如何比較Firepower裝置上的NAP策略

目錄

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：

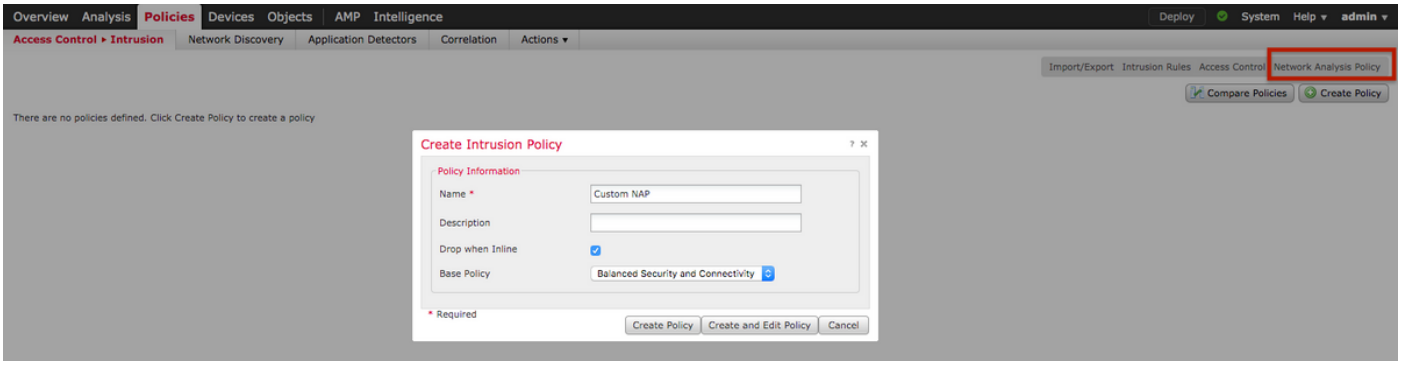
- 用於進一步檢測的流量規範化
- 確定協定異常

：

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

驗證NAP配置

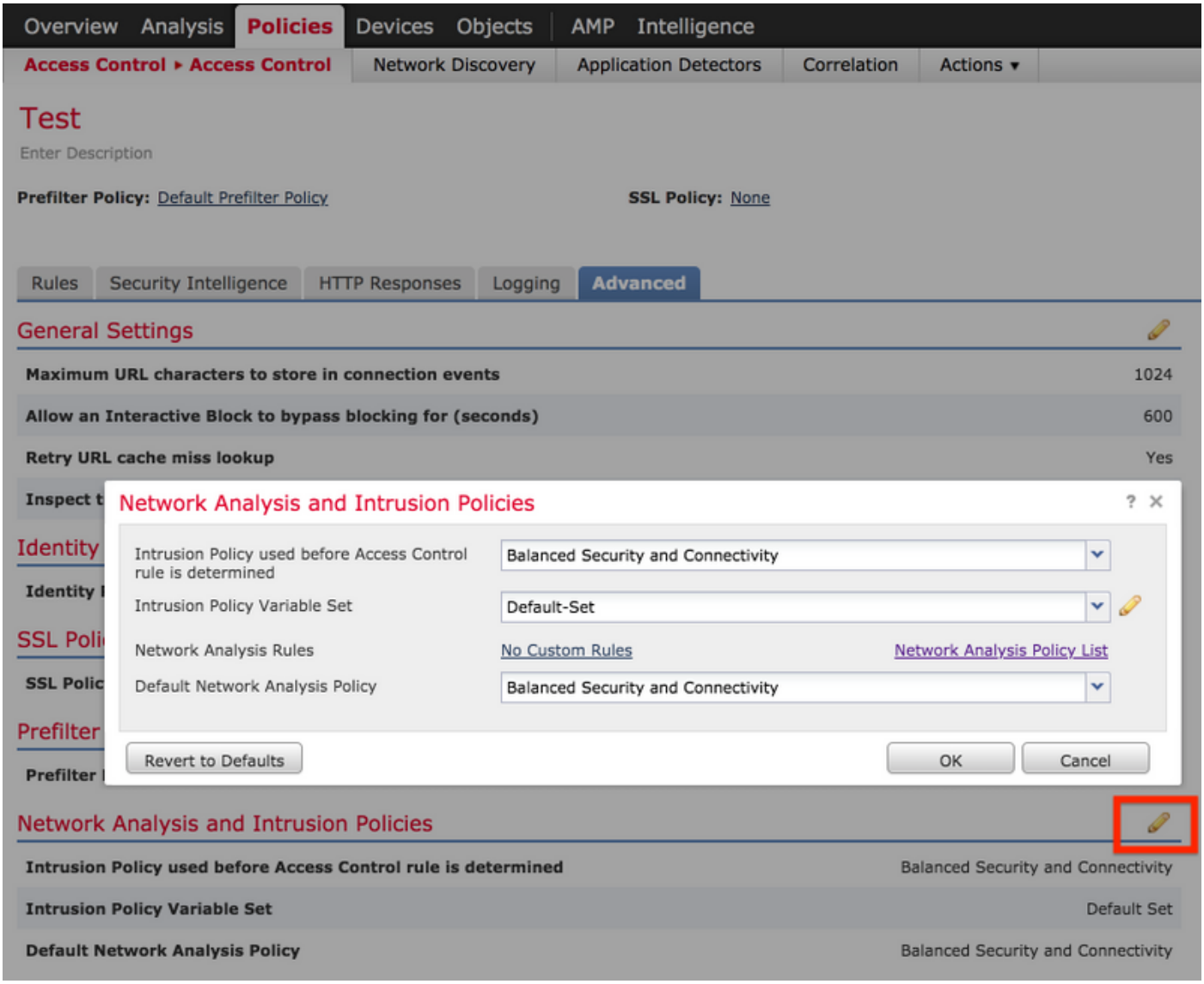
要建立或編輯firepower NAP策略，請導航到**FMC Policies > Access Control > Intrusion，然**後按一下右上角的**Network Analysis Policy** 選項，如下圖所示：



