

لأصتاء ةلهم طبض :ثءءالاء اراراءصإل او ASA 8.3 MPF نلوكء لاءم مءءءءس اب SSH/Telnet/HTTP

المءءواء

- [المءءماء](#)
- [المءءواء الأساسلاء](#)
- [المءءواء](#)
- [المءءواء المسءءءماء](#)
- [الاصءلاءءاء](#)
- [الءءوءن](#)
- [الرسم الءءءبءل للشءءاء](#)
- [الءءوءنءاء](#)
- [مءءاء إءءوءنلاء](#)
- [اسءءءشاف الأءءاء واصلءاء](#)
- [مءءواء ءاء صلاء](#)

المءءماء

لءءم هءاء المسءءءء نموءءاء لءءوءن ءءاء الأمان الءابل للءءلف (ASA) من Cisco مع الإصءاء 8.3(1) والإصءاءءاء الأءءء من مءءاء ءءوءن مءءءاء لءءبءق معلن مثل SSH/Telnet/HTTP، بءلاء من واءء ٱنءبءق على ءمعل الءءبءقاء. لءسءءءم مءءال الءءوءن هءاء إءاءر عمل السلاءاء النمءبلاء (MPF) الءل ءم ءءءلمه فل ءءاء الأمان الءابل للءءلف (ASA) من Cisco، الإصءاء 7.0. راءء [إسءءءام إءاءر عمل السلاءاء النمءبلاء](#) للءءوءل على مزبء من المءءواء.

فل هءاء الءءوءن النموءءءل، لءم ءءوءن Cisco ASA للسماء لمءءاء العمل (10.77.241.129) بء
Telnet/SSH/HTTP بالءاءم البءبء (10.1.1.1) ءلف الموءء. ءما ءم ءءوءن مءءاء اءصال منءصلاء لءءاء مرور بلاءاء
Telnet/SSH/HTTP. ءسءم ءمعل ءرءاء مرور TCP الأءرى فل الءءوءل على ءلءاء اءءءاء مءءاء الاءصال العاءلاء
المءءءءءة بمءءاء 1:00:00 conn.

ارءء إلى [PIX/ASA 7.x والإصءاءءاء الأءءء/FWSM](#): ءعسل مءءاء اءصال SSH/Telnet/HTTP باءسءءءام مءءال ءءوءن
MPF لنفس الءءوءن على Cisco ASA مع الإصءاءءاء 8.2 والإصءاءءاء الأءءم.

المءءواء الأساسلاء

المءءواء

لا ءوءء مءءواءءاء ءاءاء لهءاء المسءءءء.

المءءواء المسءءءماء

ءسءءء المءءواء الوارءاء فل هءاء المسءءءء إلى برنامء ءءاء الأمان Cisco ASA Security Appliance، الإصءاء
8.3(1) مع Adaptive Security Device Manager (ASDM) 6.3.

تم إنشاء المعلومات الواردة في هذا المستند من الأجهزة الموجودة في بيئة معملية خاصة. بدأت جميع الأجهزة المستخدمة في هذا المستند بتكوين ممسوح (افتراضي). إذا كانت شبكتك مباشرة، فتأكد من فهمك للتأثير المحتمل لأي أمر.

الاصطلاحات

راجع اصطلاحات تلميحات Cisco التقنية للحصول على مزيد من المعلومات حول اصطلاحات المستندات.

