

Firepower 디바이스에서 NAP 정책을 비교하는 방법

목차

[소개](#)

[사전 요구 사항](#)

[요구 사항](#)

[사용되는 구성 요소](#)

[배경 정보](#)

[NAP 컨피그레이션 확인](#)

소개

이 문서에서는 FMC(Firepower Management Center)에서 관리하는 Firepower 디바이스에 대해 서로 다른 NAP(Network Analysis Policies)를 비교하는 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- 오픈 소스 Snort 지식
- FMC(Firepower Management Center)
- Firepower Threat Defense(FTD)

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- 이 문서는 모든 Firepower 플랫폼에 적용됩니다.
- 소프트웨어 버전 6.4.0을 실행하는 Cisco Firepower Threat Defense(FTD)
- 소프트웨어 버전 6.4.0을 실행하는 FMC(Firepower Management Center Virtual)

배경 정보

Snort는 패턴 일치 기술을 사용하여 네트워크 패킷에서 익스플로잇을 찾고 방지합니다. 이를 위해 Snort 엔진은 이러한 비교를 수행할 수 있도록 네트워크 패킷을 준비해야 합니다. 이 프로세스는 NAP의 도움을 받아 수행되며 다음 3단계를 진행할 수 있습니다.

- 디코딩
- 표준화
- 사전 처리

네트워크 분석 정책은 다음 단계에서 패킷을 처리합니다. 먼저 시스템은 처음 3개의 TCP/IP 레이어를 통해 패킷을 디코딩한 다음 표준화, 사전 처리, 프로토콜 이상 징후 탐지를 계속합니다.

프리프로세서는 두 가지 주요 기능을 제공합니다.

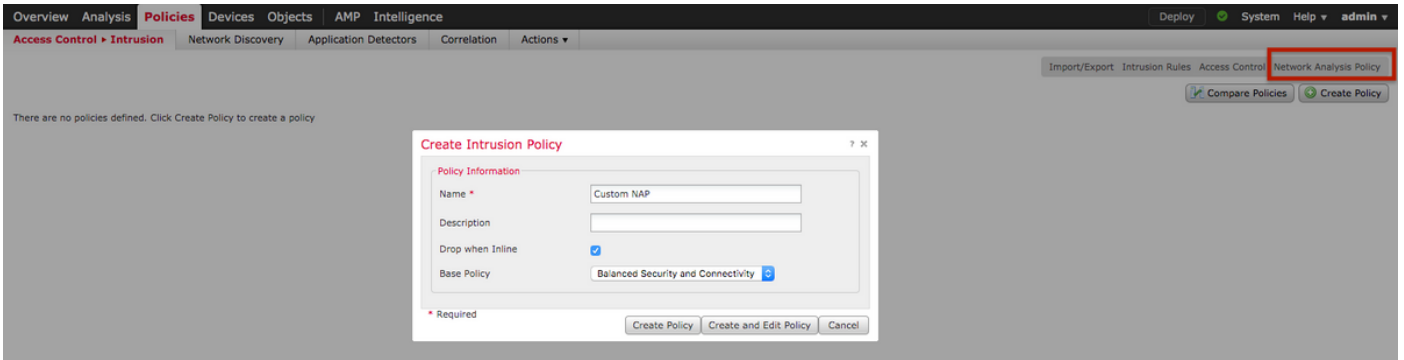
- 추가 검사를 위한 트래픽 표준화

- 프로토콜 이상 징후 식별

오픈 소스 Snort에 대한 자세한 내용은 <https://www.snort.org/>

NAP 컨피그레이션 확인

Firepower NAP 정책을 생성하거나 수정하려면 FMC Policies(**FMC 정책**) > **Access Control(액세스 제어)** > **Intrusion(침입)**으로 이동한 다음 이미지에 표시된 것처럼 오른쪽 상단의 Network Analysis Policy(네트워크 분석 정책) 옵션을 클릭합니다.



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() .

> ACP .Advanced() Network Analysis and Intrusion Policies() .

ACP [] .

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](#)

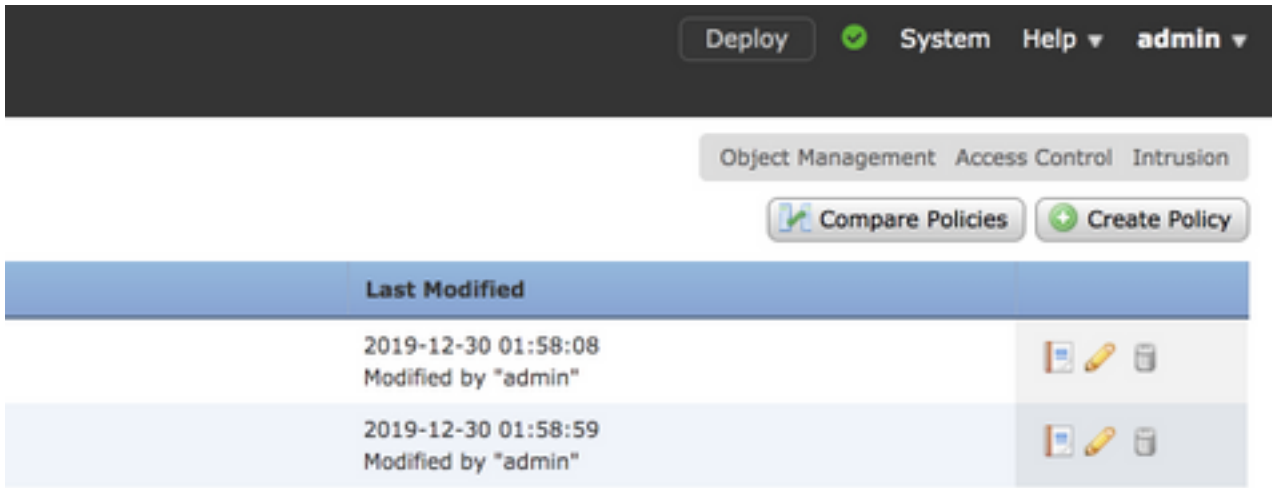
Default Network Analysis Policy [Balanced Security and Connectivity](#)

