

ASA 8.3 et plus tard : Exemple de configuration de définition de l'expiration de la connexion SSH/Telnet/HTTP à l'aide de MPF

Contenu

[Introduction](#)

[Conditions préalables](#)

[Conditions requises](#)

[Composants utilisés](#)

[Conventions](#)

[Configurer](#)

[Diagramme du réseau](#)

[Configurations](#)

[Délai d'attente d'Ebryonic](#)

[Dépanner](#)

[Informations connexes](#)

[Introduction](#)

Ce document fournit un exemple de configuration d'un délai d'attente spécifique à une application particulière (telle que SSH/Telnet/HTTP) par opposition à un délai d'attente qui s'applique à toutes les applications avec l'appliance de sécurité adaptable Cisco (ASA) version 8.3(1) et ultérieures. Cet exemple de configuration utilise le cadre de stratégie modulaire (MPF) qui a été introduit dans la version 7.0 de l'appliance de sécurité adaptable Cisco (ASA). Référez-vous [utilisant le](#) pour en savoir plus [modulaire de cadre de stratégie](#).

Dans cette configuration d'échantillon, Cisco ASA est configuré pour permettre le poste de travail (10.77.241.129) à Telnet/SSH/HTTP au serveur distant (10.1.1.1) derrière le routeur. Un délai d'attente de connexion distinct au trafic Telnet/SSH/HTTP est également configuré. Tout autre trafic TCP continue à avoir la valeur du dépassement de durée normale de connexion associée avec `conn. 1:00:00 de délai d'attente`.

Référez-vous à [PIX/ASA 7.x et later/FWSM : Placez le délai d'attente de connexion SSH/Telnet/HTTP utilisant l'exemple de configuration MPF](#) pour la même configuration sur Cisco ASA avec des versions 8.2 et antérieures.

[Conditions préalables](#)

[Conditions requises](#)

Aucune spécification déterminée n'est requise pour ce document.

Composants utilisés

Les informations dans ce document sont basées sur la version de logiciel d'appareils de Sécurité de Cisco ASA 8.3(1) avec Adaptive Security Device Manager (ASDM) 6.3.

Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est opérationnel, assurez-vous que vous comprenez l'effet potentiel de toute commande.

Conventions

Pour plus d'informations sur les conventions utilisées dans ce document, reportez-vous à [Conventions relatives aux conseils techniques Cisco](#).

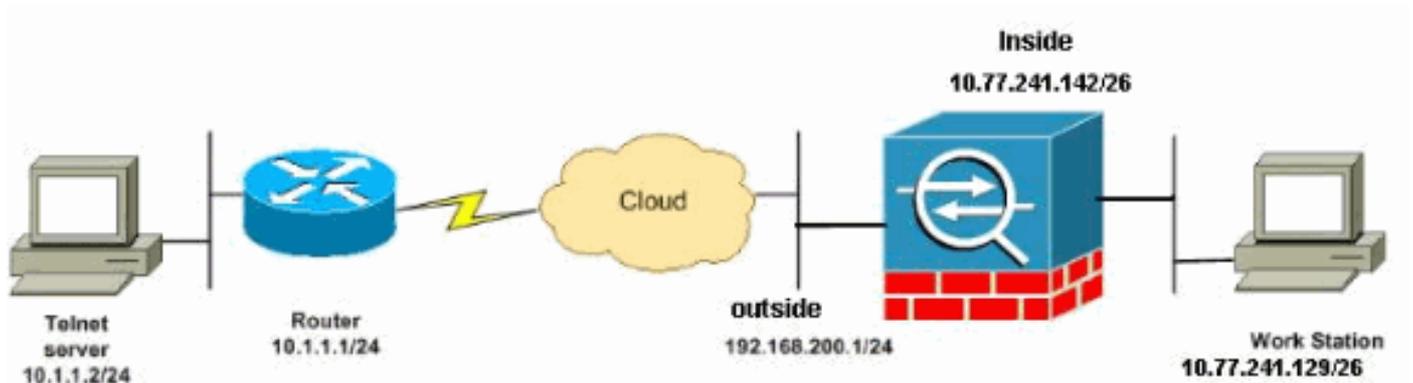
Configurer

Cette section vous fournit des informations pour configurer les fonctionnalités décrites dans ce document.

