كيفية مقارنة سياسات NAP على أجهزة FirePOWER

المحتويات

المقدمة

يوضح هذا المستند كيفية مقارنة سياسات تحليل الشبكة المختلفة (NAP) لأجهزة FirePOWER التي يديرها مركز إدارة FirePOWER (FMC).

المتطلبات الأساسية

المتطلبات

توصي Cisco بأن تكون لديك معرفة بالمواضيع التالية:

- معرفة الشخير مفتوح المصدر
- مركز إدارة Firepower (FMC)
- Firepower Threat Defense (FTD)

المكونات المستخدمة

تستند المعلومات الواردة في هذا المستند إلى إصدارات البرامج والمكونات المادية التالية:

- تنطبق هذه المقالة على جميع منصات Firepower
- برنامج الدفاع ضد تهديد FirePOWER (FTD) من Cisco الذي يشغل الإصدار 6.4.0 من البرنامج
- Firepower Management Center Virtual (FMC) الذي يشغل الإصدار 6.4.0 من البرنامج

معلومات أساسية

يستخدم الشخير تقنيات مطابقة النمط للعثور على عمليات الاستغلال ومنعها في حزم الشبكة. للقيام بهذا الإجراء، يحتاج محرك الشبكة إلى حزم شبكة ليتم إعدادها بطريقة يمكن من خلالها إجراء هذه المقارنة. وتتم هذه العملية بمساعدة برنامج العمل الوطني ويمكن أن تمر بالمراحل الثلاث التالية:

- فك الترميز
- تطبيع
- تجهيز مسبق

معالجة سياسة تحليل الشبكة لحزم في مرحلة: يقوم النظام أولا بفك ترميز الحزم من خلال طبقات TCP/IP الثلاث الأولى، ثم يستمر في التطبيع والمعالجة المسبقة واكتشاف شذوذ البروتوكول.

توفر المعالجات المسبقة وظيفتين رئيسيتين:

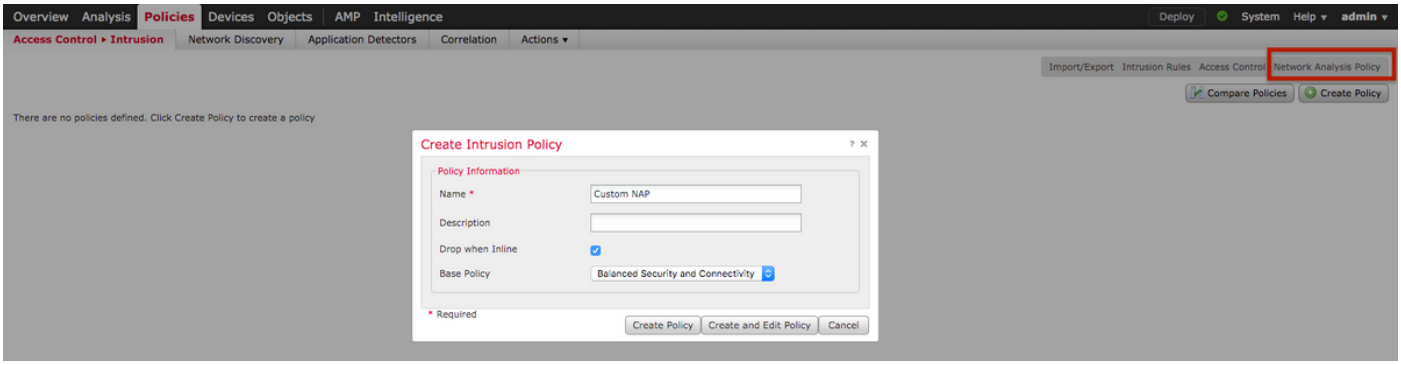
- تطبيع حركة المرور لمزيد من التفتيش
- التعرف على الحالات الشاذة للبروتوكول

