

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

Document ID: 68332

Updated: 2008 年 10 月 16 日



[PDF のダウンロード](#)



[印刷](#)

[\[+\] フィードバック](#)

関連製品

- [Cisco Adaptive Security Device Manager](#)
- [Cisco ASA 5500-X シリーズ次世代ファイアウォール](#)
- [Cisco PIX 500 シリーズ セキュリティ アプライアンス](#)

目次

[概要](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[表記法](#)

[設定](#)

[ネットワーク図](#)

[設定](#)

[初期タイムアウト](#)

[確認](#)

[トラブルシューティング](#)

[関連情報](#)

[Cisco サポート コミュニティ - 特集対話](#)

概要

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、PIX 7.1(1) 以降を対象として示します。この設定例では、PIX 7.0 で導入された新しいモジュラ ポリシー フレームワークを使用します。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、PIX ファイアウォールを設定します。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。

[AASA 8.3 およびそれ以降を参照して下さい](#)。バージョン 8.3 および それ 以降との Cisco 適応型セキュリティ アプライアンス (ASA) ソフトウェアの ASDM を使用して同一の構成に関する詳細については [MPF 設定例を使用して SSH/Telnet/HTTP 接続 タイムアウトを \(ASA \) 設定して下さい](#)。

[前提条件](#)

[要件](#)

このドキュメントに関する固有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 PIX/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 7.1 (1) と Adaptive Security Device Manager (ASDM) 5.1 が稼働する環境に基づいています。

このドキュメントの情報は、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、クリアな (デフォルト) 設定で作業を開始しています。ネットワークが稼働中の場合は、コマンドが及ぼす潜在的な影響を十分に理解しておく必要があります。

[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。

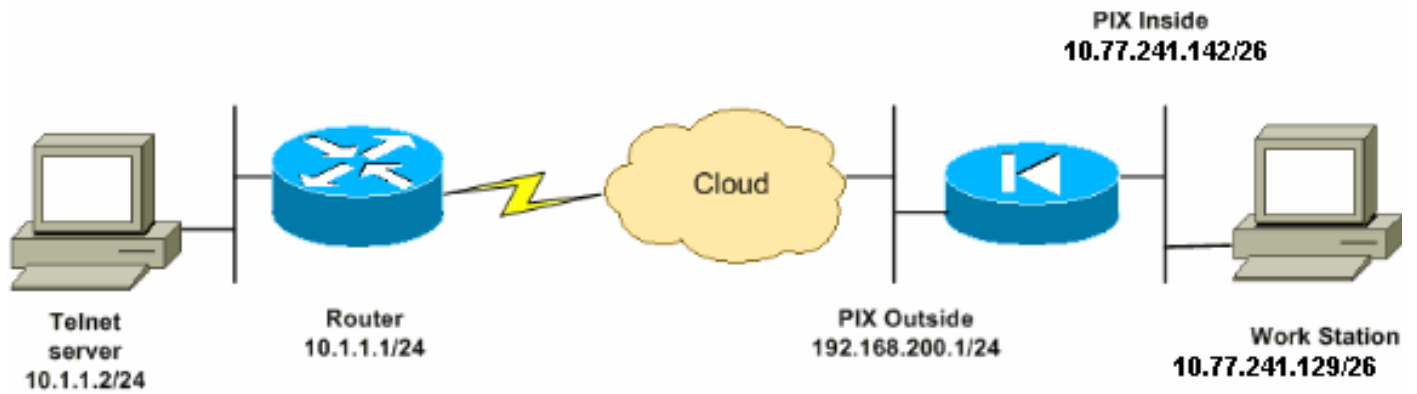
[設定](#)

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ています。

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

CLI による設定 :

