如何比较Firepower设备上的NAP策略

目录

简介

本文档介绍如何比较由Firepower管理中心(FMC)管理的firepower设备的不同网络分析策略(NAP)。

先决条件

要求

Cisco 建议您了解以下主题：

- 开源Snort知识
- Firepower管理中心(FMC)
- Firepower威胁防御(FTD)

使用的组件

本文档中的信息基于以下软件和硬件版本：

- 本文适用于所有Firepower平台
- 运行软件版本6.4.0的思科Firepower威胁防御(FTD)
- 运行软件版本6.4.0的Firepower管理中心虚拟(FMC)

背景信息

Snort使用模式匹配技术来查找和防止网络数据包中的漏洞。为此，Snort引擎需要准备网络数据包，以便进行此比较。此过程在NAP的帮助下完成，可以经历以下三个阶段：

- 解码
- 规范化
- 预处理

网络分析策略分阶段处理数据包：首先，系统通过前三个TCP/IP层对数据包进行解码，然后继续进行规范化、预处理和检测协议异常。

预处理器提供两个主要功能：

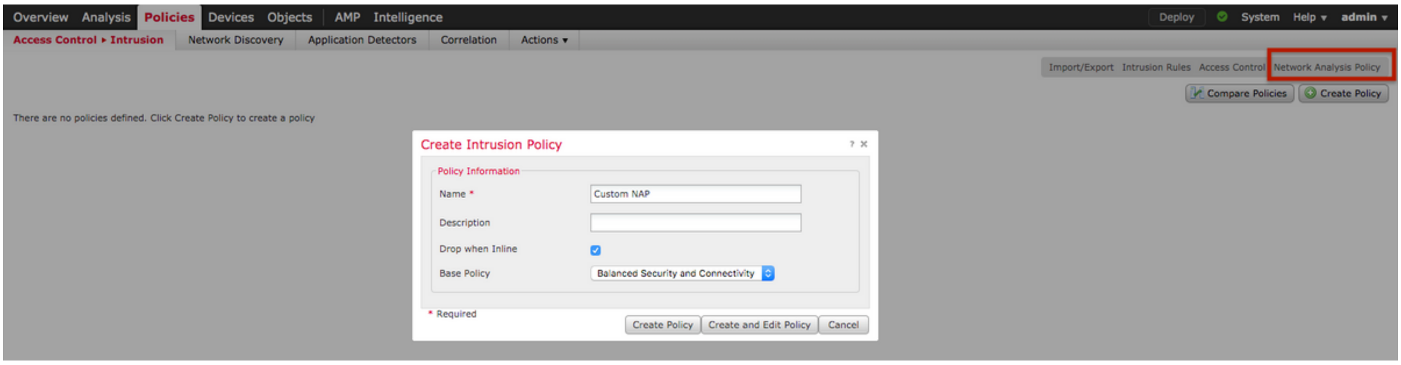
- 流量规范化以进一步检查
- 识别协议异常

：

有关开源Snort的信息，请访问 https://www.snort.org/

检验NAP配置

要创建或编辑firepower NAP策略，请导航至**FMC Policies > Access Control > Intrusion，然后单击右上角的**Network Analysis Policy选项，如图所示：



