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 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 the following 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

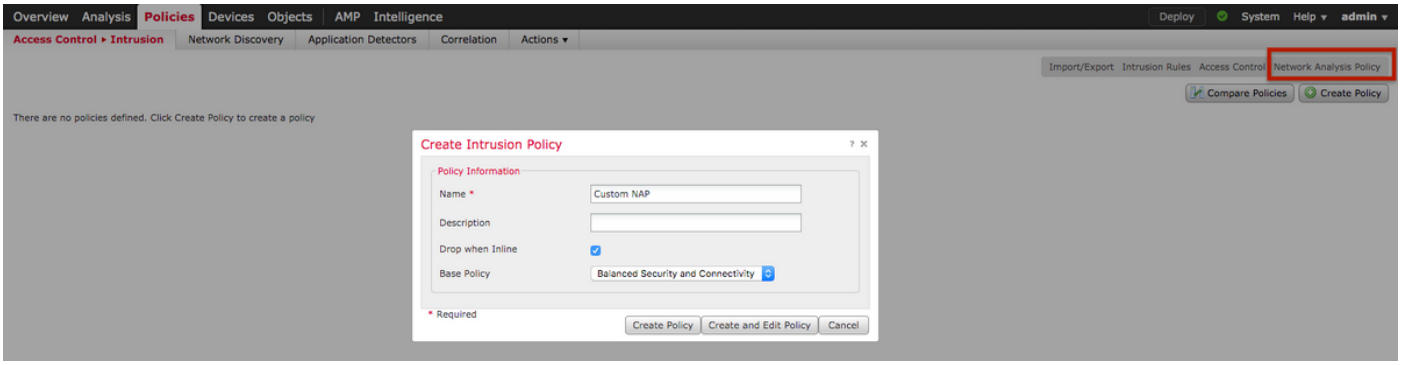
- Identify protocol anomalies

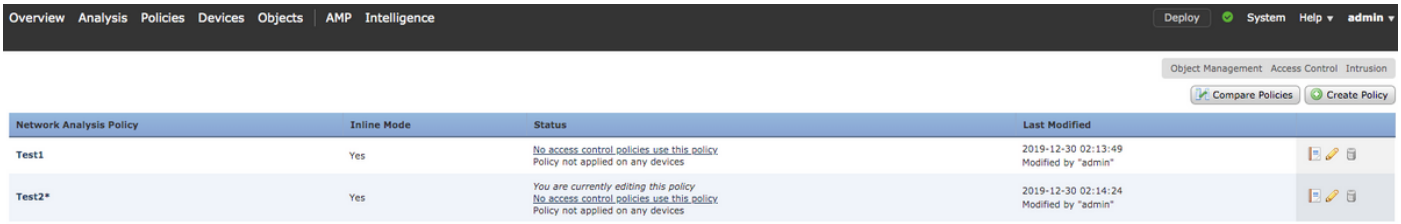
Note: Some Intrusion Policy rules require certain pre-processor options in order to perform detection

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:



