ASA 8.3 以降： MPF を使用した SSH/Telnet/HTTP 接続のタイムアウトの設定例

目次

はじめに

このドキュメントでは、すべてのアプリケーションではなく SSH/Telnet/HTTP などの特定のアプリケーションに固有のタイムアウトの設定例を、Cisco 適応型セキュリティ アプライアンス（ASA）バージョン 8.3(1) 以降を対象として示します。 この設定例では、Cisco 適応型セキュリティ アプライアンス（ASA）バージョン 7.0 で導入されたモジュラ ポリシー フレームワーク（MPF）を使用します。 詳細は、『モジュラ ポリシー フレームワークの使用』を参照してください。

この設定例では、ワークステーション（10.77.241.129）から Telnet、SSH、HTTP により、ルータの背後にあるリモート サーバ（10.1.1.1）に接続できるよう、Cisco ASA を設定します。 Telnet/SSH/HTTP トラフィックに対する別の接続タイムアウトも設定します。 他のすべての TCP トラフィックでは引き続き、**timeout conn 1:00:00** に関連付けられている通常の接続タイムアウト値を使用します。

バージョン 8.2 以前の Cisco ASA での同じ設定については、『PIX/ASA 7.x 以降/FWSM： MPF を使用した SSH/Telnet/HTTP 接続のタイムアウトの設定例』を参照してください。

前提条件

要件

このドキュメントに関しては個別の要件はありません。

使用するコンポーネント

このドキュメントの情報は、Cisco ASA セキュリティ アプライアンス ソフトウェア バージョン 8.3 (1) と Adaptive Security Device Manager (ASDM) 6.3 が稼働する環境に基づいています。

本書の情報は、特定のラボ環境にあるデバイスに基づいて作成されたものです。 このドキュメントで使用するすべてのデバイスは、初期 (デフォルト) 設定の状態から起動しています。 稼働中のネットワークで作業を行う場合、コマンドの影響について十分に理解したうえで作業してください。

表記法

ドキュメント表記の詳細は、『シスコ テクニカル ティップスの表記法』を参照してください。

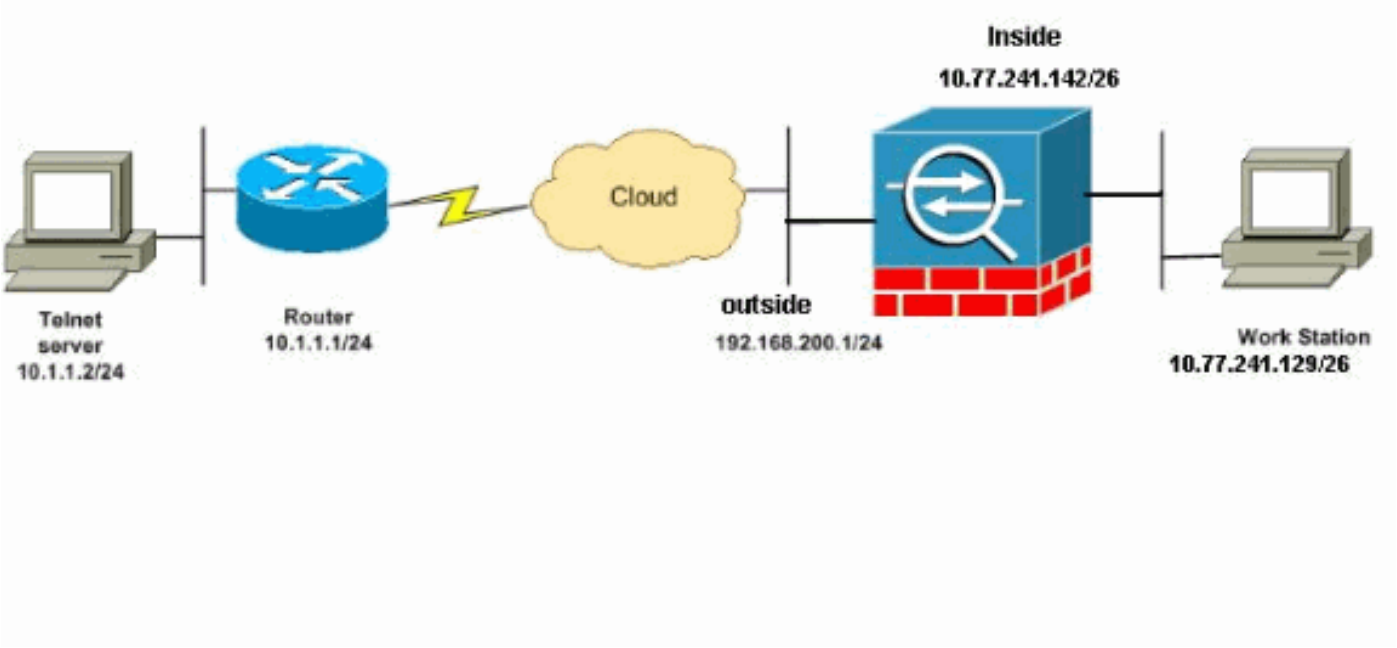
設定

この項では、このドキュメントで説明する機能の設定に必要な情報を提供します。

注: このセクションで使用されているコマンドの詳細を調べるには、Command Lookup Tool (登録ユーザ専用) を使用してください。

ネットワーク図

このドキュメントでは、次のネットワーク構成を使用しています。



注: この設定で使用している IP アドレス スキームは、インターネット上で正式にルーティング可能なものではありません。 これらはラボ環境で使用された RFC 1918 でのアドレスです。

