

How to Compare NAP Policies on Firepower Devices

Contents

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 was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command. 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 these 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

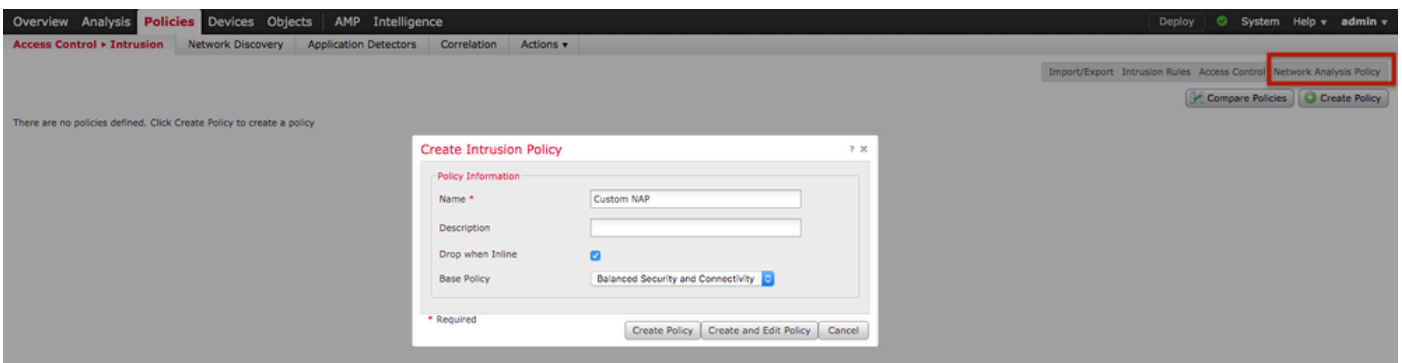


Note: Some Intrusion Policy rules require certain pre-processor options in order to perform detection

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:



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"

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

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](#) [Network Analysis Policy List](#)

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)

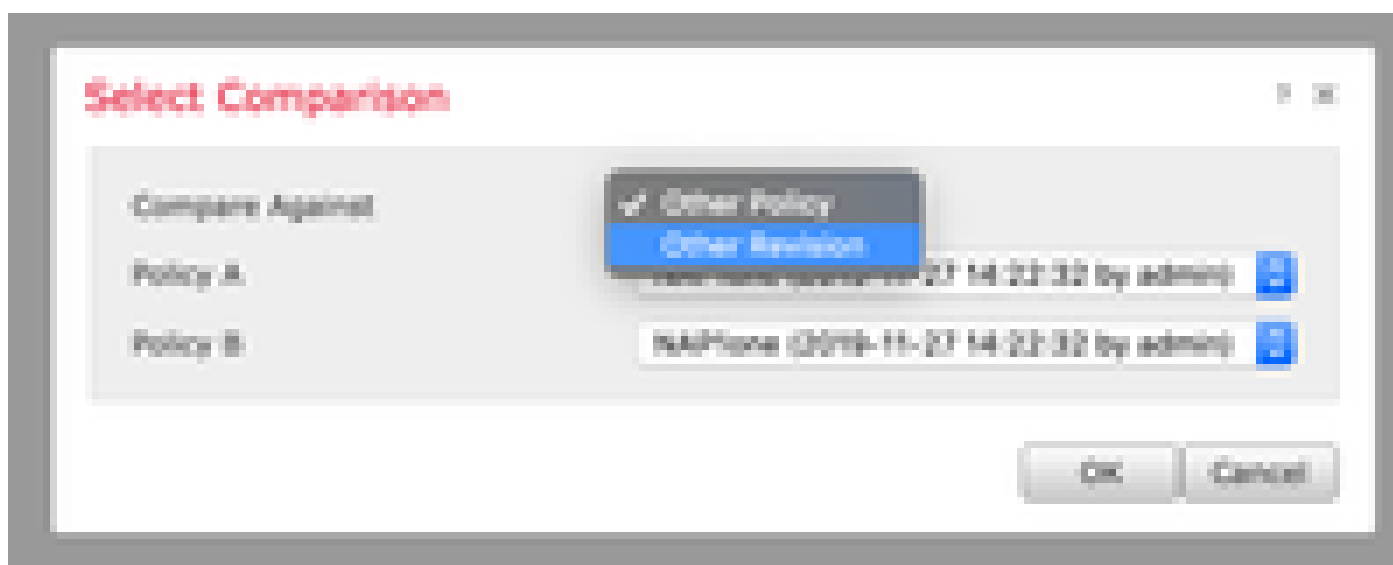
The NAP policies can be compared for changes done and this feature could help in identifying and troubleshooting the issues. In addition, NAP comparison reports could also be generated and exported at the same time.

