Como comparar as políticas de NAP em dispositivos Firepower

Contents

Introduction

Este documento descreve como comparar diferentes políticas de análise de rede **(**NAP) para dispositivos firepower gerenciados pelo Firepower Management Center (FMC).

Prerequisites

Requirements

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Conhecimento do Snort de código aberto
- Firepower Management Center (FMC)
- Firepower Threat Defense (FTD)

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- Este artigo se aplica a todas as plataformas Firepower
- Cisco Firepower Threat Defense (FTD), que executa a versão de software 6.4.0
- Firepower Management Center Virtual (FMC) que executa a versão de software 6.4.0

Informações de Apoio

O Snort usa técnicas de correspondência de padrões para localizar e impedir explorações em pacotes de rede. Para fazer isso, o mecanismo Snort precisa que os pacotes de rede sejam preparados de forma que essa comparação possa ser feita. Esse processo é feito com o auxílio do NAP e pode passar pelas três etapas a seguir:

- Decodificação
- Normalizando
- Pré-processamento

Uma política de análise de rede processa o pacote em fases: primeiro, o sistema decodifica pacotes através das três primeiras camadas TCP/IP e, em seguida, continua com a normalização, o pré-processamento e a detecção de anomalias de protocolo.

Os pré-processadores oferecem duas funcionalidades principais:

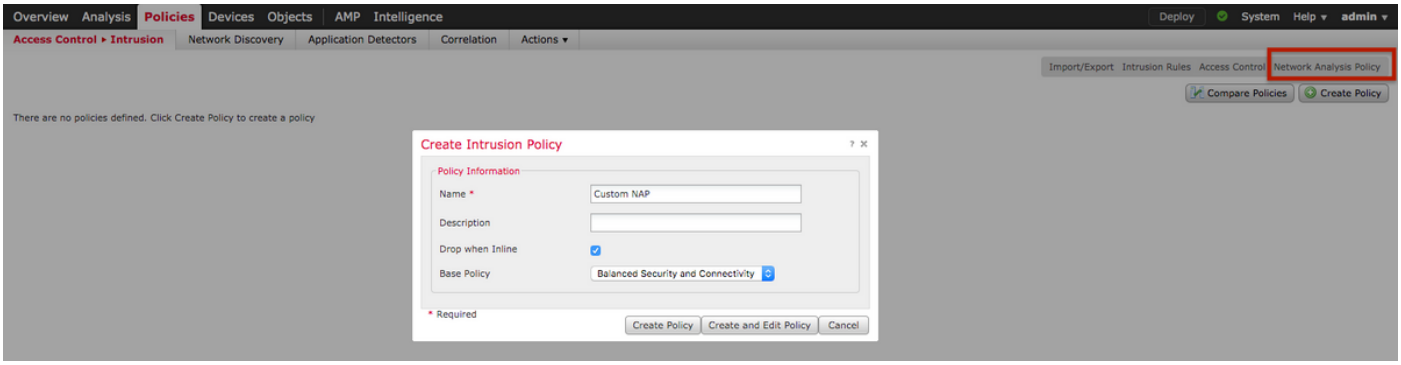
- Normalização do tráfego para inspeção posterior
- Identificar anomalias de protocolo

Nota: Algumas regras de política de intrusão exigem determinadas opções de pré-processador para executar a detecção

Para obter informações sobre o Snort de código aberto, visite https://www.snort.org/

Verificar a configuração do NAP

Para criar ou editar políticas NAP do firepower, navegue até **FMC Policies > Access Control > Intrusion,** depois clique na opção **Network Analysis Policy** no canto superior direito, como mostrado na imagem:

