Comment comparer des stratégies de PETIT SOMME sur des périphériques de FirePOWER

Contenu

Introduction

Ce document décrit comment comparer différentes stratégies d'analyse réseau (PETIT SOMME) pour des périphériques de firePOWER gérés par le centre de Gestion de FirePOWER (FMC).

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- La connaissance de l'open-source reniflent
- Centre de Gestion de FirePOWER (FMC)
- Défense contre des menaces de FirePOWER (FTD)

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Cet article s'applique à toutes les Plateformes de FirePOWER
- Défense contre des menaces de Cisco FirePOWER (FTD) qui exécute la version de logiciel 6.4.0
- Centre de Gestion de FirePOWER virtuel (FMC) qui exécute la version de logiciel 6.4.0

Informations générales

Le renifler emploie des techniques de filtrage pour trouver et empêcher des exploits dans des paquets du réseau. Afin de faire ceci, l'engine de renifler a besoin de paquets du réseau pour être préparés de telle manière que cette comparaison puisse être faite. Ce processus est fait avec l'aide du PETIT SOMME et peut subir les trois étapes suivantes :

- Décoder
- Normalisation
- Prétraitement

Une stratégie d'analyse réseau traite le paquet en quelques phases : d'abord le système décode des paquets par les trois premières couches TCP/IP, puis continue normaliser, prétraiter, et détecter des anomalies de protocole.

Les préprocesseurs fournissent la fonctionnalité de deux canalisations :

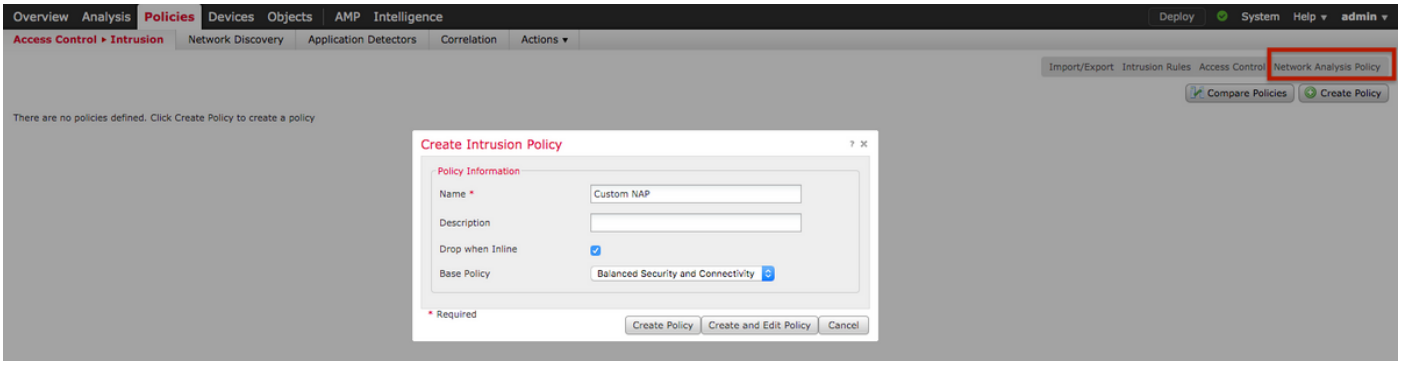
- Normalisation du trafic pour davantage d'inspection
- Identifiez les anomalies de protocole

> Remarque: Quelques règles de stratégie d'intrusion exigent de certaines options de préprocesseur afin d'exécuter la détection

Pour les informations sur l'open-source reniflez, veuillez visitent https://www.snort.org/

Vérifiez la configuration de PETIT SOMME

Pour créer ou éditer des stratégies de PETIT SOMME de firePOWER, naviguez vers les **stratégies FMC > le contrôle d'accès > l'intrusion,** cliquent sur ensuite l'option de **stratégie d'analyse réseau** dans le coin haut droit, suivant les indications de l'image :