(ACP)(NAP)

Policies > Access ControlACP**Advanced Network Analysis and Intrusion Policies**

ACP**Balanced Security and Connectivity:**

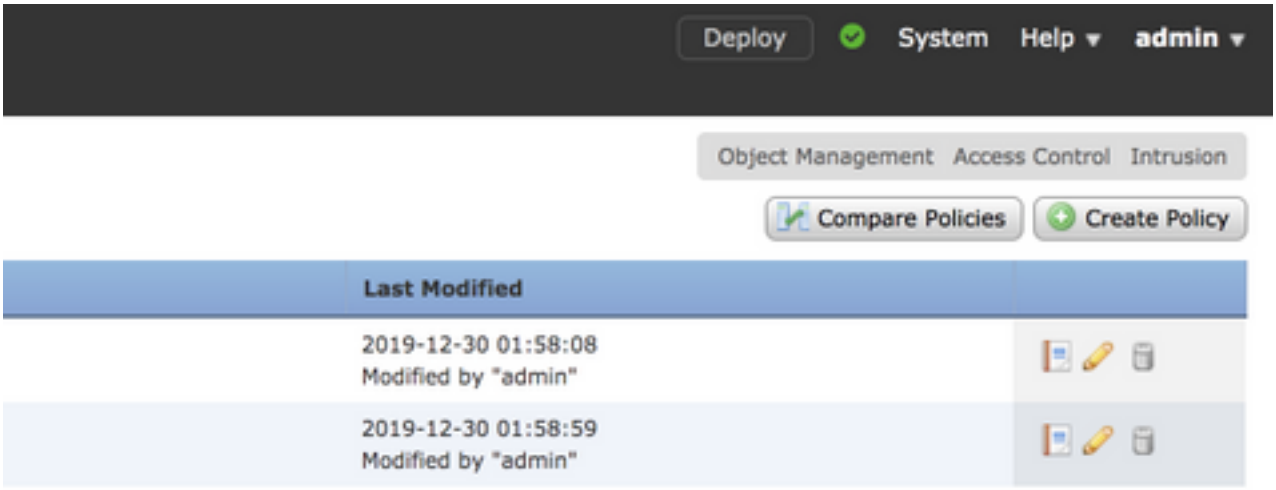


Balanced Security and Connectivity for Intrusion Policies Balanced Security and Connectivity for **Network Analysis**Snort

比較網路分析策略(NAP)