PIX の設定

```
PIX Version - 7.1(1)
!
hostname PIX
domain-name Cisco.com
enable password 8Ry2YjIyt7RRXU24 encrypted
names
!
interface Ethernet0
 nameif outside
 security-level 0
 ip address 192.168.200.1 255.255.255.0
!
interface Ethernet1
 nameif inside
 security-level 100
 ip address 10.77.241.142 255.255.255.192
!

access-list inside_nat0_outbound extended permit ip
10.77.241.128 255.255.255.192 any

!--- Define the traffic that has to be matched in the
class map. !--- Telnet is defined in this example.
access-list outside_mpc_in extended permit tcp host
10.77.241.129 any eq telnet access-list outside_mpc_in
extended permit tcp host 10.77.241.129 any eq ssh
access-list outside_mpc_in extended permit tcp host
10.77.241.129 any eq www access-list 101 extended permit
tcp 10.77.241.128 255.255.255.192 any eq telnet access-
list 101 extended permit tcp 10.77.241.128
255.255.255.192 any eq ssh access-list 101 extended
permit tcp 10.77.241.128 255.255.255.192 any eq www
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 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 telnet 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 telnet description telnet match access-list
outside_mpc_in 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
esmtip inspect sqlnet inspect sunrpc inspect tftp inspect
sip inspect xdmcp !--- Use the pre-defined class map
telnet in the policy map. policy-map telnet !--- Set the
connection timeout under the class mode in which !---
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 telnet set connection timeout tcp
00:10:00 reset ! ! service-policy global_policy global
!--- Apply the policy-map telnet on the interface. !---
You can apply the service-policy command to any
interface that !--- can be defined by the nameif
command. service-policy telnet interface outside end

```

ASDM による設定：

後述のステップを実行して、ASDM を使用するアクセスリストに基づき、Telnet トラフィックの TCP 接続タイムアウトを図のように設定します。

注: ASDM 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. インターフェイスの設定[Configuration] > [Interfaces] > [Add] を選択して、インターフェイス Ethernet0 (outside) と Ethernet1 (inside) を図のように設定します。

Hardware Port:

Ethernet0

Configure Hardware Properti

Enable Interface

Dedicate this interface to management only

Interface Name:

outside

Security Level:

0

IP Address

Use Static IP

Obtain Address via DHCP

IP Address:

192.168.200.1

Subnet Mask:

255.255.255.0

MTU:

1500

Description:

OK

Cancel

Help

Hardware Port: **Ethernet1** Configure Hardware Properties

Enable Interface Dedicate this interface to management only

Interface Name:

Security Level:

IP Address

Use Static IP Obtain Address via DHCP

IP Address:

Subnet Mask:

MTU:

Description:

[OK] をクリックします。

Configuration > Interfaces

Interface	Name	Enabled	Security Level	IP Address	Subnet Mask	Management Only	MTU
Ethernet0	outside	Yes	0	192.168.200.1	255.255.255.0	No	1500
Ethernet1	inside	Yes	100	10.77.241.142	255.255.255.192	No	1500

これを CLI で設定すると、次のようになります。interface Ethernet0

```

nameif outside
security-level 0
ip address 192.168.200.1 255.255.255.0
!
interface Ethernet1
nameif inside
security-level 100
ip address 10.77.241.142 255.255.255.192

```

2. NAT 0 の設定[Configuration] > [NAT] > [Translation Exemption Rules] > [Add] を選択して、ネットワーク 10.77.241.128/26 からのトラフィックが変換なしにインターネットにアクセスできるようにします。

Configuration > NAT > Translation Exemption Rules

Add Address Exemption Rule

Action

Select an action:

Host/Network Exempted From NAT

IP Address Name Group

Interface:

IP address:

Mask:

When Connecting To

IP Address Name Group

Interface:

IP address:

Mask:

Rule Flow Diagram

Rule applied to traffic incoming to source interface

Please enter the description below (optional):

OK Cancel Help

[OK] をクリックします。

Configuration > NAT > Translation Exemption Rules

Enable traffic through the firewall without address translation

Translation Rules Translation Exemption Rules

Show Rules for Interface:

#	Rule Enabled	Action	Interface	Host/Network	When Connecting To Host/Network
1	<input checked="" type="checkbox"/>	exempt	inside (outbound)	10.77.241.128/26	any

これを CLI で設定すると、次のようになります。 `access-list inside_nat0_outbound extended permit ip 10.77.241.128 255.255.255.192 any`

```
nat (inside) 0 access-list inside_nat0_outbound
```

3. **ACL の設定**[Configuration] > [Security Policy] > [Access Rules] を選択して、ACL を図のように設定します。[Add] をクリックして ACL 101 を設定し、ネットワーク 10.77.241.128/26 から発信された Telnet トラフィックが任意の宛先ネットワークに到達できるようにし、それを outside インターフェイス上の発信トラフィックに適用します。

The screenshot shows the configuration for an Access Rule. The 'Action' is set to 'permit' and 'Apply to Traffic' is 'outgoing from destination interface'. The source is configured as 'IP Address' on the 'inside' interface with IP address '10.77.241.128' and mask '255.255.255.192'. The destination is configured as 'IP Address' on the 'outside' interface with IP address '0.0.0.0' and mask '0.0.0.0'. The 'Protocol and Service' section shows 'TCP' selected, with 'Source Port' set to 'any' and 'Destination Port' set to 'telnet'. A 'Rule Flow Diagram' shows traffic from '10.77.241.128/26' on the 'inside' interface being allowed to the 'outside' interface, with the text 'Rule applied to traffic outgoing from destination interface' and 'Allow traffic'.