ملاحظة: تتطلب بعض قواعد سياسة الاقتحام خيارات معينة سابقة للمعالجة لإجراء الكشف

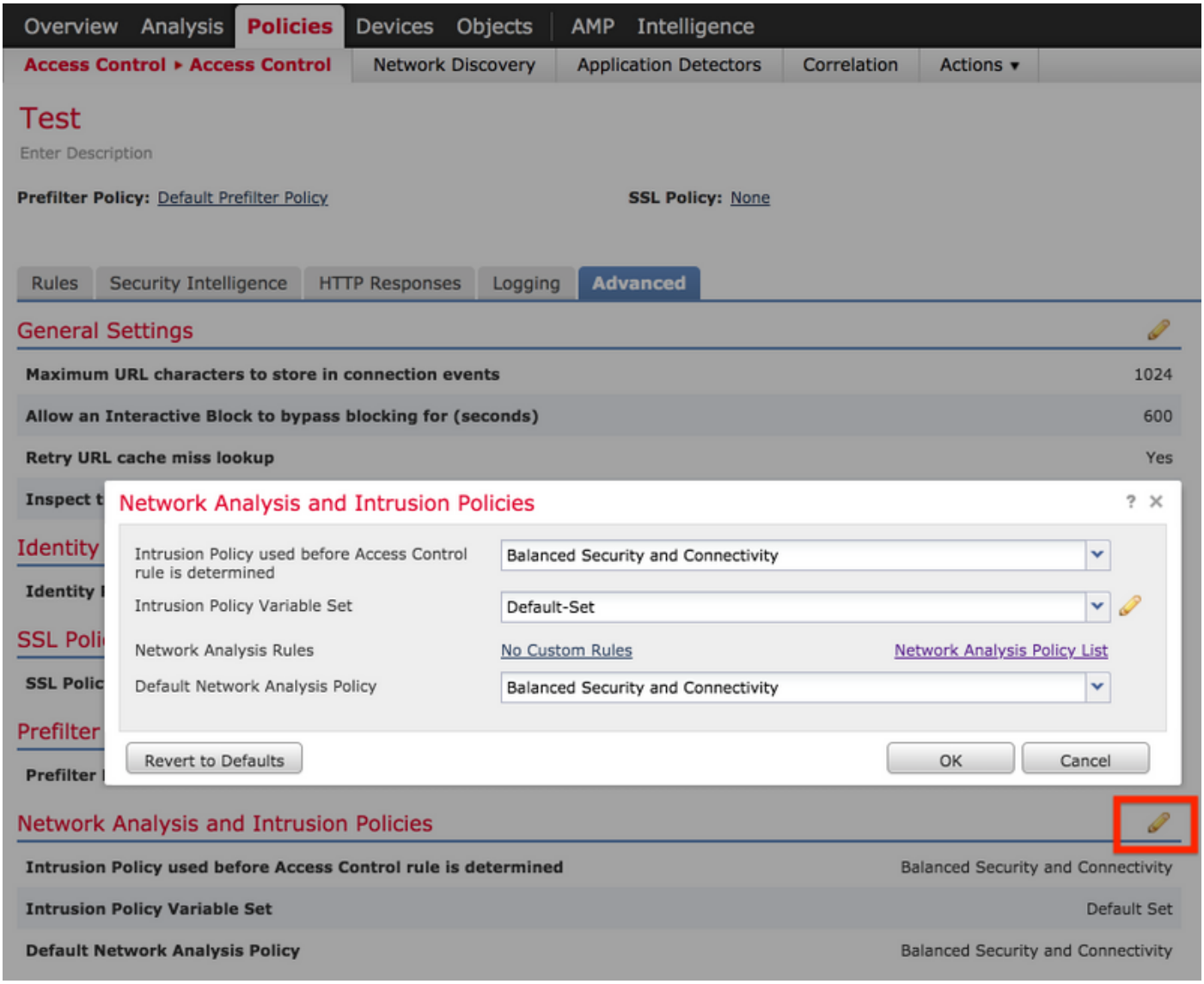
للحصول على معلومات حول برنامج Snort مفتوح المصدر، يرجى زيارة الموقع https://www.snort.org/