設定

このドキュメントでは、次の設定を使用します。

- CLI 設定
- ASDM の設定

注: 後述の CLI および ASDM の設定は、ファイアウォール サービス モジュール（FWSM）に適用できます。

CLI 設定

ASA 8.3(1) の設定

```
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 1mZfSd48bl0UdPgP 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.
```

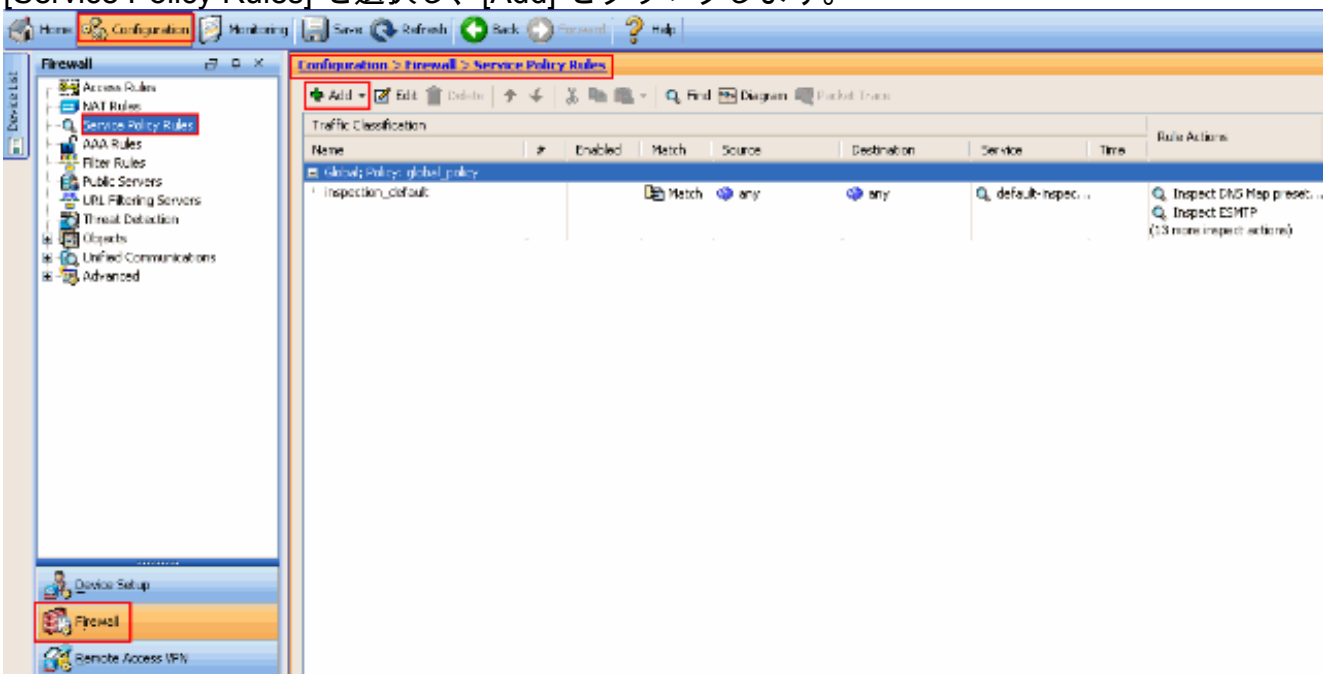
```
service-policy Cisco-policy interface outside
end
```

