

FirepowerデバイスのNAPポリシーを比較する方法

内容

[概要](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[背景説明](#)

[NAP構成の確認](#)

概要

このドキュメントでは、Firepower Management Center(FMC)によって管理されるFirepowerデバイスのさまざまなネットワーク分析ポリシー(NAP)を比較する方法について説明します。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- オープンソースSnortに関する知識
- Firepower Management Center (FMC)
- Firepower Threat Defense(FTD)

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- この記事は、すべてのFirepowerプラットフォームに適用されます
- ソフトウェアバージョン6.4.0が稼働するCisco Firepower Threat Defense(FTD)
- ソフトウェアバージョン6.4.0が稼働するFirepower Management Center Virtual(FMC)

背景説明

Snortは、パターンマッチング技術を使用して、ネットワークパケットの不正利用を検出し、防止します。これを行うには、Snortエンジンでは、この比較を行えるようにネットワークパケットを準備する必要があります。このプロセスはNAPを使用して実行され、次の3つの段階を経ることができます。

- デコード
- 正規化
- 前処理

ネットワーク分析ポリシーは、次のフェーズでパケットを処理します。最初に、システムは最初の3つのTCP/IPレイヤを通じてパケットをデコードし、次にプロトコル異常の正規化、前処理、検出を続けます。

プリプロセッサには、次の2つの主な機能があります。

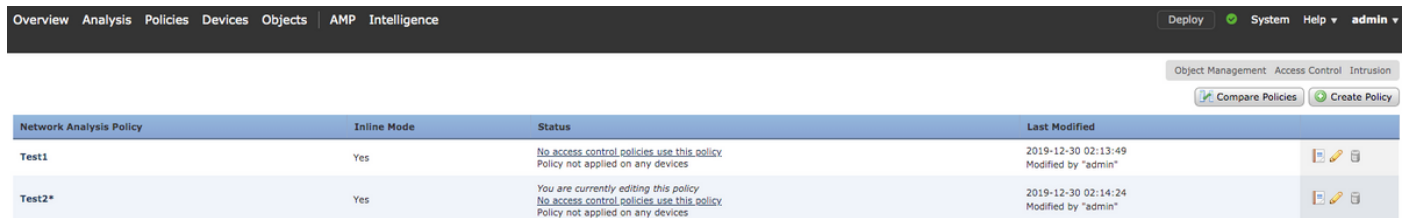
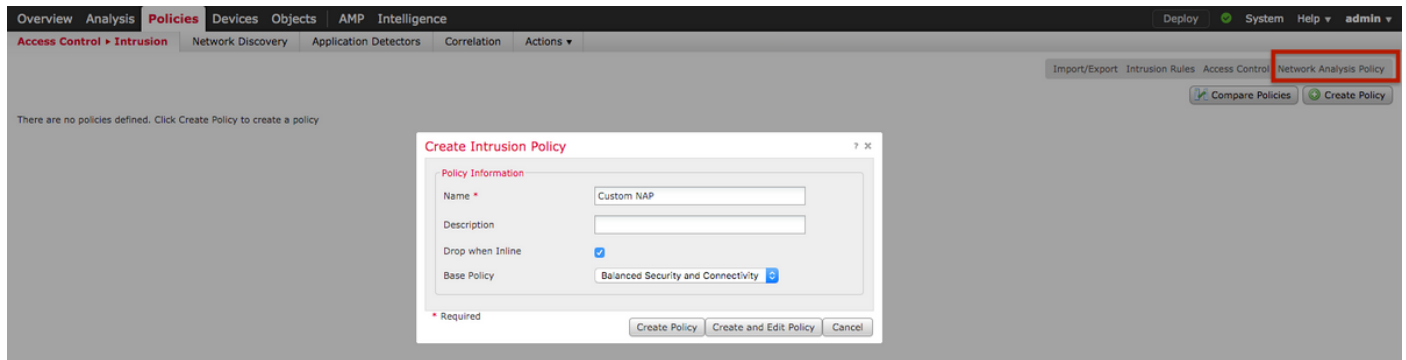
- トラフィックの正規化による詳細な検査

- プロトコルの異常の特定

オープンソースSnortの詳細については、次を参照してください。 <https://www.snort.org/>

NAP構成の確認

Firepower NAPポリシーを作成または編集するには、[FMC Policies] > [Access Control] > [Intrusion]に移動し、右上隅の[Network Analysis Policy]オプションをクリックします (図を参照)。



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

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](#)

Snort

ネットワーク分析ポリシー(NAP)の比較







NAPポリシーを比較して変更を行うことができます。この機能は、問題の特定とトラブルシューティングに役立ちます。また、NAP比較レポートを同時に生成およびエクスポートすることもできます。

[Policies] > [Access Control] > [Intrusion] の順に選択します。次に、右上の[ネットワーク分析ポリシー]オプションをクリックします。NAPポリシーページの右上に、図に示すように[Compare Policies]タブが表示されます。

Deploy ✔ System Help ▼ admin ▼

Object Management Access Control Intrusion

Compare Policies Create Policy

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

ネットワーク分析ポリシーの比較には、次の2つのタイプがあります。

- 2つの異なるNAPポリシー間
- 同じNAPポリシーの2つの異なるリビジョン間

Select Comparison ? ✕

Compare Against
 Other Policy
 Other Revision

Policy A NAP1one (2019-11-27 14:22:32 by admin) ▾

Policy B NAP1one (2019-11-27 14:22:32 by admin) ▾

OK Cancel

比較ウィンドウには、選択した2つのNAPポリシーの比較が行ごとに表示されます。図に示すように、右上の比較レポートタブからレポートとしてエクスポートできます。

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)
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: 16384
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	

同じNAPポリシーの2つのバージョンを比較するために、リビジョンオプションを選択して、必要なリビジョンIDを選択できます (図を参照)。

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	CYS, 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	CYS, DCE/RPC, DNS, , IMAP,
Perform Stream Reassembly on Both Ports	80, 443, 465, 636, 992, 993,
Perform Stream Reassembly on Both Services	HTTP