pcap

```

> 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
  
```

SYN packet has TCP Timestamps

Packet that triggered event

```

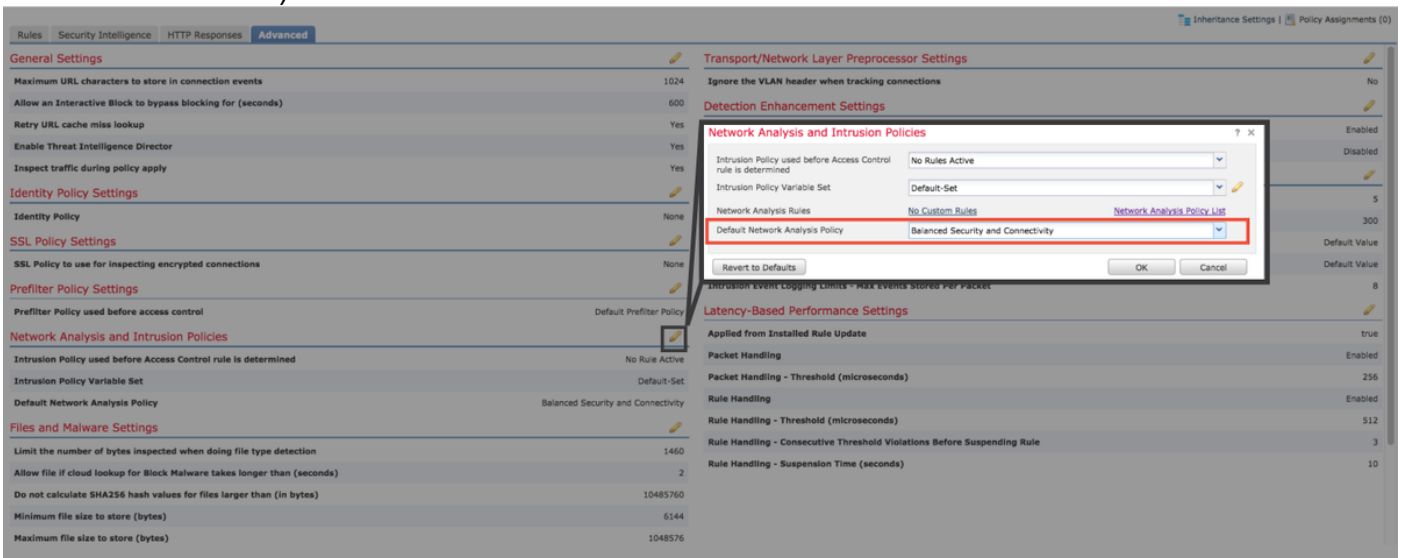
> Internet Protocol Version 4, Src: 172.16.111.226, Dst: 50.19.123.95
  > Transmission Control Protocol, Src Port: 51174, Dst Port: 443, Seq: 3849839667, Ack: 1666843207, Len: 0
    Source Port: 51174
    Destination Port: 443
    [Stream index: 0]
    [TCP Segment Len: 0]
    Sequence number: 3849839667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

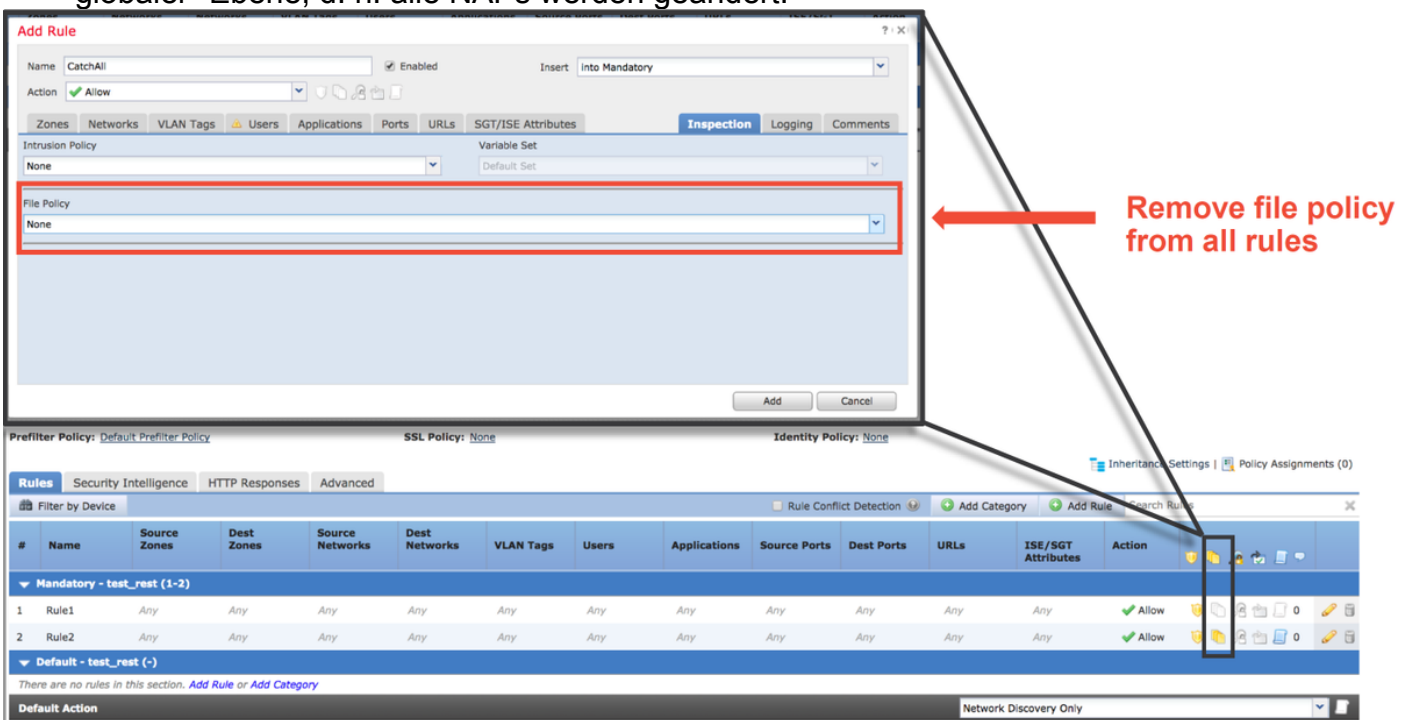
Schritte zur Risikominimierung

Um mögliche Probleme mit dem NAP schnell zu beheben, können die folgenden Schritte ausgeführt werden.

- Wenn ein benutzerdefiniertes NAP verwendet wird und Sie nicht sicher sind, ob eine NAP-Einstellung den Datenverkehr verwirft, aber vermuten, dass dies der Fall sein könnte, können Sie versuchen, es durch eine Richtlinie für "Balanced Security and Connectivity" (Ausgewogene Sicherheit und Konnektivität) oder "Connectivity over Security" (Konnektivität über Sicherheit) zu ersetzen.



