Comment comparer les stratégies NAP sur les périphériques Firepower

Contenu

Introduction

Ce document décrit comment comparer différentes stratégies d'analyse de réseau (NAP) pour les périphériques Firepower gérés par Firepower Management Center (FMC).

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Connaissance de Snort open source
- Firepower Management Center (FMC)
- Firepower Threat Defense (FTD)

Components Used

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

- Cet article s'applique à toutes les plates-formes Firepower
- Cisco Firepower Threat Defense (FTD) qui exécute la version 6.4.0 du logiciel
- Firepower Management Center Virtual (FMC) qui exécute le logiciel version 6.4.0

Informations générales

Le Snort utilise des techniques de mise en correspondance de modèles pour détecter et empêcher les exploits dans les paquets réseau. Pour ce faire, le moteur Snort a besoin que les paquets réseau soient préparés de manière à pouvoir effectuer cette comparaison. Ce processus est effectué à l'aide du PAN et peut se dérouler en trois étapes :

- Décodage
- Normalisation
- Prétraitement

Une politique d'analyse du réseau traite les paquets par phases : d'abord, le système décode les paquets à travers les trois premières couches TCP/IP, puis poursuit la normalisation, le prétraitement et la détection des anomalies de protocole.

Les préprocesseurs offrent deux fonctionnalités principales :

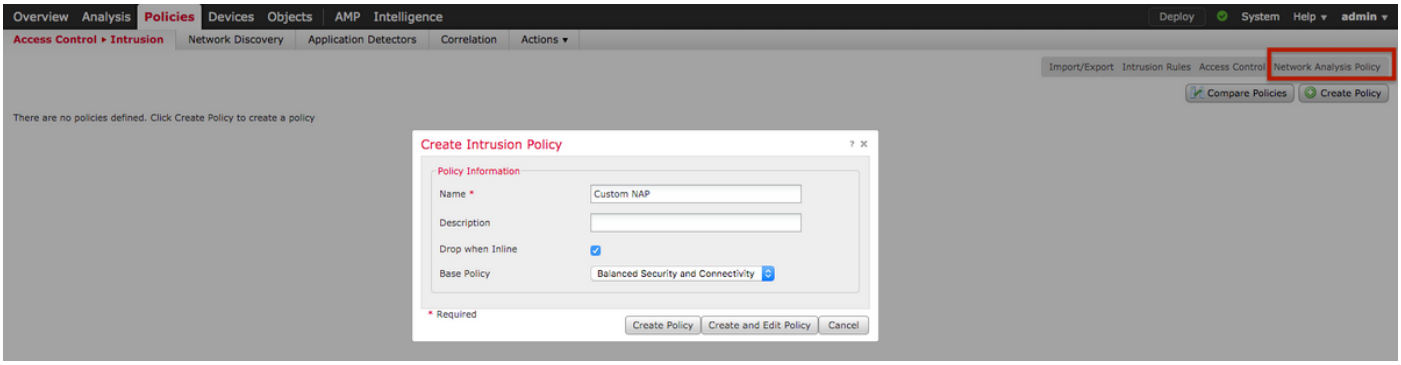
- Normalisation du trafic pour une inspection plus poussée
- Identifier les anomalies de protocole

Remarque : Certaines règles de stratégie d'intrusion nécessitent certaines options de préprocesseur pour effectuer la détection

Pour plus d'informations sur Snort open-source, visitez https://www.snort.org/

Vérifier la configuration NAP

Pour créer ou modifier des stratégies NAP Firepower, accédez à **Stratégies FMC > Contrôle d'accès > Intrusion,** puis cliquez sur l'option Stratégie d'**analyse du réseau** dans le coin supérieur droit, comme illustré dans l'image :