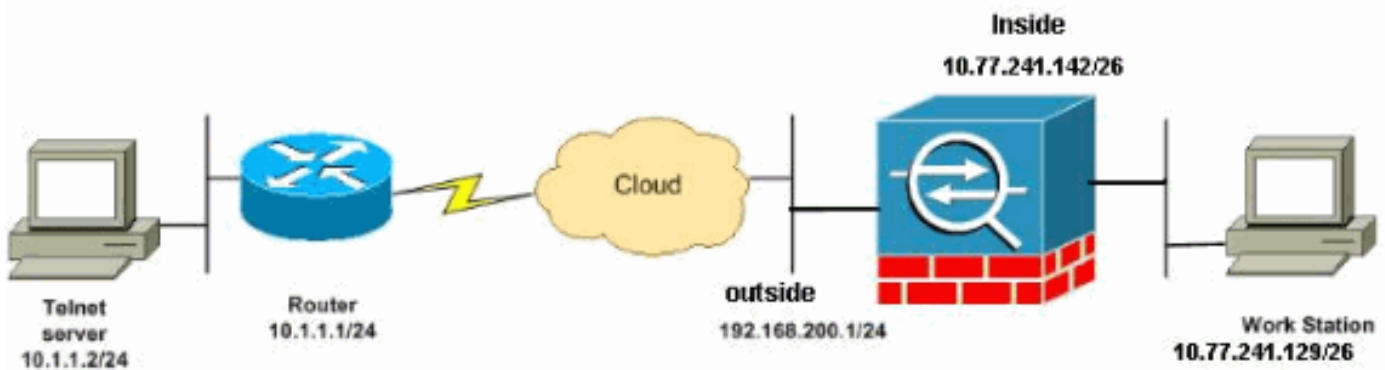
التكوين

في هذا القسم، تُقدّم لك معلومات تكوين الميزات الموضحة في هذا المستند.

ملاحظة: أستخدم أداة بحث الأوامر (للعلماء المسجلين فقط) للحصول على مزيد من المعلومات حول الأوامر المستخدمة في هذا القسم.

الرسم التخطيطي للشبكة

يستخدم هذا المستند إعداد الشبكة التالي:



ملاحظة: ال ip ليس يخاطب خطة يستعمل في هذا تشكيل قانونيا routable على الإنترنت. هم rfc 1918 عنوان، أي يتلقى يكون استعملت في مختبر بيئة.

التكوينات

يستخدم هذا المستند التكوينات التالية:

- تكوين واجهة سطر الأوامر (CLI)
- تكوين ASDM

ملاحظة: تنطبق تكوينات CLI و ASDM هذه على الوحدة النمطية لخدمة جدار الحماية (FWSM).

تكوين واجهة سطر الأوامر (CLI)

```

(ASA Version 8.3(1
!
hostname ASA
domain-name nantes-port.fr
enable password S39lgaewi/JM5WyY level 3 encrypted
enable password 2KFQnbNIdI.2KYOU encrypted
passwd lmZfSd48bl0UdPgP encrypted
no names

dns-guard
!
interface Ethernet0/0
nameif outside
security-level 0
ip address 192.168.200.1 255.255.255.0
!
interface Ethernet0/1
nameif inside
security-level 100
ip address 10.77.241.142 255.255.255.0

boot system disk0:/asa831-k8.bin
ftp mode passive
dns domain-lookup outside

Creates an object called DM_INLINE_TCP_1. This ---!
defines the traffic !--- that has to be matched in the
class map. object-group service DM_INLINE_TCP_1 tcp
port-object eq www
port-object eq ssh
port-object eq telnet

access-list outside_mpc extended permit tcp host
10.77.241.129 any object-group DM_INLINE_TCP_1

pager lines 24
mtu inside 1500
mtu outside 1500
no failover
no asdm history enable
arp timeout 14400
nat (inside) 0 access-list inside_nat0_outbound
access-group 101 in interface outside

route outside 0.0.0.0 0.0.0.0 192.168.200.2 1
timeout xlate 3:00:00

The default connection timeout value of one hour is ---!
applicable to !--- all other TCP applications. timeout
conn 1:00:00 half-closed 0:10:00 udp 0:02:00 icmp
0:00:02
timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp
0:05:00
timeout mgcp-pat 0:05:00 sip 0:30:00 sip_media 0:02:00
timeout uauth 0:05:00 absolute
timeout tcp-proxy-reassembly 0:01:00
no snmp-server location
no snmp-server contact
snmp-server enable traps snmp authentication linkup

```

```

linkdown coldstart
telnet timeout 5
ssh timeout 5
console timeout 0
!
```

