

Como comparar as políticas de NAP em dispositivos Firepower

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Informações de Apoio](#)

[Verificar a configuração do NAP](#)

Introduction

Este documento descreve como comparar diferentes políticas de análise de rede (NAP) para dispositivos firepower gerenciados pelo Firepower Management Center (FMC).

Prerequisites

Requirements

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Conhecimento do Snort de código aberto
- Firepower Management Center (FMC)
- Firepower Threat Defense (FTD)

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- Este artigo se aplica a todas as plataformas Firepower
- Cisco Firepower Threat Defense (FTD), que executa a versão de software 6.4.0
- Firepower Management Center Virtual (FMC) que executa a versão de software 6.4.0

Informações de Apoio

O Snort usa técnicas de correspondência de padrões para localizar e impedir explorações em pacotes de rede. Para fazer isso, o mecanismo Snort precisa que os pacotes de rede sejam preparados de forma que essa comparação possa ser feita. Esse processo é feito com o auxílio do NAP e pode passar pelas três etapas a seguir:

- Decodificação
- Normalizando
- Pré-processamento

Uma política de análise de rede processa o pacote em fases: primeiro, o sistema decodifica pacotes através das três primeiras camadas TCP/IP e, em seguida, continua com a normalização, o pré-processamento e a detecção de anomalias de protocolo.

Os pré-processadores oferecem duas funcionalidades principais:

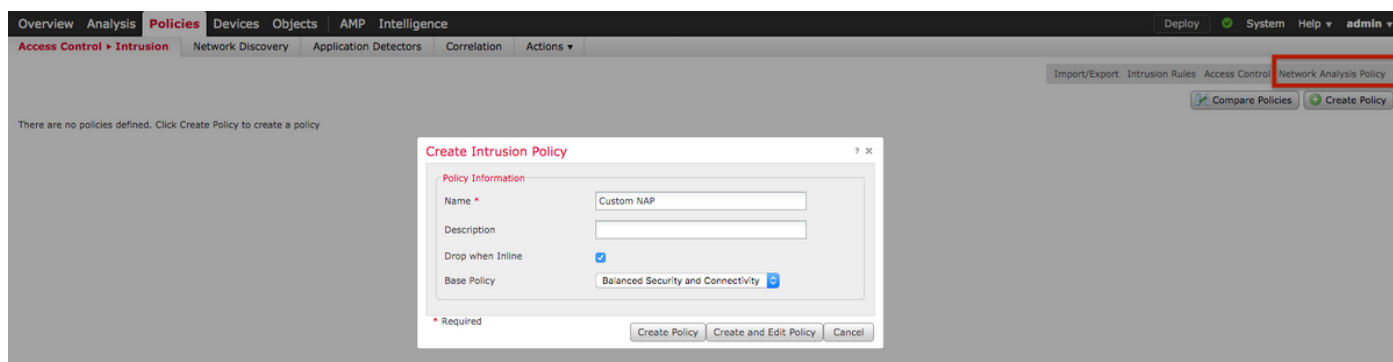
- Normalização do tráfego para inspeção posterior
- Identificar anomalias de protocolo

Nota: Algumas regras de política de intrusão exigem determinadas opções de pré-processador para executar a detecção

Para obter informações sobre o Snort de código aberto, visite <https://www.snort.org/>

Verificar a configuração do NAP

Para criar ou editar políticas NAP do firepower, navegue até **FMC Políticas > Access Control > Intrusion**, depois clique na opção **Network Analysis Policy** no canto superior direito, como mostrado na imagem:



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"

Verificando a política de análise de rede padrão

Verifique a política de análise de rede (NAP) padrão aplicada na política de controle de acesso (ACP)

Navegue até **Políticas > Controle de acesso** e edite o ACP que deseja verificar. Clique na guia **Avançado** e role para baixo até a seção **Análise de rede e políticas de intrusão**.

A política de análise de rede padrão associada ao ACP é a **segurança e a conectividade equilibradas**, como mostrado na imagem:

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](#)