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

Network Analysis Policy comparison is available in two variants:

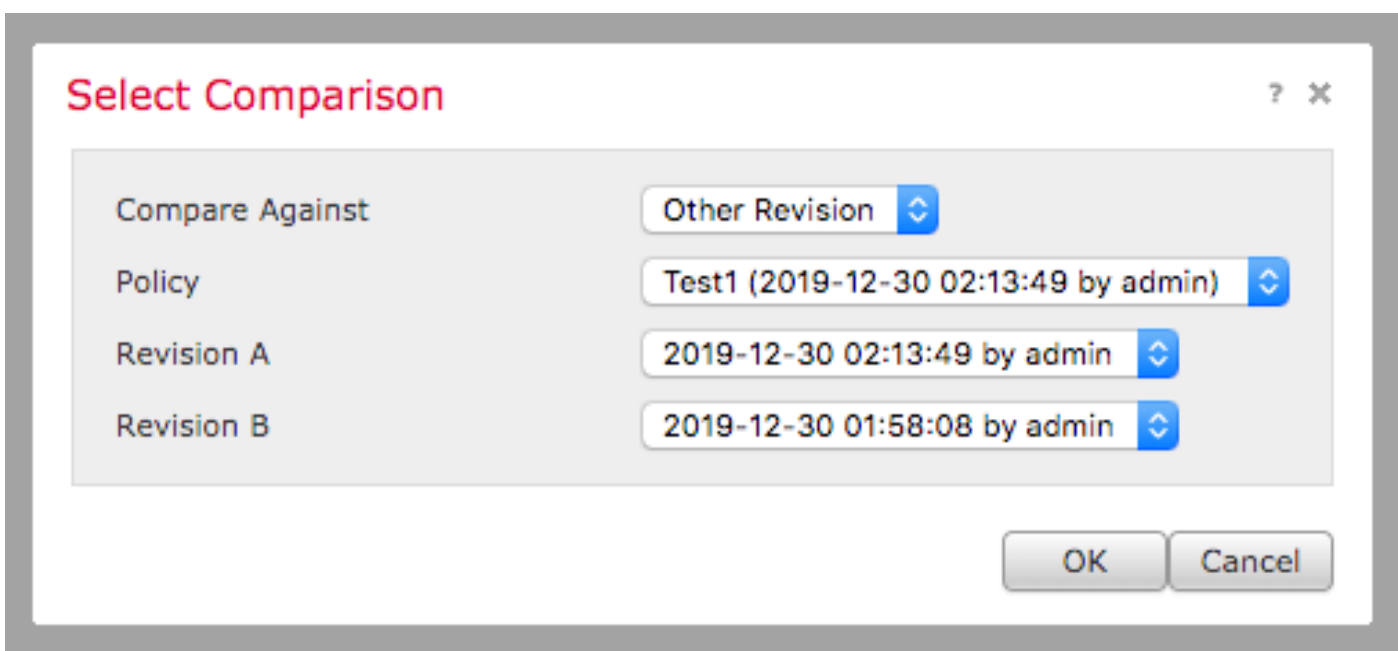
- Between two different NAP policies
- Between two different revisions of same NAP policy



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:



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

Home Host (Difference 1 of 1)

Compare Hosts New Comparison

Host1 (2018-12-01 00:00:00 by admin)	
Policy Information	
Hostid	2018-12-01 00:00:00 by admin
Base Policy	Connectivity Over Security
Settings	
OSPF Configuration	
OSPF Configuration	
Network	
Default	
BFD over OSPF Server Auto Detect Ports	Enabled
TCP Auto Detect Ports	Enabled
UDP Auto Detect Ports	Enabled
OSPF Configuration	
Network	
Default	
Ports	80, 443, 1521, 1741, 2000, 8
Service Flow Depth	300
OSPF Configuration	
Ports	
Ports	803, 805, 806, 808, 809, 810
OSPF Neighbor Configuration	
Network	
Default	
Neighbor Stream Residency on Client Ports	20, 25, 35, 40, 55, 60, 120, 1
Neighbor Stream Residency on Client Services	0x0, 0x0000, 0x00, ... 0x70
Neighbor Stream Residency on Server Ports	0x00, 0x00, 0x00

Host2 (2018-12-01 00:00:00 by admin)	
Policy Information	
Hostid	2018-12-01 00:00:00 by admin
Base Policy	Enhanced Security and Control
Settings	
OSPF Configuration	
OSPF Configuration	
Network	
Default	
BFD over OSPF Server Auto Detect Ports	Enabled 0x0000
TCP Auto Detect Ports	Enabled 0x0000
UDP Auto Detect Ports	Enabled 0x0000
OSPF Configuration	
Network	
Default	
Ports	80, 443, 1521, 1741, 2000, 8
Service Flow Depth	300
OSPF Configuration	
Ports	
Ports	803, 805, 806, 808, 809, 810
OSPF Neighbor Configuration	
Network	
Default	
Neighbor Stream Residency on Client Ports	20, 25, 35, 40, 55, 120, 120
Neighbor Stream Residency on Client Services	0x0, 0x0000, 0x00, ... 0x00
Neighbor Stream Residency on Server Ports	80, 403, 403, 424, 403, 403
Neighbor Stream Residency on Server Services	0x00