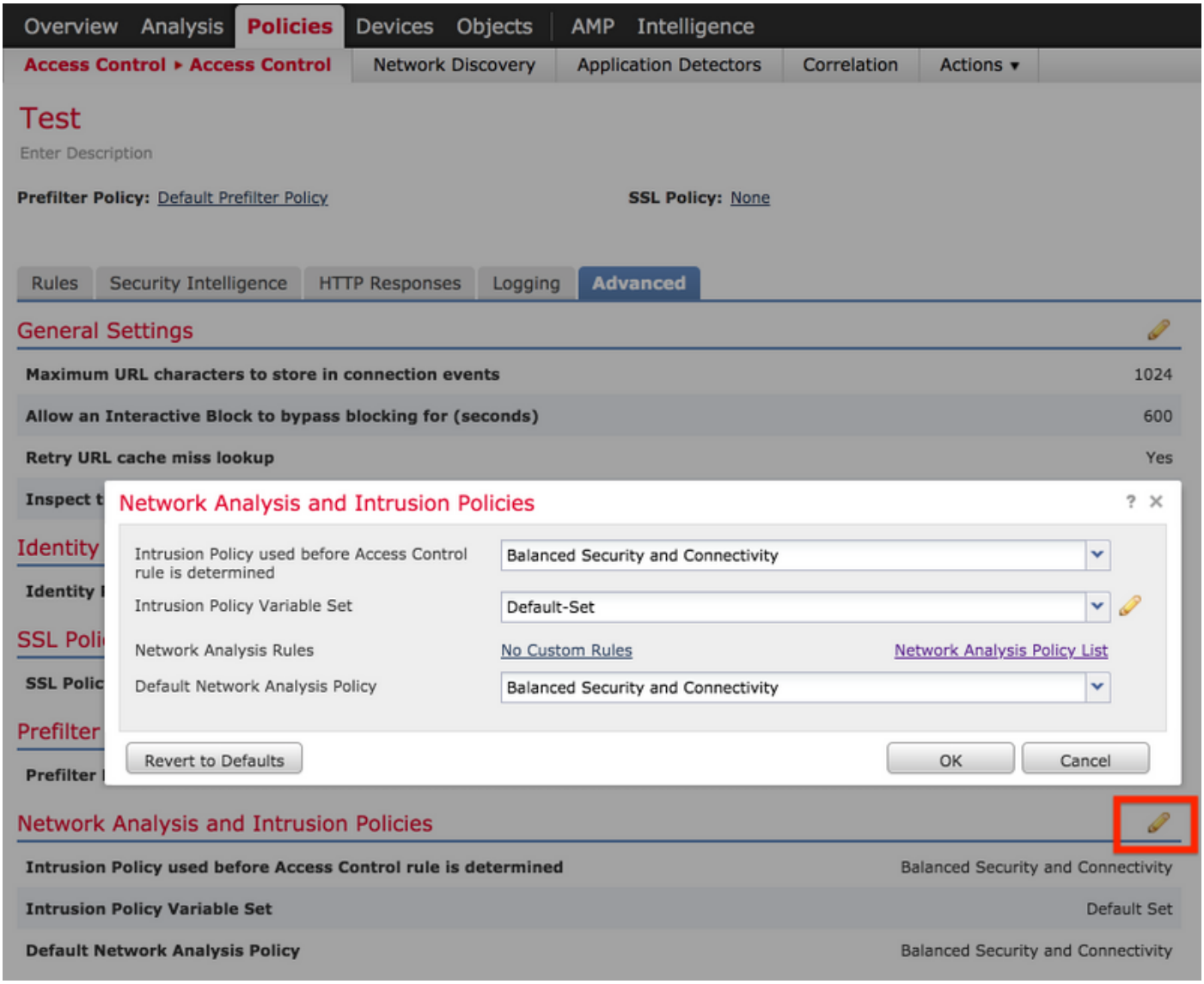


Vérification de la stratégie d'analyse réseau par défaut

Vérifier la stratégie NAP (Network Analysis) par défaut appliquée à la stratégie de contrôle d'accès (ACP)

Accédez à **Stratégies > Contrôle d'accès** et modifiez le PVA que vous voulez vérifier. Cliquez sur l'onglet **Avancé** et faites défiler jusqu'à la section **Analyse du réseau et stratégies d'intrusion**.