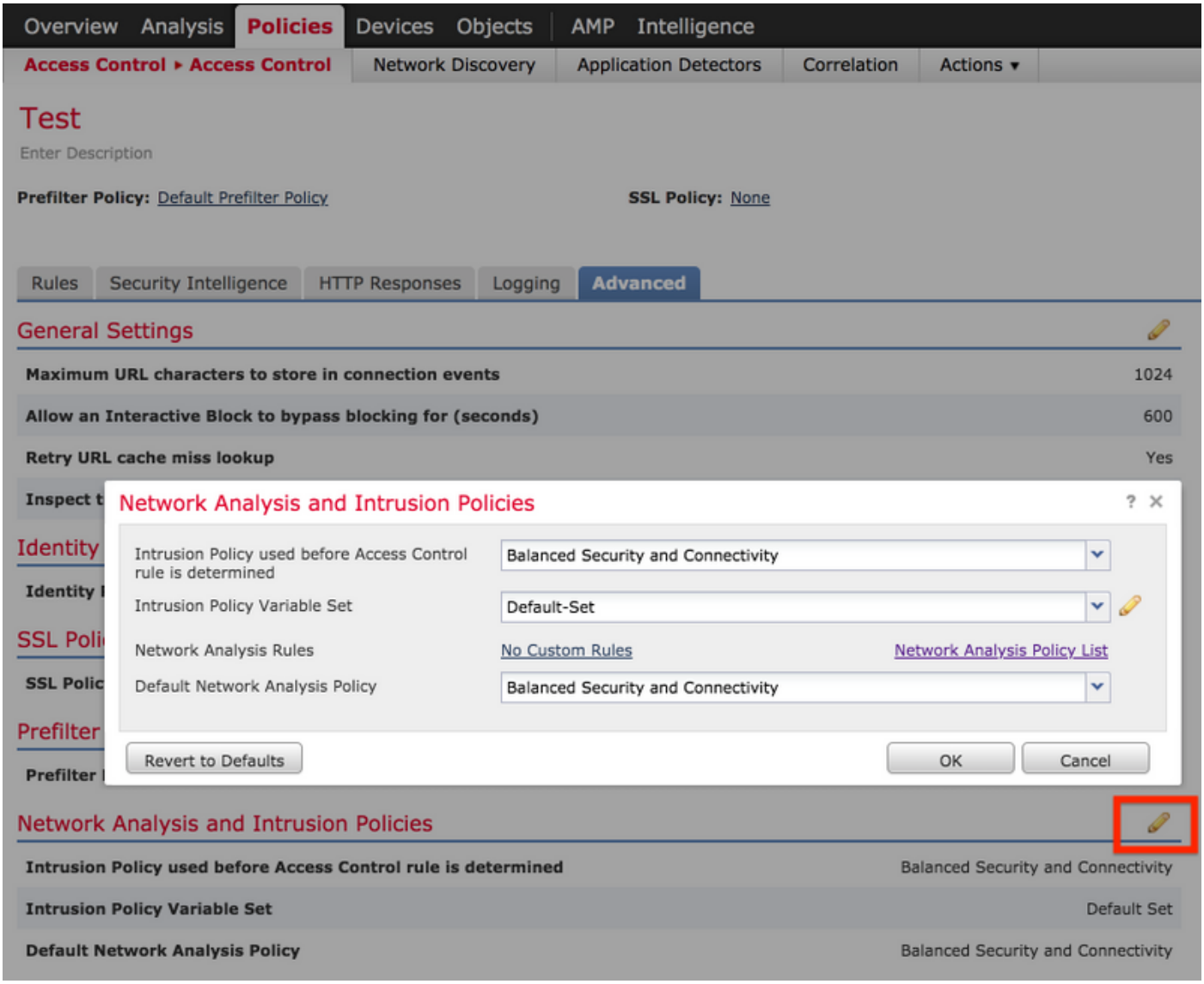


Verificando a política de análise de rede padrão

Verifique a política de análise de rede (NAP) padrão aplicada na política de controle de acesso (ACP)

Navegue até **Políticas > Controle de acesso** e edite o ACP que deseja verificar. Clique na guia **Avançado** e role para baixo até a seção **Análise de rede e políticas de intrusão**.

A política de análise de rede padrão associada ao ACP é a **segurança e a conectividade equilibradas,** como mostrado na imagem**:**