*Define the class map Cisco-class in order !--- to ---!
 classify Telnet/ssh/http traffic when you use Modular
 Policy Framework !--- to configure a security feature.
 .!--- Assign the parameters to be matched by class map*

```

class-map Cisco-class
match access-list outside_mpc

class-map inspection_default
match default-inspection-traffic
!
!
policy-map global_policy
class inspection_default
inspect dns maximum-length 512
inspect ftp
inspect h323 h225
inspect h323 ras
inspect netbios
inspect rsh
inspect rtsp
inspect skinny
inspect esmtp
inspect sqlnet
inspect sunrpc
inspect tftp
inspect sip
inspect xdmcp
```

*Use the pre-defined class map Cisco-class in the ---!
 .policy map*

```

policy-map Cisco-policy
```

*Set the connection timeout under the class mode ---!
 where !--- the idle TCP (Telnet/ssh/http) connection is
 disconnected. !--- There is a set value of ten minutes
 in this example. !--- The minimum possible value is five
 minutes. class Cisco-class*

```

set connection timeout idle 0:10:00 reset
!
```

```

service-policy global_policy global
```

*Apply the policy-map Cisco-policy on the interface. ---!
 !--- You can apply the service-policy command to any
 interface that !--- can be defined by the nameif
 .command*

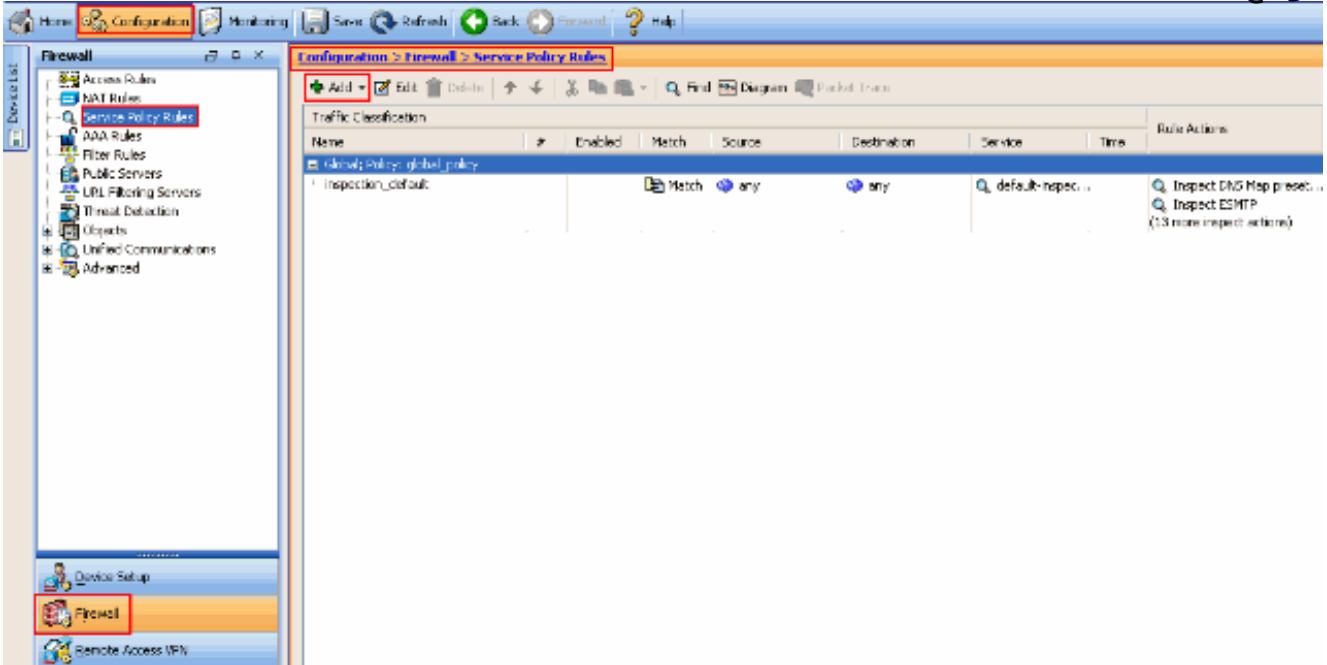
```

service-policy Cisco-policy interface outside
end
```

أكمل هذه الخطوات لإعداد مهلة اتصال TCP لحركة مرور Telnet و SSH و HTTP باستخدام ASDM كما هو موضح.