La stratégie d'analyse de réseau par défaut associée à l'ACP est **Sécurité et connectivité équilibrées,** comme le montre l'image **:**

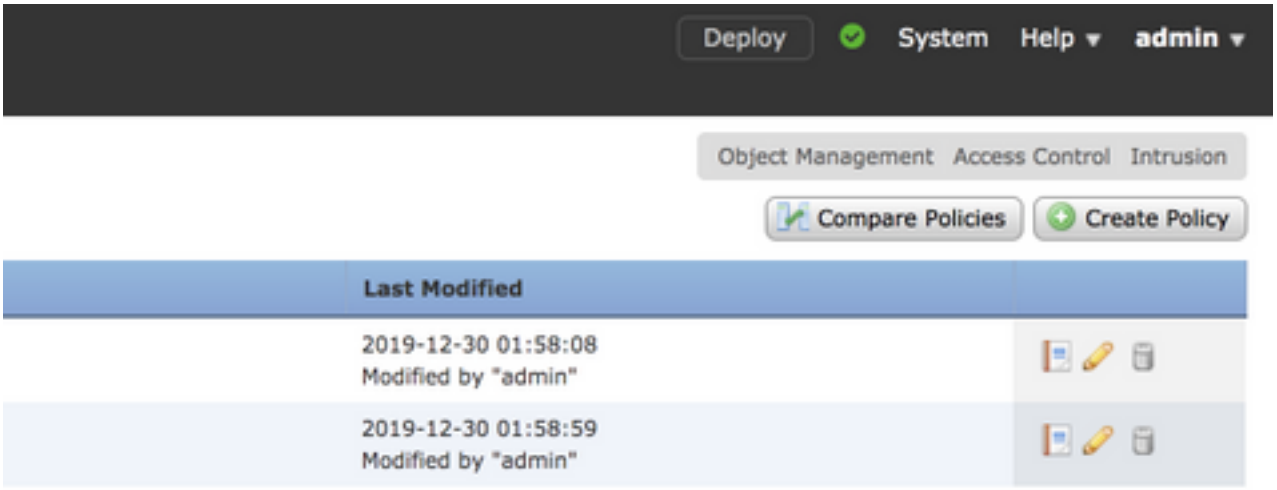


> **Note**: Ne confondez pas la **sécurité et la connectivité équilibrées** pour les **politiques d'intrusion** et la **sécurité et la connectivité équilibrées** pour l'**analyse du réseau**. Le premier concerne les règles Snort, tandis que le second concerne le prétraitement et le décodage.

Comparer la stratégie d'analyse de réseau (NAP)

