

# Vergleich von NAP-Richtlinien auf FirePOWER-Geräten

## Inhalt

[Einführung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Hintergrundinformationen](#)

[NAP-Konfiguration überprüfen](#)

### Einführung

In diesem Dokument wird beschrieben, wie Sie verschiedene Network Analysis Policies (NAP) für vom FirePOWER Management Center (FMC) verwaltete Firepower-Geräte vergleichen.

### Voraussetzungen

### Anforderungen

Cisco empfiehlt, über Kenntnisse in folgenden Bereichen zu verfügen:

- Kenntnisse von Open-Source-Snort
- FirePOWER Management Center (FMC)
- Firepower Threat Defense (FTD)

### Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf den folgenden Software- und Hardwareversionen:

- Dieser Artikel gilt für alle Firepower-Plattformen
- Cisco FirePOWER Threat Defense (FTD) mit Softwareversion 6.4.0
- FirePOWER Management Center Virtual (FMC) mit Softwareversion 6.4.0

### Hintergrundinformationen

Snort verwendet Verfahren zum Musterabgleich, um Exploits in Netzwerkpaketen zu suchen und zu verhindern. Dazu benötigt die Snort Engine Netzwerkpakete, die so vorbereitet sind, dass dieser Vergleich möglich ist. Dieser Prozess wird mithilfe von NAP durchgeführt und kann in den folgenden drei Phasen durchgeführt werden:

- Dekodierung
- Normal
- Vorverarbeitung

Ein Richtlinienpaket zur Netzwerkanalyse verarbeitet Pakete in mehreren Phasen: Zunächst dekodiert das System Pakete über die ersten drei TCP/IP-Schichten und setzt dann die Normalisierung, Vorverarbeitung und Erkennung von Protokollanomalien fort.

Vorprozessoren bieten zwei Hauptfunktionen:

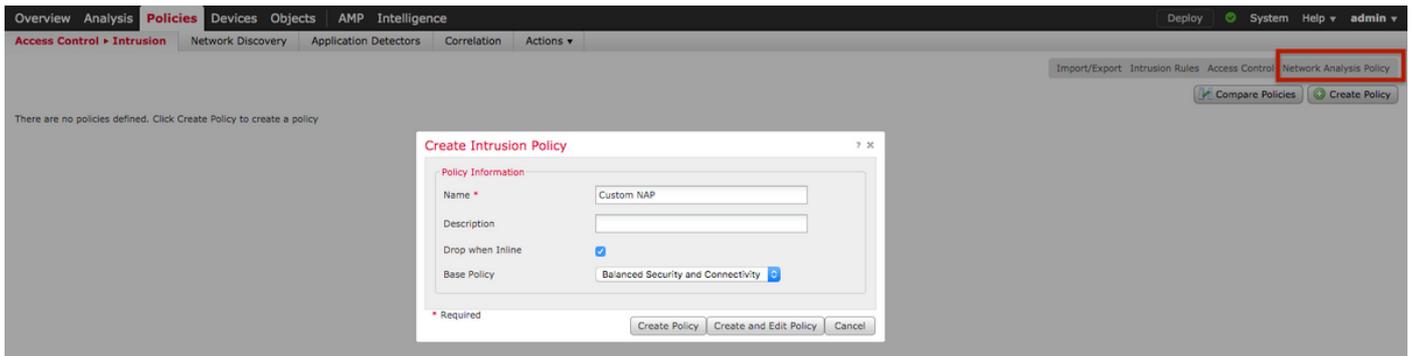
- Normalisierung des Datenverkehrs zur weiteren Überprüfung
- Identifizierung von Protokollanomalien

**Hinweis:** Einige Intrusion Policy-Regeln erfordern bestimmte Präprozessoroptionen, um die Erkennung durchzuführen.

Informationen zu Open-Source Snort finden Sie unter <https://www.snort.org/>

## NAP-Konfiguration überprüfen

Um Firewall-NAP-Richtlinien zu erstellen oder zu bearbeiten, navigieren Sie zu **FMC Policies > Access Control > Intrusion (FMC-Richtlinien > Zugriffskontrolle > Zugriffskontrolle)**, und klicken Sie anschließend in der oberen rechten Ecke auf **Network Analysis Policy** (Netzwerkanalyse-richtlinie), wie im Bild gezeigt:



Network Analysis Policy	Inline Mode	Status	Last Modified
Test1	Yes	No access control policies use this policy. Policy not applied on any devices	2019-12-30 02:13:49 Modified by "admin"
Test2*	Yes	You are currently editing this policy. No access control policies use this policy. Policy not applied on any devices	2019-12-30 02:14:24 Modified by "admin"

## Überprüfen der Standard-Netzwerkanalyse-richtlinie

Überprüfen Sie die standardmäßige Network Analysis (NAP)-Richtlinie, die auf die Zugriffskontrollrichtlinie (ACP) angewendet wird.

