

# How To Compare NAP Policies on Firepower Devices

## Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Components Used](#)

[Background Information](#)

[Verify NAP Configuration](#)

### Introduction

This document describes how to compare different Network Analysis Policies (NAP) for firepower devices managed by Firepower Management Centre (FMC).

### Prerequisites

## Requirements

Cisco recommends that you have knowledge of these topics:

- Knowledge of open-source Snort
- Firepower Management Center (FMC)
- Firepower Threat Defense (FTD)

## Components Used

The information in this document is based on these software and hardware versions:

- This article is applicable to all Firepower platforms
- Cisco Firepower Threat Defense (FTD) which runs software version 6.4.0
- Firepower Management Center Virtual (FMC) which runs software version 6.4.0

## Background Information

The Snort uses pattern matching techniques to find and prevent exploits in network packets. In order to do this, the Snort engine needs network packets to be prepared in such a way that this comparison can be done. This process is done with the help of NAP and can undergo the following three stages:

- Decoding
- Normalizing
- Pre-processing

A network analysis policy processes packet in phases: first the system decodes packets through the first three TCP/IP layers, then continues with normalizing, pre-processing, and detecting protocol anomalies.

Pre-processors provide two main functionality:

- Traffic Normalization for further inspection

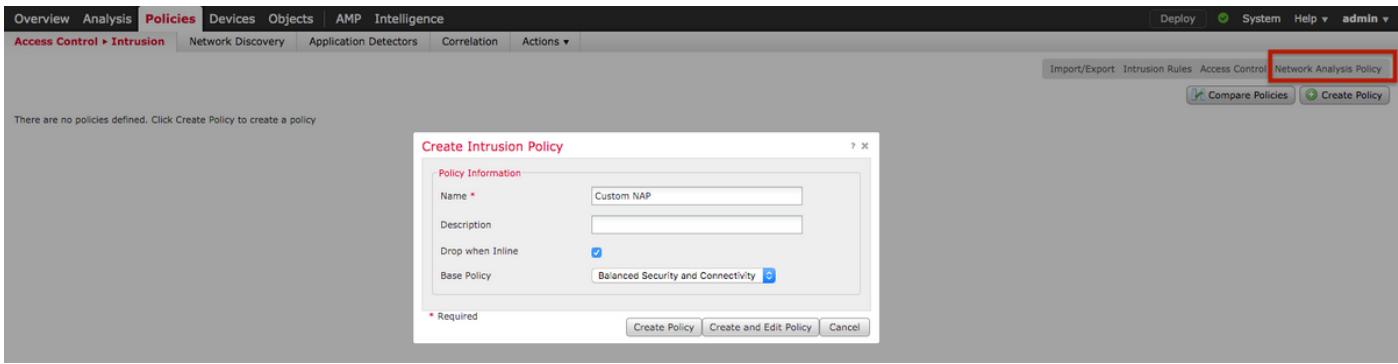
- Identify protocol anomalies

**Note:** Some Intrusion Policy rules require certain pre-processor options in order to perform detection

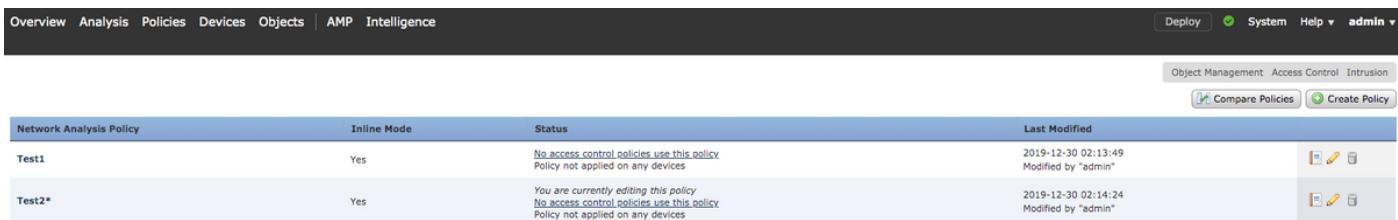
For information on open-source Snort, please visit <https://www.snort.org/>