التحقق من تكوين NAP

لإنشاء سياسات حماية مستوى التحكم (NAP) الخاصة بقوة الحماية أو تحريرها، انتقل إلى **سياسات وحدة التحكم في الإدارة الأساسية (FMC) > التحكم في الوصول > التطفل**، ثم انقر فوق **خيار سياسة تحليل الشبكة** في الركن العلوي الأيمن، كما هو موضح في الصورة:



(NAP) (ACP)
> (ACP) . .
ACP :

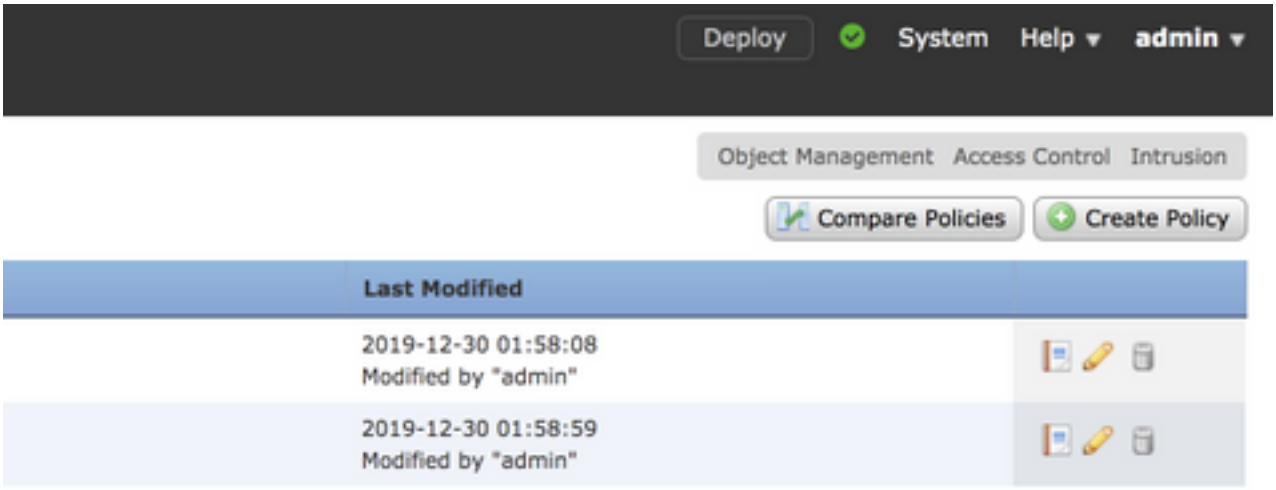


ملاحظة: تحليل الشبكة. .

مقارنة سياسة تحليل الشبكة (NAP)