Remarque: Utilisez l'[Outil de recherche de commande](#) (clients [enregistrés](#) seulement) pour obtenir plus d'informations sur les commandes utilisées dans cette section.

Diagramme du réseau

Ce document utilise la configuration réseau suivante :



Remarque: Les schémas d'adressage d'IP utilisés dans cette configuration ne sont pas légalement routables sur Internet. Ce sont des adresses [RFC 1918](#) qui ont été utilisées dans un environnement de laboratoire.

Configurations

Ce document utilise les configurations suivantes :

- [Configuration CLI](#)
- [Configuration ASDM](#)

Remarque: Ces les configurations CLI et ASDM s'appliquent au module de service de Pare-feu (FWSM).

[Configuration CLI](#)

Configuration ASA 8.3(1)

```
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.

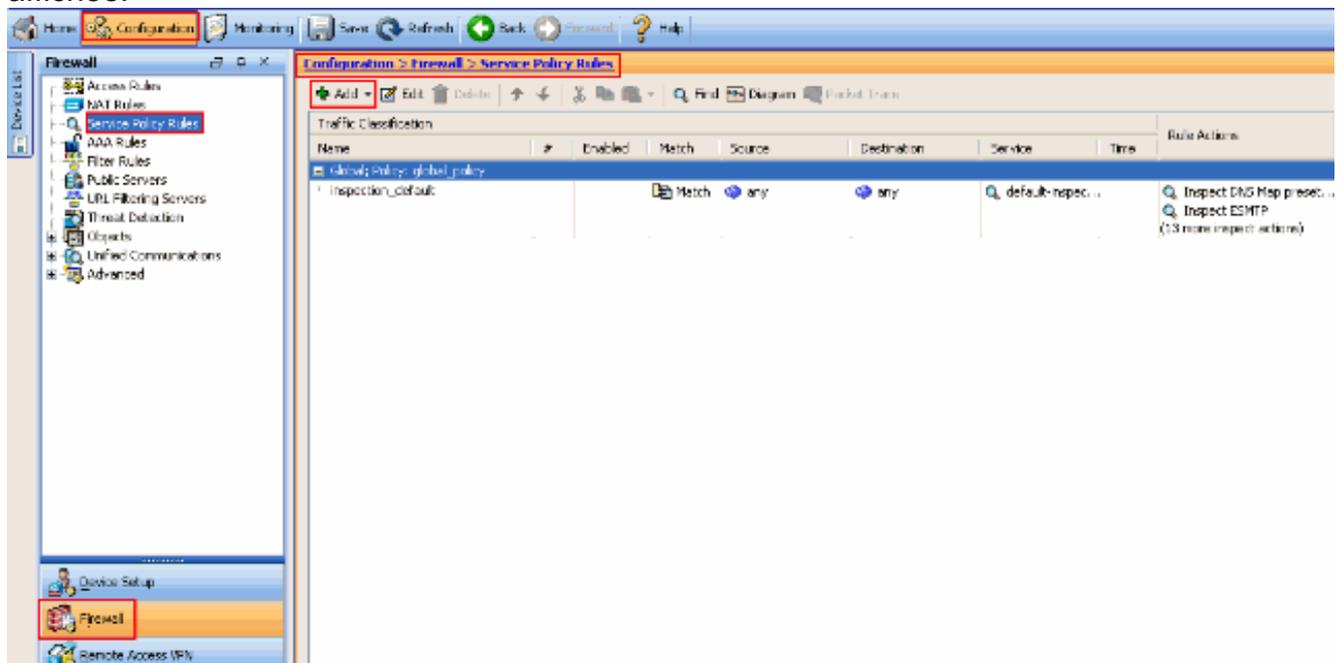
service-policy Cisco-policy interface outside
end
```

Configuration ASDM

Terminez-vous ces étapes afin d'installer le délai d'attente de connexion TCP pour le telnet, le SSH et le trafic http utilisant l'ASDM comme affiché.