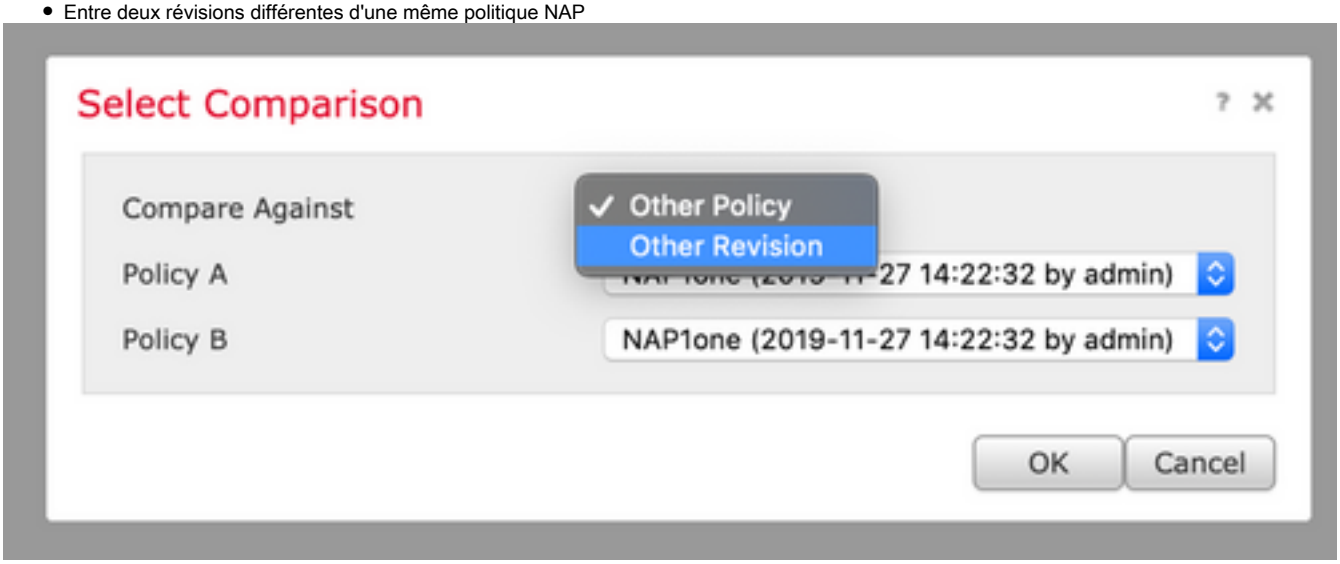
Les stratégies NAP peuvent être comparées pour les modifications effectuées et cette fonctionnalité peut aider à identifier et à résoudre les problèmes. En outre, des rapports de comparaison des PAN pourraient également être générés et exportés en même temps.

Accédez à **Politiques > Contrôle d'accès > Intrusion**. Cliquez ensuite sur l'option **Stratégie d'analyse réseau** en haut à droite. Sous la page Stratégie NAP, vous pouvez voir l'onglet **Comparer les stratégies** en haut à droite, comme l'illustre l'image :

