Cómo comparar las políticas NAP en los dispositivos Firepower

Contenido

Introducción

Este documento describe cómo comparar diferentes políticas de análisis de red (NAP) para dispositivos de potencia de fuego administrados por Firepower Management Center (FMC).

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Conocimiento del Snort de código abierto
- Firepower Management Center (FMC)
- Firepower Threat Defense (FTD)

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Este artículo se aplica a todas las plataformas Firepower
- Cisco Firepower Threat Defense (FTD) que ejecuta la versión de software 6.4.0
- Firepower Management Center Virtual (FMC), que ejecuta la versión de software 6.4.0

Antecedentes

El Snort utiliza técnicas de coincidencia de patrones para encontrar y evitar ataques de vulnerabilidades en los paquetes de red. Para hacer esto, el motor Snort necesita que los paquetes de red se preparen de tal manera que se pueda hacer esta comparación. Este proceso se lleva a cabo con la ayuda del PAN y puede pasar por las siguientes tres etapas:

- Decodificación
- Normalización
- Preprocesamiento

Una política de análisis de red procesa el paquete en fases: en primer lugar, el sistema decodifica los paquetes a través de las primeras tres capas TCP/IP y, a continuación, continúa con la normalización, el preprocesamiento y la detección de anomalías de protocolo.

Los preprocesadores proporcionan dos funciones principales:

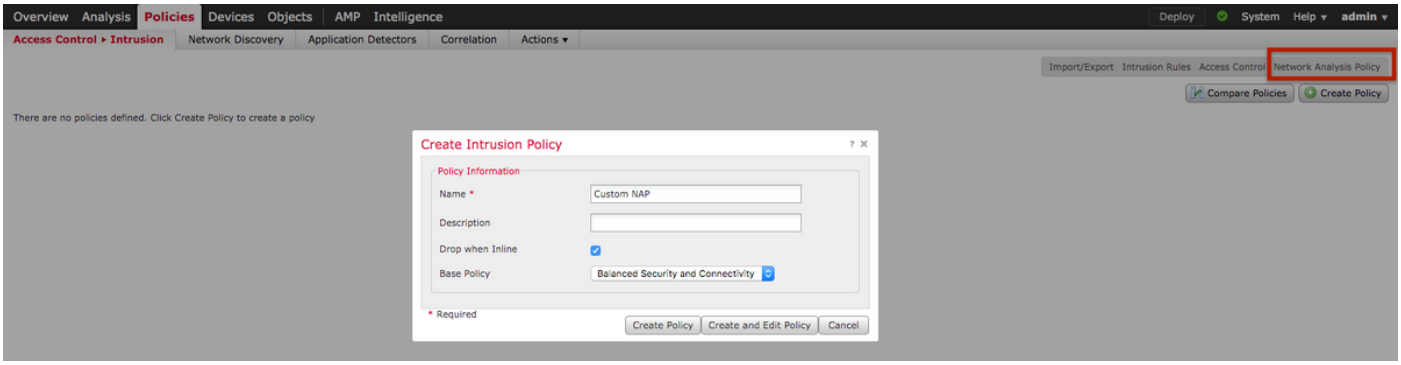
- Normalización del tráfico para una inspección posterior
- Identificación de anomalías en el protocolo

Nota: Algunas reglas de la política de intrusiones requieren ciertas opciones previas al procesador para realizar la detección

Para obtener información sobre el Snort de código abierto, visite https://www.snort.org/

Verificación de la Configuración NAP

Para crear o editar políticas NAP de firepower, navegue hasta **FMC Policies > Access Control > Intrusion,** a continuación haga clic en la opción **Network Analysis Policy en la esquina superior derecha, como se muestra en la imagen:**

