

# PIX/ASA 7.x 이상/FWSM: MPF 컨피그레이션 예를 사용하여 SSH/텔넷/HTTP 연결 시간 초과 설정

## 목차

[소개](#)

[사전 요구 사항](#)

[요구 사항](#)

[사용되는 구성 요소](#)

[표기규칙](#)

[구성](#)

[네트워크 다이어그램](#)

[구성](#)

[ebryonic 시간 초과](#)

[다음을 확인합니다.](#)

[문제 해결](#)

## 소개

이 문서에서는 모든 애플리케이션에 적용되는 것과 달리 SSH/Telnet/HTTP와 같은 특정 애플리케이션에 특정한 시간 제한의 PIX 7.1(1) 이상에 대한 샘플 컨피그레이션을 제공합니다. 이 컨피그레이션 예에서는 PIX 7.0에 도입된 새로운 Modular Policy Framework를 사용합니다. 자세한 내용은 [Modular Policy Framework 사용](#)을 참조하십시오.

이 샘플 컨피그레이션에서는 워크스테이션(10.77.241.129)이 라우터 뒤에 있는 원격 서버(10.1.1.1)에 텔넷/SSH/HTTP를 사용하도록 PIX 방화벽이 구성됩니다. 텔넷/SSH/HTTP 트래픽에 대한 별도의 연결 시간 초과도 구성됩니다. 다른 모든 TCP 트래픽은 계속해서 timeout conn 1:00:00과 연결된 정상적인 연결 시간 제한 값을 갖습니다.

[ASA 8.3 이상](#)을 참조하십시오. 버전 8.3 이상 [의](#) Cisco ASA(Adaptive Security Appliance)[와](#) 함께 ASDM을 사용하는 동일한 컨피그레이션에 대한 자세한 내용은 MPF 컨피그레이션 예를 [사용하여 SSH/텔넷/HTTP 연결 시간 제한을 설정합니다.](#)

## 사전 요구 사항

### 요구 사항

이 문서에 대한 특정 요건이 없습니다.

## 사용되는 구성 요소

이 문서의 정보는 Cisco PIX/ASA Security Appliance Software Version 7.1(1) with Adaptive

Security Device Manager(ASDM) 5.1을 기반으로 합니다.

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우, 모든 명령어의 잠재적인 영향을 미리 숙지하시기 바랍니다.

## 표기 규칙

문서 규칙에 대한 자세한 내용은 [Cisco 기술 팁 규칙](#)을 참조하십시오.

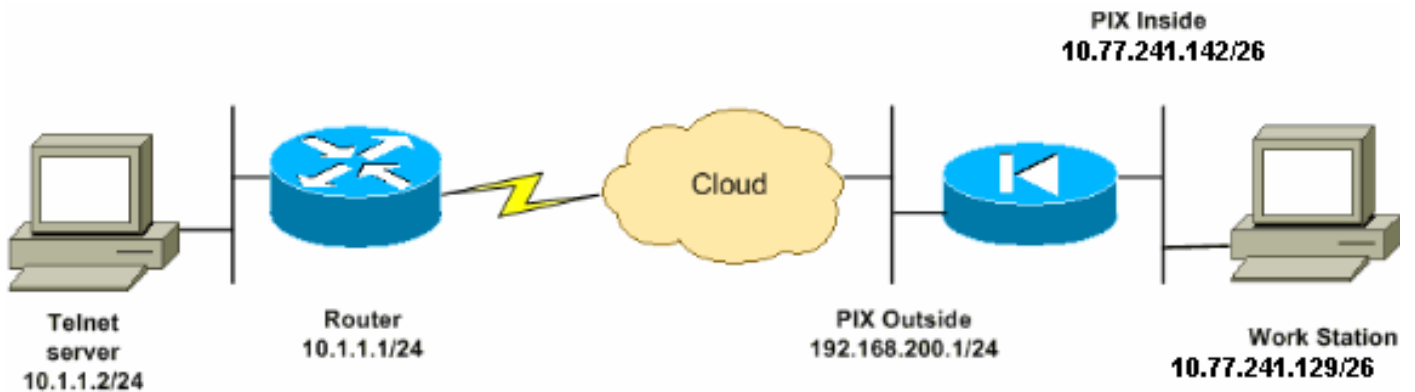
## 구성

이 섹션에는 이 문서에서 설명하는 기능을 구성하기 위한 정보가 표시됩니다.