ASDM の設定

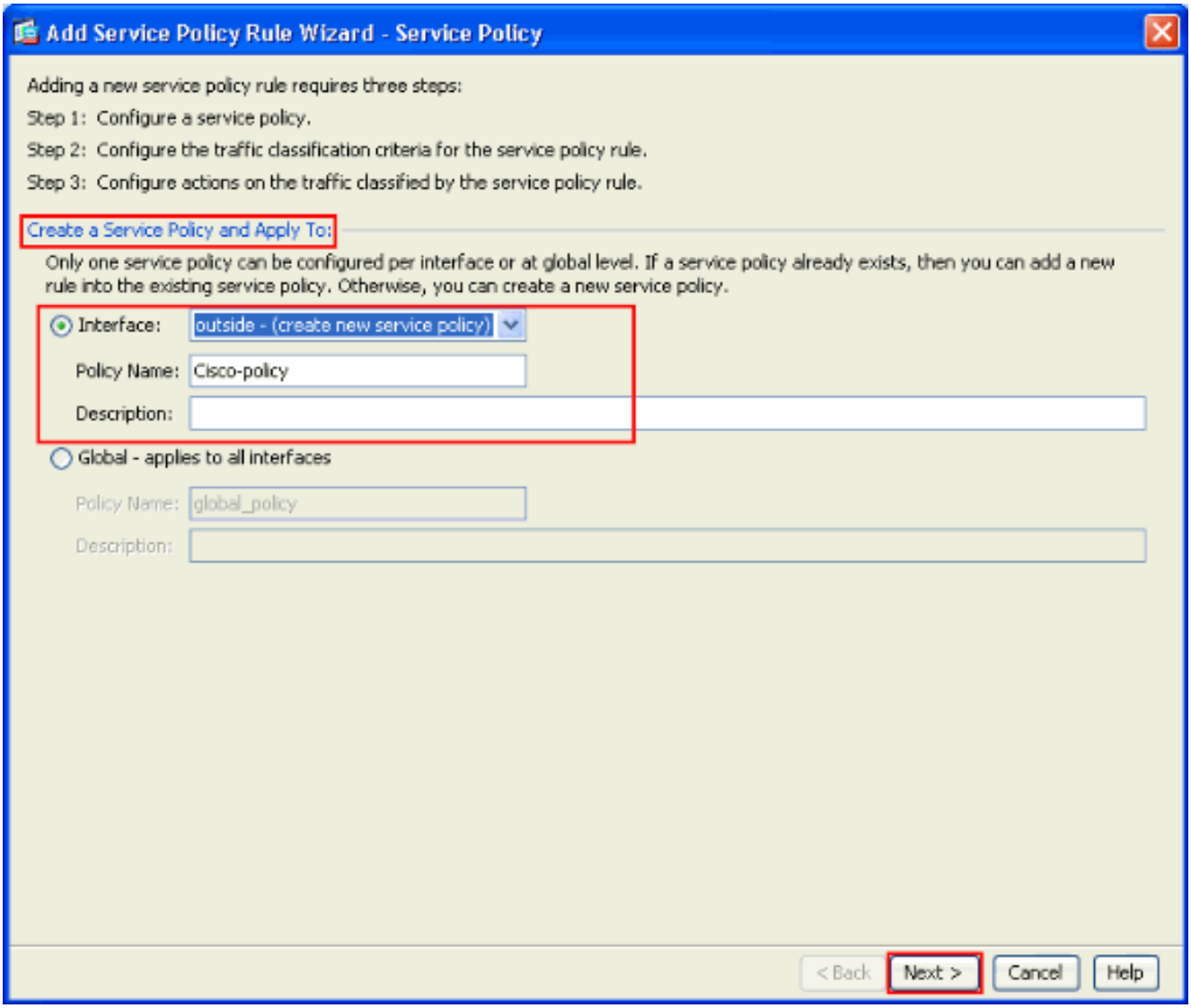
次に示す ASDM を使用して、Telnet、SSH、HTTP のトラフィックに対して TCP 接続のタイムアウトを設定するには、以下の手順を実行します。