ملاحظة: راجع [السماح بوصول HTTPS ل ASDM](#) للإعدادات الأساسية للوصول إلى PIX/ASA من خلال ASDM.

1. اخترت تشكيل <جدار حماية> خدمة سياسة قاعدة وطققة يضيف in order to شكلت الخدمة سياسة قاعدة كما هو موضح.



2. من معالج "إضافة قاعدة سياسة الخدمة" - إطار نهج الخدمة، اختر الزر "إختيار" الموجود بجوار الواجهة ضمن المقطع إنشاء نهج خدمة والتطبيق على. اختر الآن الواجهة المطلوبة من القائمة المنسدلة وقم بتوفير اسم نهج. اسم النهج المستخدم في هذا المثال هو Cisco-policy. ثم انقر فوق التالي.

Add Service Policy Rule Wizard - Service Policy

Adding a new service policy rule requires three steps:
Step 1: Configure a service policy.
Step 2: Configure the traffic classification criteria for the service policy rule.
Step 3: Configure actions on the traffic classified by the service policy rule.

Create a Service Policy and Apply To:

Only one service policy can be configured per interface or at global level. If a service policy already exists, then you can add a new rule into the existing service policy. Otherwise, you can create a new service policy.

Interface: outside - (create new service policy) ▾
Policy Name: Cisco-policy
Description:

Global - applies to all interfaces
Policy Name: global_policy
Description:

< Back **Next >** Cancel Help

3. قم بإنشاء اسم خريطة فئة Cisco-class وحدد عنوان IP للمصدر والوجهة (يستخدم قائمة التحكم في الوصول (ACL) خانة الاختيار في معايير مطابقة حركة المرور. ثم انقر فوق التالي.

Add Service Policy Rule Wizard - Traffic Classification Criteria

Create a new traffic class: Cisco-class

Description (optional):

Traffic Match Criteria

- Default Inspection Traffic
- Source and Destination IP Address (uses ACL)
- Tunnel Group
- TCP or UDP Destination Port
- RTP Range
- IP DiffServ CodePoints (DSCP)
- IP Precedence
- Any traffic

Use an existing traffic class: inspection_default

Use class-default as the traffic class.

If traffic does not match a existing traffic class, then it will match the class-default traffic class. Class-default can be used in catch all situation.

< Back **Next >** Cancel Help

4. من معالج إضافة قاعدة سياسة الخدمة - مطابقة حركة المرور - نافذة مصدر وعنوان مصدر، أختار زر الخيار المجاور للمطابقة ثم قم بتوفير عنوان المصدر والوجهة كما هو موضح. انقر فوق الزر المنسدل الموجود بجوار الخدمة لاختيار الخدمات المطلوبة.