**참고:** 이 섹션에 사용된 명령에 대한 자세한 내용을 보려면 [명령 조회 도구](#)([등록된](#) 고객만 해당)를 사용하십시오.

## 네트워크 다이어그램

이 문서에서는 다음 네트워크 설정을 사용합니다.



**참고:** 이 구성에 사용된 IP 주소 지정 체계는 인터넷에서 합법적으로 라우팅할 수 없습니다. 실습 환경에서 사용된 RFC 1918 주소입니다.

## 구성

이 문서에서는 다음 구성을 사용합니다.

**참고:** 이러한 CLI 및 ASDM 구성은 FWSM(Firewall Service Module)에 적용됩니다.

### CLI 구성:

PIX 컨피그레이션
<pre> PIX Version - 7.1(1) ! hostname PIX domain-name Cisco.com enable password 8Ry2YjIyt7RRXU24 encrypted names </pre>

```
!  
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 esmtp
    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 구성:

표시된 대로 ASDM을 사용하는 액세스 목록을 기반으로 텔넷 트래픽에 대한 TCP 연결 시간 제한을 설정하려면 다음 단계를 완료합니다.

**참고:** ASDM을 통해 PIX/ASA에 액세스하려면 [ASDM](#)에 대한 HTTPS 액세스 허용을 참조하십시오.

1. 인터페이스 구성 Configuration > Interfaces > Add를 선택하여 표시된 대로 Ethernet0(외부) 및 Ethernet1(내부) 인터페이스를 구성합니다

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:

확인을 클릭합니다

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

표시된 것과 동일한 CLI 컨피그레이션:

```
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 구성네트워크 10.77.241.128/26의 트래픽이 변환 없이 인터넷에 액세스하도록 허용하려면 **Configuration > NAT > Translation Exemption Rules > Add**를 선택합니다

Configuration > NAT > Translation Exemption Rules

### Add Address Exemption Rule

Action

Select an action: **exempt**

Host/Network Exempted From NAT

IP Address  Name  Group

Interface: **inside**

IP address: **10.77.241.128**

Mask: **255.255.255.192**

When Connecting To

IP Address  Name  Group

Interface: **outside**

IP address: **0.0.0.0**

Mask: **0.0.0.0**

Rule Flow Diagram

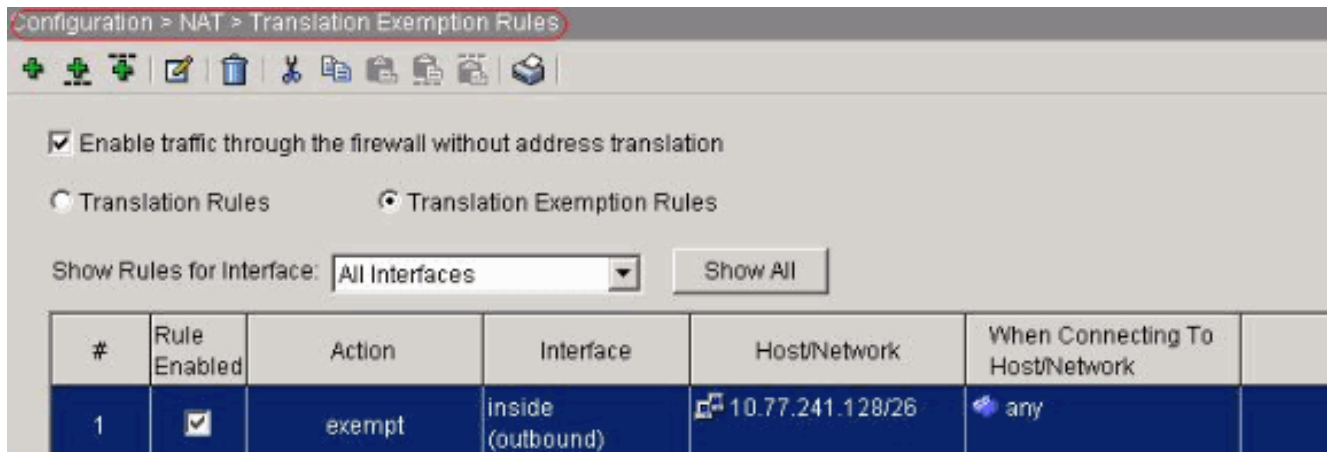
Rule applied to traffic incoming to source interface