注: ADSM を介して PIX/ASA にアクセスするための基本的な設定については、『ASDM 用の HTTPS アクセスの許可』を参照してください。

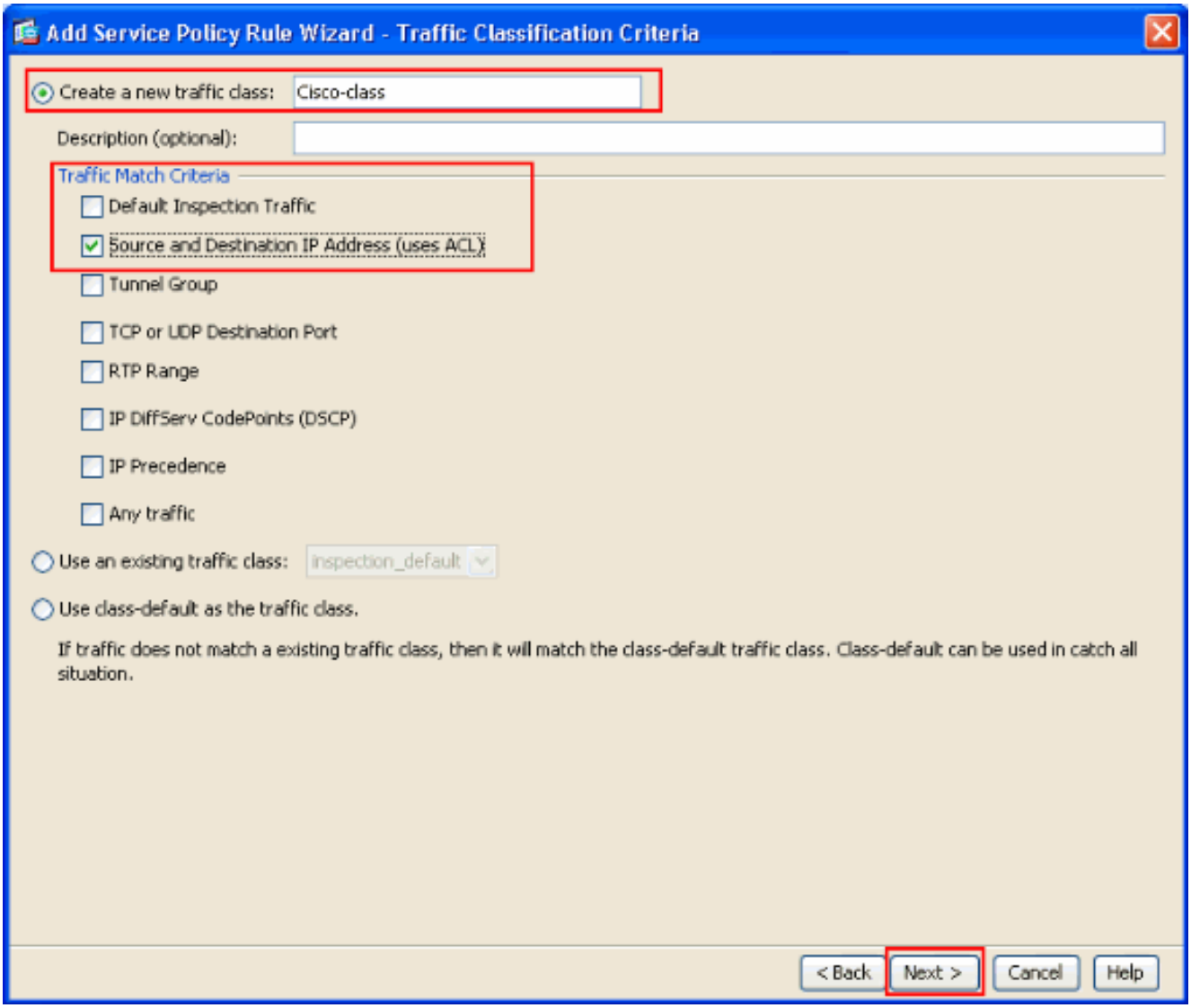
1. 次に示すようにサービス ポリシー ルールを設定するには、[Configuration] > [Firewall] > [Service Policy Rules] を選択し、[Add] をクリックします。



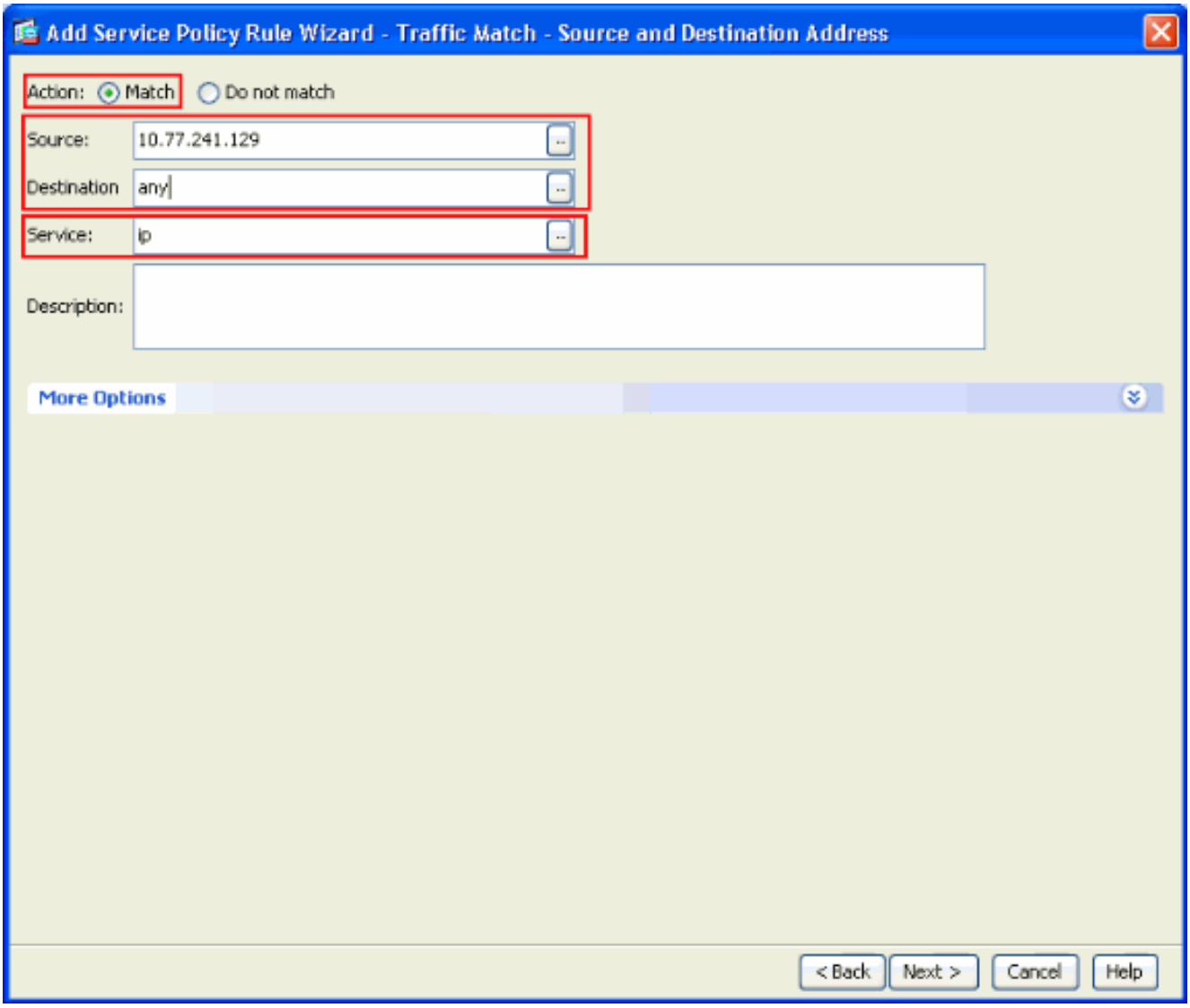
2. [Add Service Policy Rule Wizard - Service Policy] ウィンドウで、[Create a Service Policy and Apply To] セクションの [Interface] の横のオプション ボタンを選択します。 次に、目的のインターフェイスをドロップダウン リストから選択し、[Policy Name] にポリシー名を入力します。 この例で使用しているポリシー名は **Cisco-policy** です。 次に、[Next] をクリックします。