Navigieren Sie zu **Policies > Access Control (Richtlinien > Zugriffskontrolle)**, und bearbeiten Sie das zu überprüfende ACP. Klicken Sie auf die Registerkarte **Erweitert**, und führen Sie einen Bildlauf nach unten zum Abschnitt **Netzwerkanalyse und Zugriffsrichtlinien** durch.

Die dem ACP zugeordnete Standard-Netzwerkanalyse-richtlinie ist **Balanced Security and Connectivity (Ausgewogene Sicherheit und Konnektivität)**, wie im Bild gezeigt:

Overview Analysis **Policies** Devices Objects AMP Intelligence

Access Control ▶ Access Control Network Discovery Application Detectors Correlation Actions ▼

## Test

Enter Description

Prefilter Policy: [Default Prefilter Policy](#) SSL Policy: [None](#)

Rules Security Intelligence HTTP Responses Logging **Advanced**

### General Settings

Maximum URL characters to store in connection events 1024

Allow an Interactive Block to bypass blocking for (seconds) 600

Retry URL cache miss lookup Yes

**Network Analysis and Intrusion Policies** ? X

Intrusion Policy used before Access Control rule is determined

Intrusion Policy Variable Set  

Network Analysis Rules [No Custom Rules](#) [Network Analysis Policy List](#)

Default Network Analysis Policy

### Network Analysis and Intrusion Policies

Intrusion Policy used before Access Control rule is determined [Balanced Security and Connectivity](#)

Intrusion Policy Variable Set [Default Set](#)

Default Network Analysis Policy [Balanced Security and Connectivity](#)



**Hinweis:** Verwechseln Sie nicht die **Balanced Security and Connectivity** für **Intrusion Policies** und die **Balanced Security and Connectivity** for **Network Analysis**. Das erste ist für Snort-Regeln, das zweite für die Vorverarbeitung und Decodierung.

### Network Analysis Policy (NAP) vergleichen

Die NAP-Richtlinien können mit den vorgenommenen Änderungen verglichen werden. Diese Funktion könnte bei der Identifizierung und Behebung der Probleme helfen. Darüber hinaus können auch NAP-Vergleichsberichte erstellt und gleichzeitig exportiert werden.

Navigieren Sie zu **Richtlinien > Zugriffskontrolle > Zugriffskontrolle**. Klicken Sie dann oben rechts auf **Network Analysis Policy** (Netzwerkanalyserichtlinie). Auf der Seite für die NAP-Richtlinie sehen Sie oben rechts die Registerkarte **Compare Policies** (**Richtlinien vergleichen**), wie im Bild gezeigt:

Deploy ✔ System Help ▼ admin ▼

Object Management Access Control Intrusion

Compare Policies Create Policy

Last Modified		
2019-12-30 01:58:08	Modified by "admin"	  
2019-12-30 01:58:59	Modified by "admin"	  

Der Richtlinienvergleich für die Netzwerkanalyse ist in zwei Varianten verfügbar:

- Zwischen zwei verschiedenen NAP-Richtlinien
- Zwischen zwei verschiedenen Revisionen derselben NAP-Richtlinie

### Select Comparison ? ✕

Compare Against

Policy A NAP1one (2019-11-27 14:22:32 by admin) ▾

Policy B NAP1one (2019-11-27 14:22:32 by admin) ▾

✔ Other Policy

Other Revision

OK Cancel

Das Vergleichsfenster bietet einen Vergleich der einzelnen Zeilen zwischen zwei ausgewählten NAP-Richtlinien, der als Bericht über die Registerkarte **Vergleichsbericht** oben rechts exportiert werden kann, wie im Bild gezeigt:

