How to Compare NAP Policies on Firepower Devices

Contents

Introduction

This document describes how to compare different Network Analysis Policies (NAP) for firepower devices managed by Firepower Management Centre (FMC).

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Knowledge of open-source Snort
- Firepower Management Center (FMC)
- Firepower Threat Defense (FTD)

Components Used

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command. The information in this document is based on these software and hardware versions:

- This article is applicable to all Firepower platforms
- Cisco Firepower Threat Defense (FTD) which runs software version 6.4.0
- Firepower Management Center Virtual (FMC) which runs software version 6.4.0

Background Information

The Snort uses pattern matching techniques to find and prevent exploits in network packets. In order to do this, the Snort engine needs network packets to be prepared in such a way that this comparison can be done. This process is done with the help of NAP and can undergo these three stages:

- Decoding
- Normalizing
- Pre-processing

A network analysis policy processes packet in phases: first the system decodes packets through the first three TCP/IP layers, then continues with normalizing, pre-processing, and detecting protocol anomalies.

Pre-processors provide two main functionality:

- Traffic Normalization for further inspection
- Identify protocol anomalies

Note: Some Intrusion Policy rules require certain pre-processor options in order to perform detection

For information on open-source Snort, please visit https://www.snort.org/

Verify NAP Configuration

To create or edit firepower NAP policies, navigate to **FMC Policies > Access Control > Intrusion**, thereafter click **Network Analysis Policy** option in the top right corner, as shown in the image:

Overview Analysis Policies Devices Objects AMP Intelli	gence	Deploy System Help v admin v
Access Control > Intrusion Network Discovery Application Detecto	rs Correlation Actions •	
		Import/Export Intrusion Rules Access Control Network Analysis Policy
		Compare Policies Create Policy
There are no policies defined. Click Create Policy to create a policy		
	Create Intrusion Policy	x 1
	Policy Information	
	Name *	Custom NAP
	Description	
	Drop when Inline	0
	Base Policy	Balanced Security and Connectivity
	Required	Create Bolicy Create and Edit Bolicy Cancel
Overview Analysis Policies Devices Objects AMP Intellig	ence	Deploy 🥏 System Help 🔻 admin 🕯
		Object Management Access Control Intrusion
		Compare Policies Create Policy
Network Analysis Policy Inline Mode	s Status	Last Modified
Test1 Yes	No access Policy not	<u>control colicies use this policy</u> 2019-12-30 02:13:49 applied on any devices Modified by "admin" □ 🖉 🗍
Test2* Yes	You are co No access Policy not	arrently editing this policy 2019-12-30 02:14:24 💽 🥔 🗇 applied on any devices

Verifying the default Network Analysis Policy

Check the default Network Analysis (NAP) policy applied on the Access Control Policy (ACP) Navigate to **Policies > Access Control** and edit the ACP that you want to verify. Click **Advanced** tab and scroll down to **Network Analysis and Intrusion Policies** section.

The Default Network Analysis Policy associated with the ACP is **Balanced Security and Connectivity**, as shown in the image:

Overview	Analysis Policies	Devices Obje	cts AMP	Intelligence					
Access Co	ntrol + Access Control	Network Disco	very Appl	ication Detectors	Correlation	Actions +			
Test	ption								
Prefilter Po	licy: Default Prefilter Policy			SSL Policy: None					
Rules S	iecurity Intelligence HT	TP Responses L	.ogging 🗛	lvanced					
General S	Settings						_	1	
Maccimum	URL characters to store in	connection events						1024	
Allow an D	nteractive Block to bypass	blocking for (seco	ends)					600	
Retry URL	cache miss lookup							Yes	
Inspect t	Network Analysis and	Intrusion Polis	cies					9 ×	
Identity	Intrusion Policy used before rule is determined	e Access Control	Balanced Sec.	rity and Connectivity			¥		l
Identity I	Intrusion Policy Variable Se	rt.	Default-Set				*	/	l
SSL Poli	Network Analysis Rules		No Custom Rul	55	Ne	twork Analysis Po	licy List		l
SSL Polic	Default Network Analysis P	olicy	Balanced Sec.	rity and Connectivity			¥		l
Prefilter	Revert to Defaults					ок	Cancel		l
									ĥ
Network	Analysis and Intrusion	1 Policies						ø	
Intrusion 8	Policy used before Access (Control rule is dete	ermined		Bi	lanced Security a	ind Conni	ectivity	
Intrusion I	Policy Variable Set						Defe	wit Set	
Default Ne	twork Analysis Policy				Be	lanced Security a	ind Conni	ectivity	

Note: Do not confuse the Balanced Security and Connectivity for Intrusion Policies and the Balanced Security and Connectivity for Network Analysis. The former one is for Snort rules while the latter is for pre-processing and decoding.

Compare Network Analysis Policy (NAP)

The NAP policies can be compared for changes done and this feature could help in identifying and troubleshooting the issues. In addition, NAP comparison reports could also be generated and exported at the same time.