[OK] をクリックします。ssh および http トラフィックの場合も、同様に設定します。

Action

Select an action:

Apply to Traffic:

Syslog

Default Syslog

Time Range

Time Range:

Source Host/Network

IP Address Name Group

Interface:

IP address:

Mask:

Destination Host/Network

IP Address Name Group

Interface:

IP address:

Mask:



Protocol and Service

TCP UDP ICMP IP

Source Port

Service =

Service Group

Destination Port

Service =

Service Group

Action

Select an action:

Apply to Traffic:

Syslog

Default Syslog

Time Range

Time Range:

Source Host/Network

IP Address Name Group

Interface:

IP address:

Mask:

Destination Host/Network

IP Address Name Group

Interface:

IP address:

Mask:

Rule Flow Diagram

Rule applied to traffic outgoing from destination interface

Protocol and Service

TCP UDP ICMP IP

Source Port

Service =

Service Group

Destination Port

Service =

Service Group

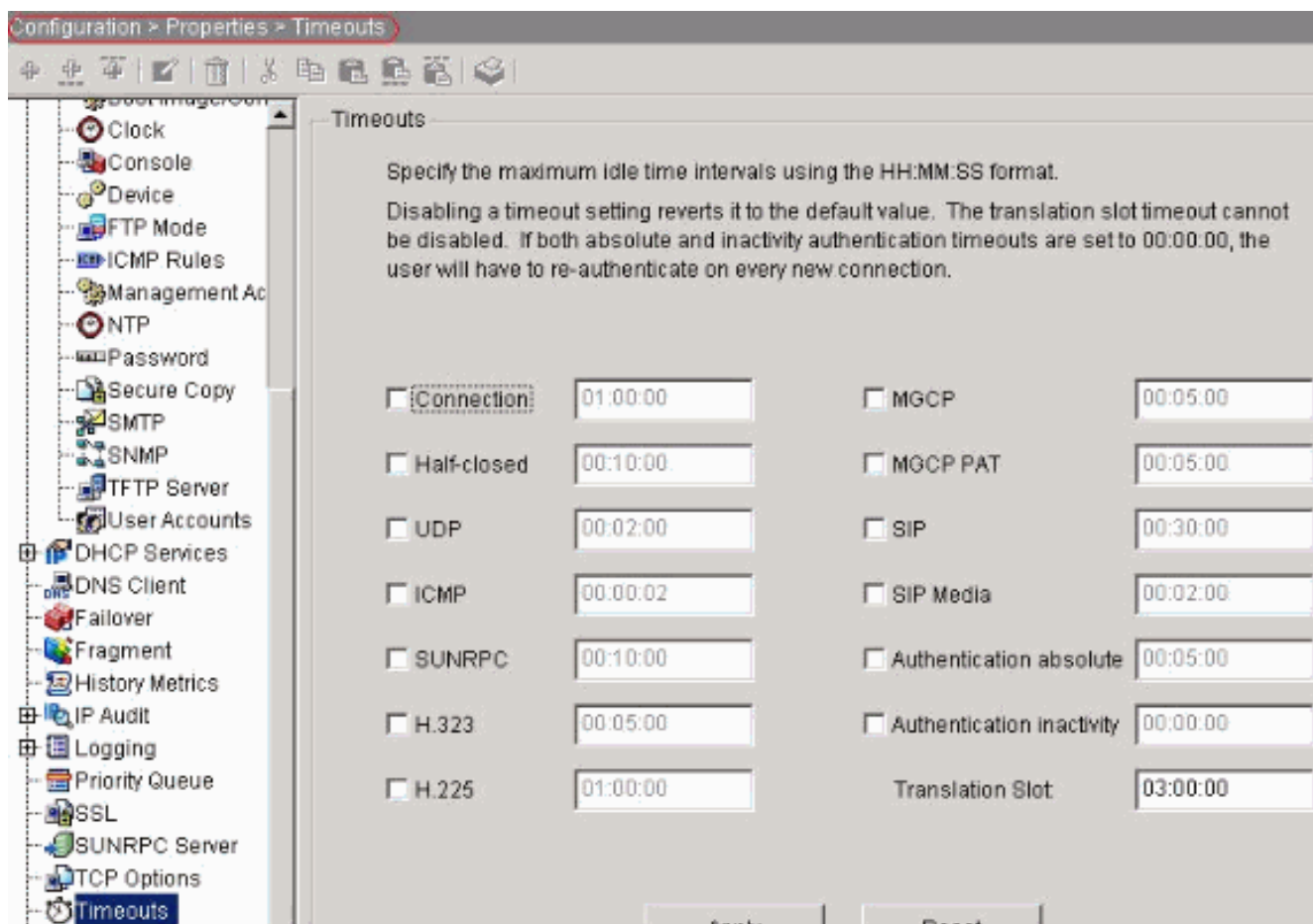
これを CLI で設定すると、次のようになります。

```

access-list 101 extended permit tcp
10.77.241.128 255.255.255.192 any eq telnet
access-list 101 extended permit tcp 10.77.241.128 255.255.255.192 any eq ssh
access-list 101 extended permit tcp 10.77.241.128 255.255.255.192 any eq www
access-group 101 out interface outside