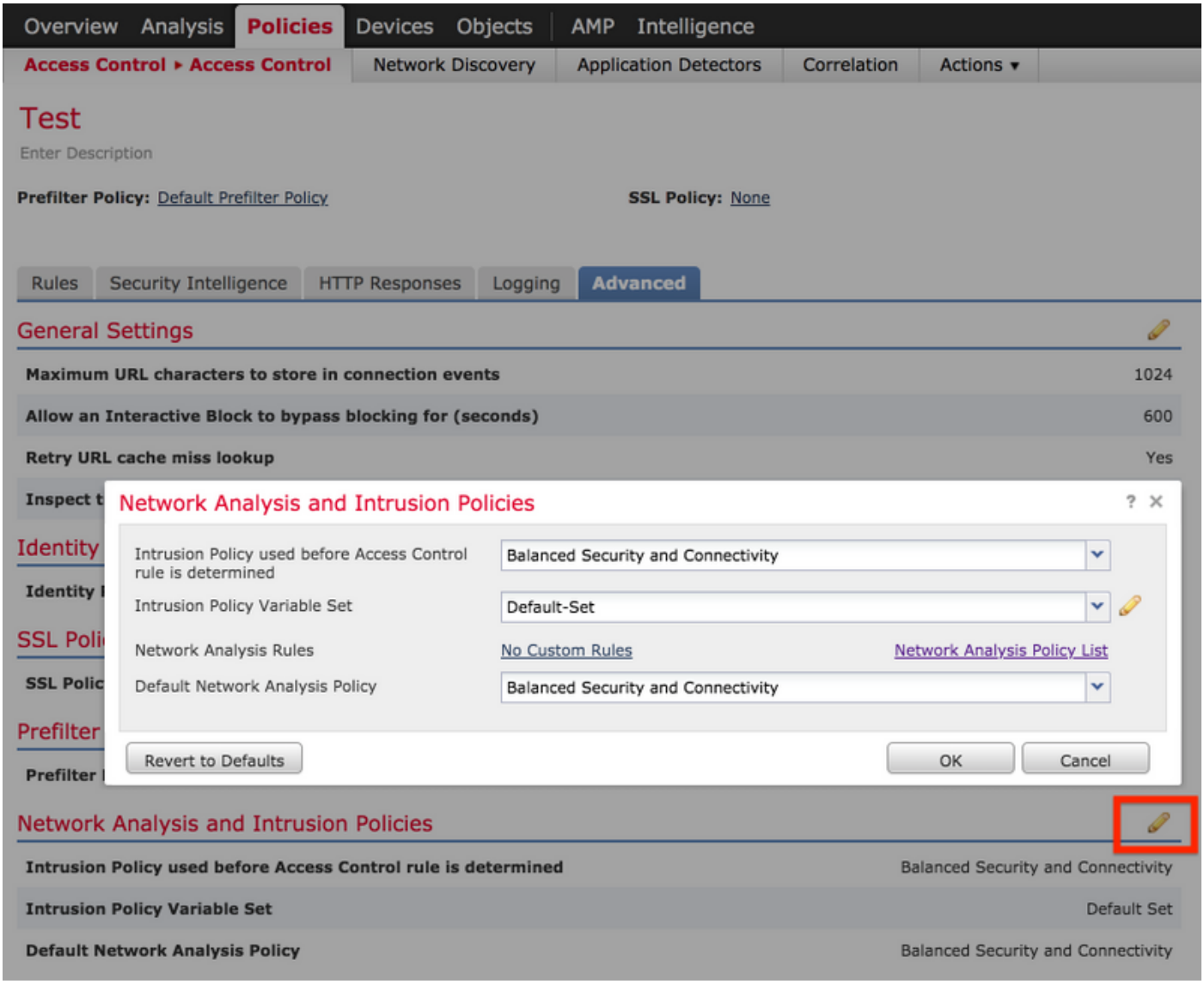


Vérifier la stratégie par défaut d'analyse réseau

Vérifiez la stratégie par défaut d'analyse réseau (PETIT SOMME) appliquée sur la stratégie de contrôle d'accès (l'ACP)

Naviguez vers les **stratégies > le contrôle d'accès** et éditez l'ACP que vous voulez vérifier. Cliquez sur l'**onglet Avancé** et le faites descendre l'écran à l'**analyse réseau et à la** section de **stratégies d'intrusion**.

