

# NAP-beleid op FirePOWER-apparaten vergelijken

## Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Achtergrondinformatie](#)

[Controleer NAP-configuratie](#)

### Inleiding

Dit document beschrijft hoe u verschillende beleid voor netwerkanalyse (NAP) kunt vergelijken voor vuurstroomapparaten die worden beheerd door FireSIGHT Management Center (FMC).

### Voorwaarden

### Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Kennis van opensource-ort
- FireSIGHT Management Center (FMC)
- Firepower Threat Defense (FTD)

### Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Dit artikel is van toepassing op alle FirePOWER-platforms
- Cisco Firepower Threat Defense (FTD) die softwareversie 6.4.0 uitvoert
- Firepower Management Center Virtual (FMC), die softwareversie 6.4.0 uitvoert

### Achtergrondinformatie

De Snort gebruikt patroon matching technieken om explosies in netwerkpakketten te vinden en te voorkomen. Om dit te doen, moet de snijmotor netwerkpakketten zodanig worden voorbereid dat deze vergelijking mogelijk is. Dit proces wordt uitgevoerd met behulp van het NAP en kan de volgende drie fasen ondergaan:

- decoderen
- Normaliseren
- Voorbehandeling

Een beleid voor netwerkanalyse verwerkt pakketten in fasen: Eerst decodeert het systeem pakketten door de eerste drie TCP/IP lagen, dan gaat hij door met het normaliseren, pre-Processing en het detecteren van protocol anomalieën.

Pre-processoren leveren twee hoofdfuncties:

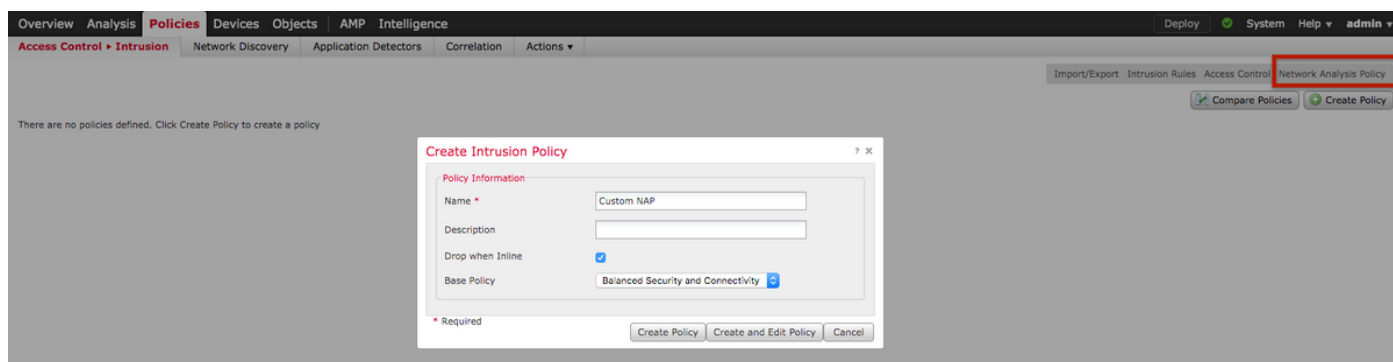
- Verkeersnormalisatie voor verdere inspectie
- Protocolanomalieën identificeren

**Opmerking:** Sommige inbraakbeleidsregels vereisen bepaalde opties van voorprocessors om de detectie uit te voeren

Kijk voor informatie over opensource <https://www.snort.org/>

## Controleer NAP-configuratie

Als u beleid voor firepower NAP wilt maken of bewerken, navigeer dan naar **FMC Policy > Access Control > Inbraaklegging**, klik vervolgens op **Network Analysis Policy** in de rechterbovenhoek, zoals in de afbeelding wordt getoond:



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"

## Het beleid voor netwerkanalyse controleren

Controleer het standaard Network Analysis (NAP) beleid dat van toepassing is op het Access Control Policy (ACS)  
 Navigeer naar **beleid > Toegangsbeheer** en bewerk de ACS die u wilt controleren. Klik op **het** tabblad **Geavanceerd** en ga naar het gedeelte **Netwerkanalyse en inbraakbeleid**.

Het standaardbeleid voor netwerkanalyse dat bij de ACS-landen hoort, is **gebalanceerde beveiliging en connectiviteit**, zoals in de afbeelding wordt getoond:

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**

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](#)

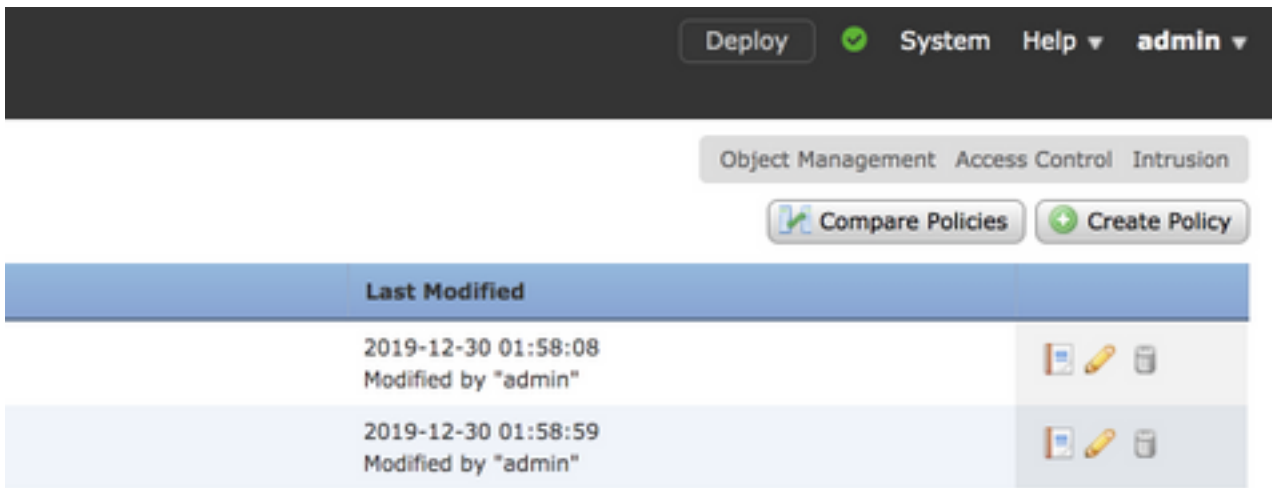
Default Network Analysis Policy [Balanced Security and Connectivity](#)