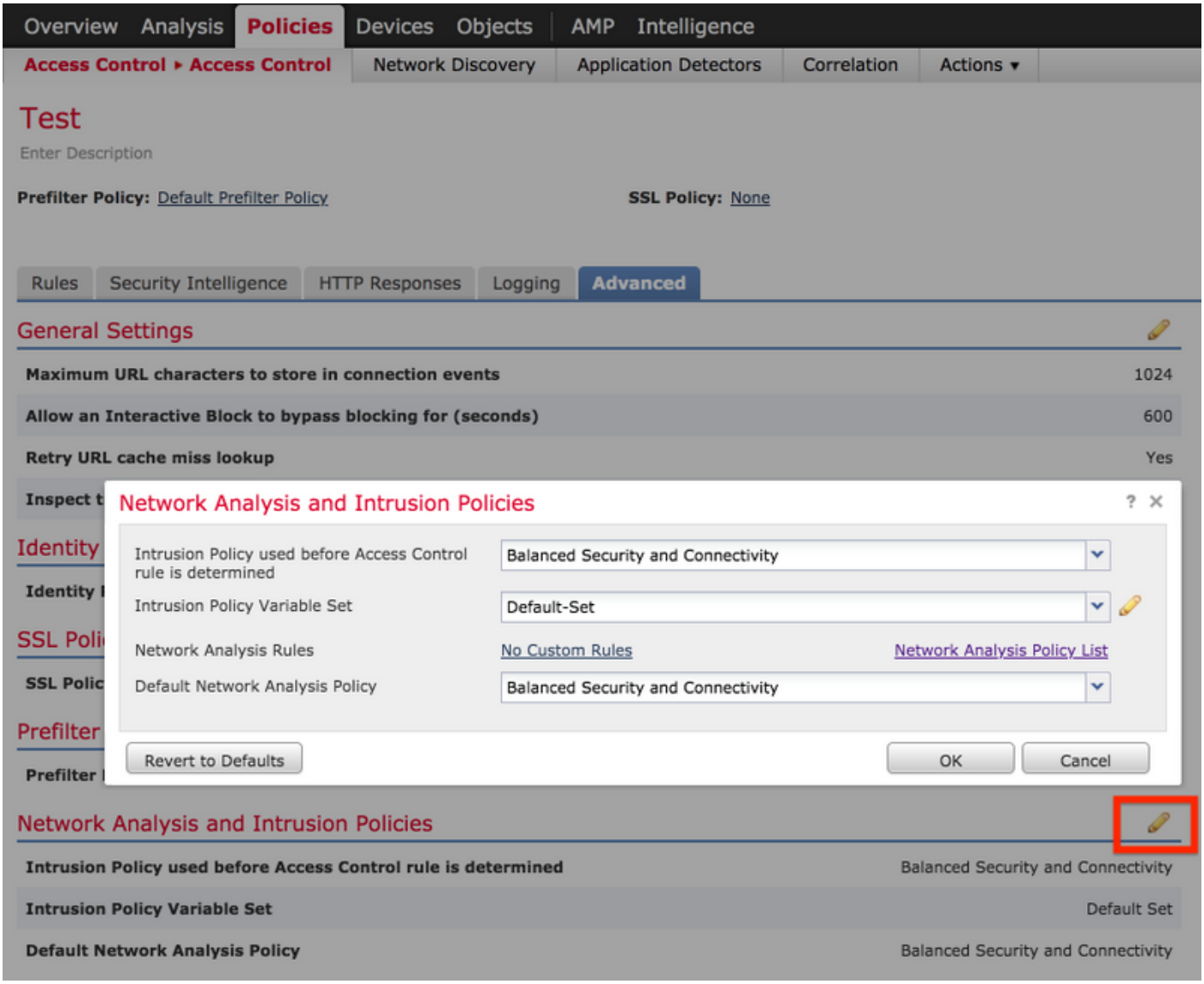


Verificación de la Política de Análisis de Red predeterminada

Compruebe la política predeterminada de análisis de red (NAP) aplicada en la política de control de acceso (ACP)

Navegue hasta **Políticas > Control de acceso** y edite el ACP que desea verificar. Haga clic en la ficha **Avanzadas** y desplácese hacia abajo hasta la sección **Análisis de red y Políticas de intrusión**.

La Política de Análisis de Red Predeterminada asociada con el ACP es **Seguridad y Conectividad Equilibradas,** como se muestra en la imagen**:**