## Verify NAP Configuration

To create or edit firepower NAP policies, navigate to **FMC Policies > Access Control > Intrusion**, thereafter click **Network Analysis Policy** option in the top right corner, as shown in the image:



The screenshot shows the FMC navigation bar with 'Policies' selected. In the main content area, there is a message: 'There are no policies defined. Click Create Policy to create a policy.' A modal window titled 'Create Intrusion Policy' is open, showing fields for 'Name' (set to 'Custom NAP'), 'Description' (empty), 'Drop when Inline' (checkbox checked), and 'Base Policy' (set to 'Balanced Security and Connectivity'). At the bottom of the modal are buttons for 'Create Policy', 'Create and Edit Policy', and 'Cancel'.

The screenshot shows the FMC navigation bar with 'Policies' selected. The main content area displays a table of 'Network Analysis Policy' entries. The table has columns: 'Network Analysis Policy', 'Inline Mode', 'Status', and 'Last Modified'. Two rows are visible: 'Test1' (Yes, 'No access control policies use this policy. Policy not applied on any devices.', 2019-12-30 02:13:49) and '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). Each row has edit and delete icons in the last column.

## Verifying the default Network Analysis Policy

Check the default Network Analysis (NAP) policy applied on the Access Control Policy (ACP)

Navigate to **Policies > Access Control** and edit the ACP that you want to verify. Click **Advanced** tab and scroll down to **Network Analysis and Intrusion Policies** section.

The Default Network Analysis Policy associated with the ACP is **Balanced Security and Connectivity**, as shown in the image:

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

Inspect traffic for policy enforcement

#### Network Analysis and Intrusion Policies

Intrusion Policy used before Access Control rule is determined	Balanced Security and Connectivity
Intrusion Policy Variable Set	Default-Set
Network Analysis Rules	No Custom Rules <a href="#">Network Analysis Policy List</a>
Default Network Analysis Policy	Balanced Security and Connectivity

[Revert to Defaults](#) [OK](#) [Cancel](#)

### 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

Note: Do not confuse the **Balanced Security and Connectivity** for **Intrusion Policies** and the **Balanced Security and Connectivity** for **Network Analysis**. The former one is for Snort rules while the latter is for pre-processing and decoding.

### Compare Network Analysis Policy (NAP)

The NAP policies can be compared for changes done and this feature could help in identifying and troubleshooting the issues. In addition, NAP comparison reports could also be generated and exported at the same time.