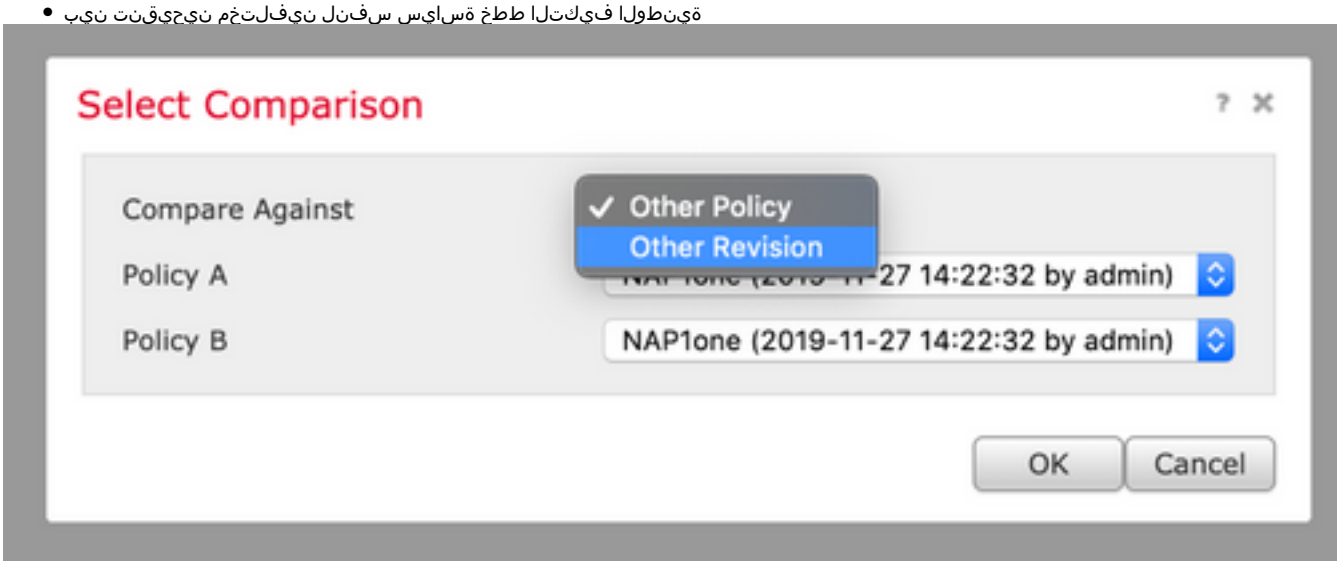
ويمكن مقارنة سياسات برامج العمل الوطنية بالتغييرات التي تم إجراؤها، ويمكن أن تساعد هذه الميزة في تحديد المشكلات واستكشاف أخطائها وإصلاحها. وبالإضافة إلى ذلك، يمكن أيضا إعداد تقارير مقارنة برامج العمل الوطنية وتصديرها في الوقت نفسه.

انتقل إلى **السياسات > التحكم في الوصول > التطفل**. بعد ذلك، انقر فوق خيار نهج **تحليل الشبكة** في أعلى اليمين. تحت صفحة سياسة NAP يمكنك مشاهدة علامة التبويب **مقارنة السياسات** في الجانب العلوي الأيمن، كما هو موضح في الصورة:

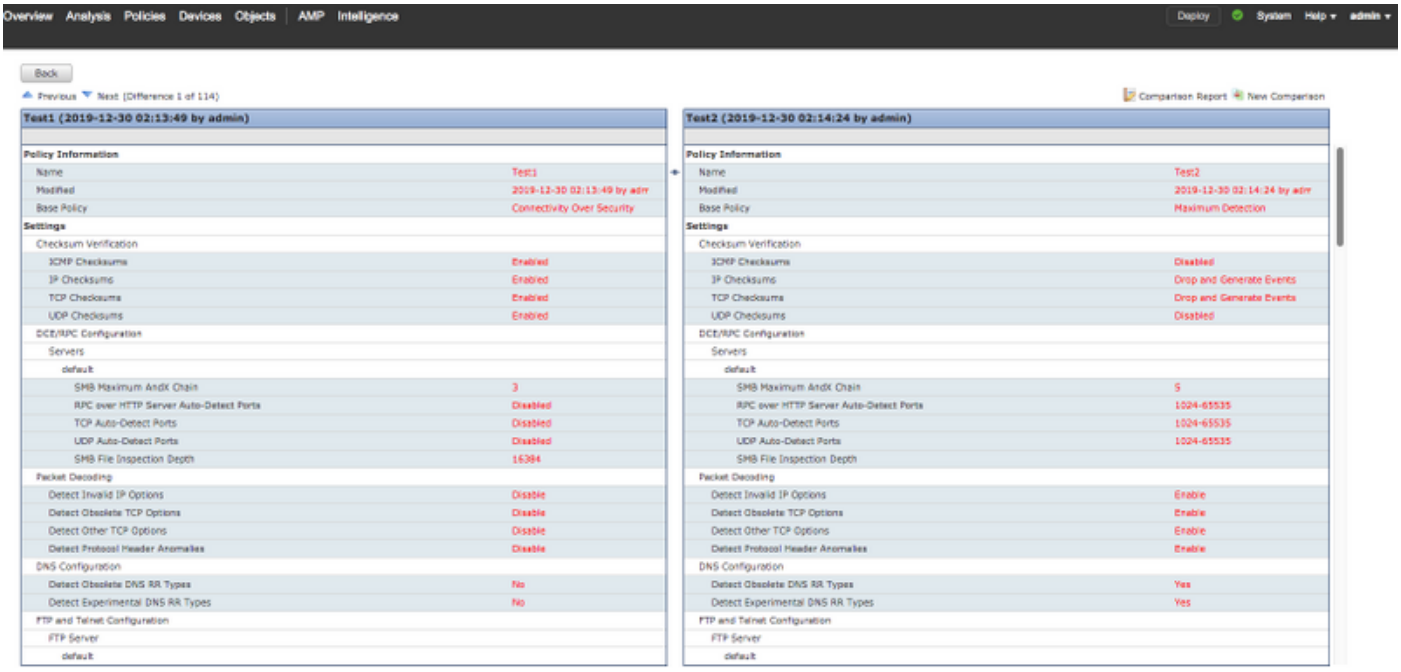


تتوفر مقارنة نهج تحليل الشبكة في متغيرين:

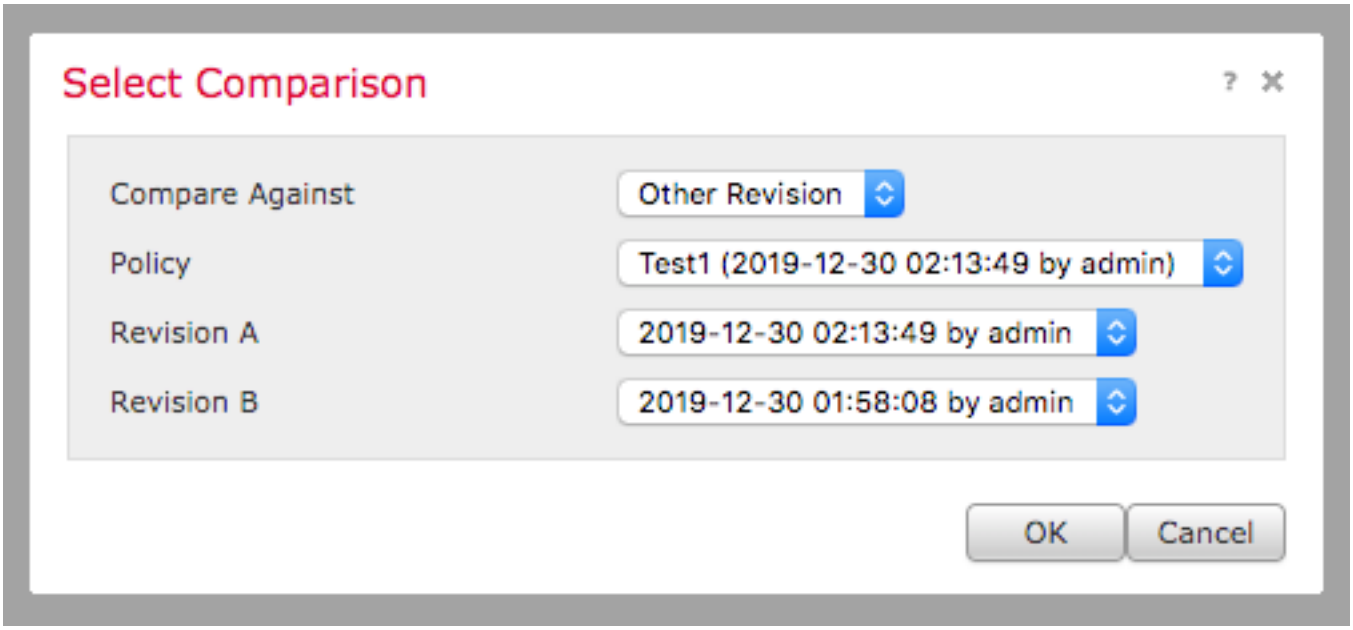
- بين سياستين مختلفتين لخطط العمل الوطنية
- بين تنقيحين مختلفين لنفس سياسة خطط التكيف الوطنية