:Balanced **Security and Connectivity** for **Intrusion Policies** [Balanced Security and Connectivity for Network Analysis](#) . Snort .

NAP(네트워크 분석 정책) 비교

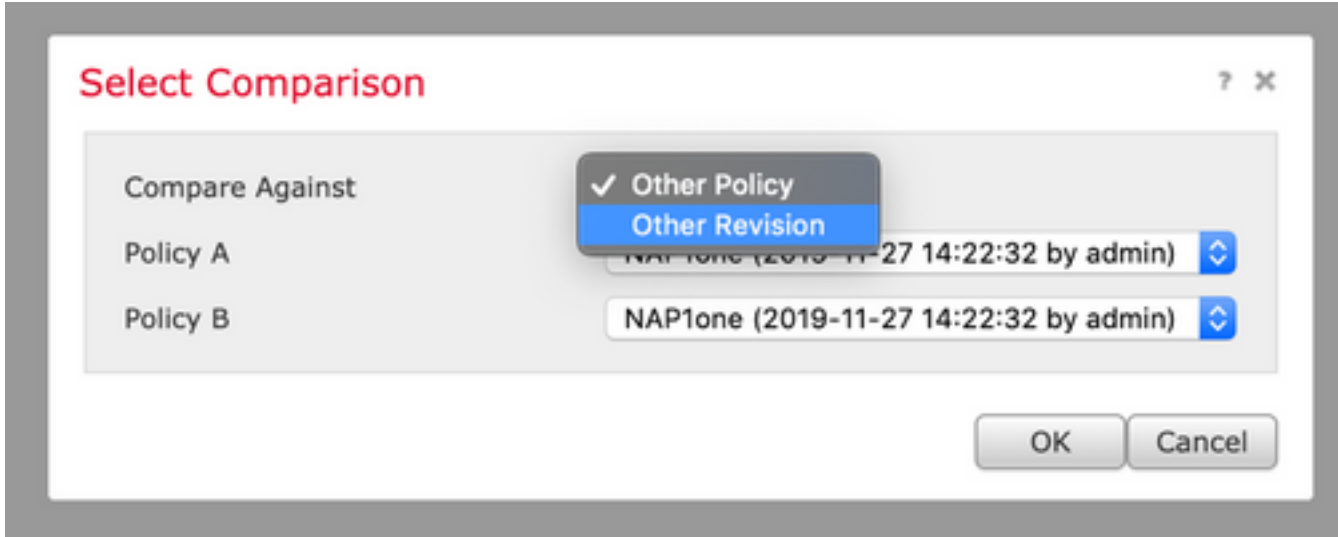
NAP 정책을 비교하여 변경 사항을 적용할 수 있으며 이 기능을 통해 문제를 파악하고 해결할 수 있습니다. 또한 NAP 비교 보고서를 생성하고 동시에 내보낼 수도 있습니다.

Policies(정책) > Access Control(액세스 제어) > Intrusion(침입)으로 이동합니다. 그런 다음 오른쪽 상단의 **Network Analysis Policy** 옵션을 클릭합니다. NAP 정책 페이지에서 이미지에 표시된 것처럼 오른쪽 상단에 **Compare Policies**(정책 비교) 탭이 표시됩니다.



Network Analysis Policy 비교는 다음 두 가지 변형으로 제공됩니다.

- 서로 다른 두 NAP 정책 간
- 동일한 NAP 정책의 서로 다른 두 수정 버전 간



비교 창은 두 개의 선택한 NAP 정책 간의 선 비교별로 비교 라인을 제공하며, 이미지에 표시된 대로 오른쪽 위의 **비교 보고서** 탭에서 보고서로 내보낼 수 있습니다.

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)
Policy Information	
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
Settings	
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	

동일한 NAP 정책의 두 버전 간의 비교를 위해 수정 옵션은 이미지에 표시된 대로 필요한 개정 ID를 선택하도록 선택할 수 있습니다.

Select Comparison ? X

Compare Against	Other Revision ▾
Policy	Test1 (2019-12-30 02:13:49 by admin) ▾
Revision A	2019-12-30 02:13:49 by admin ▾
Revision B	2019-12-30 01:58:08 by admin ▾

OK
Cancel

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 admin
Base Policy	Connectivity Over Security
Settings	
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	CVS, DCE/RPC, DNS, , HTTP,
Perform Stream Reassembly on Both Ports	5000, 9800, 9111

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 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