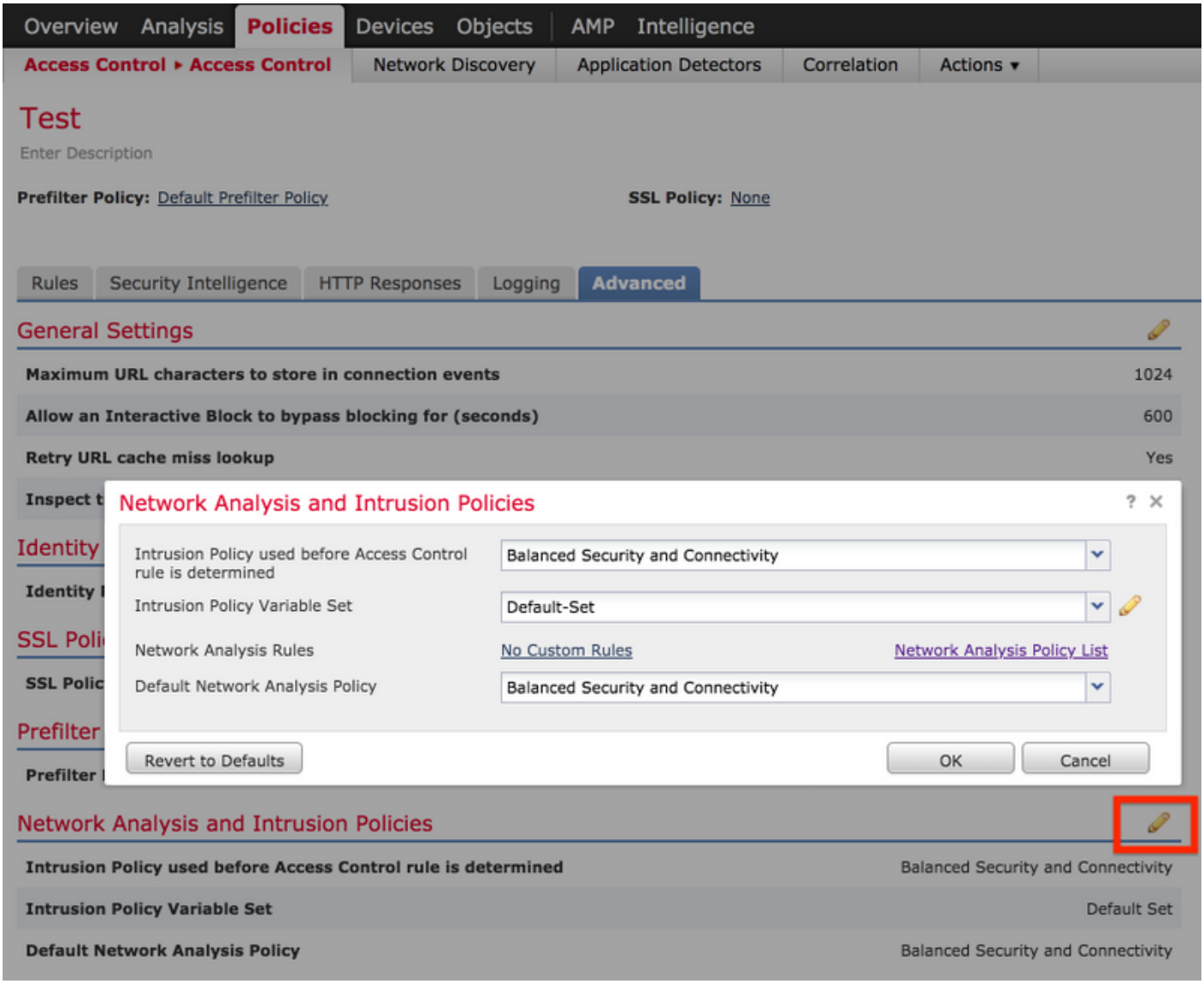


Verifying the default Network Analysis Policy

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**:**

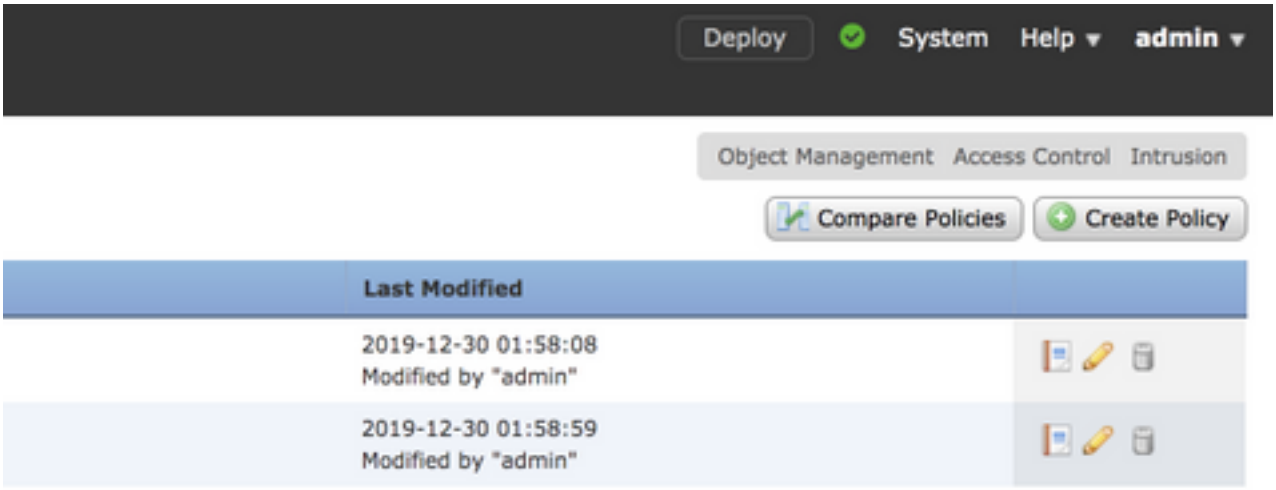


> **Note**: Do not confuse the **Balanced Security and Connectivity** for **Intrusion Policies** and the **Balanced Security and Connectivity** for **Network Analysis**. The former one is for Snort rules while the latter is for pre-processing and decoding.