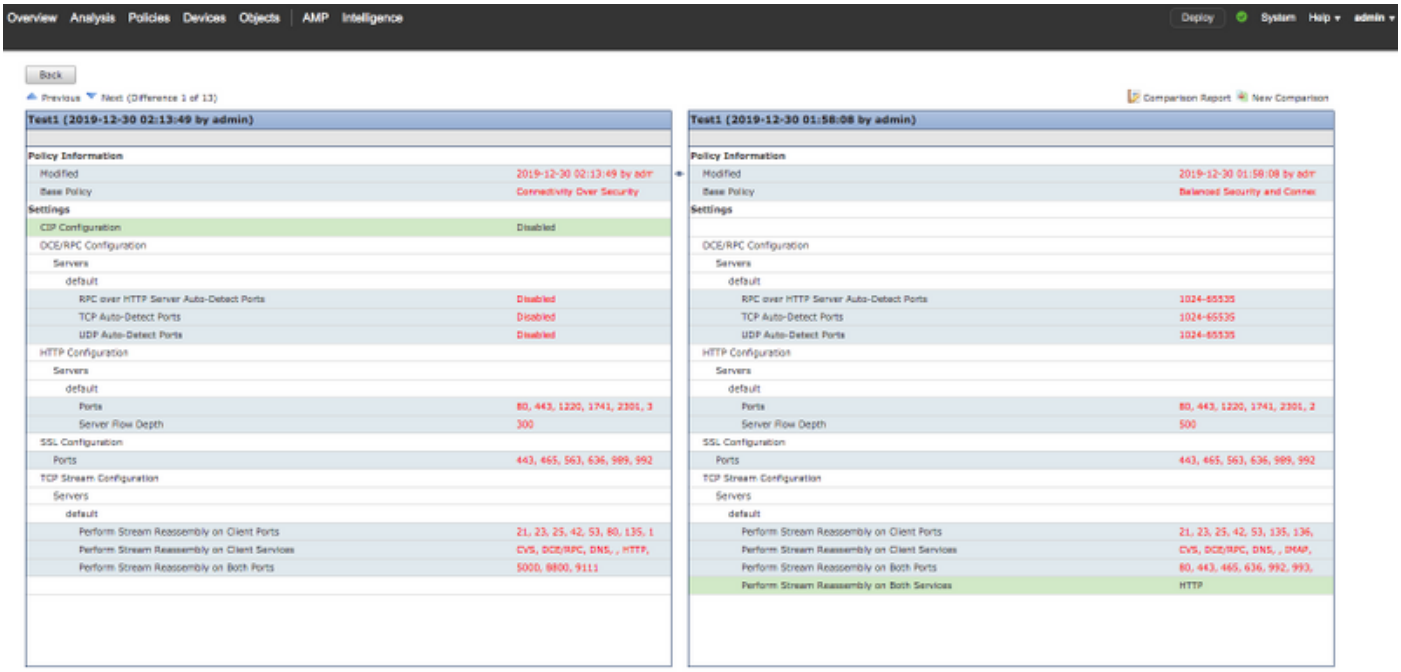


توفر نافذة المقارنة مقارنة سطر بسطر بين سياستين محددتين لخطط العمل الوطنية، كما يمكن تصدير نفس النهج كتقرير من علامة التبويب **تقرير المقارنة** في أعلى اليمين، كما هو موضح في الصورة:



للمقارنة بين إصدارين من سياسة NAP نفسها، يمكن إختيار خيار المراجعة لتحديد **معرف المراجعة** المطلوب، كما هو موضح في الصورة:




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

حول هذه الترجمة
ترجمت Cisco هذا المستند باستخدام مجموعة من التقنيات الآلية والبشرية لتقديم محتوى دعم للمستخدمين في جميع أنحاء العالم بلغتهم الخاصة. يُرجى ملاحظة أن أفضل ترجمة آلية لن تكون دقيقة كما هو الحال مع الترجمة الاحترافية التي يقدمها مترجم محترف. تخلي Cisco Systems مسئوليتها عن دقة هذه الترجمات وتُوصي بالرجوع دائمًا إلى المستند الإنجليزي الأصلي (الرابط متوفر).