Remarque: Référez-vous à [permettre à HTTPS Access pour l'ASDM](#) pour des paramètres de base afin d'accéder au PIX/ASA par l'ASDM.

1. Choisissez les **règles de configuration > de stratégie de Pare-feu > de service** et cliquez sur Add afin de configurer la règle de stratégie de service comme affichée.



2. De l'assistant de règle de stratégie de service d'ajouter - la fenêtre de stratégie de service, choisissez la case d'option à côté de l'interface sous la création une stratégie de service et s'appliquent pour sectionner. Maintenant choisissez l'interface désirée de la liste déroulante et fournissez un **nom de stratégie**. Le nom de stratégie utilisé dans cet exemple est Cisco-stratégie. Cliquez ensuite sur **Next**.

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:

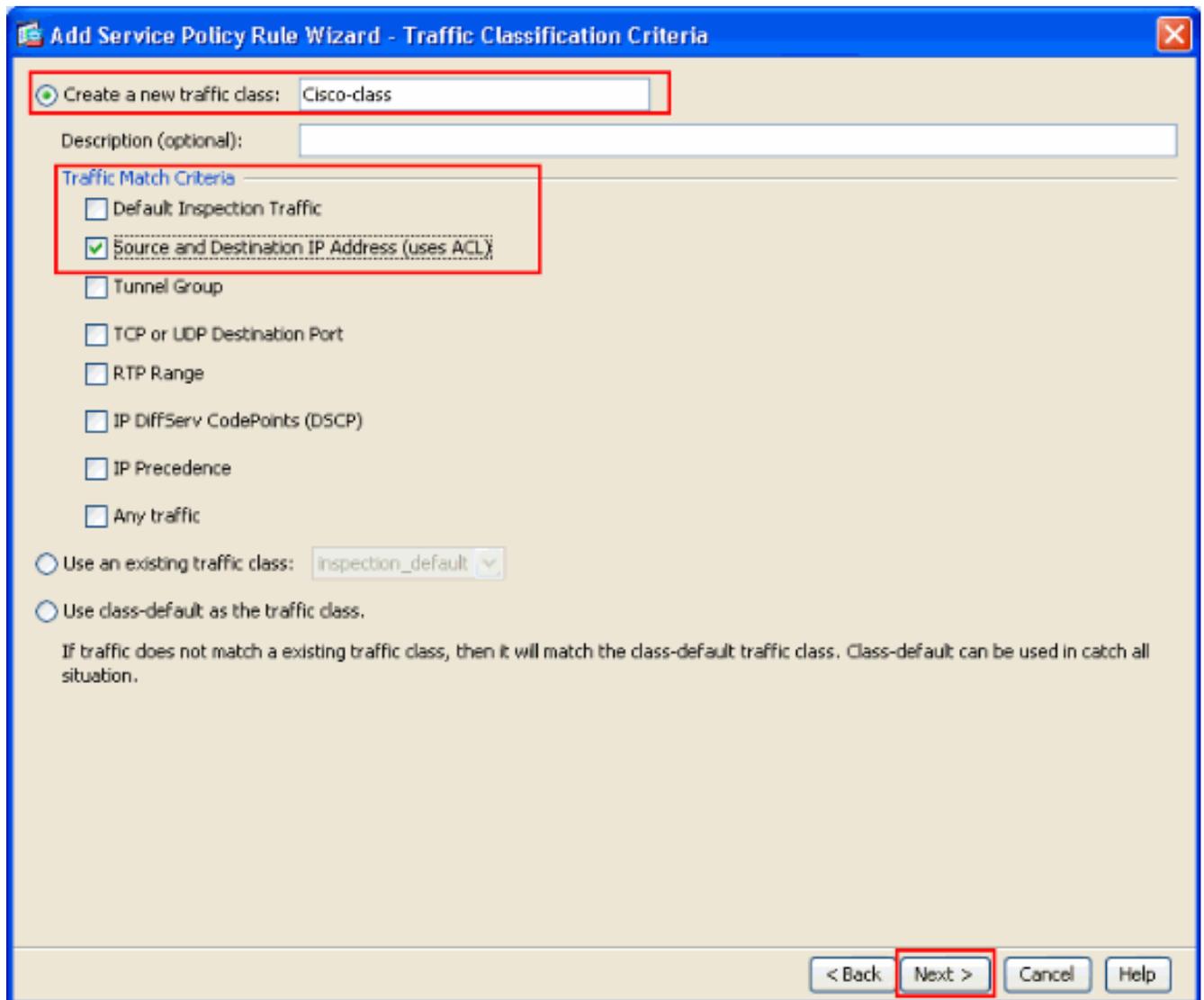
Only one service policy can be configured per interface or at global level. If a service policy already exists, then you can add a new rule into the existing service policy. Otherwise, you can create a new service policy.