```

4. タイムアウトの設定[Configuration] > [Properties] > [Timeouts] を選択し、さまざまなタイムアウトを設定します。このシナリオでは、すべてのタイムアウトに対して、デフォルト値のままとします。



これを CLI で設定すると、次のようになります。timeout conn 1:00:00 half-closed 0:10:00
udp 0:02:00 icmp 0:00:02

5. **Service Policy Rules** の設定 [Configuration] > [Security Policy] > [Service Policy Rules] > [Add] を選択してクラス マップおよびポリシーマップを設定し、TCP 接続タイムアウトを 10 分にします。そして、outside インターフェイスのサービス ポリシーを図のように適用します。[Interface] オプション ボタンを選択して、作成する [outside - (create new service policy)] を選択し、ポリシー名として **telnet** を割り当てます。

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:

telnet

Description:

Global - applies to all interfaces

Policy Name:

global_policy

[Next] をクリックします。クラス マップ名 **telnet** を作成し、[Traffic match criteria] の [Source and Destination IP address (uses ACL)] チェックボックスを選択します。

Create a new traffic class:

telnet

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

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.

Use class-default as the traffic class.


[Next] をクリックします。ネットワーク 10.77.241.128/26 から任意の宛先ネットワークに発信される Telnet トラフィックに照合させるための ACL を作成し、それをクラス telnet に適用します。

Action
Select an action: **match**

Time Range
Time Range: -- Not Applied -- New...

Source Host/Network
 IP Address Name Group
 Interface: **outside**
 IP address: **10.77.241.128** ...
 Mask: **255.255.255.128**

Destination Host/Network
 IP Address Name Group
 Interface: **inside**
 IP address: **0.0.0.0** ...
 Mask: **0.0.0.0**

Rule Flow Diagram
 Rule applied to traffic incoming to source interface


Protocol and Service
 TCP UDP ICMP IP Manage Service Groups...

Source Port
 Service = **any** ...
 Service Group

Destination Port
 Service = **telnet** ...
 Service Group

[Next] をクリックします。 ssh および http トラフィックの場合も、同様に設定します。

Action
Select an action:

Time Range
Time Range:

Source Host/Network
 IP Address Name Group
Interface:
IP address:
Mask:

Destination Host/Network
 IP Address Name Group
Interface:
IP address:
Mask:

Rule Flow Diagram
Rule applied to traffic incoming to source interface

```
graph LR; S[10.77.241.128/25] --> R((Router)); R --> D[any]; R --> M[match]; R --> O[outside]; R --> I[inside];
```

Protocol and Service
 TCP UDP ICMP IP

Source Port
 Service
 Service Group

Destination Port
 Service
 Service Group

Action
Select an action: **match**

Time Range
Time Range: -- Not Applied -- New...

Source Host/Network
 IP Address Name Group
 Interface: outside
 IP address: 10.77.241.128 ...
 Mask: 255.255.255.128

Destination Host/Network
 IP Address Name Group
 Interface: inside
 IP address: 0.0.0.0 ...
 Mask: 0.0.0.0

Rule Flow Diagram
 Rule applied to traffic incoming to source interface

 10.77.241.128/25 → outside → [Router] → inside → any
 match

Protocol and Service
 TCP UDP ICMP IP Manage Service Groups...