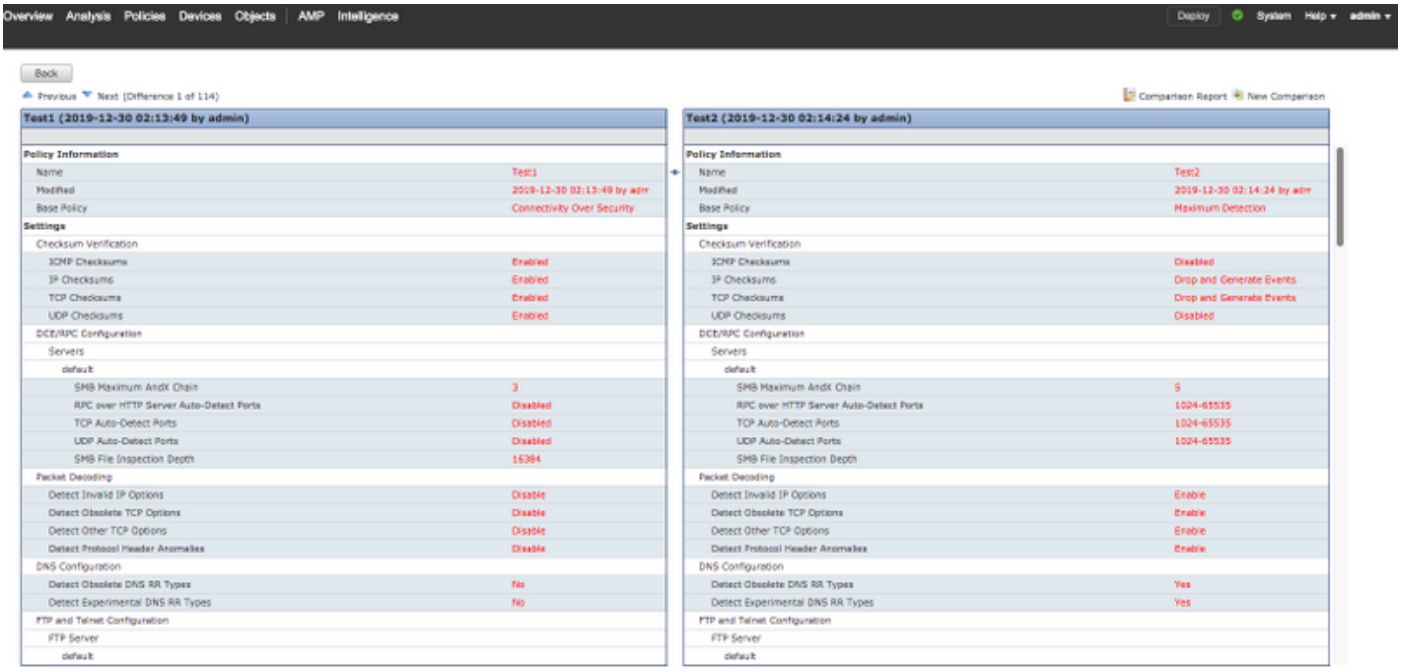


La comparaison des stratégies d'analyse du réseau est disponible en deux variantes :

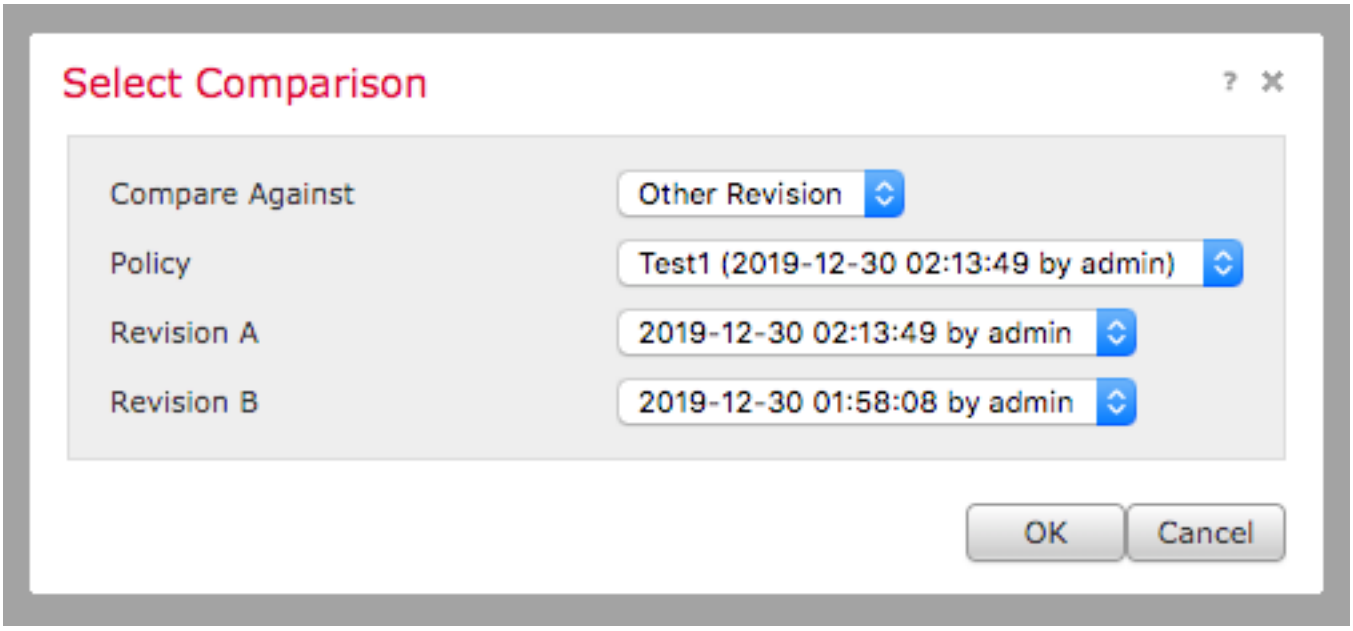
- Entre deux stratégies NAP différentes
- Entre deux révisions différentes d'une même politique NAP