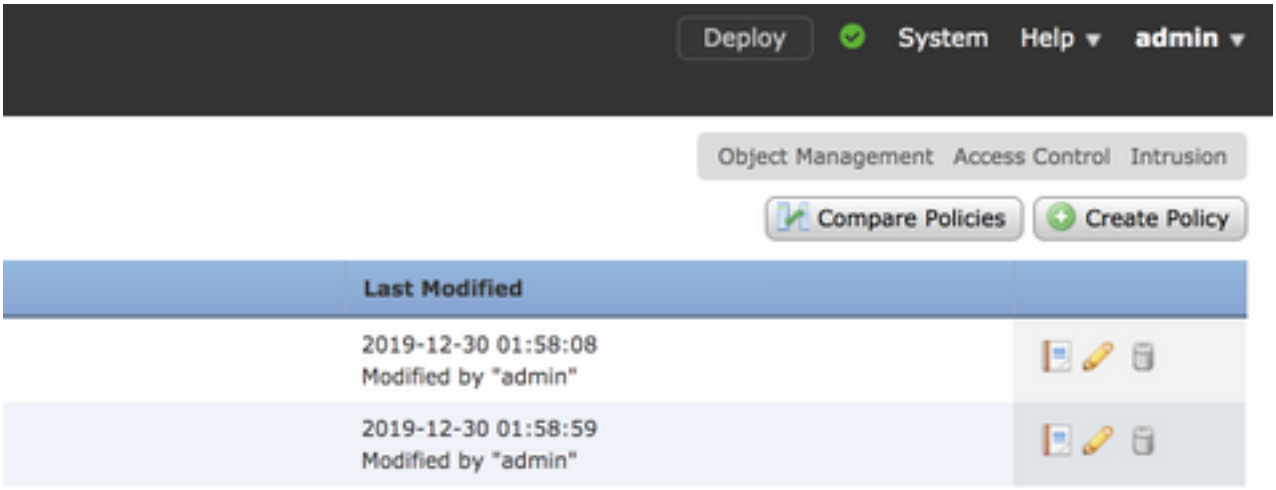


> **Nota:** No confunda la **seguridad equilibrada y la conectividad** para las **políticas de intrusión** y la **seguridad y conectividad equilibradas** para el **análisis de red**. La primera es para las reglas de Snort mientras que la segunda es para el preprocesamiento y la decodificación.

Comparación de la política de análisis de red (NAP)

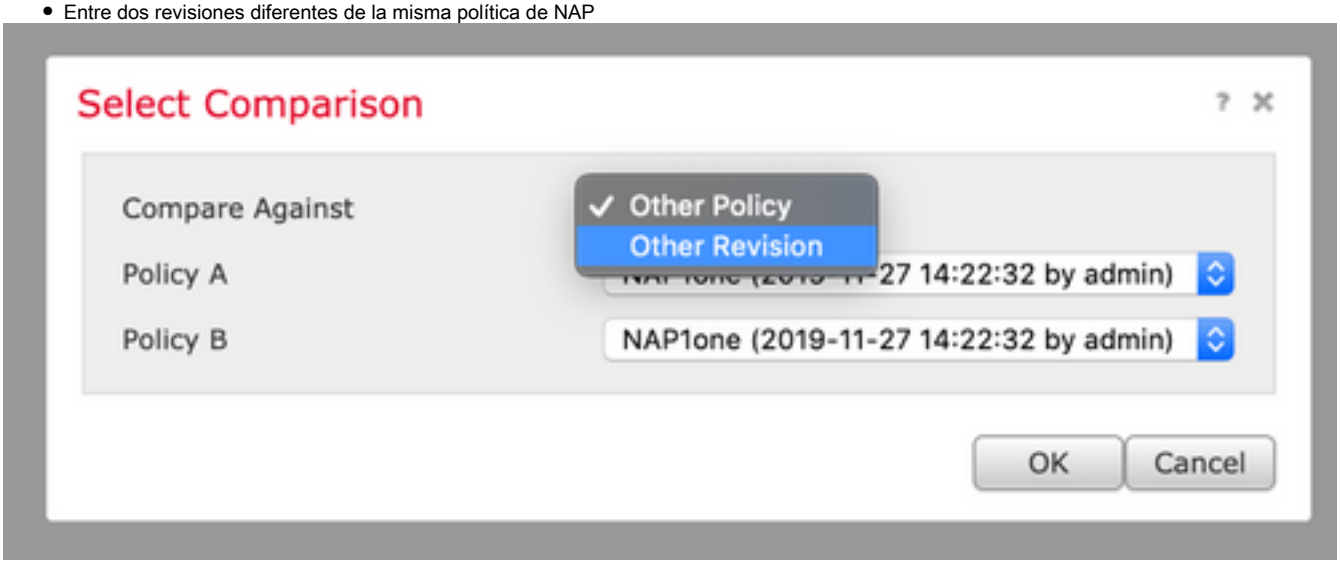
Las políticas de NAP pueden compararse con los cambios realizados y esta función puede ayudar a identificar y solucionar los problemas. Además, los informes de comparación de los PAN también podrían generarse y exportarse al mismo tiempo.