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

Global - applies to all interfaces
Policy Name:
Description:

< Back **Next >** Cancel Help

3. Créez une Cisco-classe de nom de class map et cochez la case de **source et d'adresse IP de destination (ACL d'utilisations)** dans le critère de correspondance du trafic. Cliquez ensuite sur **Next**.



4. De l'assistant de règle de stratégie de service d'ajouter - correspondance du trafic - la fenêtre de **source et d'adresse de Destination**, choisissent la case d'option à côté de la **correspondance** et puis fournissent la source et l'adresse de destination comme affichée. Cliquez sur le bouton de déroulant à côté du **service** pour choisir les services requis.

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

Action: Match Do not match

Source: 10.77.241.129

Destination: any

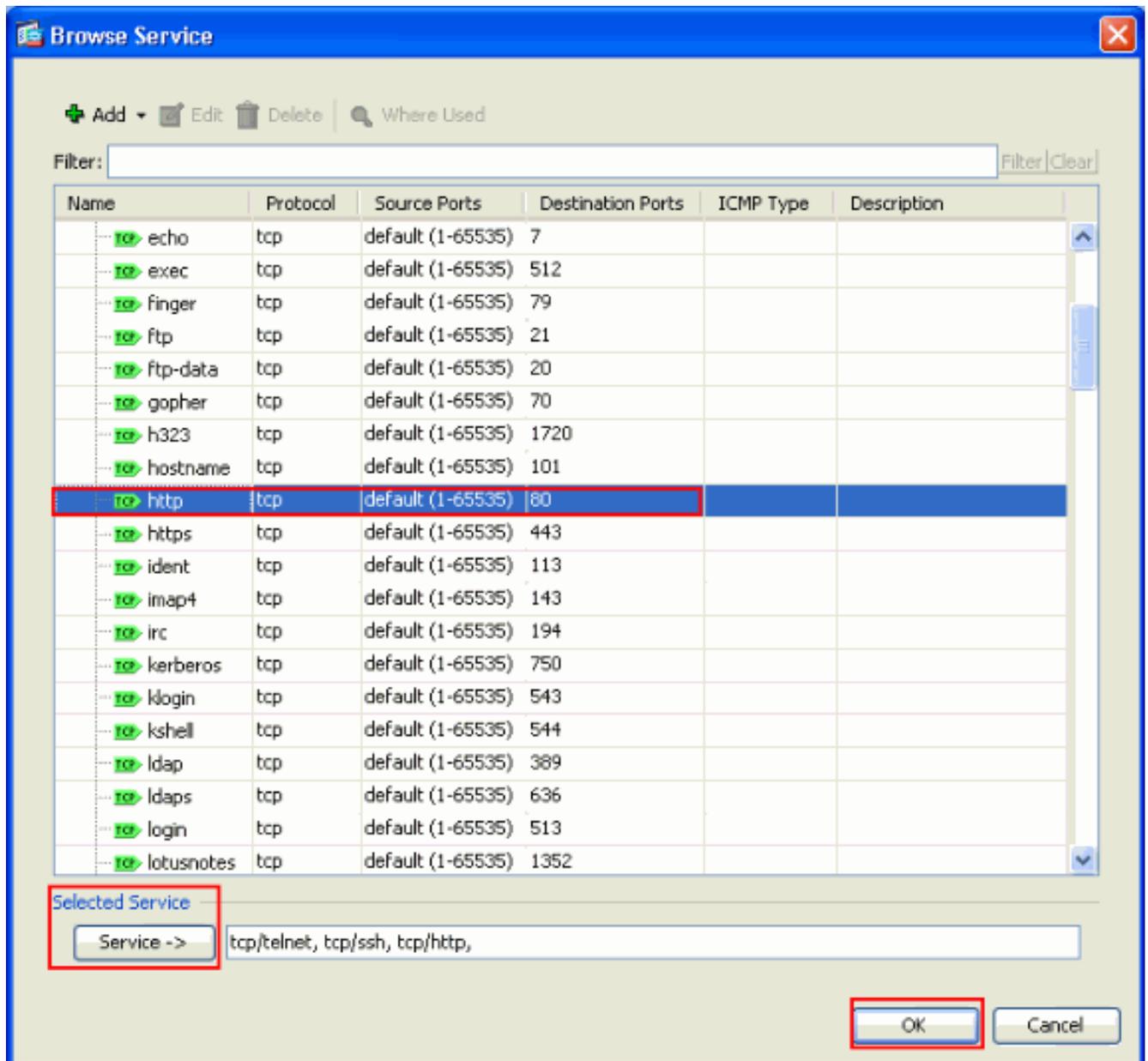
Service: ip

Description:

More Options

< Back Next > Cancel Help

5. Sélectionnez les services requis tels que le **telnet**, le **ssh** et le **HTTP**. Puis, cliquez sur **OK**.



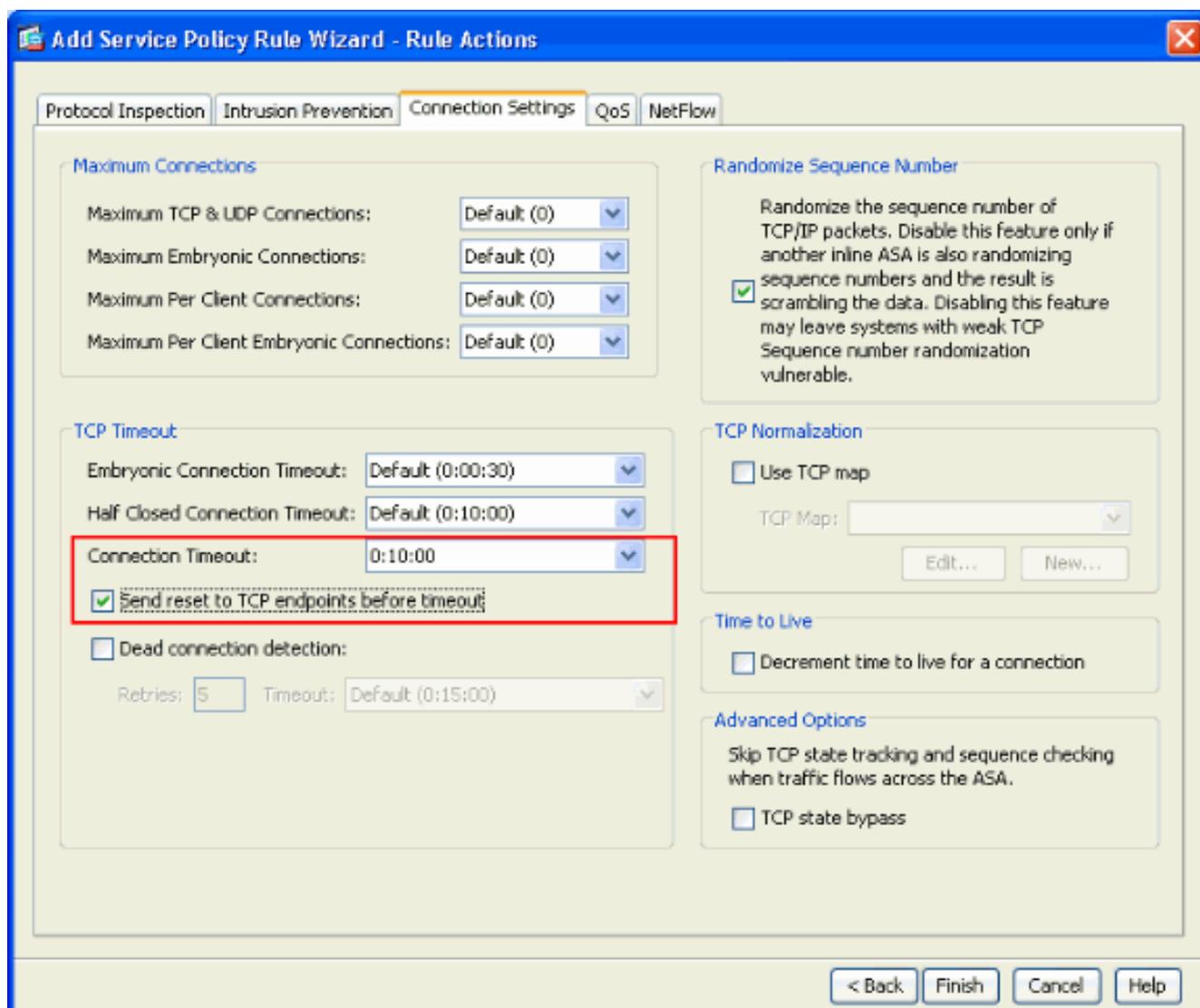
6. Configurez les délais d'attente. Cliquez sur Next (Suivant).