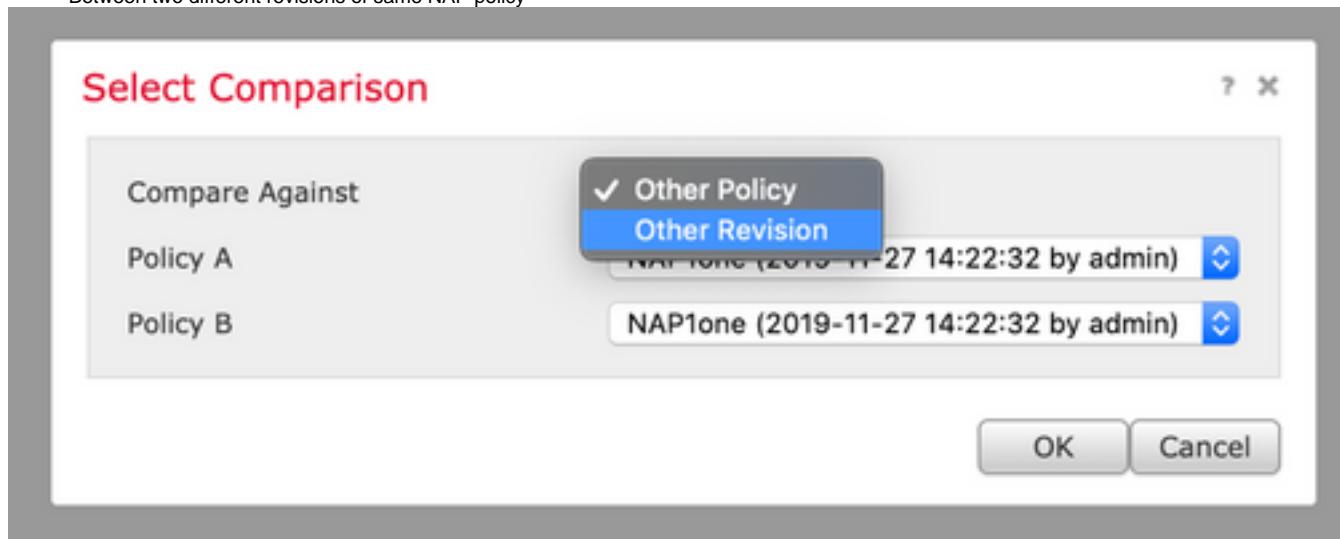
Navigate to **Policies > Access Control > Intrusion**. Then, click **Network Analysis Policy** option in the top right. Under the NAP policy page you can see **Compare Policies** tab on the top right side, as shown in the image:



Last Modified	Policy Name	Actions
2019-12-30 01:58:08 Modified by "admin"	NAP1one (2019-12-27 14:22:32 by admin)	
2019-12-30 01:58:59 Modified by "admin"	NAP1one (2019-11-27 14:22:32 by admin)	

Network Analysis Policy comparison is available in two variants:

- Between two different NAP policies
- Between two different revisions of same NAP policy



The comparison window provides a comparative line by line comparison between two selected NAP policies and the same can be exported as a report from the **comparison report** tab on the top right, as shown in the image:

Back ▲ Previous ▼ Next [Difference 1 of 114]

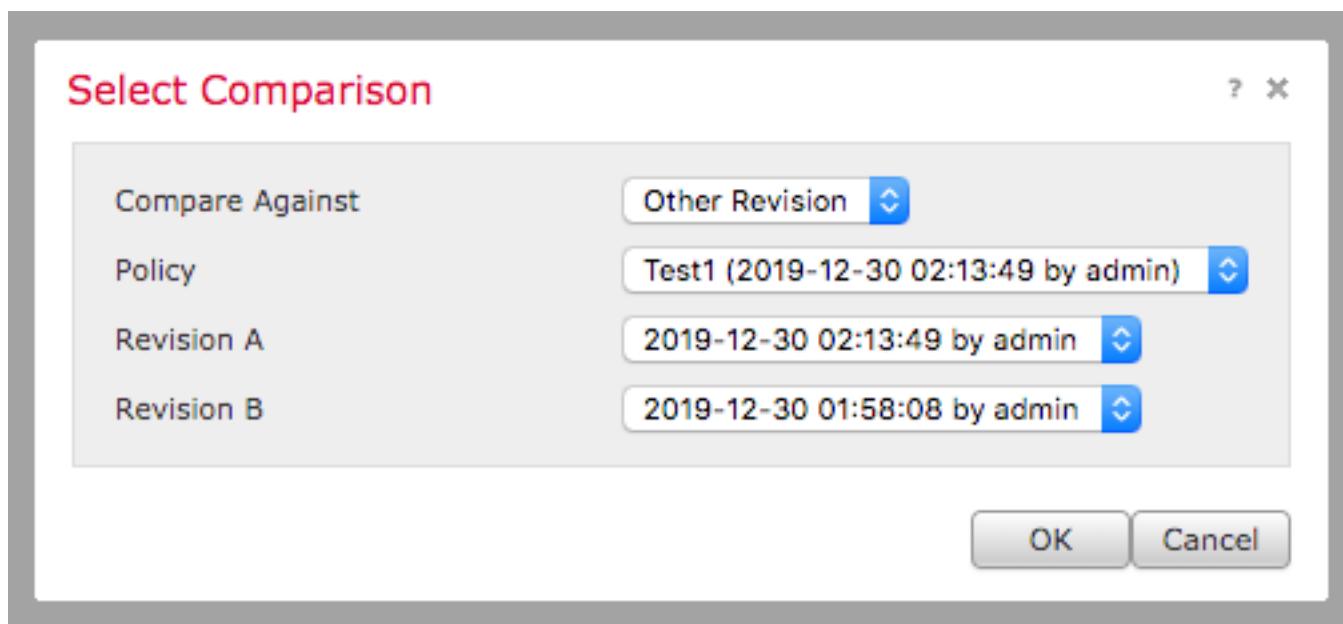
**Test1 (2019-12-30 02:13:49 by admin)**