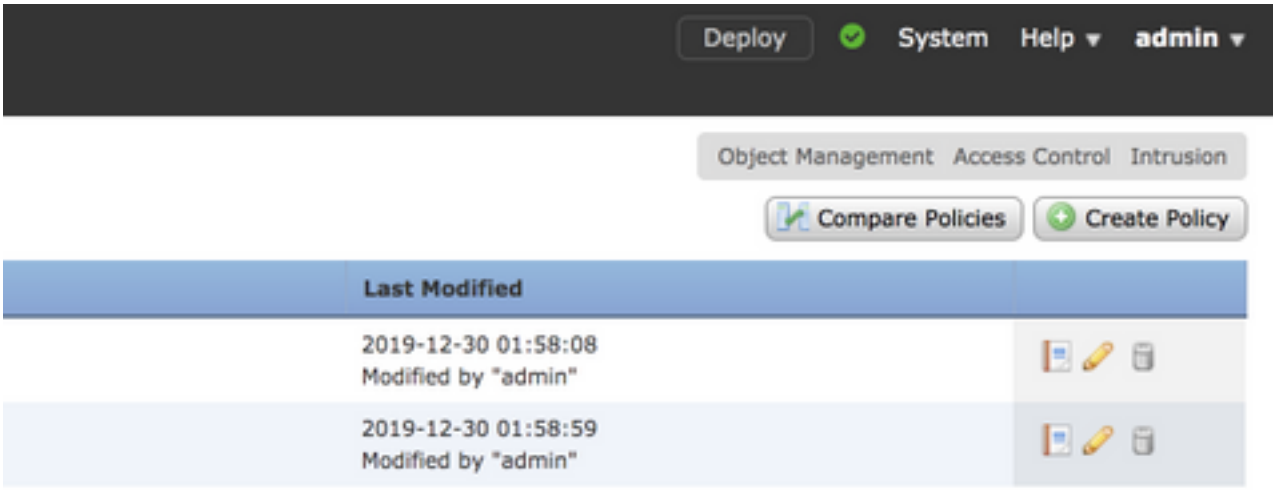


> **Note**: Não confunda a **segurança e a conectividade equilibradas** para **políticas de intrusão** e a **segurança e conectividade equilibradas** para **análise de rede**. O primeiro é para as regras do Snort, enquanto o segundo é para pré-processamento e decodificação.

Comparar política de análise de rede (NAP)

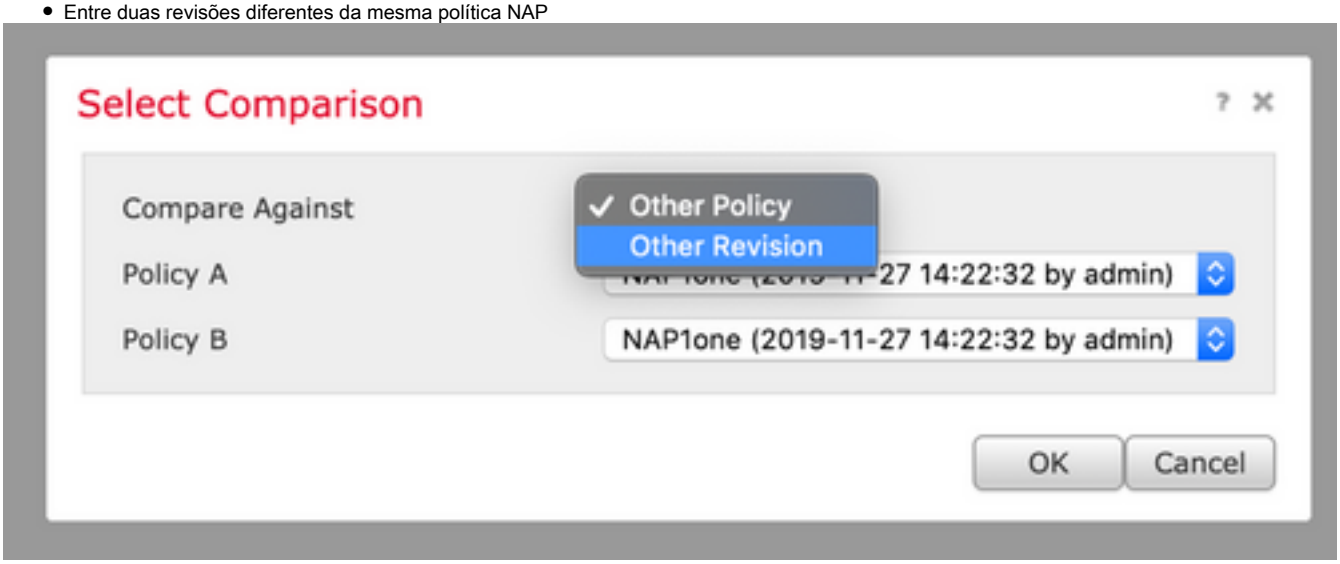
As políticas NAP podem ser comparadas para alterações feitas e esse recurso pode ajudar a identificar e solucionar problemas. Além disso, os relatórios de comparação de NAP também podem ser gerados e exportados ao mesmo tempo.