Back Previous Next (Difference 1 of 114) Comparison Report New Comparison

Test1 (2019-12-30 02:13:49 by admin)	Test2 (2019-12-30 02:14:24 by admin)
<b>Policy Information</b>	
Name: Test1	Name: Test2
Modified: 2019-12-30 02:13:49 by admin	Modified: 2019-12-30 02:14:24 by admin
Base Policy: Connectivity Over Security	Base Policy: Maximum Detection
<b>Settings</b>	
<b>Checksum Verification</b>	
ICMP Checksums: Enabled	ICMP Checksums: Disabled
IP Checksums: Enabled	IP Checksums: Drop and Generate Events
TCP Checksums: Enabled	TCP Checksums: Drop and Generate Events
UDP Checksums: Enabled	UDP Checksums: Disabled
<b>DCE/RPC Configuration</b>	
<b>Servers</b>	
default	
SMB Maximum AndX Chain: 3	SMB Maximum AndX Chain: 5
RPC over HTTP Server Auto-Detect Ports: Disabled	RPC over HTTP Server Auto-Detect Ports: 1024-65535
TCP Auto-Detect Ports: Disabled	TCP Auto-Detect Ports: 1024-65535
UDP Auto-Detect Ports: Disabled	UDP Auto-Detect Ports: 1024-65535
SMB File Inspection Depth: 16384	SMB File Inspection Depth: 16384
<b>Packet Decoding</b>	
Detect Invalid IP Options: Disable	Detect Invalid IP Options: Enable
Detect Obsolete TCP Options: Disable	Detect Obsolete TCP Options: Enable
Detect Other TCP Options: Disable	Detect Other TCP Options: Enable
Detect Protocol Header Anomalies: Disable	Detect Protocol Header Anomalies: Enable
<b>DNS Configuration</b>	
Detect Obsolete DNS RR Types: No	Detect Obsolete DNS RR Types: Yes
Detect Experimental DNS RR Types: No	Detect Experimental DNS RR Types: Yes
<b>FTP and Telnet Configuration</b>	
<b>FTP Server</b>	
default	

Zum Vergleich zwischen zwei Versionen derselben NAP-Richtlinie kann die Revisionsoption gewählt werden, um die erforderliche **Revisionsnummer** auszuwählen, wie im Bild gezeigt:

## Select Comparison ? X

Compare Against	Other Revision <span style="float: right;">⌵</span>
Policy	Test1 (2019-12-30 02:13:49 by admin) <span style="float: right;">⌵</span>
Revision A	2019-12-30 02:13:49 by admin <span style="float: right;">⌵</span>
Revision B	2019-12-30 01:58:08 by admin <span style="float: right;">⌵</span>

OK
Cancel

Back

Previous Next (Difference 1 of 13)

Comparison Report New Comparison

Test1 (2019-12-30 02:13:49 by admin)	
<b>Policy Information</b>	
Modified	2019-12-30 02:13:49 by admin
Base Policy	Connectivity Over Security
<b>Settings</b>	
CSP Configuration Disabled	
DCE/RPC Configuration	
Servers	
default	
RPC over HTTP Server Auto-Detect Ports	Disabled
TCP Auto-Detect Ports	Disabled
UDP Auto-Detect Ports	Disabled
HTTP Configuration	
Servers	
default	
Ports	80, 443, 1220, 1741, 2301, 3
Server Flow Depth	300
SSL Configuration	
Ports	443, 465, 563, 636, 989, 992
TCP Stream Configuration	
Servers	
default	
Perform Stream Reassembly on Client Ports	21, 23, 25, 42, 53, 80, 135, 1
Perform Stream Reassembly on Client Services	CYS, DCE/RPC, DNS, , HTTP,
Perform Stream Reassembly on Both Ports	5000, 9800, 9111

Test1 (2019-12-30 01:58:08 by admin)	
<b>Policy Information</b>	
Modified	2019-12-30 01:58:08 by admin
Base Policy	Balanced Security and Connec
<b>Settings</b>	
DCE/RPC Configuration	
Servers	
default	
RPC over HTTP Server Auto-Detect Ports	1024-65535
TCP Auto-Detect Ports	1024-65535
UDP Auto-Detect Ports	1024-65535
HTTP Configuration	
Servers	
default	
Ports	80, 443, 1220, 1741, 2301, 2
Server Flow Depth	500
SSL Configuration	
Ports	443, 465, 563, 636, 989, 992
TCP Stream Configuration	
Servers	
default	
Perform Stream Reassembly on Client Ports	21, 23, 25, 42, 53, 135, 136,
Perform Stream Reassembly on Client Services	CYS, DCE/RPC, DNS, , IMAP,
Perform Stream Reassembly on Both Ports	80, 443, 465, 636, 992, 993,
Perform Stream Reassembly on Both Services	HTTP