La stratégie par défaut d'analyse réseau associée avec l'ACP est **Sécurité et Connectivité équilibrées,** suivant les indications de l'image **:**

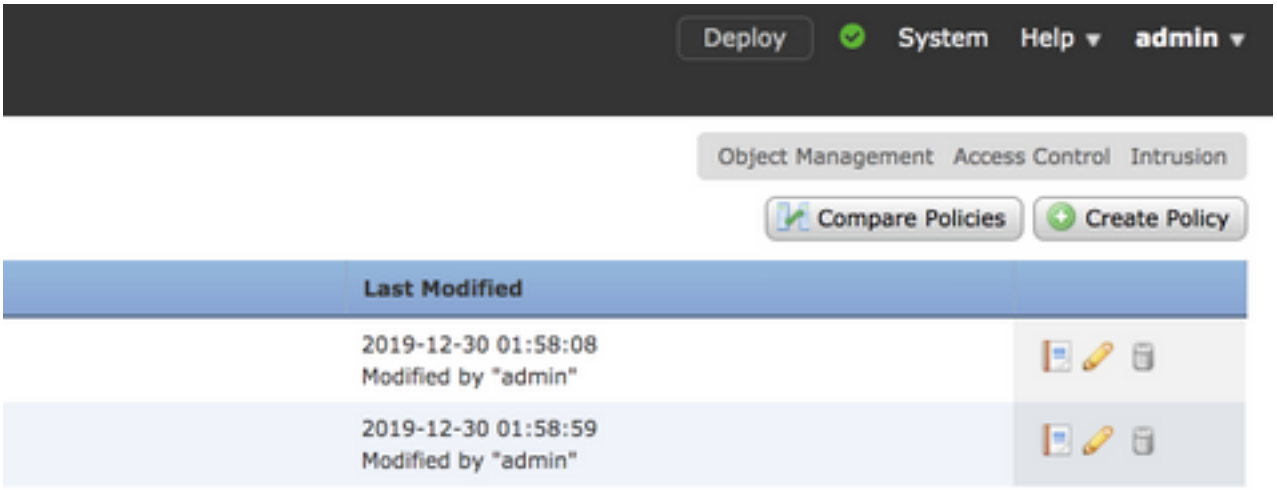


> Remarque: Ne confondez pas la **Sécurité et la Connectivité équilibrées** pour des **stratégies d'intrusion** et la **Sécurité et la Connectivité équilibrées** pour l'**analyse réseau**. L'ancien est pour des règles Snort tandis que ce dernier est pour prétraiter et décoder.

Comparez la stratégie d'analyse réseau (le PETIT SOMME)