Add Service Policy Rule Wizard - Traffic Match - Source and Destination Address

Action: Match Do not match

Source: 10.77.241.129

Destination: any

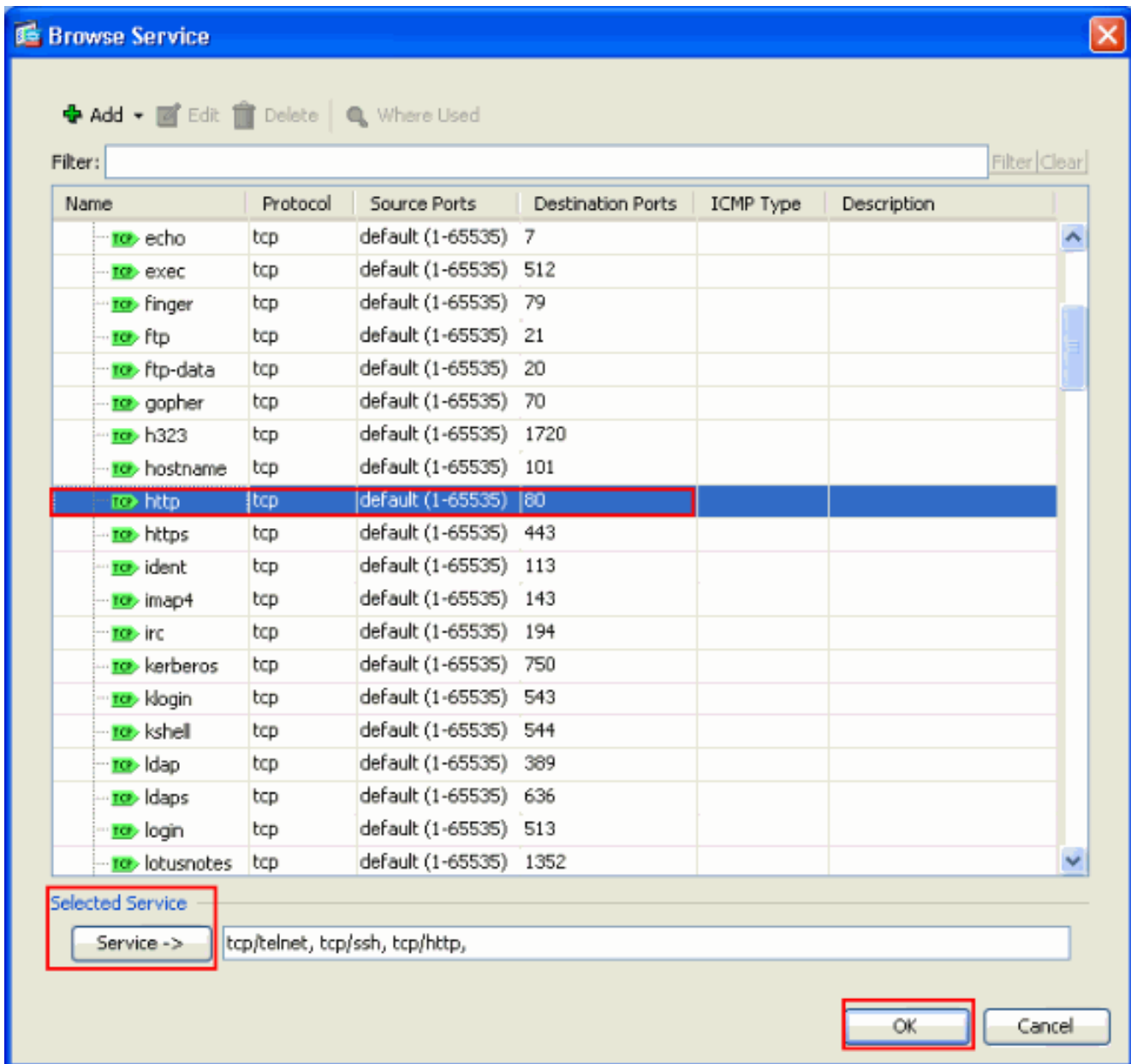
Service: ip

Description:

More Options

< Back Next > Cancel Help

5. حدد الخدمات المطلوبة مثل Telnet و SSH و http. ثم انقر فوق .OK



6. تكوين حالات انتهاء المهلة الزمنية. انقر فوق Next (التالي).

Add Service Policy Rule Wizard - Traffic Match - Source and Destination Address

Action: Match Do not match

Source: 10.77.241.129

Destination: any

Service: tcp/telnet, tcp/ssh, tcp/http

Description:

More Options

< Back **Next >** Cancel Help

7. أخترت توصيل عملية إعداد إعداد TCP in order to setup توصيل مهلة 10 دقيقة. تحقق أيضا من خانة الاختيار إعادة تعيين الإرسال إلى نقاط نهاية TCP قبل المهلة. انقر فوق إنهاء.