Opmerking: Verwar de **gebalanceerde beveiliging en connectiviteit** niet voor **inbraakbeleid** en de **gebalanceerde beveiliging en connectiviteit** voor **netwerkanalyse**. De eerste is voor de regels van de Snort, terwijl de tweede voor de voorbewerking en decodering.

### Network Analysis Policy (NAP) vergelijken

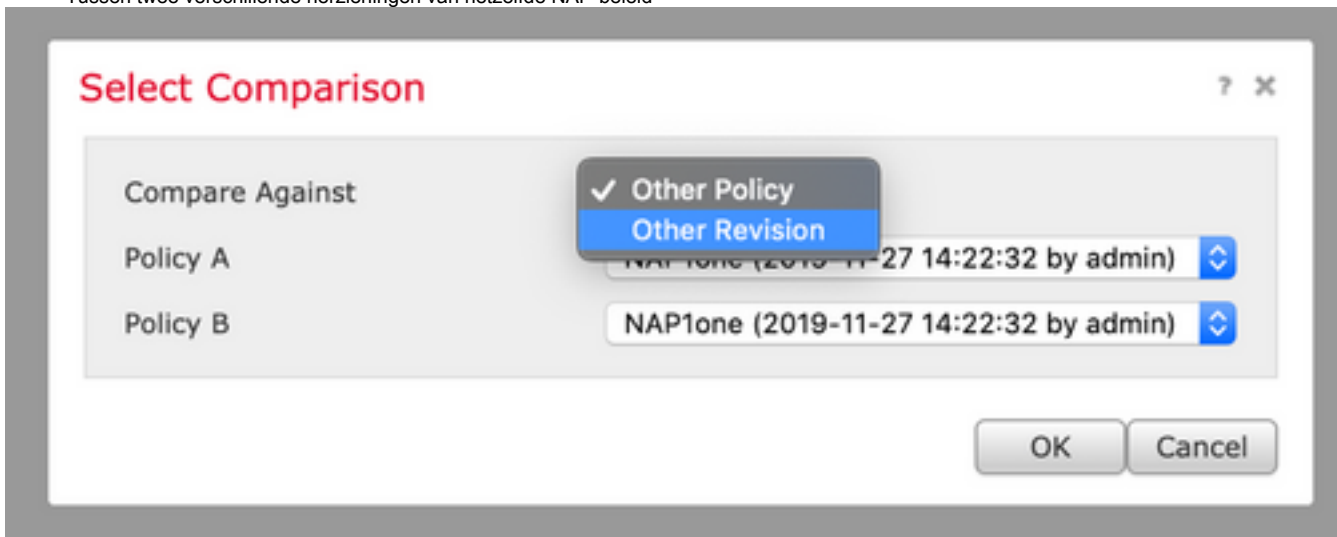
Het NAP-beleid kan voor uitgevoerde veranderingen worden vergeleken en deze optie kan helpen bij het identificeren en oplossen van problemen. Daarnaast zouden ook vergelijkende verslagen van de NAP's tegelijk kunnen worden gegenereerd en geëxporteerd.

Navigeren in op **beleid > Toegangsbeheer > Inbraakcontrole**. Klik vervolgens rechtsboven op de optie **Network Analysis Policy**. Onder de pagina NAP-beleid kunt u het tabblad **Beleid vergelijken** aan de rechterbovenzijde, zoals in de afbeelding wordt getoond:



De vergelijking van het beleid van de netwerkanalyse is beschikbaar in twee varianten:

- Tussen twee verschillende NAP-beleidsmaatregelen
- Tussen twee verschillende herzieningen van hetzelfde NAP-beleid



Het vergelijkingsvenster biedt een vergelijkende lijn per lijn vergelijking tussen twee geselecteerde NAP beleid en het zelfde kan als een rapport van het tabblad van het vergelijkingsrapport in de bovenkant rechts worden geëxporteerd, zoals in de afbeelding:

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>			
Checksum Verification			
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
DCE/RPC Configuration			
Servers			
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	
Packet Decoding			
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
DNS Configuration			
Detect Obsolete DNS RR Types	No	Detect Obsolete DNS RR Types	Yes
Detect Experimental DNS RR Types	No	Detect Experimental DNS RR Types	Yes
FTP and Telnet Configuration			
FTP Server			
default			

Ter vergelijking tussen twee versies van hetzelfde NAP-beleid kan de optie voor de herziening worden gekozen om de vereiste **herziening id** te selecteren, zoals in de afbeelding wordt getoond:

## 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	
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