Firepower デバイスの NAP ポリシーを比較する方法

目次

概要

この資料に Firepower 管理センター（FMC）によって管理される firepower デバイスのための異なるネットワーク解析ポリシー (NAP）を比較する方法を記述されています。

前提条件

要件

次の項目に関する知識が推奨されます。

- オープンソース Snort のナレッジ
- Firepower Management Center（FMC）
- Firepower Threat Defense（FTD）

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づくものです。

- この Firepower
- ソフトウェア バージョン 6.4.0 を実行する Cisco Firepower Threat Defense（FTD）
- バーチャル ソフトウェア バージョン 6.4.0 を実行する Firepower Management Center（FMC）

背景説明

ネットワーク パケットのエクスプロイトを見つけ、防ぐ Snort 使用パターン一致手法。 これをするために、Snort エンジンはこの比較がすることができるようにネットワーク パケットが準備されることを必要とします。 このプロセスは NAP の助けによって実行され、次の 3 つのステージを経ることができます:

- デコード
- 正規化すること
- 調査分析

フェーズのネットワーク解析ポリシー プロセス パケット: 最初にシステムは最初の 3 つの TCP/IP 層によってパケットをデコードしましたり、そしてプロトコル アノーマリを正規化し、調査分析し、検出することに続きます。

前処理プログラムは 2 つの本管機能性を提供します:

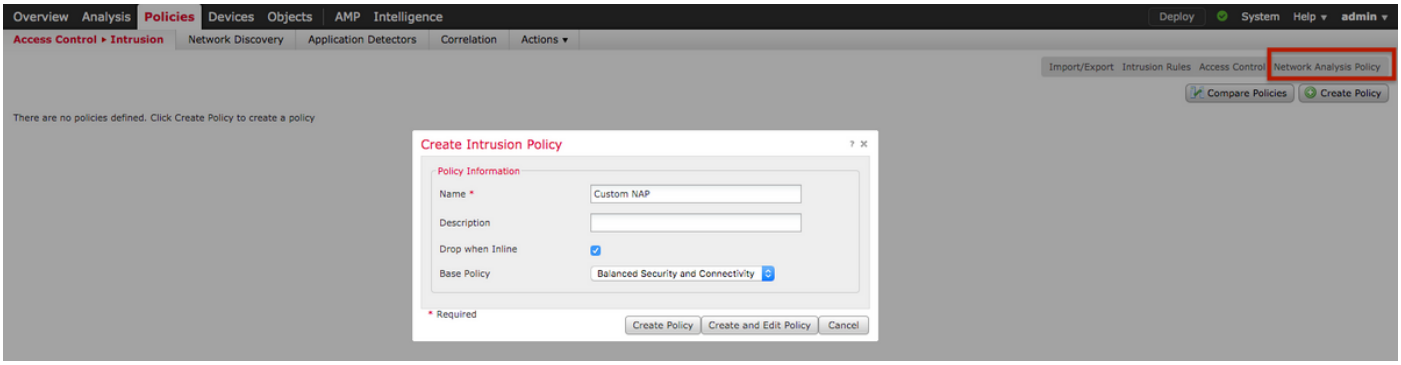
- それ以上のインスペクション用のトラフィック 正規化
- プロトコル アノーマリを識別して下さい

:

オープンソース Snort の情報に関しては、https://www.snort.org/ を参照して下さい

NAP 設定を確認して下さい

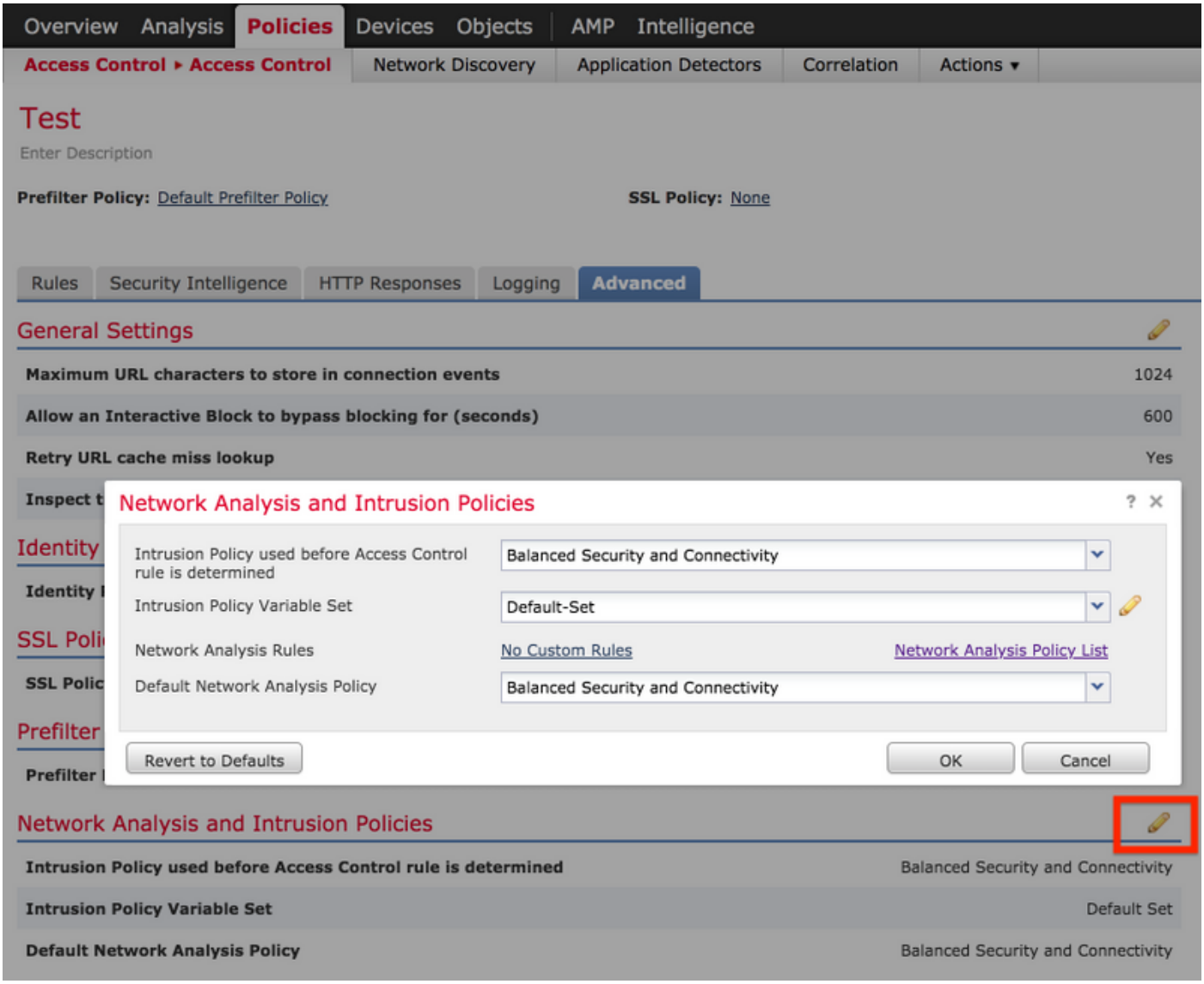
firepower NAP ポリシーを、移動はイメージに示すように編集するために **FMC ポリシー > アクセスコントロール > 不正侵入**に作成するか、または、その後右上隅の**ネットワーク解析ポリシー** オプションを、クリックします:



ACP NAP

> ACP **Advanced**

ACP :