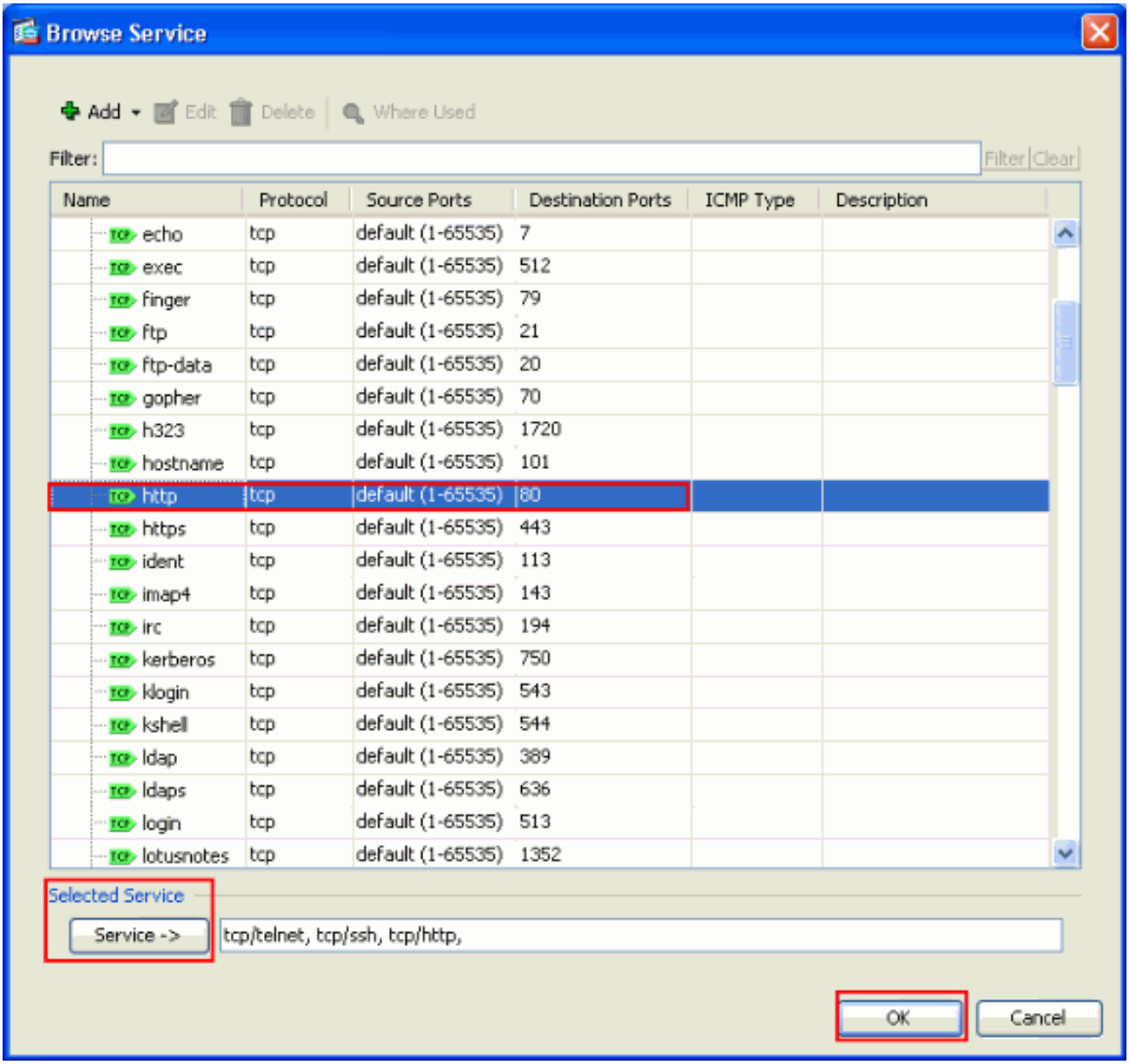
3. クラス マップ名 **Cisco-class** を作成し、[Traffic Match Criteria] の [Source and Destination IP address (uses ACL)] チェック ボックスをオンにします。 次に、[Next] をクリックします。