There are no policies defined. Click Create Policy to create a policy

Create Intrusion Policy

Policy Information

Name * Custom NAP

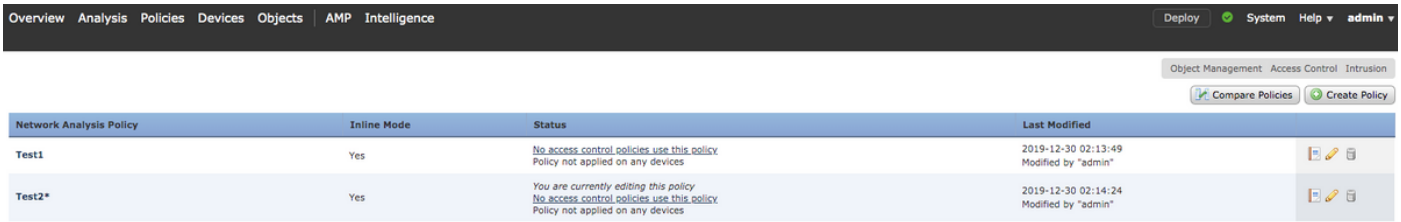
Description

Drop when Inline ☑

Base Policy Balanced Security and Connectivity

* Required

Create Policy | Create and Edit Policy | Cancel

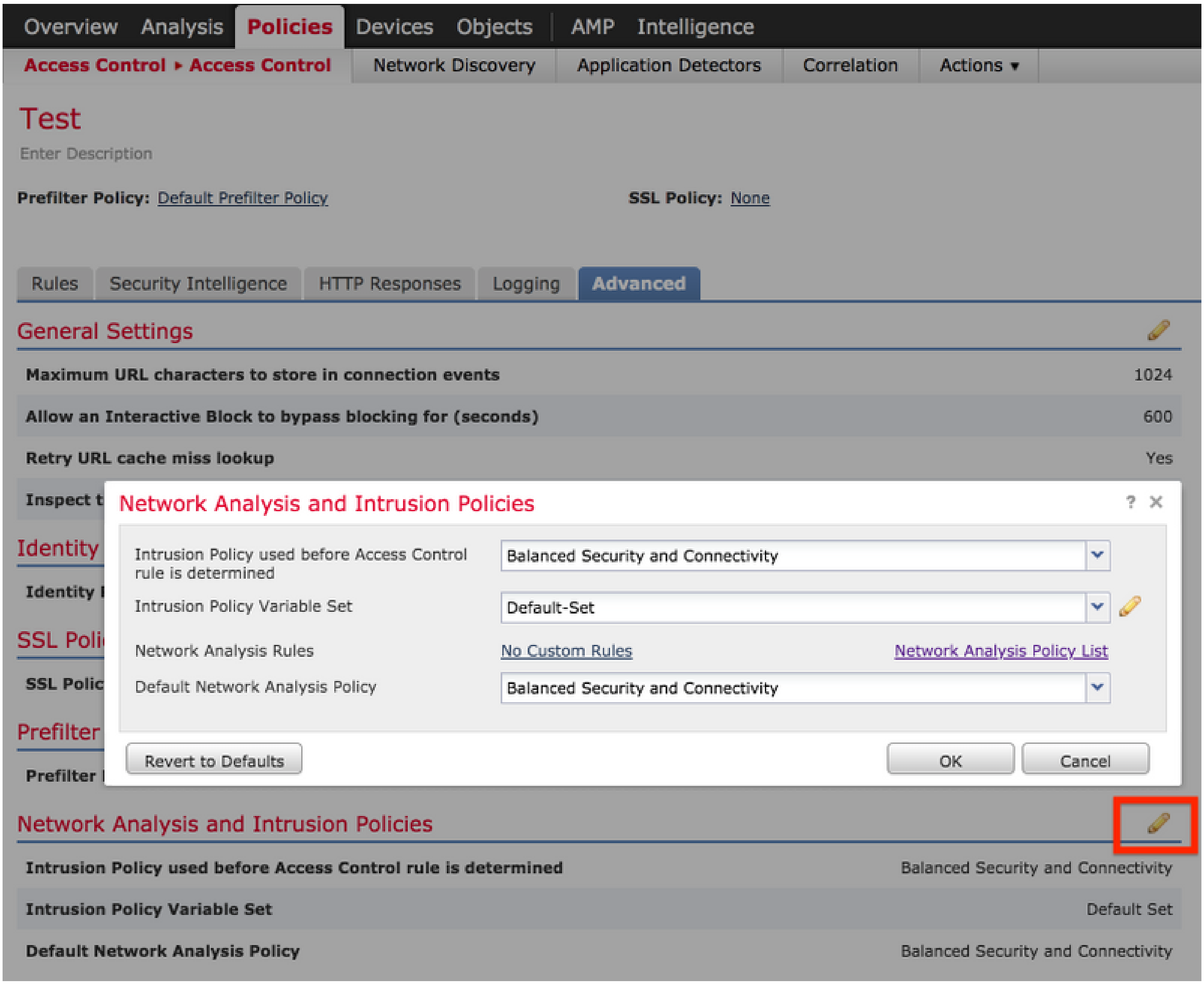


Network Analysis Policy	Inline Mode	Status	Last Modified
Test1	Yes	No access control policies use this policy Policy not applied on any devices	2019-12-30 02:13:49 Modified by "admin"
Test2*	Yes	*You are currently editing this policy* No access control policies use this policy Policy not applied on any devices	2019-12-30 02:14:24 Modified by "admin"