Navigate to **Policies > Access Control > Intrusion**. Then, click **Network Analysis Policy** option in the top right. Under the NAP policy page you can see **Compare Policies** tab on the top right side, as shown in the image:

	Deploy 🤗 System Help 🔻 admi	in v
	Object Management Access Control Intrusi	ion licy
Last Modifie	ed	
2019-12-30 Modified by "	01:58:08 admin"	
2019-12-30 Modified by "	01:58:59 📃 🖉 🕤	

Network Analysis Policy comparison is available in two variants:

- Between two different NAP policies
- Between two different revisions of same NAP policy

Select Comparison	7 X
Compare Against Policy A Policy B	NAPTione (2019-11-27 14:22:32 by edmin)
	OK Cancel

The comparison window provides a comparative line by line comparison between two selected NAP policies and the same can be exported as a report from the **comparison report** tab on the top right, as shown in the image:

Max			
Partial Theory (1997)			Province Append R. San Comparison
teact (2010-12-00 82-13-40 by pdecis)		Tearty (2010-12-00 02-14-04 by patents)	
Nite Information		Portes Information	
Terms	Texts	1 100	2001
Number	AND A REAL PROPERTY AND AN ADDRESS OF	Number	PROFESSION AND ADDRESS OF ADDRESS
lass hairy	Consultate they beaute	lines heigh	Residual Interior
and the second se		Interinger .	
Charles in Sectors		Creation in Parliance	
1000 Destaures	Brailing .	1000 Depleases	Page 1
P Declares	Ended.	P Declares	Drig and Generate Buerts
NP (balance)	Energy .	NP Oradauma	its and farmeds from a
MP Declarate	Energy Control of Cont	MP Departs	Page 1
SUBMI Collector		BORNER Configuration	
Servers .		Servera	
adm.0		444.0	
Unit Provinces and Chart	8	Unit Maximum Andri Dram	1 C C C C C C C C C C C C C C C C C C C
KPC and 1979 Server Auto-Indext Parts	Creative .	NVC year NVW Server Auto-Select Party	Line seas
ROF Auto-Ontact Ports	(rated	TOP Auto-Detect Plans	107-100
VOT NAME (MARKE PARTS	(marked	VDF Auto Datase Parts	LAN ATM
Inthin Insurance Institu	10,000	1918 File Inspection Starts	
factual Deceding		Partial Deceding	
Detail Instit P Option	Deaths	Densit Trans (P. Spring	Enter
Detail Dealers TO Sprare	(Creative)	Detail Dealers 707 Synams	E-atta
Detail Other TOP Options	Oracle	Detail Other TOP Dataset	Evalue .
Detect Potent Pagine Instruction	instead of the second se	Details Protocol Papeler (Instruction	Endine .
DHI Configuration		DNB Configuration	
Detroit Dealers 255 55 Tapes	5m	Detect Dealers 195 18 Speed	-
Dead Spectrema (NS-ND Spec	54 C	Detect Superimental Dist HD Nome	
718 and Tamas Delignation		77 and former bankgunetise	
All being		PTR between	

For comparison between two versions of the same NAP policy, the revision option can be opted to select the required **revision id**, as shown in the image:

Select Comparison	2 %
Compare Against	Other Revision 📀
Revision A	2019-12-30 02:13:49 by admin)
Revision B	2019-12-30 01:58:08 by admin ᅌ
	OK Cancel

Derive Anipits Police Derive Opens | AMP Indigens

- Anne - Anne (Marco 1 of 12) Victorian Next R for Computer Pasets (2012) 4.8-348 8.8 1.0-48 by admin) Posts (2010-12-04-01-56-08 by admin) and a second second ing being state Musified Reservices State of the latent system formation that the state State of the second sec Martine Anna Palay 100 Constant Inc. NUMBER OF STREET NULAR Competence Inner Alfaul ARC and VITE Danas Auto Datas Anto 107 Auto Datas Anto 107 Auto Datas Anto 107 Auto Datas Anto lanene lanene territe Configuration Territe 10/0.0 Auto Barrier Plan Depth 10, 100, 1200, 1700, 2000, 1 30 10, web, 12,00, 1744, 1766, 1 Rit, Golgonitor Anto KP Israen Golgonitor ML Configuration Parts NOP Service Configuration Kir Amerika Salitya kunon Sarata Makata Andrea Sanan Anasaritik ya Santi Arra Andrea Sanan Anasaritik ya Santi Arran Andrea Sanan Anasaritik ya Bati Arra Andrea Sanan Anasaritik ya Bati Arra NY KANYA LENGUNU Server Anton Malyon Scenet Assessments of Sections Antone Scenet Assessments of Sections Antone Scenet Assessments of Section Arts 20, 20, 20, 40, 50, 50, 50, 5 Col, 20, 60, 50, 50, 575, 10 Store, 600, 7011