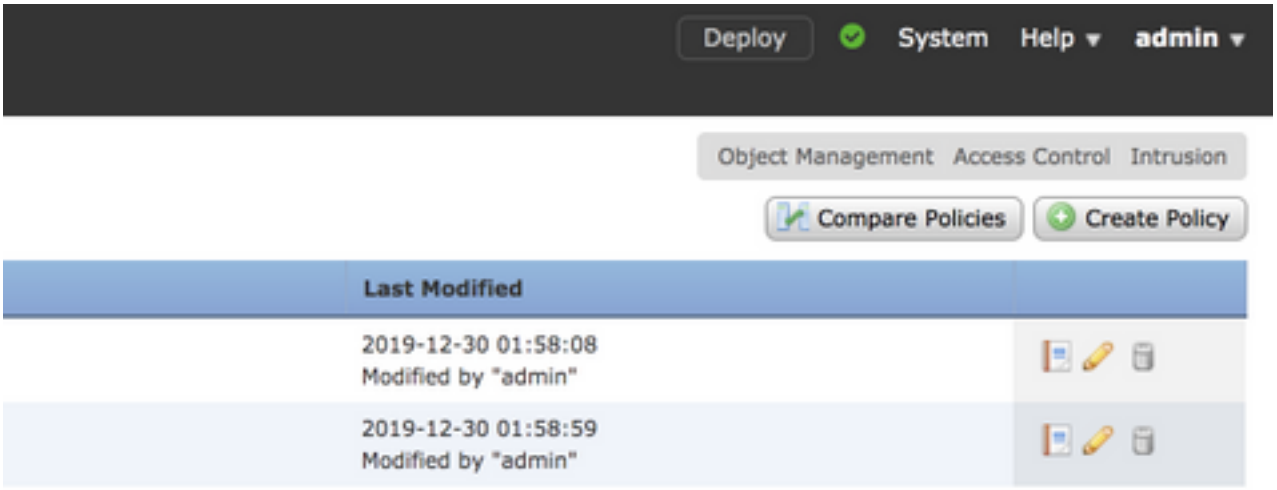


: 1 Snort

比較して下さいネットワーク解析ポリシー（NAP）を

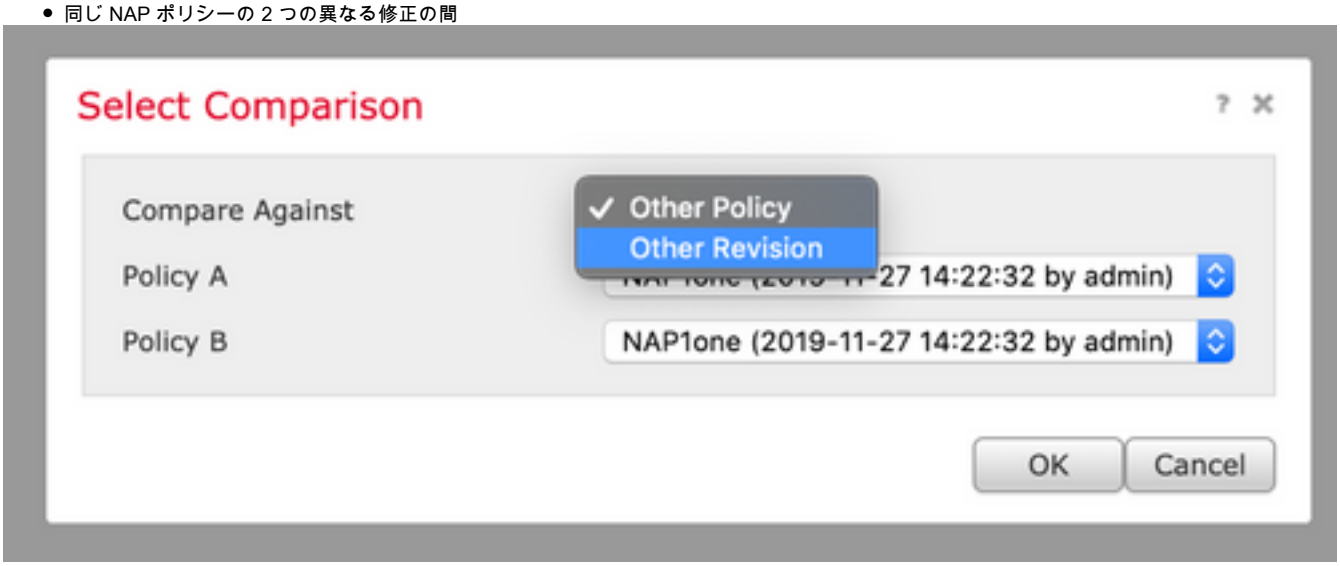
NAP ポリシーはある変更のために比較することができ、この機能は問題を識別し、解決することで助ける可能性があります。 さらに、NAP 比較レポートはまた生成され、同時にエクスポートできます。

[Policies] > [Access Control] > [Intrusion] の順に選択します。 それから、右上の**ネットワーク解析ポリシー** オプションをクリックして下さい。 NAP ポリシー ページの下でイメージに示すように右上側面の **Policies タブを、比較するために**見ることができます:

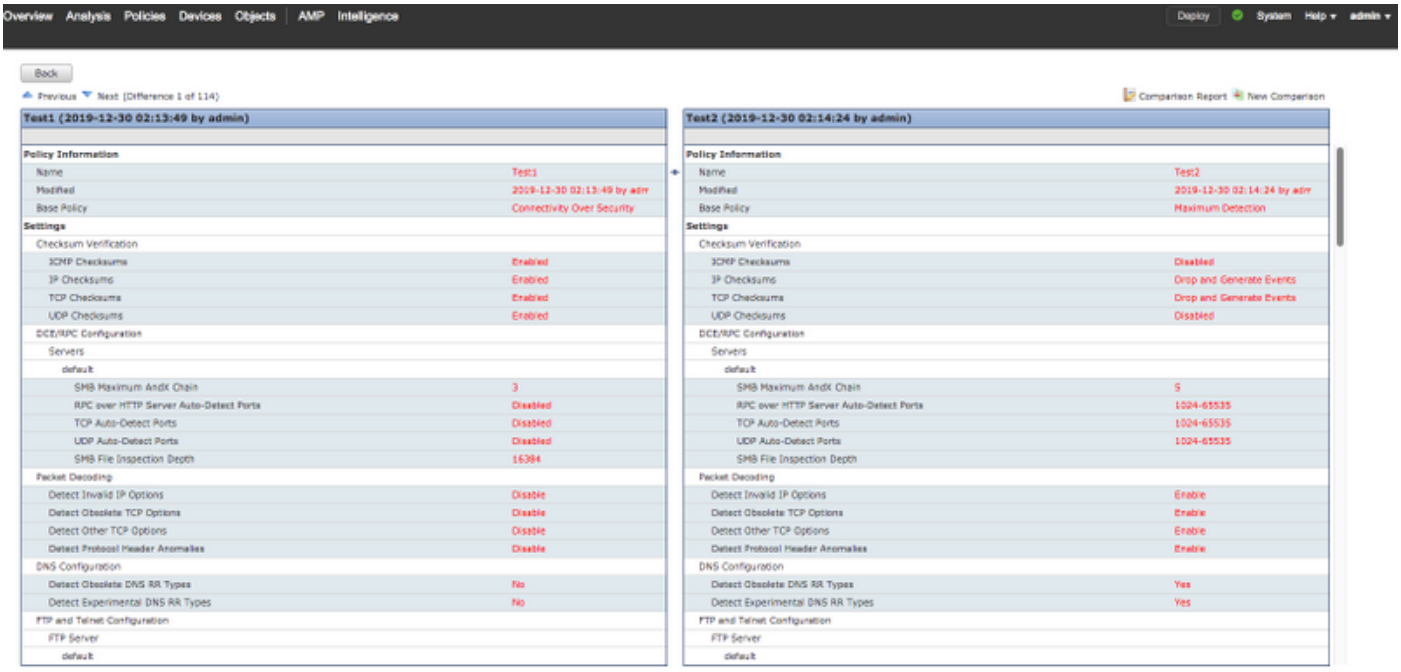


ネットワーク解析ポリシー比較は 2 つのバリアントで利用できます:

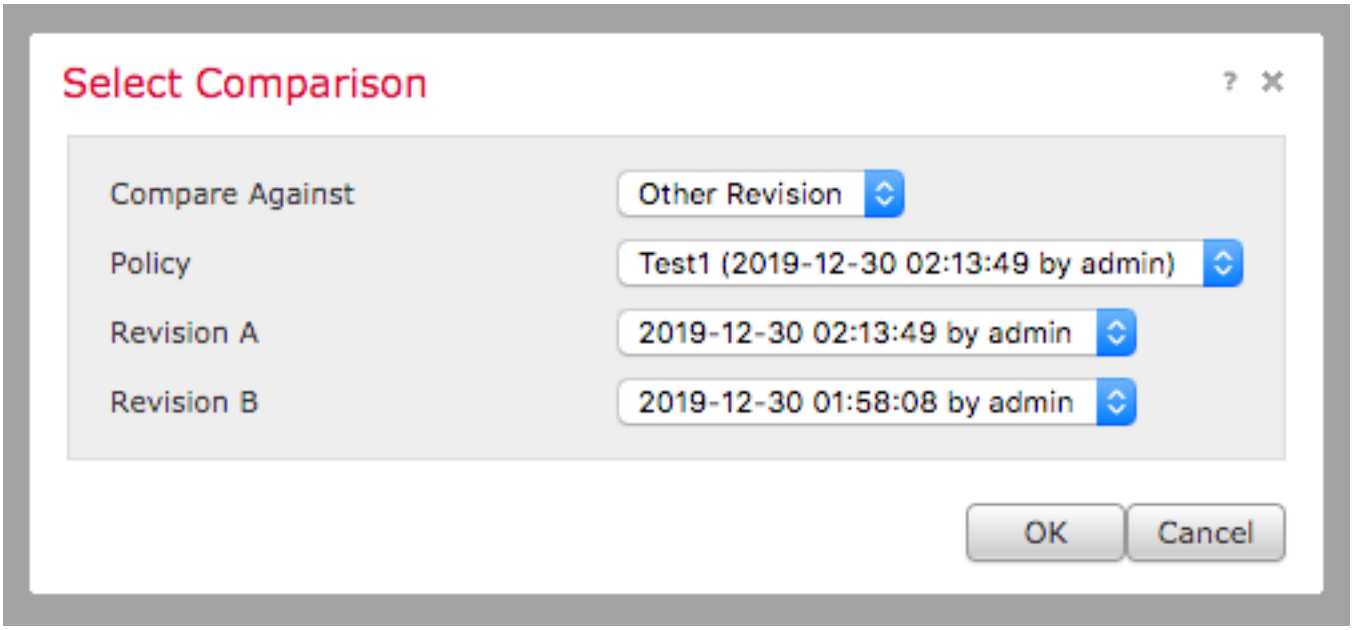
- 2 つの異なる NAP ポリシーの間
- 同じ NAP ポリシーの 2 つの異なる修正の間