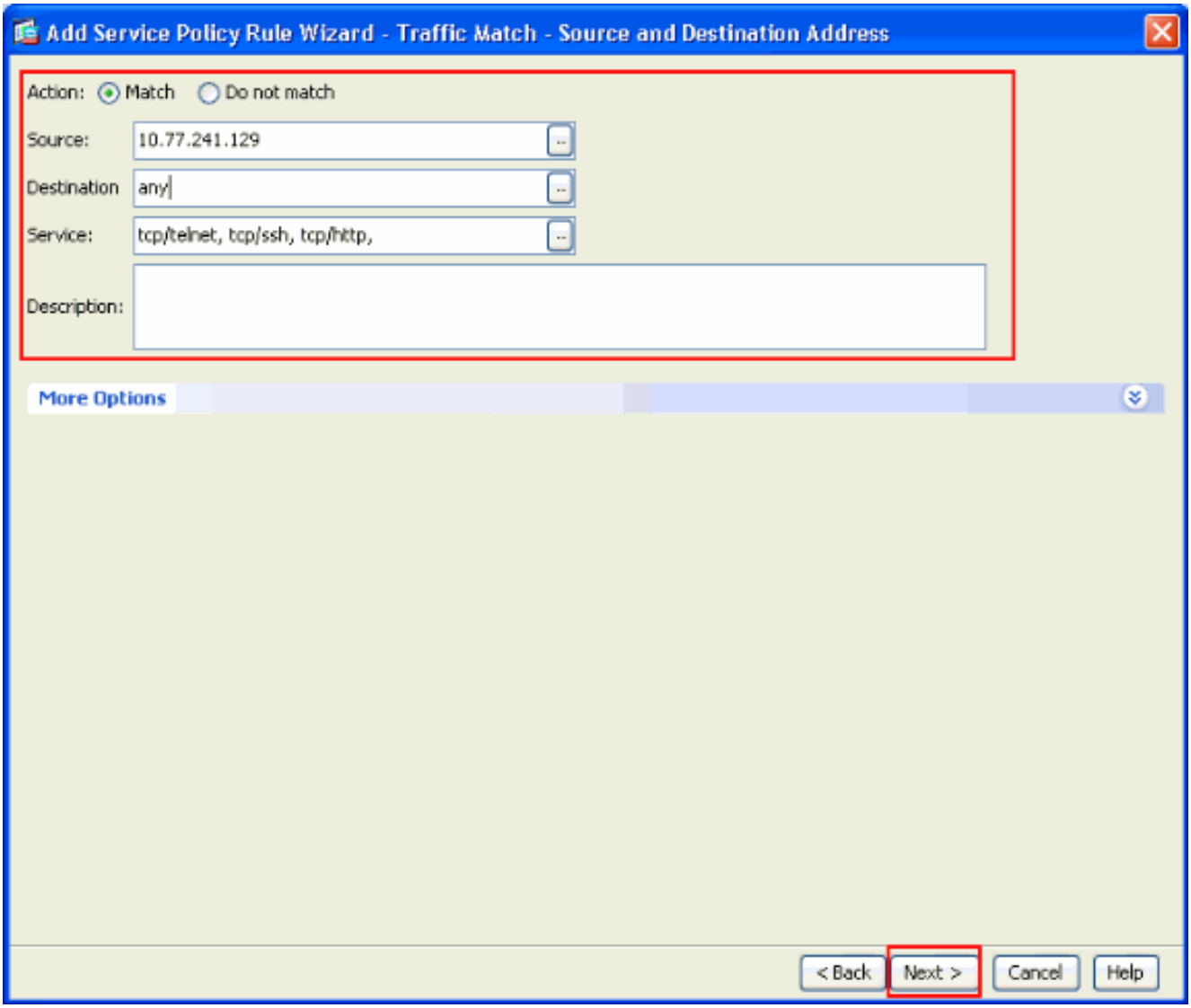
4. [Add Service Policy Rule Wizard - Traffic Match - Source and Destination Address] ウィンドウで、[Match] の横のオプション ボタンを選択し、図のように送信元アドレスと宛先アドレスを入力します。 [Service] の横のドロップダウン ボタンをクリックし、必要なサービスを選択します。