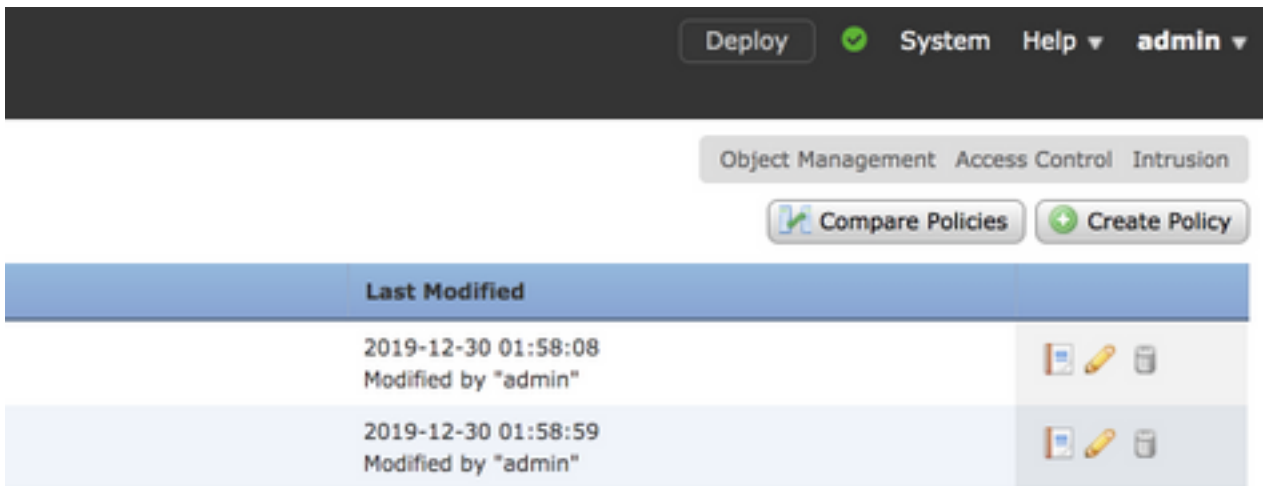
Default Network Analysis Policy [Balanced Security and Connectivity](#)

Note: Não confunda a **segurança e a conectividade equilibradas** para **políticas de intrusão** e a **segurança e conectividade equilibradas** para **análise de rede**. O primeiro é para as regras do Snort, enquanto o segundo é para pré-processamento e decodificação.

Comparar política de análise de rede (NAP)

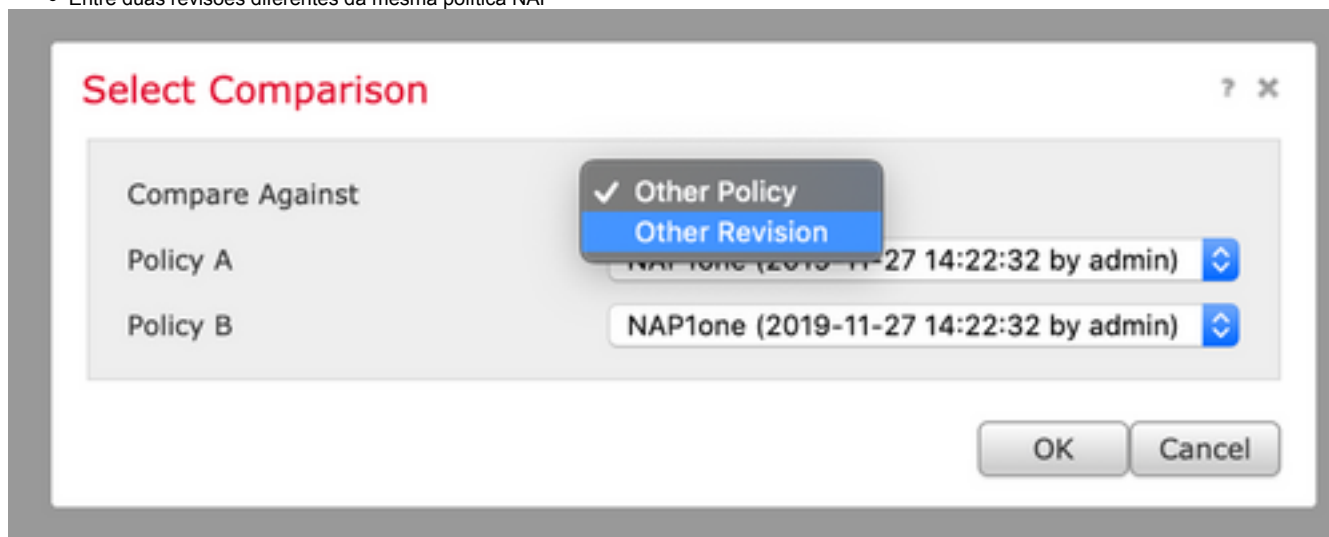
As políticas NAP podem ser comparadas para alterações feitas e esse recurso pode ajudar a identificar e solucionar problemas. Além disso, os relatórios de comparação de NAP também podem ser gerados e exportados ao mesmo tempo.

Navegue até **Políticas > Controle de acesso > Invasão**. Em seguida, clique na opção **Network Analysis Policy** no canto superior direito. Na página de política NAP, você pode ver a guia **Comparar políticas** no lado superior direito, como mostrado na imagem:



A comparação da política de análise de rede está disponível em duas variantes:

- Entre duas políticas NAP diferentes
- Entre duas revisões diferentes da mesma política NAP



A janela de comparação fornece uma comparação linha por linha entre duas políticas NAP seleccionadas e o mesmo pode ser exportado como um relatório da guia **relatório de comparação** na parte superior direita, como mostrado na imagem:

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: 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	

Para comparação entre duas versões da mesma política NAP, a opção de revisão pode ser selecionada para selecionar a **id de revisão** necessária, como mostrado na imagem:

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