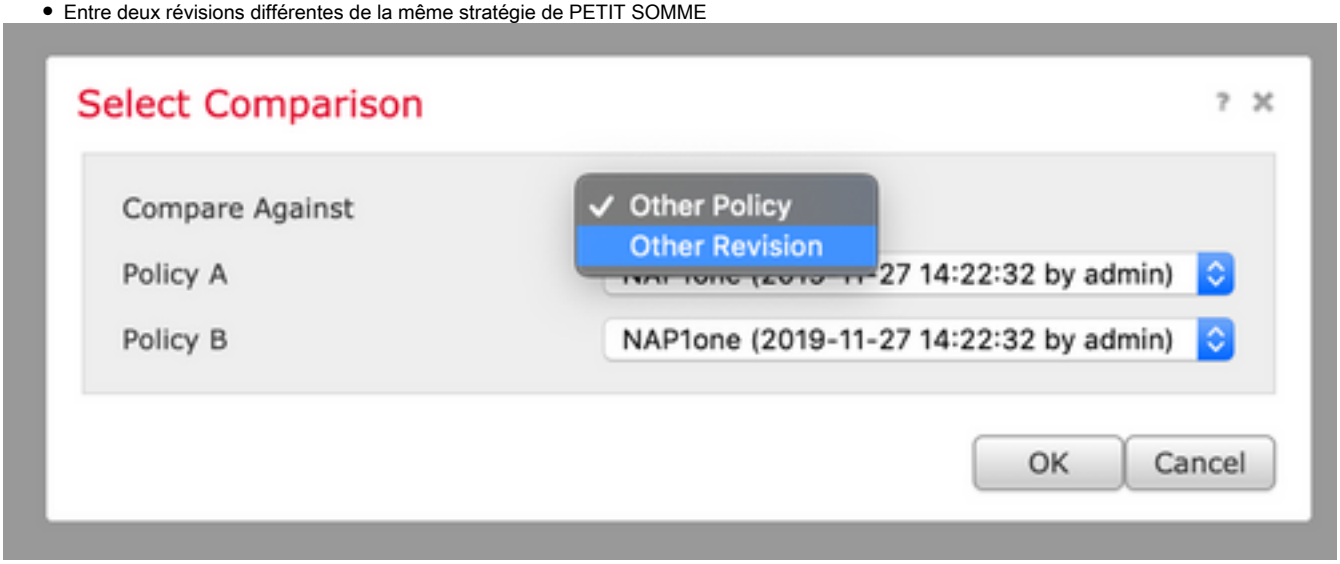
Les stratégies de PETIT SOMME peuvent être comparées pour des modifications faites et cette caractéristique pourrait aider en identifiant et en dépannant les questions. En outre, des états de comparaison de PETIT SOMME ont pu également être générés et exportés en même temps.

Naviguez vers les **stratégies > le contrôle d'accès > l'intrusion**. Puis, option de **stratégie d'analyse réseau de** clic dans l'en haut à droite. Sous la page de stratégie de PETIT SOMME vous pouvez voir **pour comparer l'**onglet de **stratégies du** côté en haut à droite, suivant les indications de l'image :