Navegue até **Políticas > Controle de acesso > Invasão**. Em seguida, clique na opção **Network Analysis Policy** no canto superior direito. Na página de política NAP, você pode ver a guia **Comparar políticas** no lado superior direito, como mostrado na imagem:

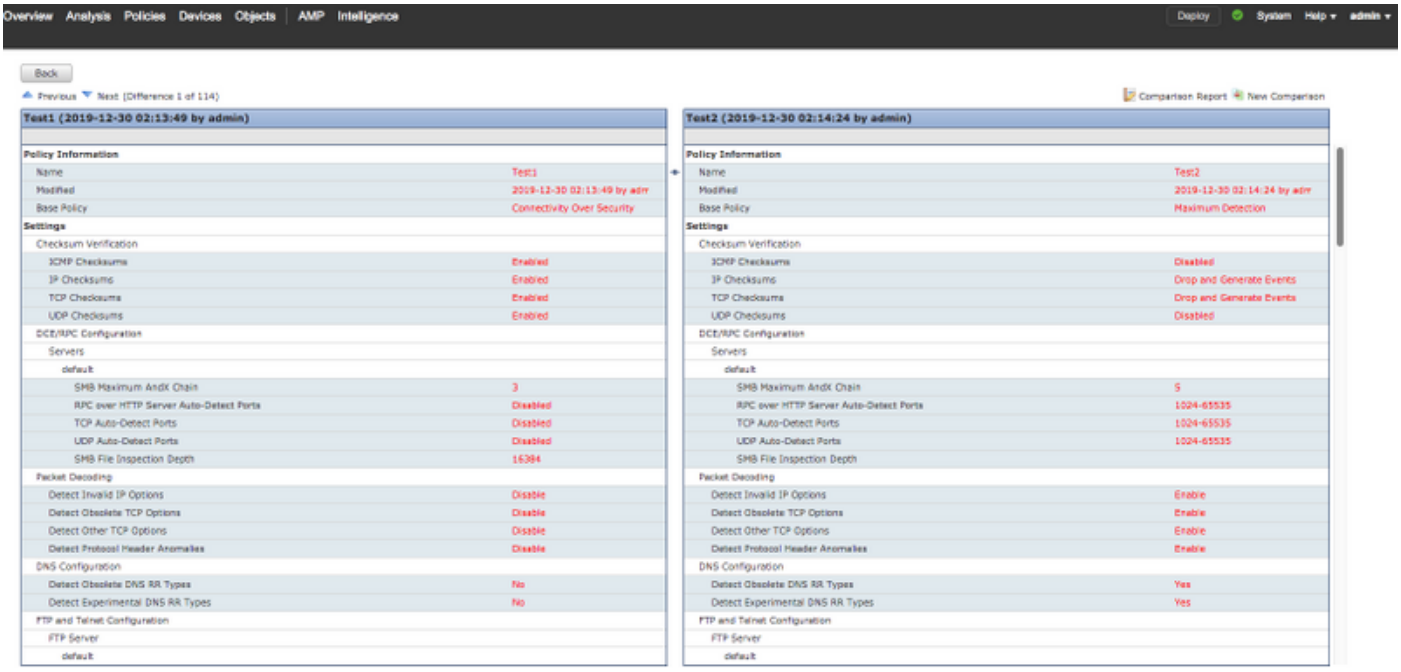


A comparação da política de análise de rede está disponível em duas variantes:

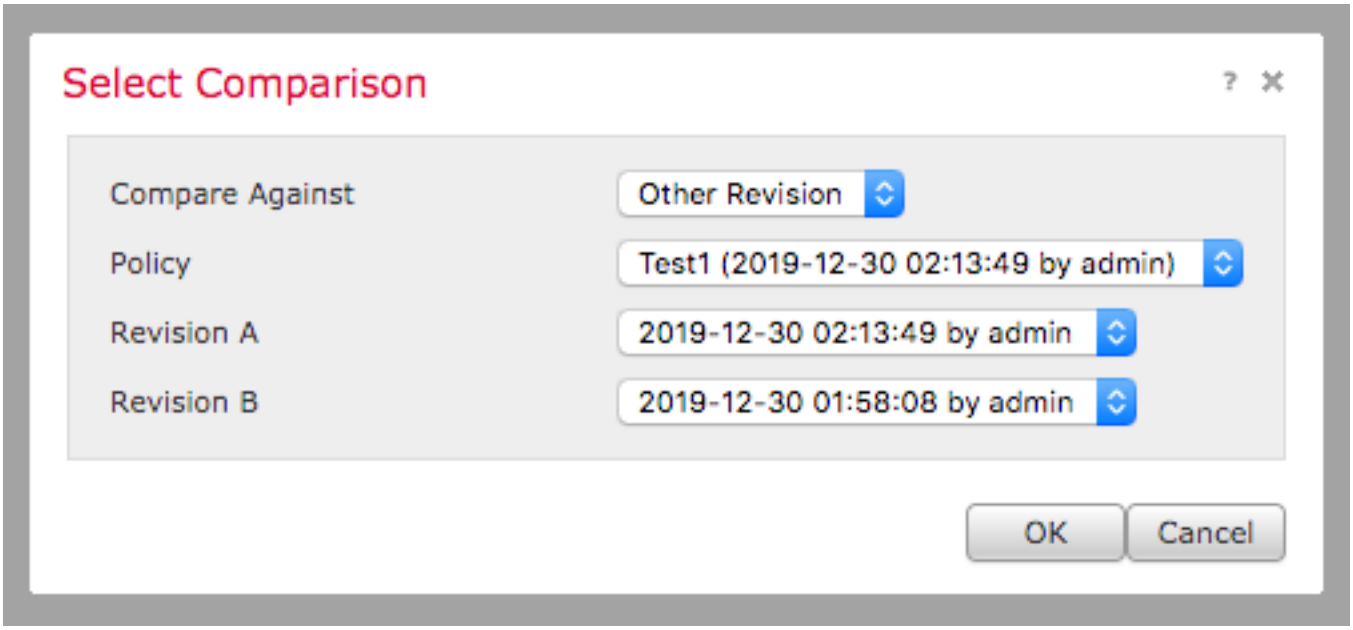
- Entre duas políticas NAP diferentes
- Entre duas revisões diferentes da mesma política NAP