Source Port
 Service = any ...
 Service Group

Destination Port
 Service = www ...
 Service Group

[Connection Settings] を選択して、TCP 接続タイムアウトを 10 分に設定し、[Send reset to TCP endpoints before timeout] チェックボックスも選択します。

Protocol Inspection | Connection Settings | QoS

Maximum Connections

TCP & UDP Connections : Default (0)

Embryonic Connections: Default (0)

Per Client Connections: Default (0)

Per Client Embryonic Connections: Default (0)

Randomize Sequence Number

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

TCP Timeout

Connection Timeout : 00:10:00

Send reset to TCP endpoints before timeout

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

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

TCP Normalization

Use TCP Map

TCP Map:

New Edit

[Finish] をクリックします。

Configuration > Security Policy > Service Policy Rules

Access Rules AAA Rules Filter Rules **Service Policy Rules**

Show Rules for Interface: All Interfaces Show All

#	Traffic Classification							
	Name	Enabled	Match	Source	Destination	Service	Time Range	
Global, Policy: global_policy								
	inspection_d...			any	any	default-inspection		inspect (1
Interface: outside, Policy: telnet								
1	telnet	<input checked="" type="checkbox"/>		10.77.241...	any	telnet/tcp	-- Not Appl...	connectio send res

これを CLI で設定すると、次のようになります。access-list outside_mpc_in extended permit

```
tcp host 10.77.241.129 any eq telnet
```

```
access-list outside_mpc_in extended permit tcp host 10.77.241.129 any eq ssh
```

```
access-list outside_mpc_in extended permit tcp host 10.77.241.129 any eq www
```

```
class-map telnet
description telnet
match access-list outside_mpc_in
```

```
policy-map telnet
class telnet
set connection timeout tcp 00:10:00 reset
service-policy telnet interface outside
```

[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 ウエ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おり、ASA 上の SYN タイムアウトのデフォルト値は 30 秒です。初期タイムアウトを設定する方法を、次に示します。

```
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
```

確認

ここでは、設定が正常に動作していることを確認します。

[Output Interpreter Tool](#) (OIT) ([登録ユーザ専用](#)) では、特定の **show** コマンドがサポートされています。OIT を使用して、**show** コマンド出力の解析を表示できます。

show service-policy interface outside コマンドを発行すると、設定を確認できます。

```
PIX#show service-policy interface outside Interface outside: Service-policy: http Class-map:
http Set connection policy: Set connection timeout policy: tcp 0:05:00 reset Inspect: http,
packet 80, drop 0, reset-drop 0
```

[show service-policy flow](#) コマンドを発行すると、特定のトラフィックがサービス ポリシーの設定に一致していることを確認できます。

次に出力の例を示します。

```
PIX#show service-policy flow tcp host 10.77.241.129 host 10.1.1.2 eq 23 Global policy: Service-
policy: global_policy Interface outside: Service-policy: telnet Class-map: telnet Match: access-
list 101 Access rule: permit tcp 10.77.241.128 255.255.255.192 any eq telnet Action: Input flow:
set connection timeout tcp 0:10:00 reset
```

トラブルシューティング

接続タイムアウトが Modular Policy Framework (MPF; モジュラ ポリシー フレームワーク) でうまく機能しない場合は、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 PIX 500 シリーズ セキュリティ アプライアンス](#)
- [Cisco ASA 5500 シリーズ 適応型 セキュリティ アプライアンス](#)
- [Cisco PIX セキュリティ アプライアンス リリース ノート](#)
- [Cisco PIX Firewall ソフトウェア](#)
- [Cisco Secure PIX ファイアウォール コマンド リファレンス](#)

- [セキュリティ製品に関する Field Notice \(PIX を含む \)](#)
- [Requests for Comments \(RFC \)](#) 
- [テクニカルサポートとドキュメント - Cisco Systems](#)

このドキュメントは有用でしたか。 [はい いいえ](#)

フィードバックいただき、ありがとうございました。

[サポート ケースのオープン](#) ([シスコ サービス契約ts generic='1' nval='P%1,2%%'が必要ですよ](#))。

Cisco サポート コミュニティ - 特集対話

[Cisco サポート コミュニティ](#)では、フォーラムに参加して情報交換することができます。

このドキュメントで使用されている表記法の詳細は、『[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。

Updated: 2008 年 10 月 16 日

Document ID: 68332