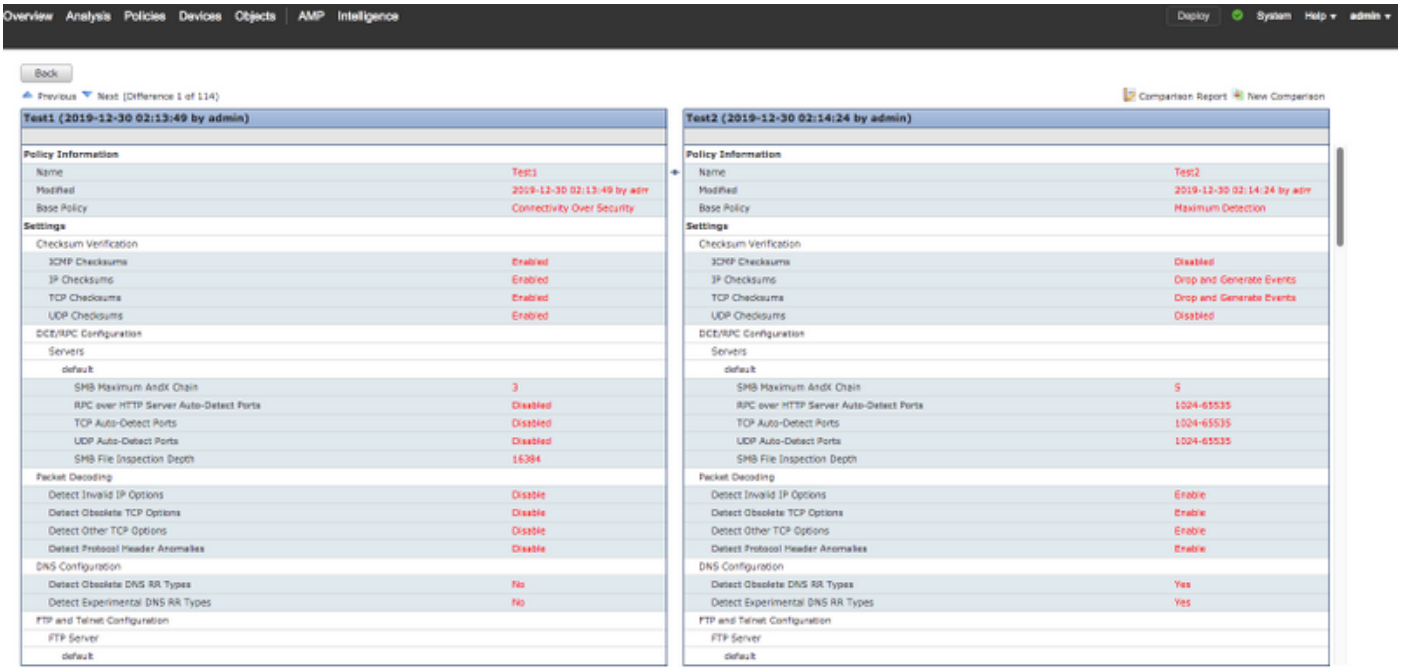


La comparaison de stratégie d'analyse réseau est disponible dans deux variantes :

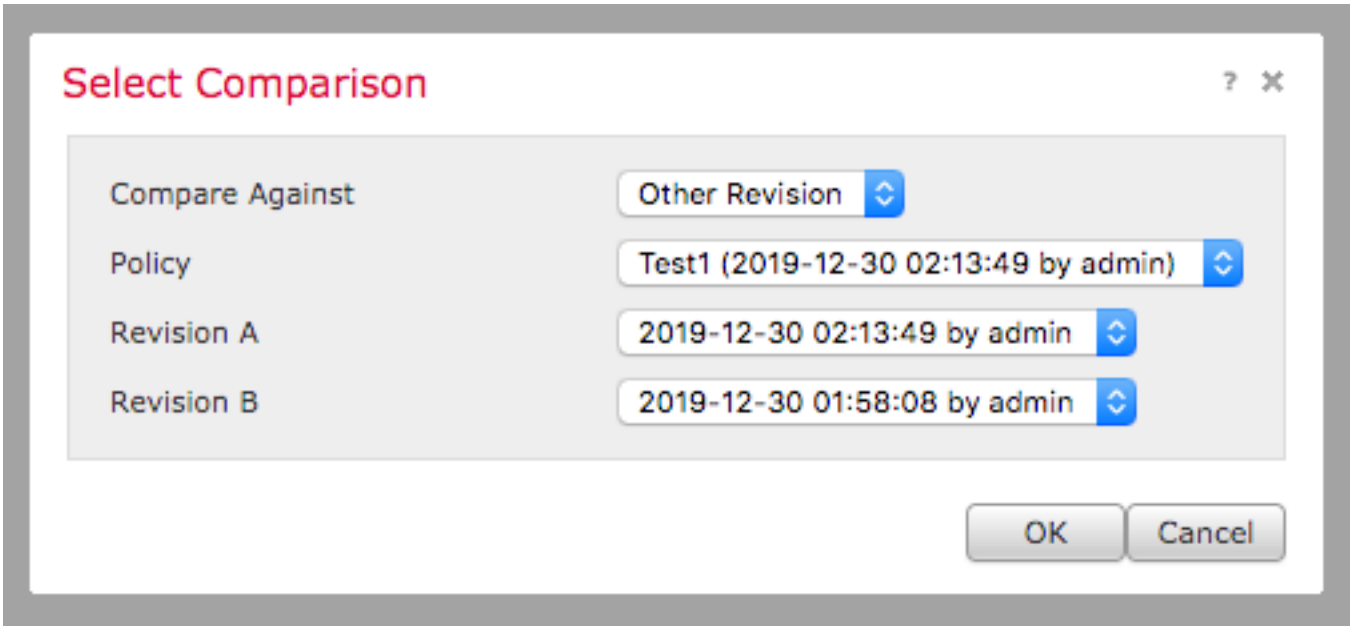
- Entre deux stratégies différentes de PETIT SOMME
- Entre deux révisions différentes de la même stratégie de PETIT SOMME