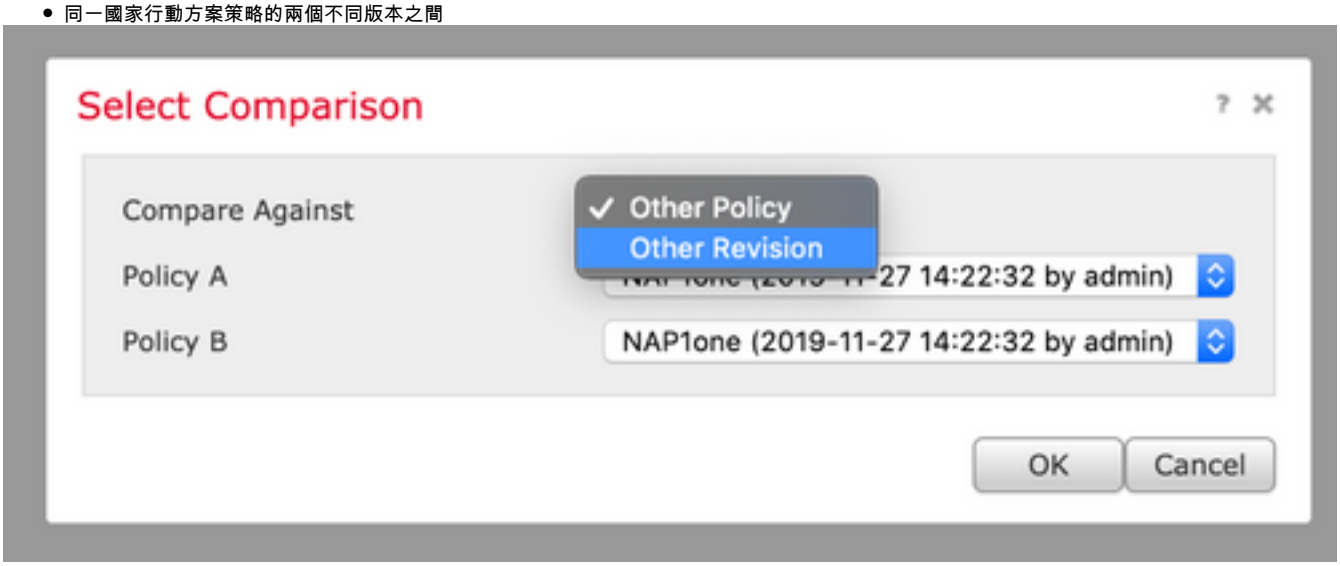
可以比較NAP策略所做的更改，並且此功能可以幫助確定和排除問題。此外，還可同時生成和匯出國家適應計畫比較報告。