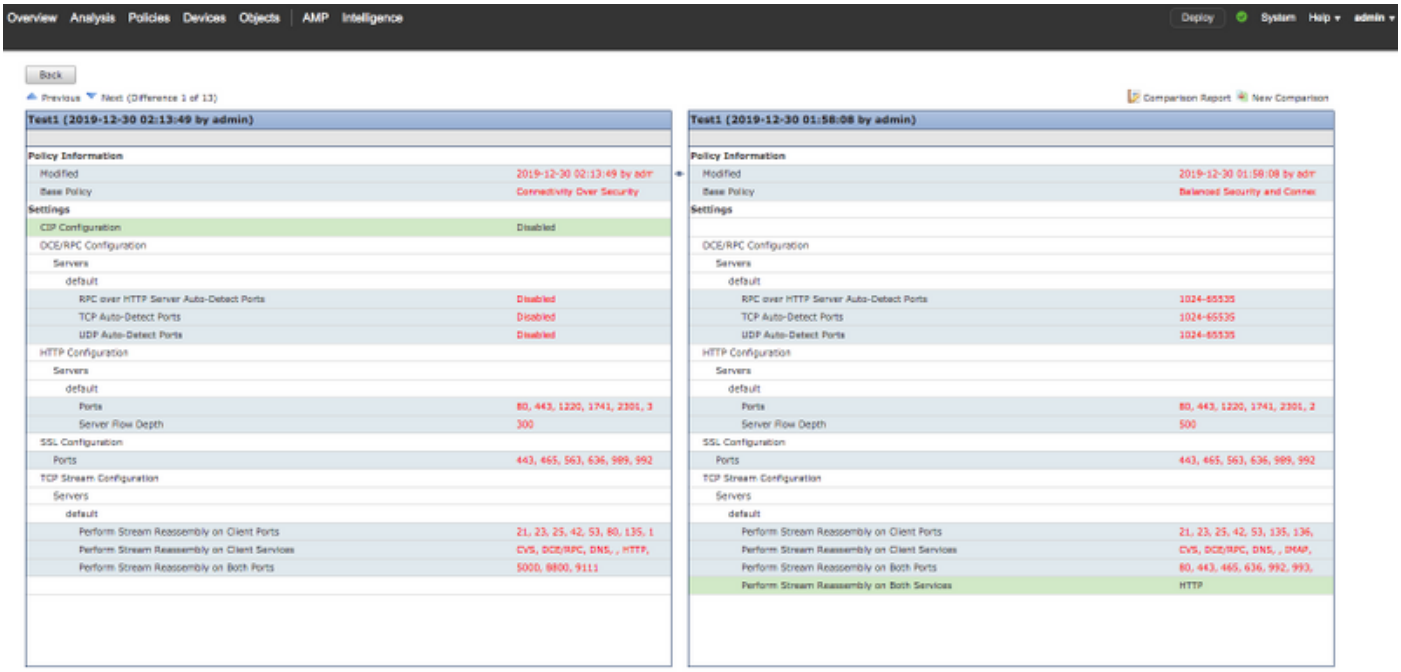


A janela de comparação fornece uma comparação linha por linha entre duas políticas NAP selecionadas e o mesmo pode ser exportado como um relatório da guia **relatório de comparação** na parte superior direita, como mostrado na imagem:



Para comparação entre duas versões da mesma política NAP, a opção de revisão pode ser selecionada para selecionar a **id de revisão** necessária, como mostrado na imagem:




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