(ACP)(NAP)

>ACP**Advanced Network Analysis and Intrusion Policies**

ACP**:**



Test

Enter Description

Prefilter Policy: Default Prefilter Policy

SSL Policy: None

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
Inspect t	

Identity

Identity I

SSL Poli

SSL Polic

Prefilter

Prefilter I

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

Network Analysis and Intrusion Policies

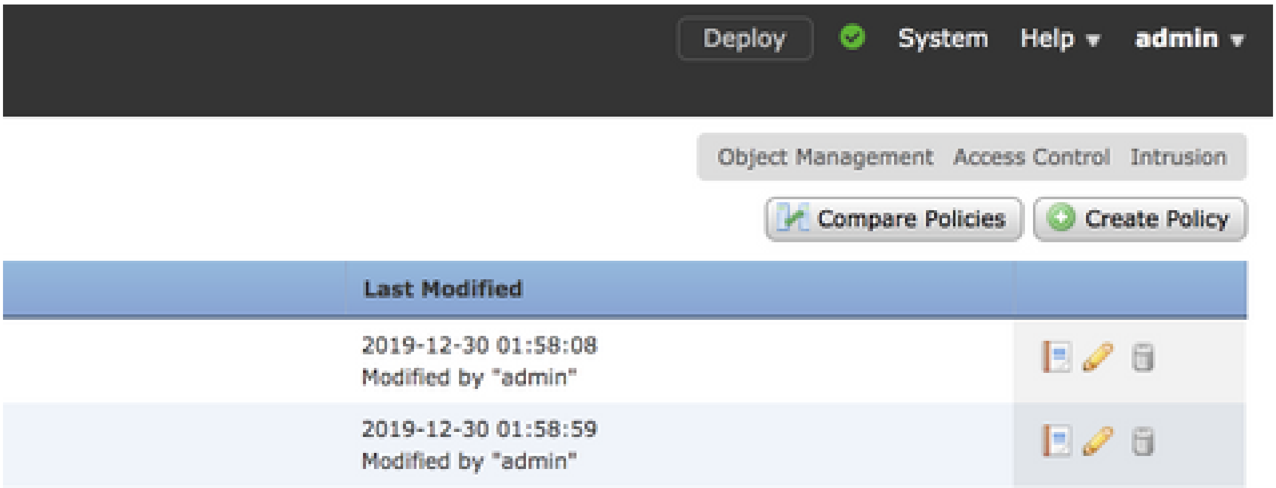
Intrusion Policy used before Access Control rule is determined	Balanced Security and Connectivity
Intrusion Policy Variable Set	Default Set
Default Network Analysis Policy	Balanced Security and Connectivity

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

比较网络分析策略(NAP)