Policy Information	
Name	Test1
Modified	2019-12-30 02:13:49 by admin
Base Policy	Connectivity Over Security
Settings	
Checksum Verification	
ICMP Checksums	Enabled
IP Checksums	Enabled
TCP Checksums	Enabled
UDP Checksums	Enabled
DCE/NPC Configurations	
Servers	default
SMB Maximum AndX Chain	3
RPC over HTTP Server Auto-Detect Ports	Disabled
TCP Auto-Detect Ports	Disabled
UDP Auto-Detect Ports	Disabled
SMB File Inspection Depth	15364
Packet Decoding	
Detect Invalid IP Options	Disable
Detect Obsolete TCP Options	Disable
Detect Other TCP Options	Disable
Detect Protocol Header Anomalies	Disable
DNS Configuration	
Detect Obsolete DNS RR Types	No
Detect Experimental DNS RR Types	No
FTP and Telnet Configuration	
FTP Server	default

**Test2 (2019-12-30 02:14:24 by admin)**

Policy Information	
Name	Test2
Modified	2019-12-30 02:14:24 by admin
Base Policy	Maximum Detection
Settings	
Checksum Verification	
ICMP Checksums	Disabled
IP Checksums	Drop and Generate Events
TCP Checksums	Drop and Generate Events
UDP Checksums	Disabled
DCE/NPC Configurations	
Servers	default
SMB Maximum AndX Chain	5
RPC over HTTP Server Auto-Detect Ports	1024-65535
TCP Auto-Detect Ports	1024-65535
UDP Auto-Detect Ports	1024-65535
SMB File Inspection Depth	
Packet Decoding	
Detect Invalid IP Options	Enable
Detect Obsolete TCP Options	Enable
Detect Other TCP Options	Enable
Detect Protocol Header Anomalies	Enable
DNS Configuration	
Detect Obsolete DNS RR Types	Yes
Detect Experimental DNS RR Types	Yes
FTP and Telnet Configuration	
FTP Server	default

For comparison between two versions of the same NAP policy, the revision option can be opted to select the required **revision id**, as shown in the image:



[Back](#)[Previous](#) ▾ [Next](#) (Difference 1 of 13)**Test1 (2019-12-30 02:13:49 by admin)****Policy Information**

Modified	2019-12-30 02:13:49 by admin
Base Policy	Connectivity Over Security

**Settings****CIP 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 Row 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

CVS, DCE/RPC, DNS, , HTTP,

Perform Stream Reassembly on Both Ports

5000, 8800, 9111

[Comparison Report](#) [New Comparison](#)**Test1 (2019-12-30 01:58:08 by admin)****Policy Information**

Modified	2019-12-30 01:58:08 by admin
Base Policy	Balanced Security and Control

**Settings****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 Row 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

CVS, DCE/RPC, DNS, , IMAP,

Perform Stream Reassembly on Both Ports

80, 443, 465, 636, 989, 993,

Perform Stream Reassembly on Both Services

HTTP