Navegue hasta **Políticas > Control de acceso > Intrusión**. A continuación, haga clic en la opción **Política de análisis de red** en la parte superior derecha. En la página de políticas NAP puede ver la pestaña **Comparar políticas** en la parte superior derecha, como se muestra en la imagen:

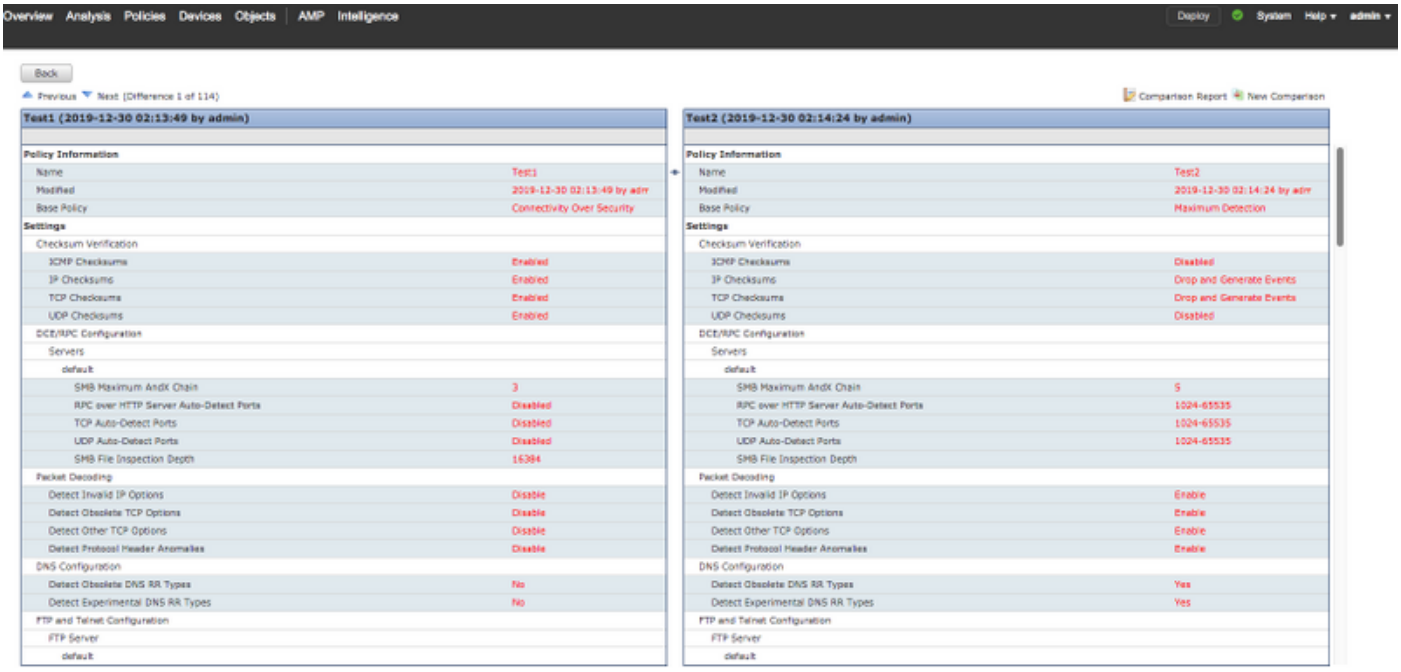


La comparación de la política de análisis de red está disponible en dos variantes:

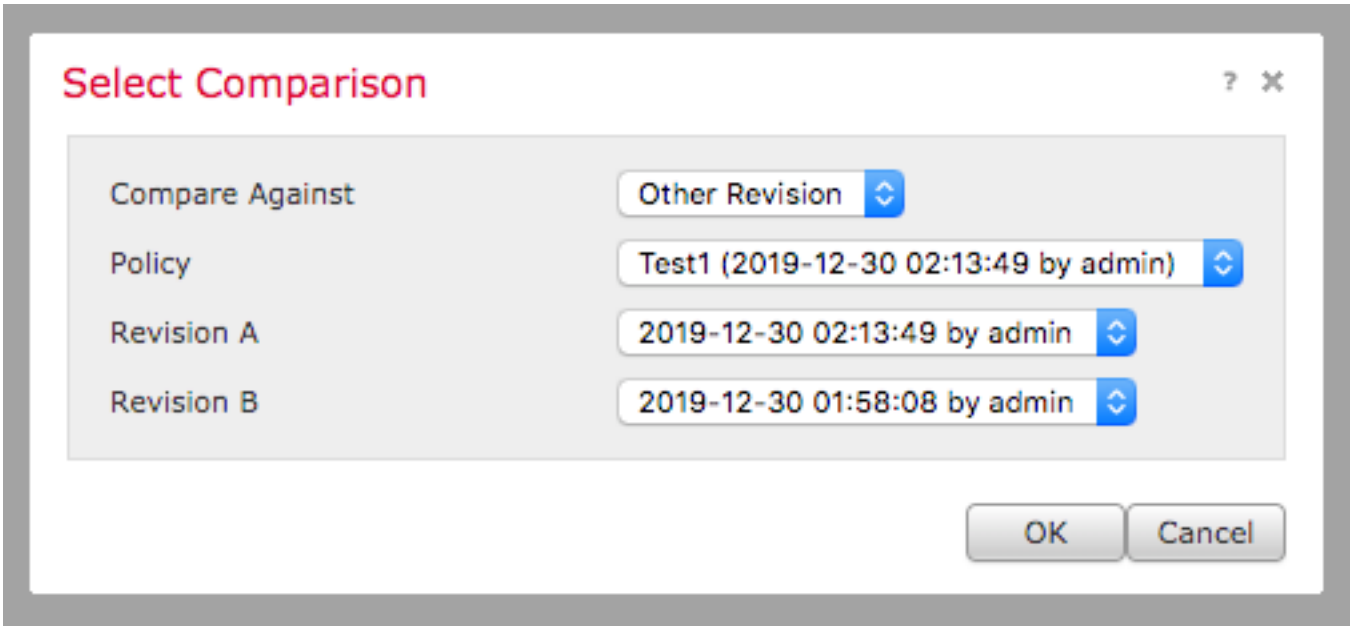
- Entre dos políticas NAP diferentes
- Entre dos revisiones diferentes de la misma política de NAP