The screenshot shows a Windows-style dialog box titled "Add Service Policy Rule Wizard - Traffic Match - Source and Destination Address". The dialog has a blue title bar with a close button in the top right corner. The main area is light beige and contains the following fields:

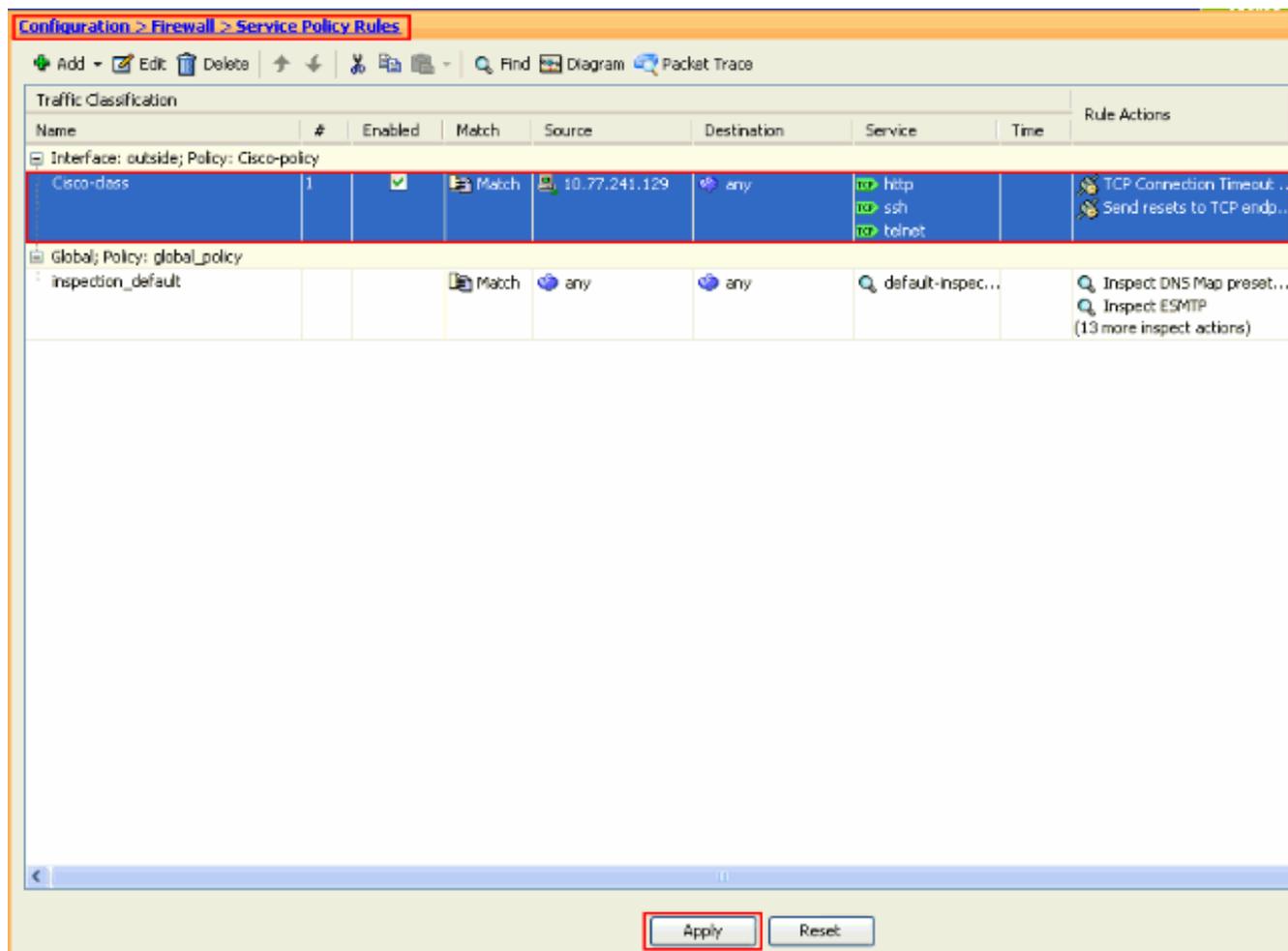
- Action:** Two radio buttons are present: "Match" (which is selected) and "Do not match".
- Source:** A text input field containing "10.77.241.129" and a small dropdown arrow on the right.
- Destination:** A text input field containing "any" and a small dropdown arrow on the right.
- Service:** A text input field containing "tcp/telnet, tcp/ssh, tcp/http," and a small dropdown arrow on the right.
- Description:** A large, empty text area.