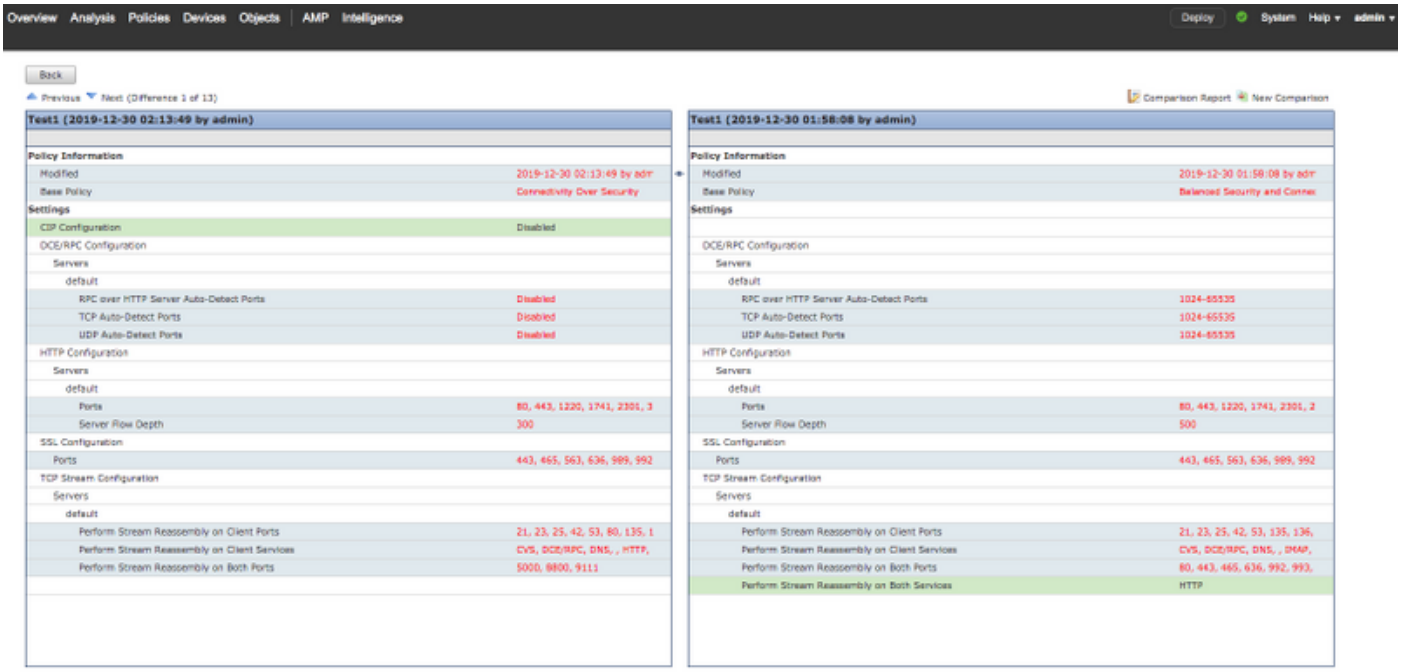


La fenêtre de comparaison fournit une comparaison ligne par ligne comparative entre deux stratégies sélectionnées de PETIT SOMME et la même chose peut être exporté qu'un état de l'onglet d'**état de comparaison** du côté droit l'en haut à droite, suivant les indications de l'image :



Pour la comparaison entre deux versions de la même stratégie de PETIT SOMME, l'option de révision peut être choisie pour sélectionner l'**id** exigé de **révision**, suivant les indications de l'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