

# 如何比較Firepower裝置上的NAP策略

## 目錄

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[背景資訊](#)

[驗證NAP配置](#)

## 簡介

本文檔介紹如何比較由Firepower管理中心(FMC)管理的firepower裝置的不同網路分析策略(NAP)。

## 必要條件

## 需求

思科建議您瞭解以下主題：

- 開源Snort知識
- Firepower Management Center (FMC)
- Firepower Threat Defense (FTD)

## 採用元件

本文中的資訊係根據以下軟體和硬體版本：

- 本文適用於所有Firepower平台
- 執行6.4.0版軟體的Cisco Firepower威脅防禦(FTD)
- Firepower管理中心虛擬(FMC)，運行軟體版本6.4.0

## 背景資訊

Snort使用模式匹配技術來查詢和防止網路資料包中的漏洞。為此，Snort引擎需要準備可以完成比較的網路資料包。這一過程是在國家行動方案的幫助下完成的，可以經歷以下三個階段：

- 解碼
- 規範化
- 預處理

網路分析策略分階段處理資料包：首先，系統通過前三個TCP/IP層對資料包進行解碼，然後繼續規範化、預處理以及檢測協定異常。

前處理器提供兩個主要功能：

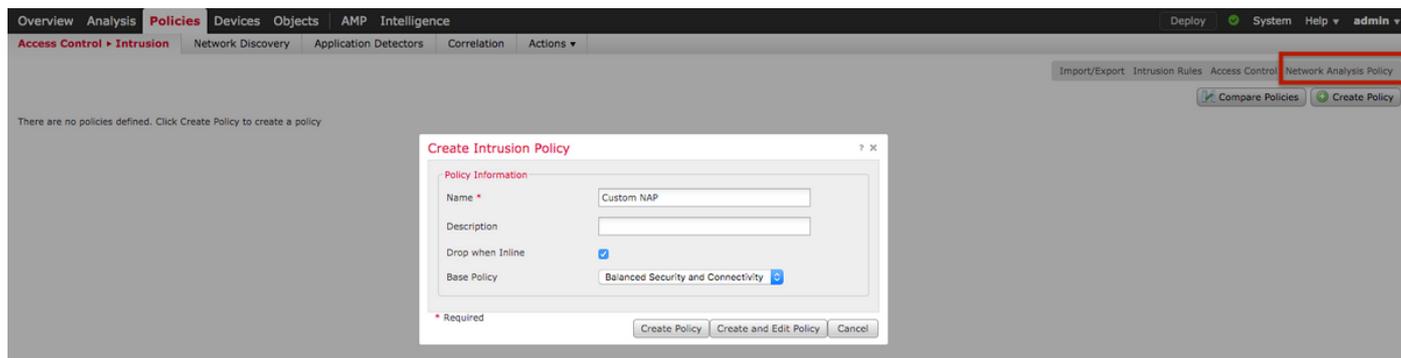
- 用於進一步檢測的流量規範化
- 確定協定異常

：

有關開源Snort的資訊，請訪問 <https://www.snort.org/>

## 驗證NAP配置

要建立或編輯firepower NAP策略，請導航到**FMC Policies > Access Control > Intrusion**，然後按一下右上角的**Network Analysis Policy** 選項，如下圖所示：



The screenshot shows the Cisco FMC interface with the 'Policies' tab selected. The 'Access Control > Intrusion' sub-tab is active. A table of Network Analysis Policies is displayed:

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"

(ACP)(NAP)

**Policies > Access Control** ACP Advanced Network Analysis and Intrusion Policies

ACP Balanced Security and Connectivity:

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](#)