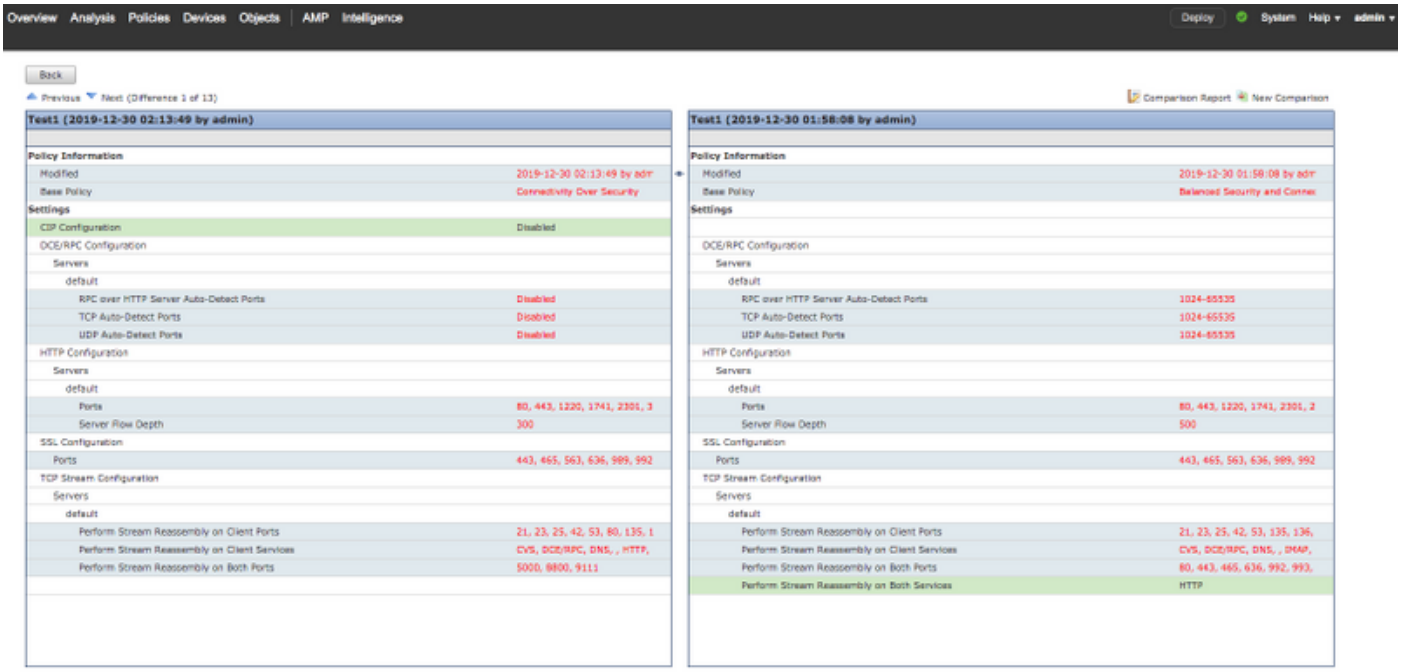


比較ウィンドウは 2 つの指定 NAP ポリシー提供しますと同じ間の比較 1 行毎比較をイメージに示すように右上の**比較 Report タブ**からレポートと、エクスポートすることができます:



同じ NAP ポリシーの 2 バージョン間の比較の場合、修正オプションはイメージに示すように必須 **Revision ID を**、選択することを選択することができます:




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