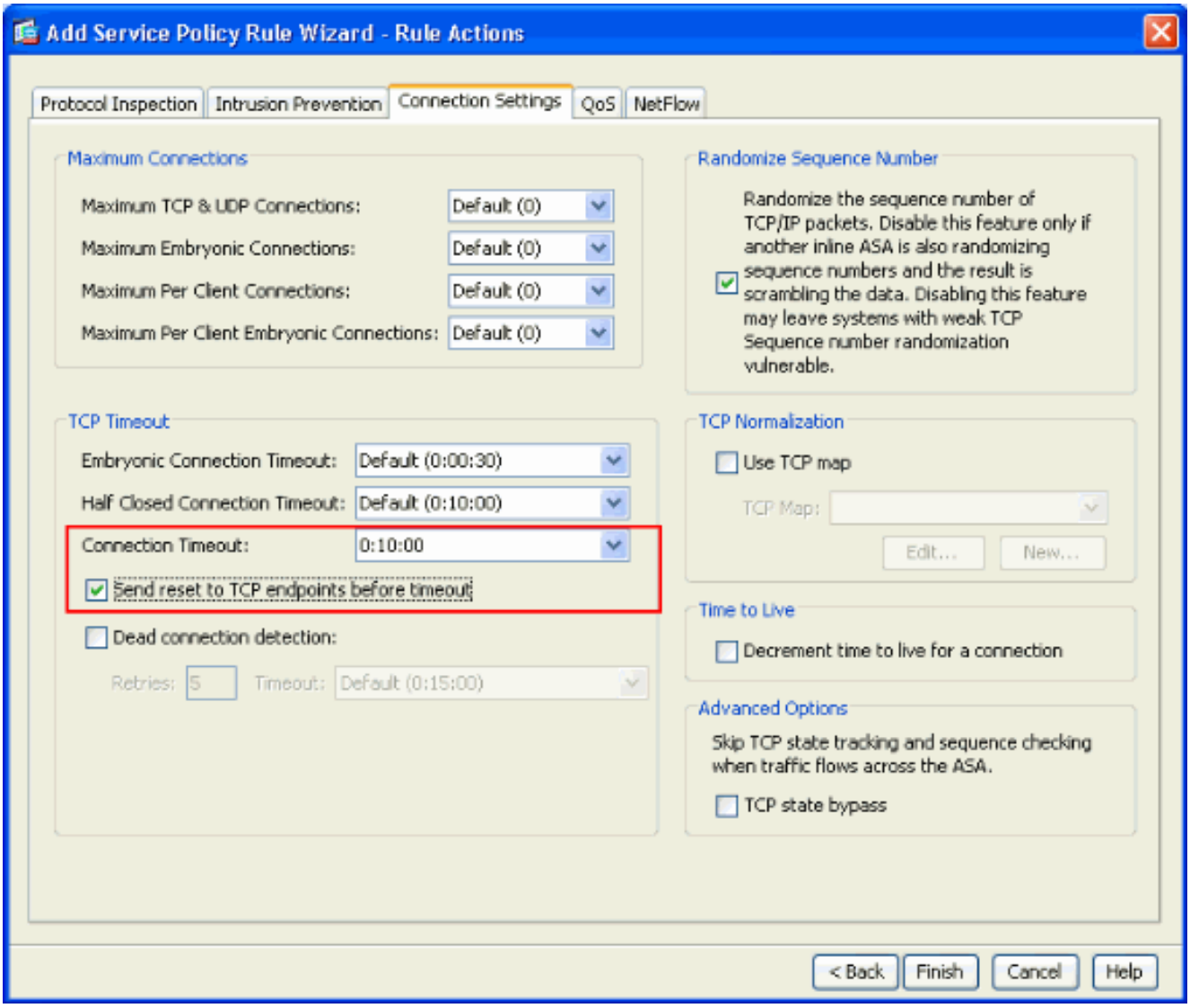
5. telnet、ssh、http などの必要なサービスを選択します。 次に、[OK] をクリックします。