Compare Network Analysis Policy (NAP)

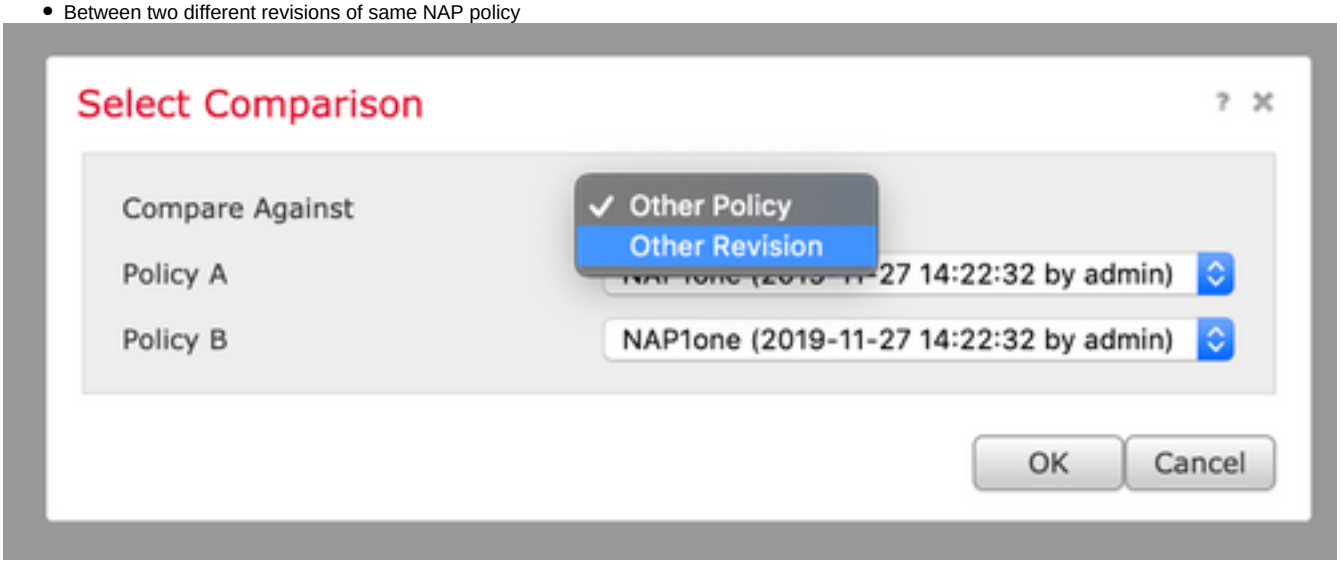
The NAP policies can be compared for changes done and this feature could help in identifying and troubleshooting the issues. In addition, NAP comparison reports could also be generated and exported at the same time.

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:

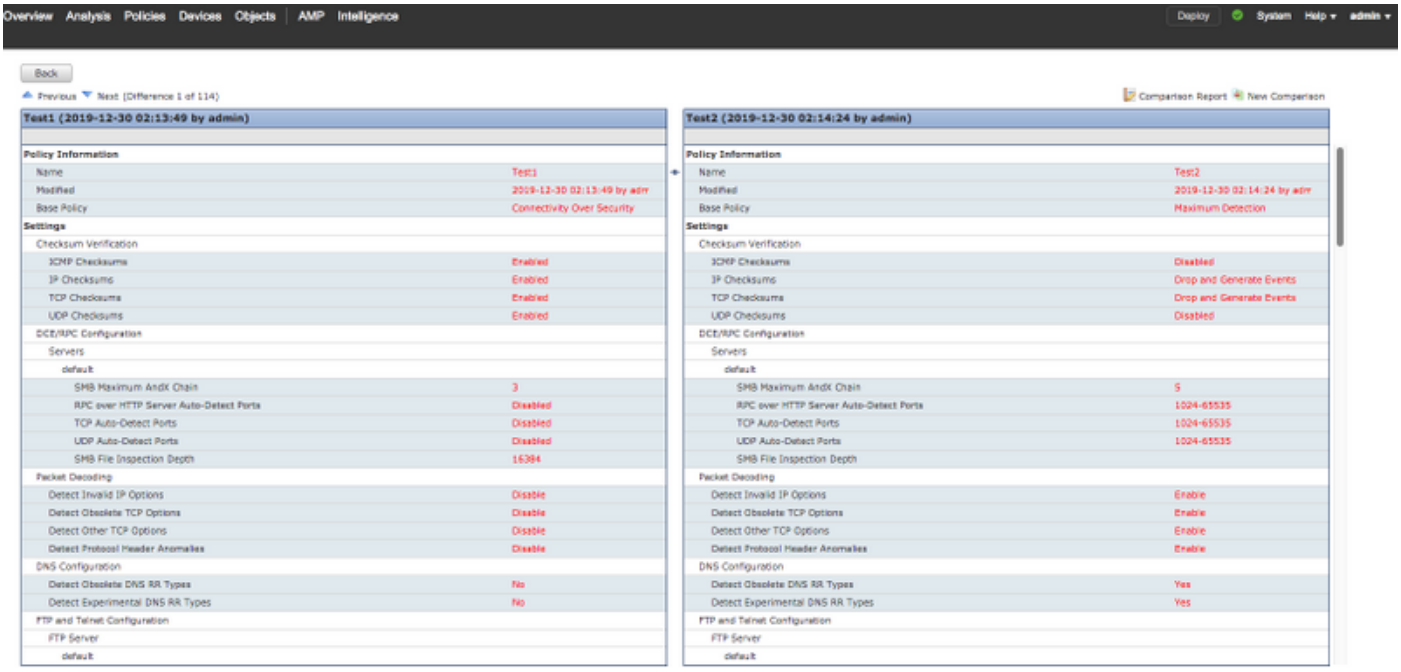


Network Analysis Policy comparison is available in two variants:

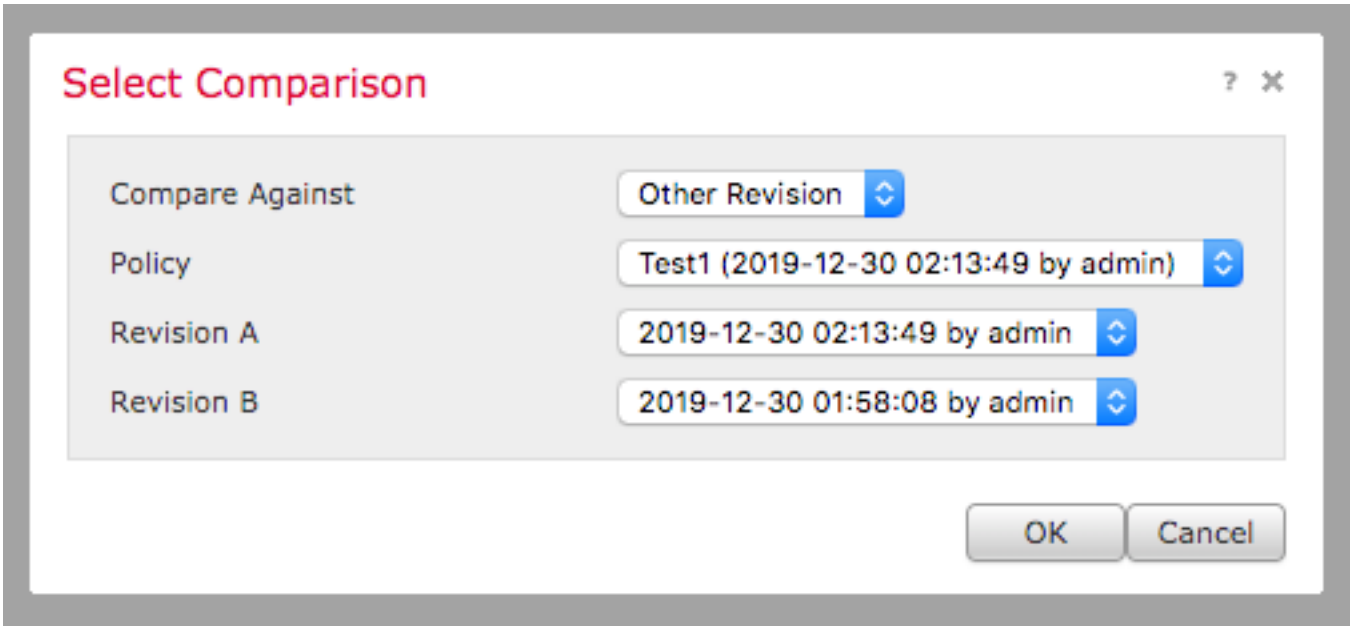
- Between two different NAP policies
- Between two different revisions of same NAP policy