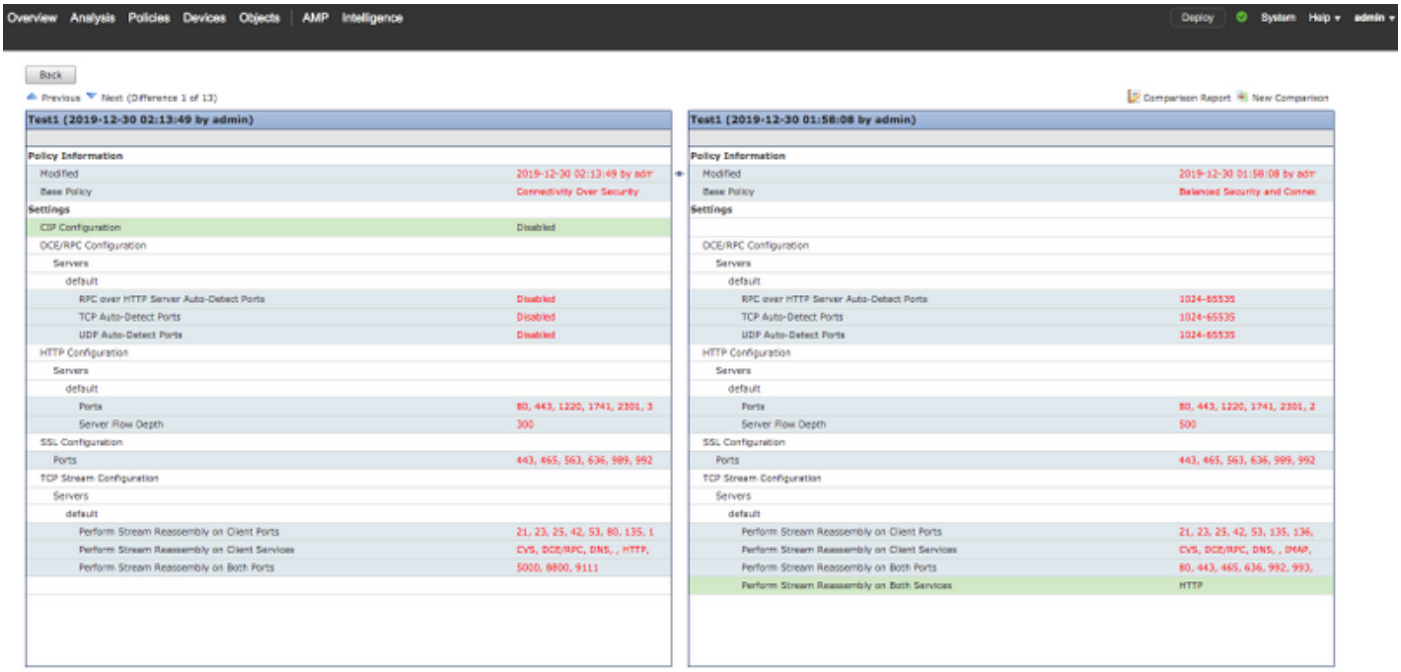


La fenêtre de comparaison fournit une comparaison ligne par ligne entre deux stratégies NAP sélectionnées et la même peut être exportée en tant que rapport à partir de l'onglet **rapport de comparaison** en haut à droite, comme illustré dans l'image :



Pour la comparaison entre deux versions de la même stratégie NAP, l'option de révision peut être sélectionnée pour sélectionner l'**ID de révision** requis, comme indiqué dans 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