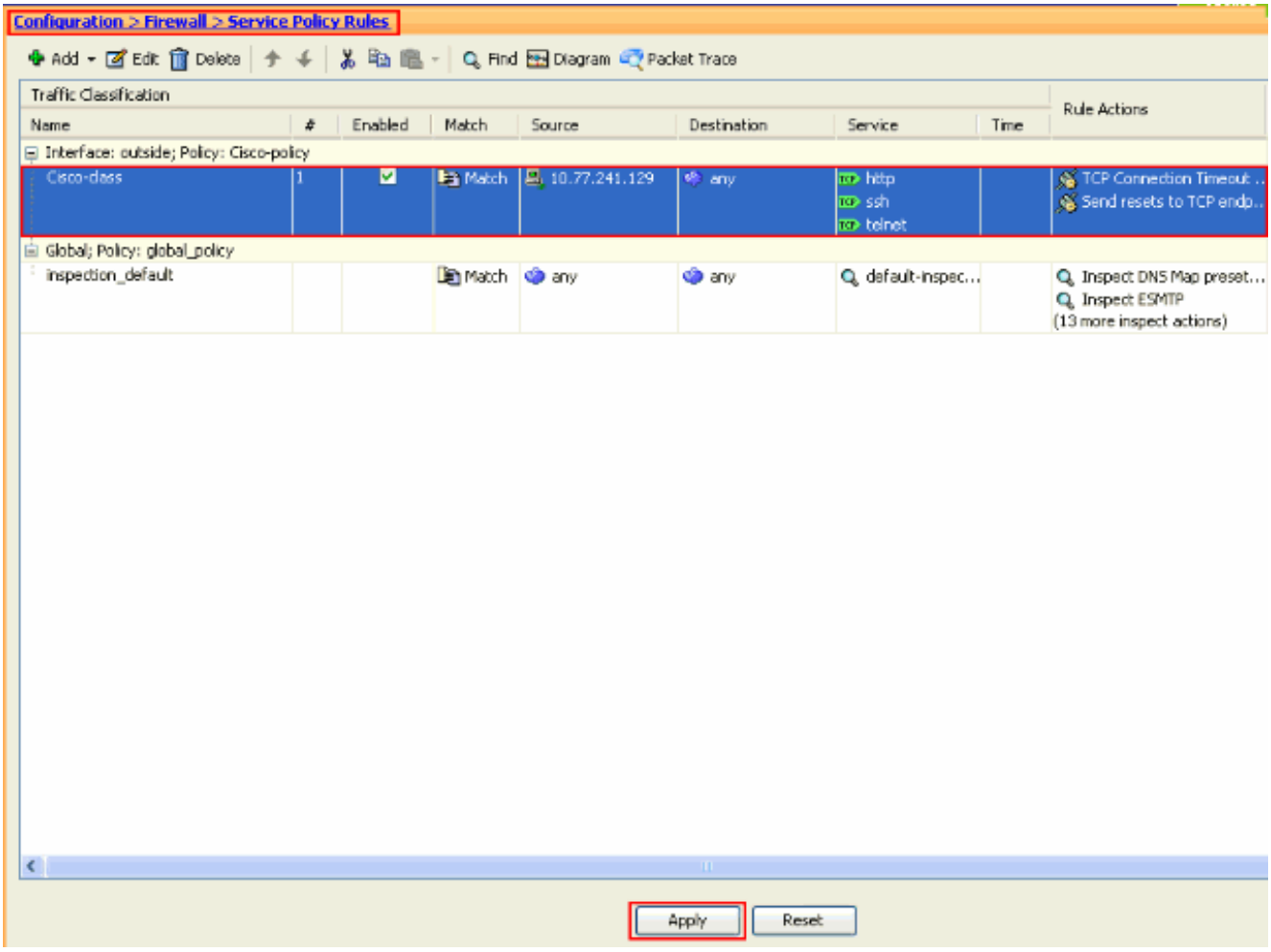
6. **タイムアウトの設定** [Next] をクリックします。



7. TCP の接続タイムアウトを 10 分に設定するには、[Connection Settings] を選択します。 また、[Send reset to TCP endpoints before timeout] チェック ボックスをオンにします。 **[Finish] をクリックします。**



8. [Apply] をクリックして、セキュリティ アプライアンスに設定を適用します。これで、設定は完了です。



初期タイムアウト

初期タイムアウトとは、ハーフ オープンの接続（3 ウェイのハンドシェイクが完了していない場合など）のことです。 ASA 上では SYN タイムアウトとして定義されています。 ASA 上の SYN タイムアウトのデフォルト値は 30 秒です。 以下に初期タイムアウトの設定方法を示します。

```
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 1mZfSd48bl0UdPgP 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
```

トラブルシューティング

接続タイムアウトが MPF で正常に機能しない場合は、TCP 初期接続をチェックしてください。この問題の原因としては、送信元と宛先の IP アドレスが逆転していることが考えられます。また、アクセス リスト内の IP アドレスの設定が間違っていて MPF 内で一致せず、該当アプリケーションでの新しいタイムアウト値の設定またはデフォルト タイムアウトの変更が行えないことも考えられます。 接続の開始に合ったアクセス リスト エントリ（送信元と宛先）を作成し、MPF で接続タイムアウトを設定します。

関連情報

- Cisco Adaptive Security Device Manager
- Cisco ASA 5500 シリーズ適応型セキュリティ アプライアンス
- Requests for Comments（RFC）
- テクニカル サポートとドキュメント – Cisco Systems