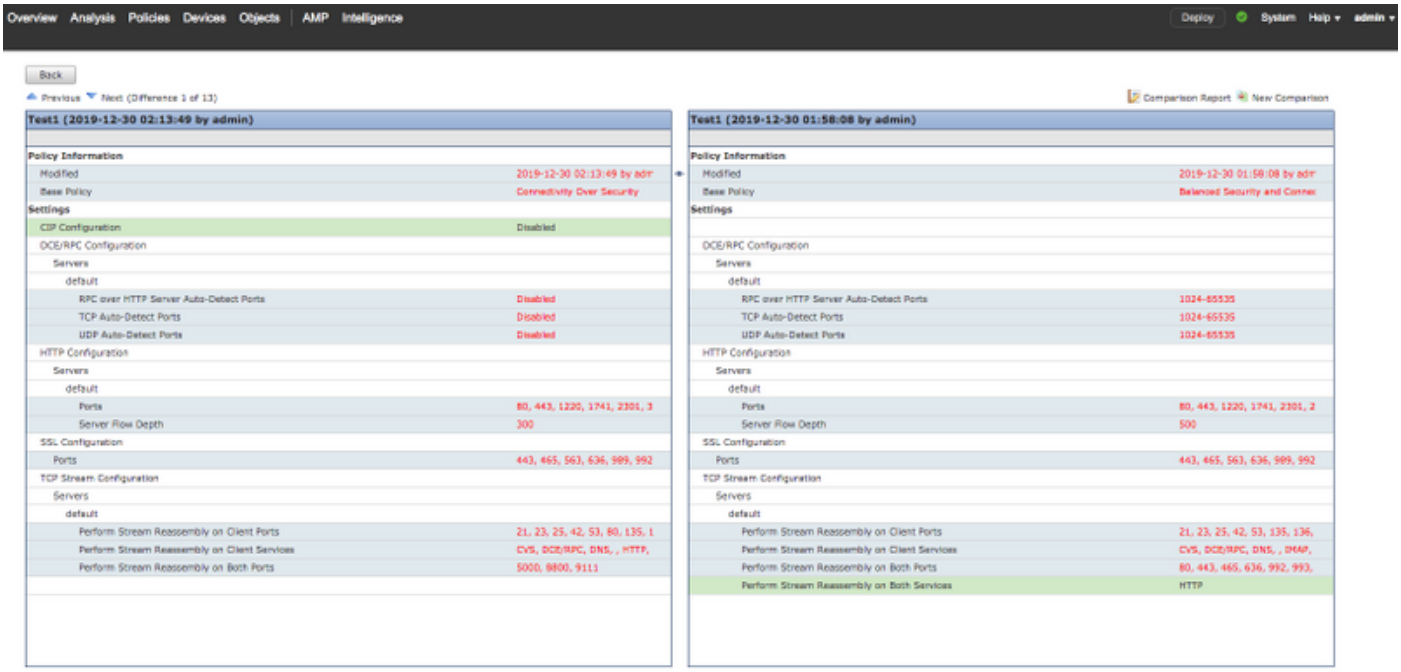


The comparison window provides a comparative line by line comparison between two selected NAP policies and the same can be exported as a report from the **comparison report** tab on the top right, as shown in the image:



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:




Overview Analysis Policies Devices Objects AMP Intelligence
Deploy System Help admin
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 adm
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, 6800, 9111
Test1 (2019-12-30 01:58:08 by admin)
Policy Information
Modified 2019-12-30 01:58:08 by adm
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