可以比较NAP策略所做的更改，此功能有助于识别和排除问题。此外，还可以同时生成和导出NAP比较报告。

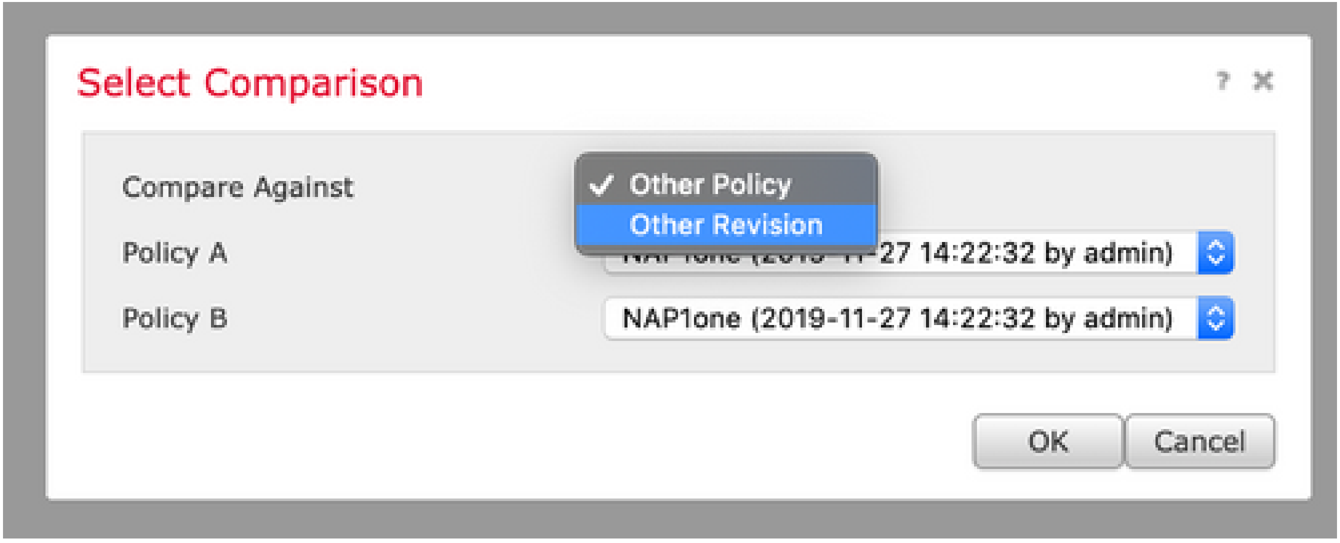
导航至**Policies > Access Control > Intrusion**。然后，单击**右上角**的“网络分析策略”选项。在NAP策略页面下，您可以看**到右**上方的“比较策略”选项卡，如图所示：