The diagram shows a central router with 'inside' and 'outside' interfaces. A red arrow points to the 'inside' interface from a source labeled 'any'. A green checkmark and the word 'exempt' are shown below the router. A dashed orange arrow points from the 'inside' interface to the 'outside' interface, which then points to a destination labeled 'any'.

Please enter the description below (optional):

OK Cancel Help

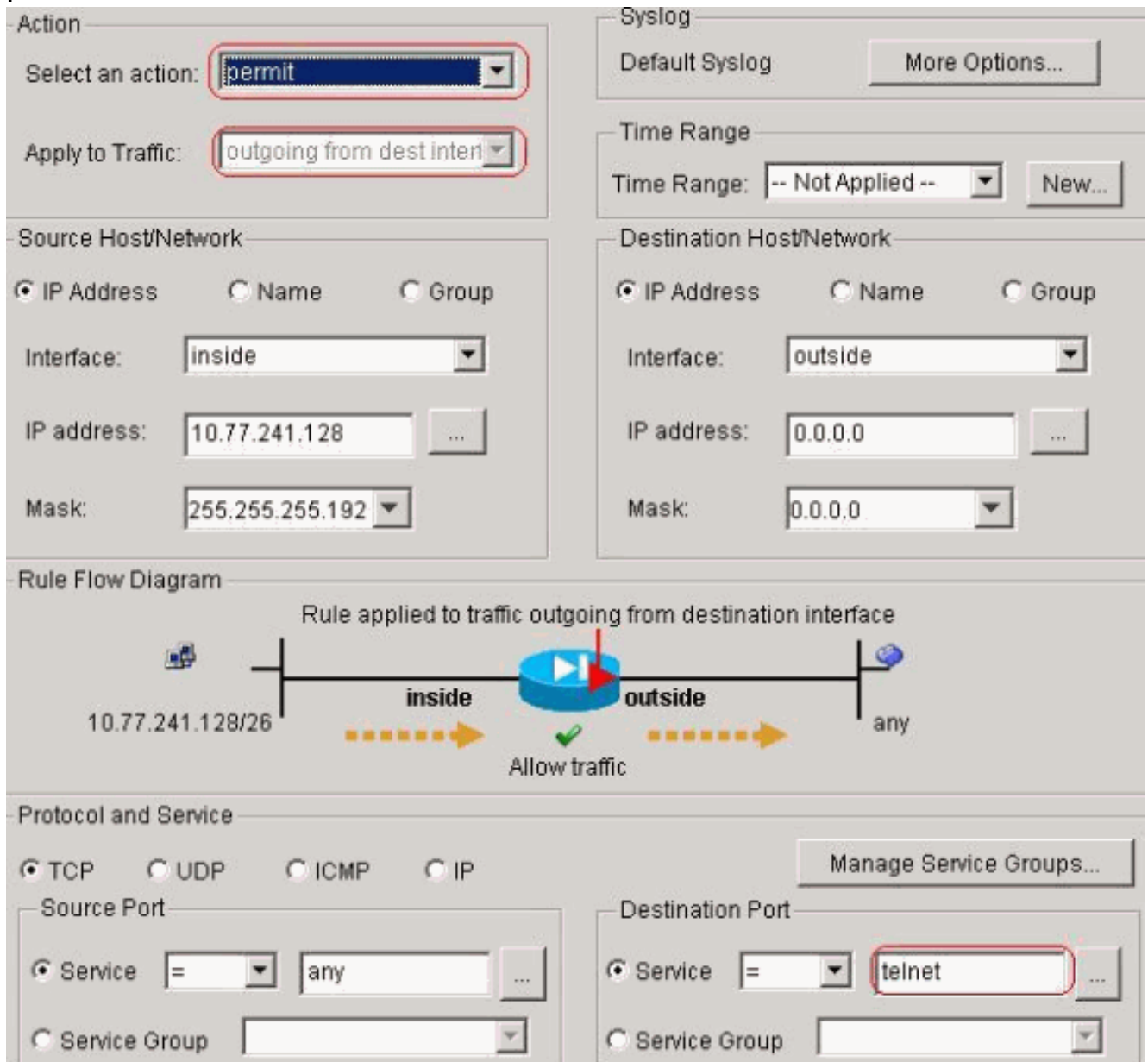