- Wenn benutzerdefinierte Regeln verwendet werden, stellen Sie sicher, dass für das NAP eine der oben genannten Standardeinstellungen festgelegt wird.
- Wenn Zugriffskontrollregeln eine Dateirichtlinie verwenden, müssen Sie versuchen, diese vorübergehend zu entfernen, da eine Dateirichtlinie die Vorprozessoreinstellungen am Backend aktivieren kann, die im FMC nicht übernommen werden. Dies geschieht auf "globaler" Ebene, d. h. alle NAPs werden geändert.



Jedes Protokoll hat einen anderen Präprozessor, und die Fehlerbehebung kann sehr spezifisch für den Präprozessor sein. In diesem Artikel werden nicht alle Präprozessoreinstellungen und

Fehlerbehebungsmethoden für jedes Präprozessor behandelt.

Sie können die Dokumentation für jeden Präprozessor überprüfen, um eine bessere Vorstellung davon zu erhalten, was jede Option tut, was bei der Fehlerbehebung eines bestimmten Präprozessors hilfreich ist.

Daten für TAC

Daten

Fehlerbehebungsdatei

vom FirePOWER-

Gerät

Vollständige

Paketerfassung über

das FirePOWER-

Gerät

Anweisungen

<http://www.cisco.com/c/en/us/support/docs/security/sourcefire-defense-center/117>

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