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

网络分析策略比较有两种形式：

- 在两个不同的NAP策略之间
- 在同一NAP策略的两个不同修订版之间



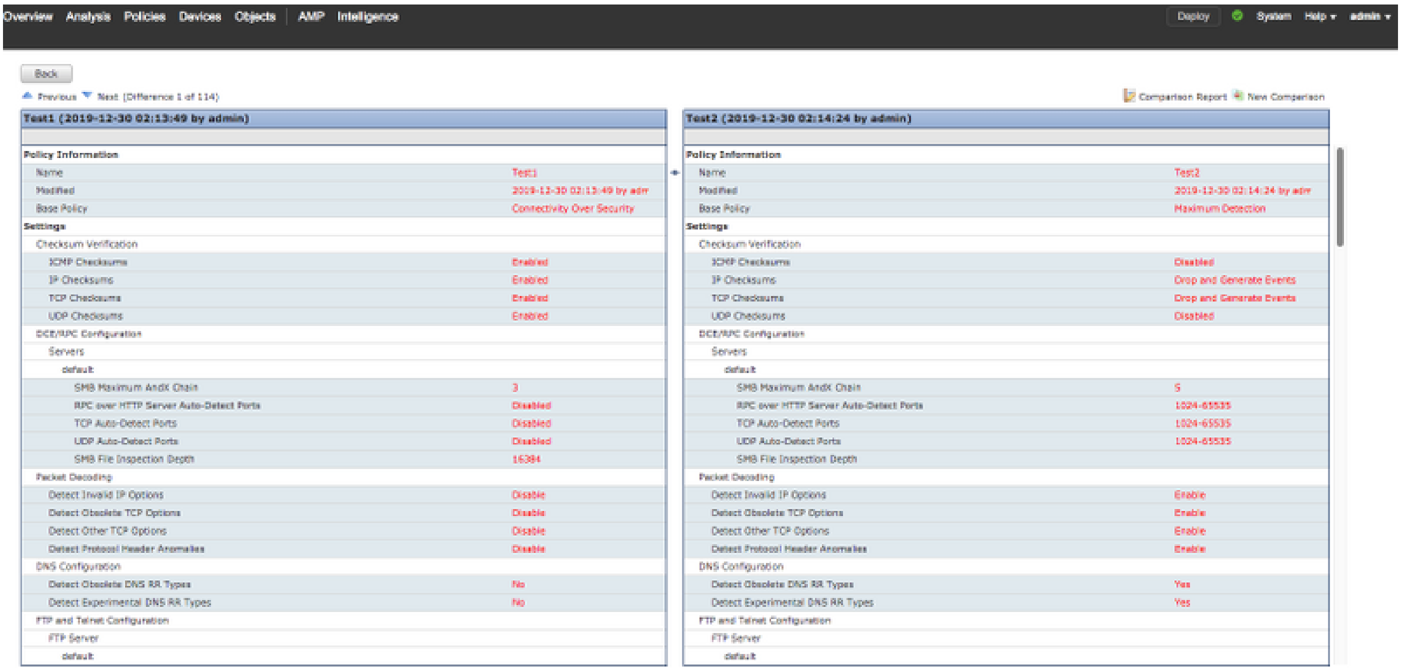
Select Comparison

Compare Against: ✓ Other Policy / Other Revision

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

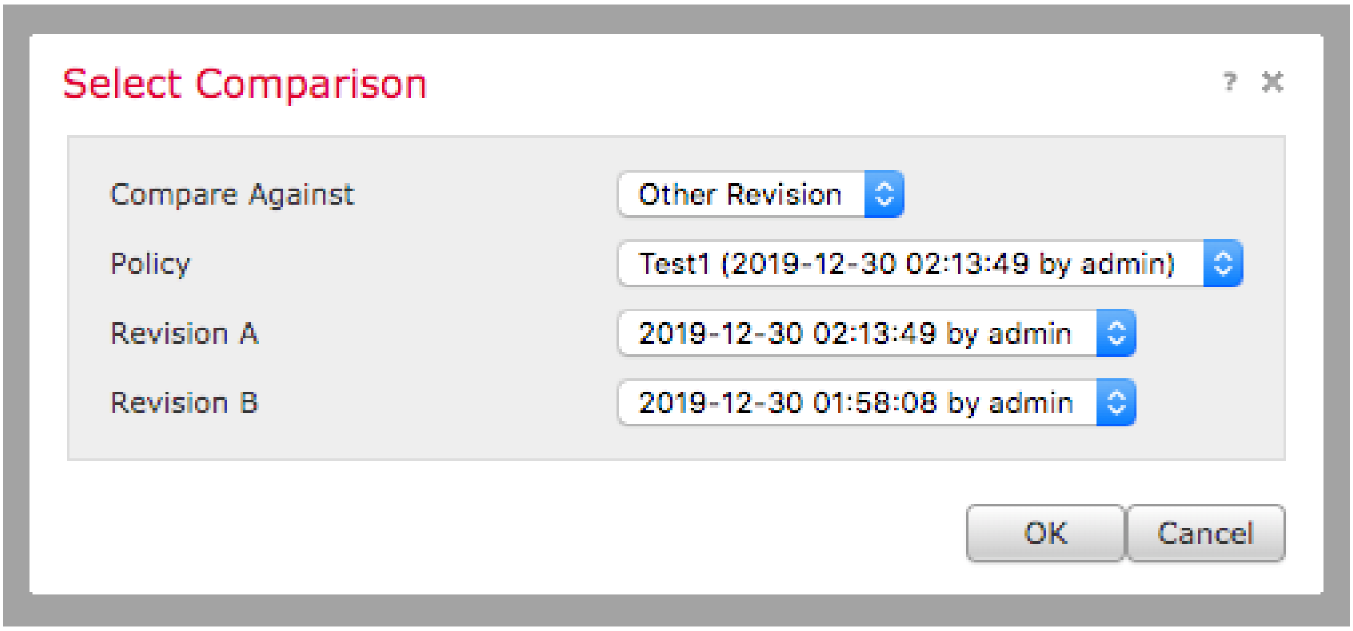
Policy B: NAP1one (2019-11-27 14:22:32 by admin)