Below these fields is a horizontal bar with the text "More Options" on the left and a downward-pointing arrow on the right. At the bottom right of the dialog, there are four buttons: "< Back", "Next >" (which is highlighted with a red rectangular box), "Cancel", and "Help".

7. Choisissez les **paramètres de connexion** afin d'installer le délai d'attente de connexion TCP en tant que 10 minutes. En outre, cochez l'**envoi remis à l'état initial aux points finaux de TCP avant case de délai d'attente**. Cliquez sur **Finish** (Terminer).



8. Cliquez sur Apply afin de s'appliquer la configuration aux dispositifs de sécurité. Ceci se termine la configuration.



Délai d'attente d'Ebryonic

Une connexion embryonnaire est la connexion qui est demi s'ouvrent ou, par exemple, la connexion en trois étapes n'a pas été terminée pour elle. Il est défini comme délai d'attente de synchronisation sur l'ASA. Par défaut, le délai d'attente de synchronisation sur l'ASA est de 30 secondes. C'est comment configurer le délai d'attente embryonnaire :

```
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
```

Dépanner

Si vous constatez que le délai d'attente de connexion ne fonctionne pas avec le MPF, alors vérifiez la connexion d'initiation de TCP. La question peut être une inversion de la source et de l'adresse IP de destination, ou une adresse IP mal configurée dans la liste d'accès ne s'assortit pas dans le MPF pour placer la nouvelle valeur du dépassement de durée ou pour changer le délai d'attente par défaut pour l'application. Créez une entrée de liste d'accès (source et destination) selon la demande de connexion afin de placer le délai d'attente de connexion avec MPF.

Informations connexes

- [Cisco Adaptive Security Device Manager](#)
- [Dispositifs de sécurité adaptatifs de la gamme Cisco ASA 5500](#)
- [Demandes de commentaires \(RFC\)](#)
- [Support et documentation techniques - Cisco Systems](#)