Add Service Policy Rule Wizard - Rule Actions

Protocol Inspection | Intrusion Prevention | **Connection Settings** | QoS | NetFlow

Maximum Connections

Maximum TCP & UDP Connections: Default (0) ▾

Maximum Embryonic Connections: Default (0) ▾

Maximum Per Client Connections: Default (0) ▾

Maximum Per Client Embryonic Connections: Default (0) ▾

Randomize Sequence Number

Randomize the sequence number of TCP/IP packets. Disable this feature only if another inline ASA is also randomizing sequence numbers and the result is scrambling the data. Disabling this feature may leave systems with weak TCP Sequence number randomization vulnerable.

TCP Timeout

Embryonic Connection Timeout: Default (0:00:30) ▾

Half Closed Connection Timeout: Default (0:10:00) ▾

Connection Timeout: 0:10:00 ▾

Send reset to TCP endpoints before timeout

Dead connection detection:

Retries: 5 Timeout: Default (0:15:00) ▾

TCP Normalization

Use TCP map

TCP Map: ▾

Edit... New...

Time to Live

Decrement time to live for a connection

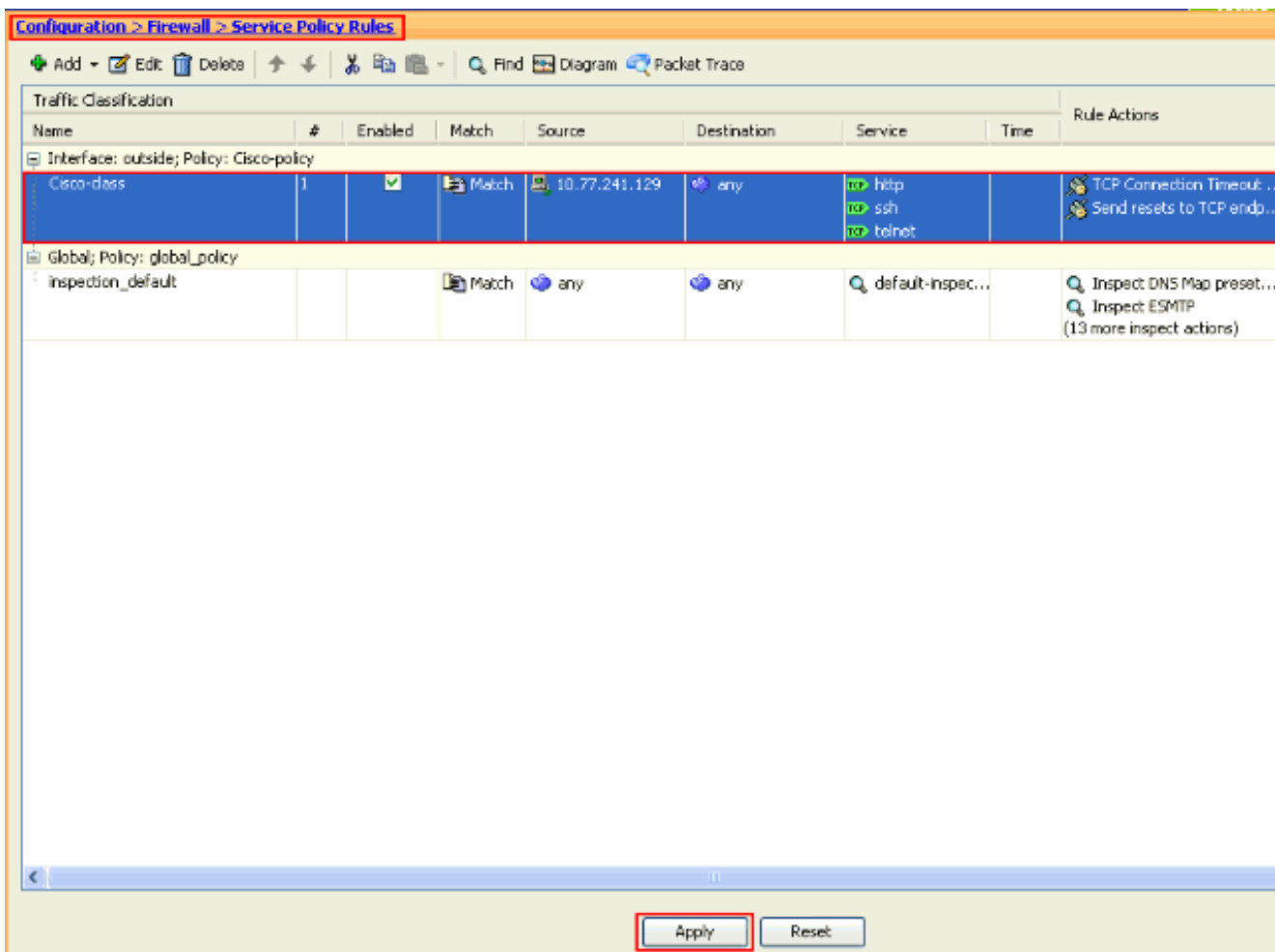
Advanced Options

Skip TCP state tracking and sequence checking when traffic flows across the ASA.

TCP state bypass

< Back Finish Cancel Help

8. انقر فوق تطبيق لتطبيق التكوين على جهاز الأمان. يؤدي هذا إلى اكتمال التكوين.



مهلة إيريونية

الاتصال الجنيني هو اتصال نصف مفتوح أو، على سبيل المثال، لم تكتمل المصافحة الثلاثية له. يتم تعريفه على أنه مهلة SYN على ASA. افتراضيا، ال مهلة syn على ال ASA 30 ثاني. هذه هي كيفية تكوين المهلة الجنينية:

```
access-list emb_map extended permit tcp any any

class-map emb_map
match access-list emb_map

policy-map global_policy
class emb_map
set connection timeout embryonic 0:02:00

service-policy global_policy global
```

استكشاف الأخطاء وإصلاحها

إذا وجدت أن مهلة الاتصال لا تعمل مع MPF، فتتحقق من اتصال بدء TCP. يمكن أن تكون المشكلة عكس عنوان IP للمصدر والوجهة، أو أن عنوان IP الذي تم تكوينه بشكل غير صحيح في قائمة الوصول لا يتطابق مع MPF لتعيين قيمة المهلة الجديدة أو تغيير المهلة الافتراضية للتطبيق. قم بإنشاء إدخال قائمة وصول (المصدر والوجهة) وفقا لبدء الاتصال لتعيين مهلة الاتصال باستخدام MPF.

معلومات ذات صلة

- [مدير أجهزة حلول الأمان المعدلة من Cisco](#)
- [أجهزة الأمان المعدلة Cisco ASA 5500 Series Adaptive Security Appliances](#)
- [طلبات التعليقات \(RFCs\)](#)
- [الدعم التقني والمستندات - Cisco Systems](#)

ةمچرتل هذه ل و ح

ةلأل تاي نقتل ن م ة و مچ م ادخت ساب دن تسم ل ا اذ ه Cisco ت مچرت
م ل ا ل ا ا ن ا ع مچ ي ف ن ي م د خ ت س م ل ل م ع د ي و ت ح م م ي د ق ت ل ة ي ر ش ب ل و
ا م ك ة ق ي ق د ن و ك ت ن ل ة ل ا ة مچرت ل ض ف ا ن ا ة ظ ح ا ل م ي ج ر ي . ة ص ا خ ل ا م ه ت غ ل ب
Cisco ي ل خ ت . ف ر ت ح م مچرت م ا ه م د ق ي ي ت ل ا ة ي ف ا ر ت ح ا ل ا ة مچرت ل ا ع م ل ا ح ل ا و ه
ي ل ا م ا ة ا د ع و ج ر ل ا ب ي ص و ت و ت ا مچرت ل ا ه ذ ه ة ق د ن ع ا ه ت ي ل و ئ س م Cisco
Systems (ر ف و ت م ط ب ا ر ل ا) ي ل ص ا ل ا ي ز ي ل ج ن ا ل ا دن ت س م ل ا