比较窗口提供两个选定NAP策略之间的逐行比较，可以从右上角的“比较报告”(comparison report)选项卡导出报告，如图所示：



	Test1 (2019-12-30 02:13:49 by admin)		Test2 (2019-12-30 02:14:24 by admin)
Policy Information		**Policy Information**	
Name	Test1	Name	Test2
Modified	2019-12-30 02:13:49 by adm	Modified	2019-12-30 02:14:24 by adm
Base Policy	Connectivity Over Security	Base Policy	Maximum Detection
Settings		**Settings**	
Checksum Verification		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		DCE/RPC Configuration	
Servers		Servers	
default		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		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		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 and Telnet Configuration	
FTP Server		FTP Server	
default		default	

为了比较同一NAP策略的两个版本，可以选择修订版选项来选择所需的修订版ID，**如图**所示：



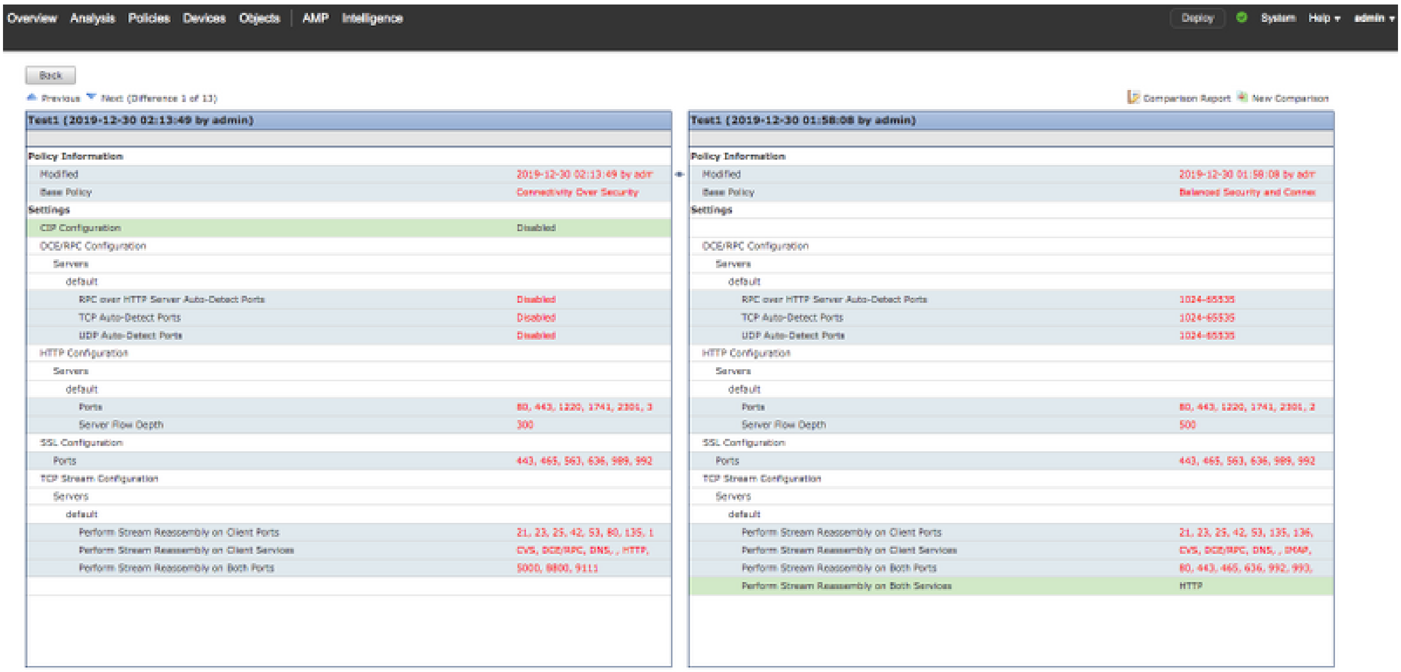
Select Comparison

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



Test1 (2019-12-30 02:13:49 by admin)	
Policy Information	
Modified	2019-12-30 02:13:49 by adr
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, 9800, 9111

Test1 (2019-12-30 01:58:08 by admin)	
Policy Information	
Modified	2019-12-30 01:58:08 by adr
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