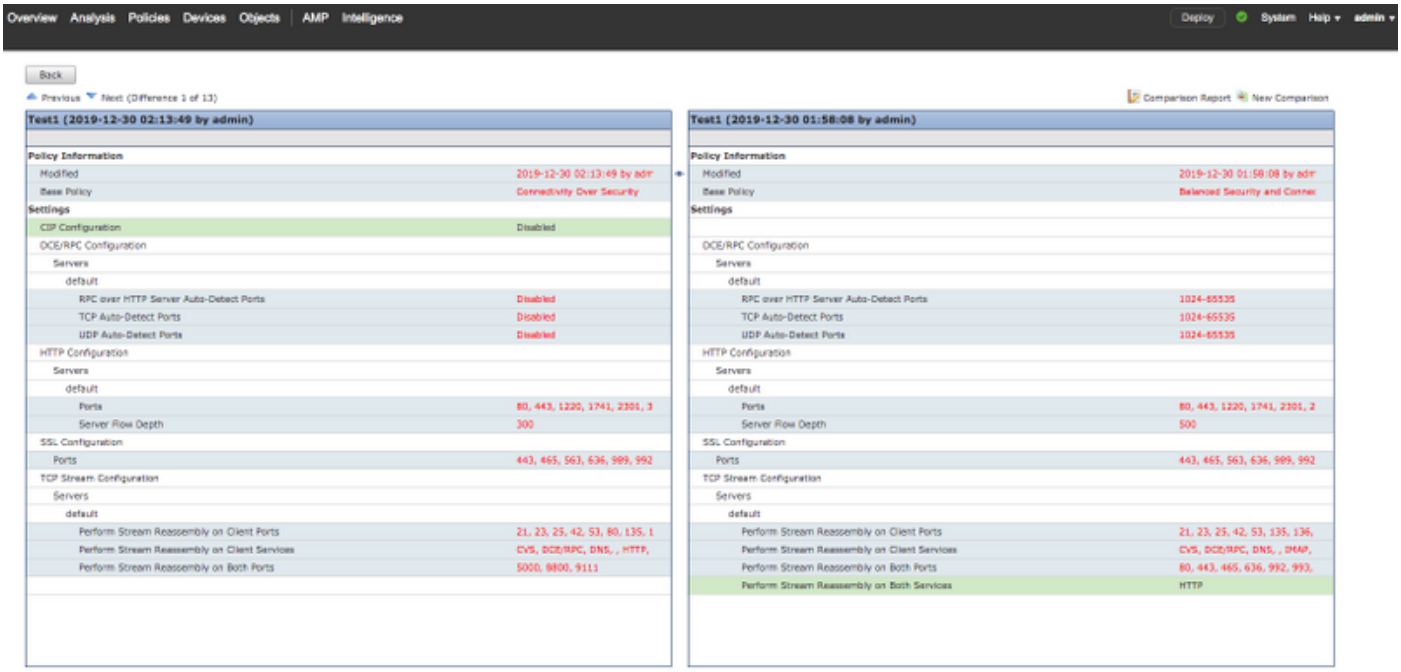


La ventana de comparación proporciona una comparación de línea por línea entre dos políticas NAP seleccionadas y las mismas se pueden exportar como un informe desde la pestaña **informe de comparación** en la parte superior derecha, como se muestra en la imagen:



Para la comparación entre dos versiones de la misma política NAP, la opción de revisión puede elegirse para seleccionar el **id de revisión** requerido, como se muestra en la imagen:




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