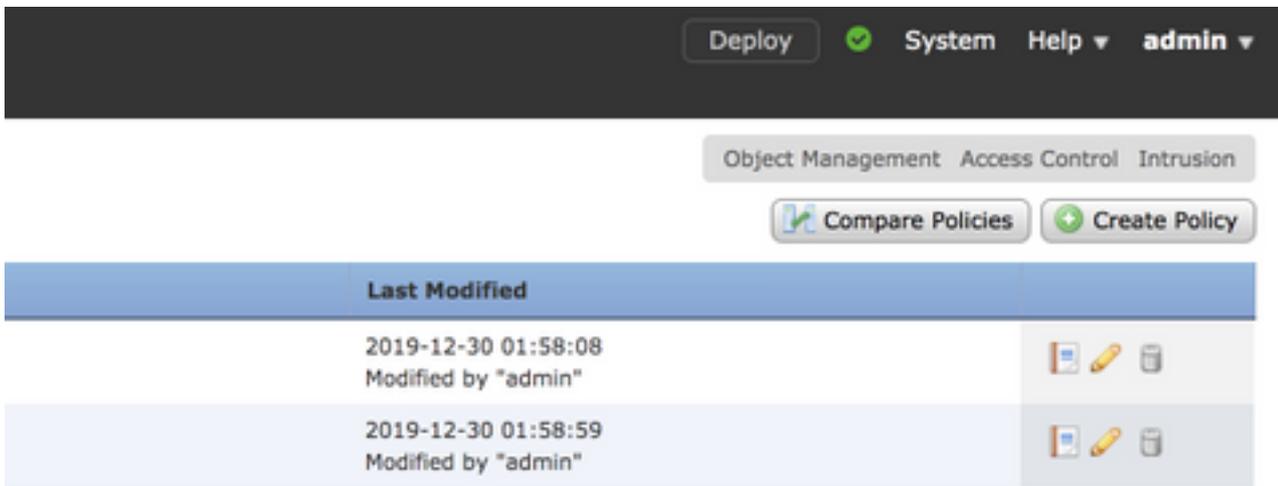
Default Network Analysis Policy [Balanced Security and Connectivity](#)

Balanced Security and Connectivity for Intrusion Policies  
Balanced Security and Connectivity for Network Analysis

### 比較網路分析策略(NAP)

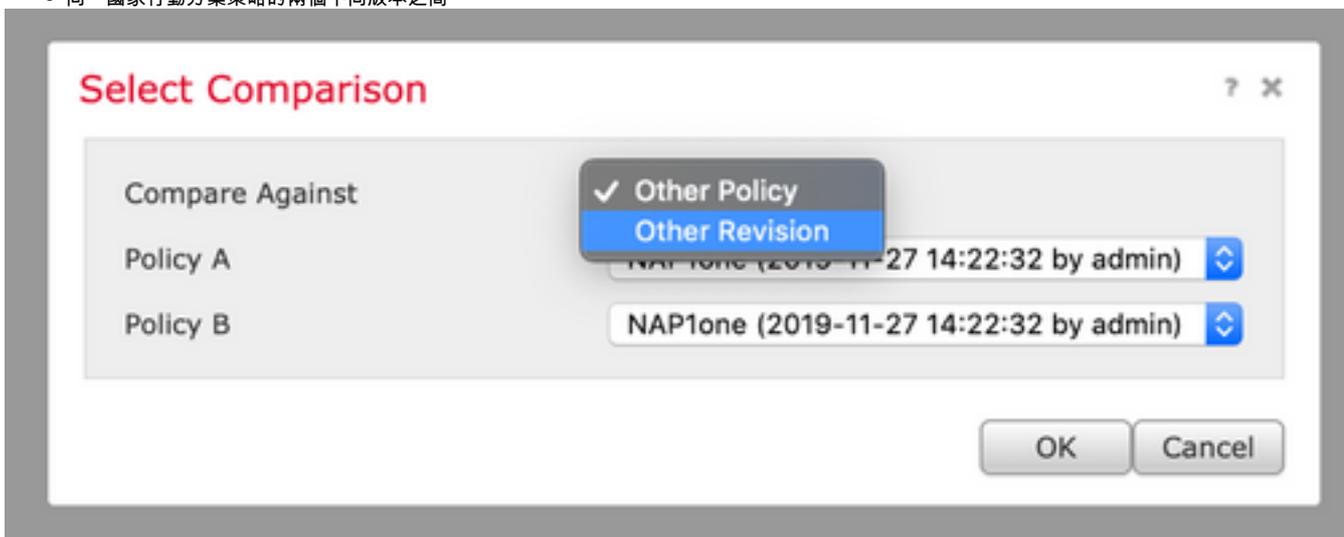
可以比較NAP策略所做的更改，並且此功能可以幫助確定和排除問題。此外，還可同時生成和匯出國家適應計畫比較報告。

導航到Policies > Access Control > Intrusion。然後，按一下右上角的Network Analysis Policy選項。在NAP策略頁面下，您可以看到右上方的Compare Policies頁籤，如下圖所示：



網路分析策略比較有兩種版本：

- 兩個不同的NAP策略之間
- 同一國家行動方案策略的兩個不同版本之間



比較視窗提供兩個選定的NAP策略之間的逐行比較，並且可以從右上角的「比較報告」頁籤將比較結果匯出為報告，如下圖所示：

Back Comparison Report New Comparison

Previous Next (Difference 1 of 114)

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:
<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	

對於同一NAP策略的兩個版本之間的比較，可以選擇修訂選項來選擇所需的修訂ID，如下圖所示：

## 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