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：

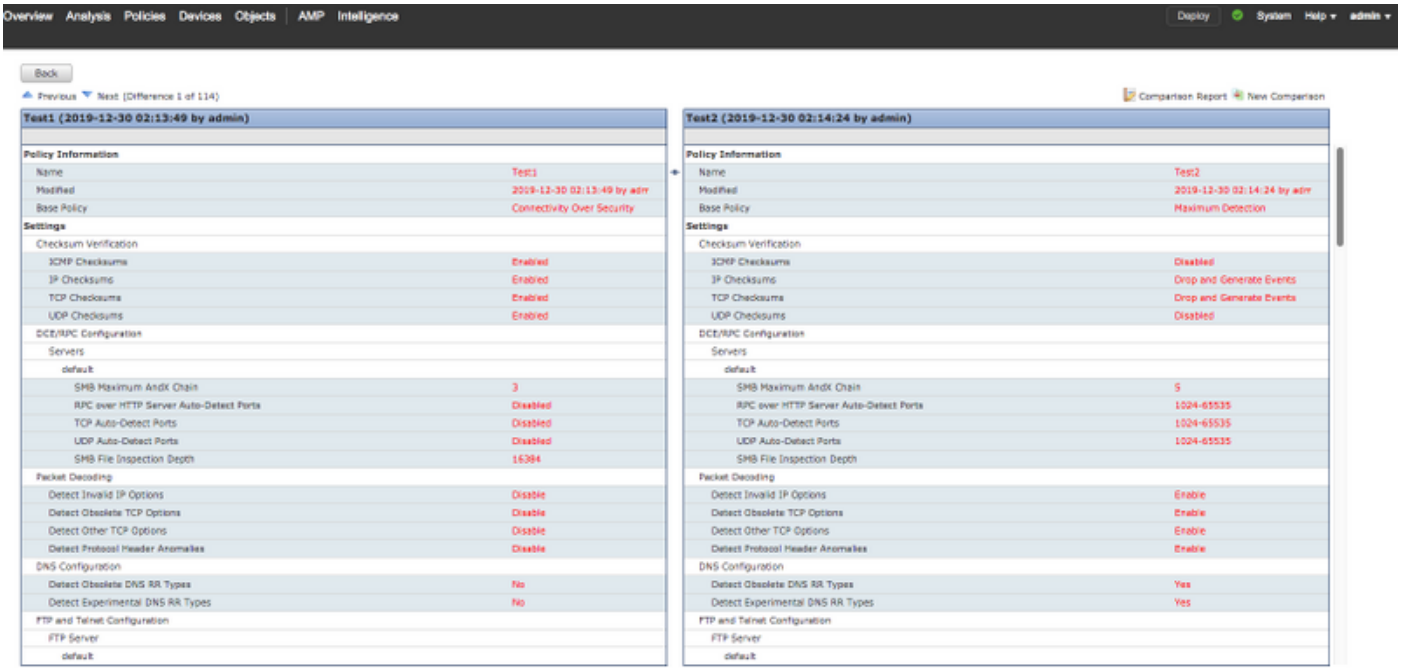


網路分析策略比較有兩種版本：

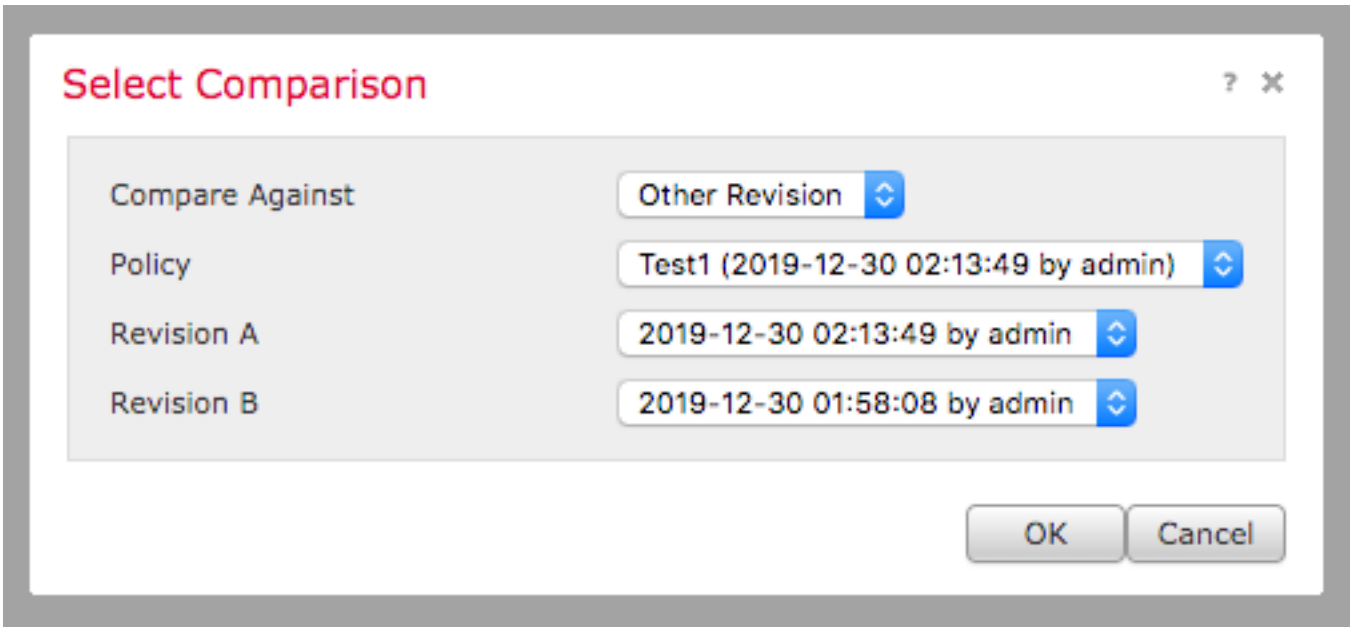
- 兩個不同的NAP策略之間
- 同一國家行動方案策略的兩個不同版本之間

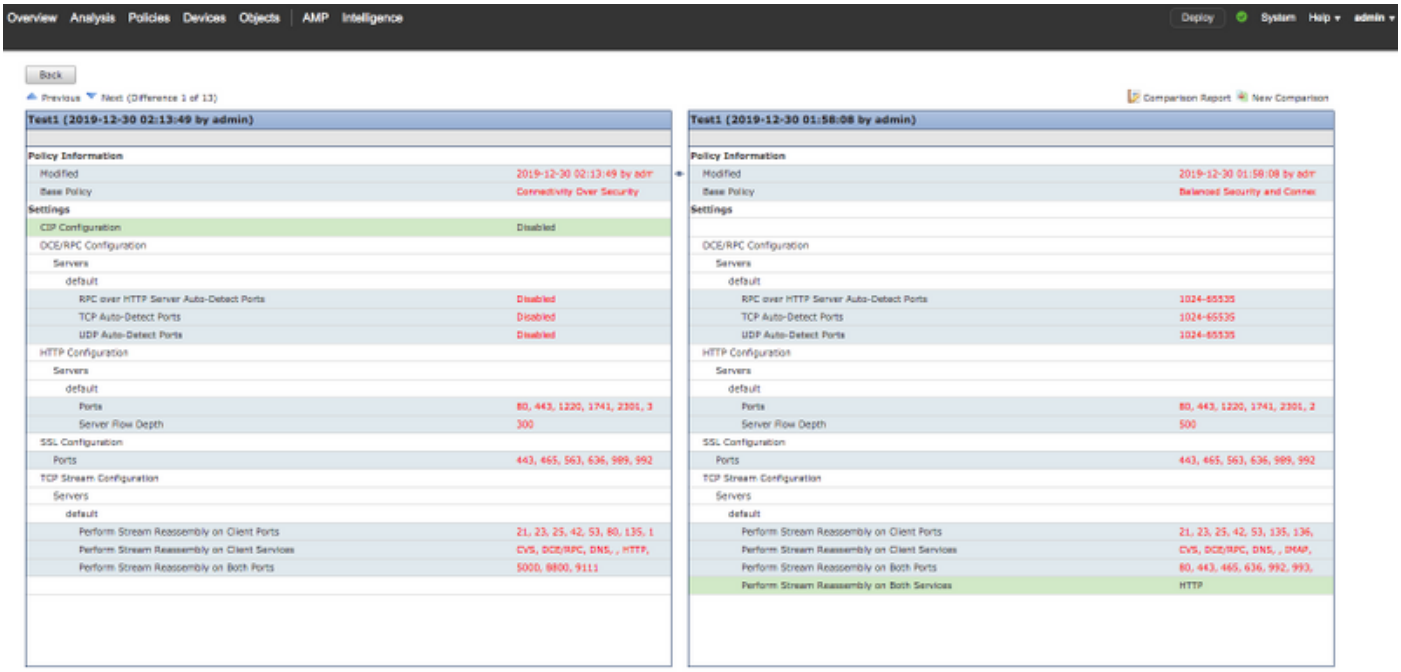


比較視窗提供兩個選定的NAP策略之間的逐行比較，並且可以從右上角的「**比較報告」頁籤將比較結果匯出為報告，如下圖所示：**



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：




Overview Analysis Policies Devices Objects AMP Intelligence
Deploy System Help admin
Back
Previous Next (Difference 1 of 13)
Comparison Report New Comparison
Test1 (2019-12-30 02:13:49 by admin)
Policy Information
Modified 2019-12-30 02:13:49 by adm
Base Policy Connectivity Over Security
Settings
CIP 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 CVS, DCE/RPC, DNS, , HTTP,
Perform Stream Reassembly on Both Ports 5000, 6800, 9111
Test1 (2019-12-30 01:58:08 by admin)
Policy Information
Modified 2019-12-30 01:58:08 by adm
Base Policy Balanced Security and Connec
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 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 CVS, DCE/RPC, DNS, , IMAP,
Perform Stream Reassembly on Both Ports 80, 443, 465, 636, 992, 993,
Perform Stream Reassembly on Both Services HTTP