확인을 클릭합니다



표시된 것과 동일한 CLI 컨피그레이션:

```
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 구성표시된 대로 ACL을 구성하려면 **Configuration > Security Policy > Access Rules**를 선택합니다. 네트워크 10.77.241.128/26에서 시작된 텔넷 트래픽을 모든 목적지 네트워크에 허용하고 외부 인터페이스의 아웃바운드 트래픽에 적용하는 ACL 101을 구성하려면 Add를 클릭합니다



확인을 클릭합니다. ssh 및 http 트래픽도 마찬가지로



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

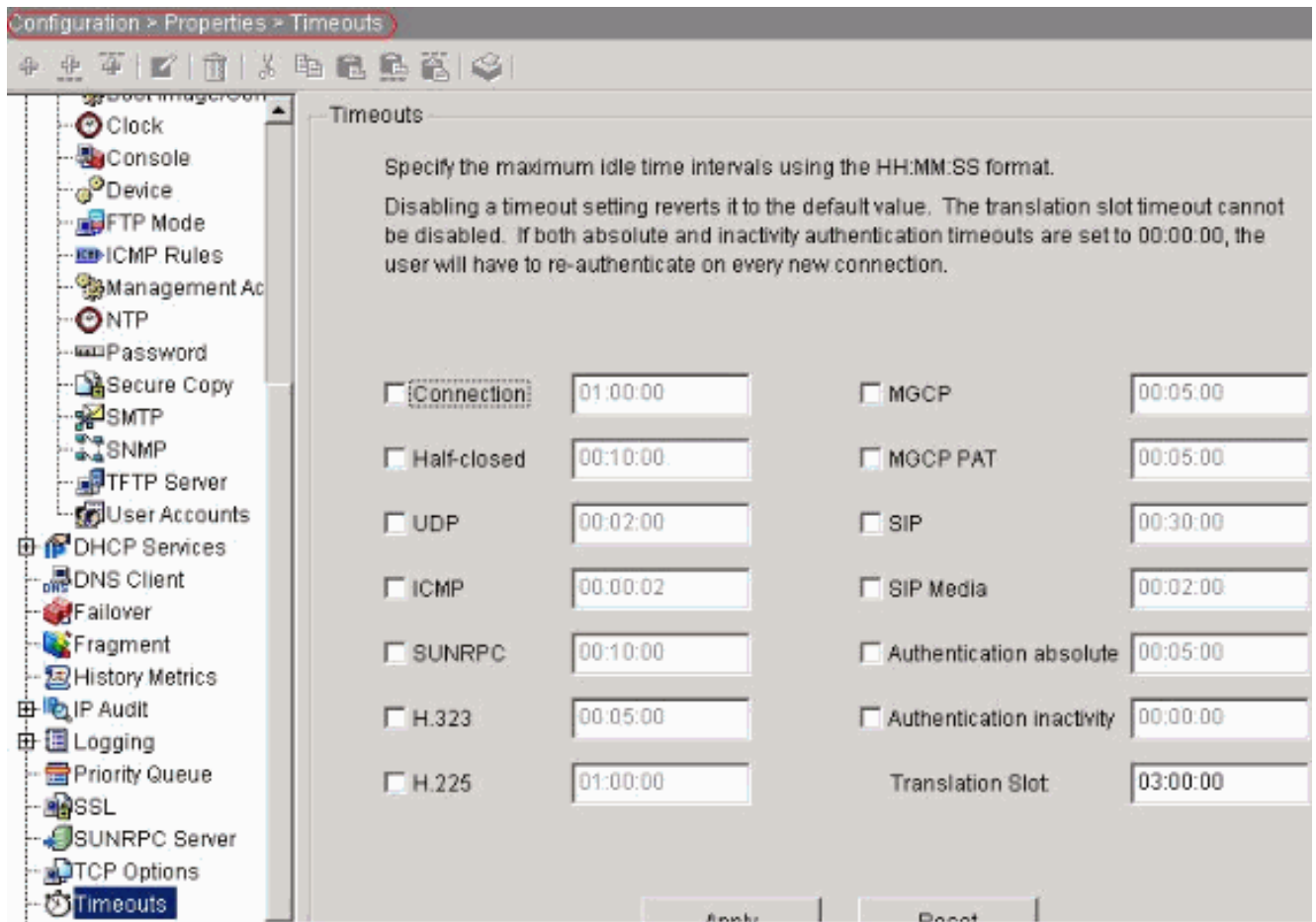
Service =

Service Group

표시된 것과 동일한 CLI 컨피그레이션:

```
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. 시간 초과 구성 다양한 시간 초과를 구성하려면 Configuration > Properties > Timeouts를 선택합니다. 이 시나리오에서는 모든 시간 제한의 기본값을 유지합니다



표시된 것과 동일한 CLI 컨피그레이션:

```
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 icmp 0:00:02
```

5. 서비스 정책 규칙을 구성합니다. 클래스 맵을 구성하고 TCP 연결 시간 제한을 10분으로 설정하기 위한 정책 맵을 구성하고, 표시된 대로 외부 인터페이스에 서비스 정책을 적용하려면 Configuration > Security Policy > Service Policy Rules > Add를 선택합니다. 생성할 **outside - (create new service policy)**를 선택하고 **텔넷**을 정책 이름으로 할당하려면 **Interface(인터페이스)** 라디오 버튼을 선택합니다

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(다음)를 클릭합니다. 클래스 맵 이름 텔넷을 생성하고 Traffic match 기준에서 **Source and Destination IP address (uses ACL)** 확인란을 선택합니다

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.

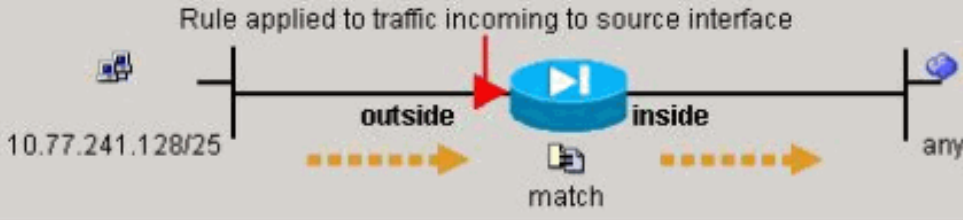
Next(다음)를 클릭합니다. 네트워크 10.77.241.128/26에서 시작된 텔넷 트래픽을 대상 네트워크에 매칭하고 클래스 텔넷에 적용하려면 ACL을 생성합니다

**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** → **match** → **inside** → any

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

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

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

Next(다음)를 클릭합니다. ssh 및 http 트래픽도 마찬가지로

**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  

The diagram shows a central router with two interfaces: 'outside' on the left and 'inside' on the right. A red arrow points to the router from the left, labeled '10.77.241.128/25'. Below this arrow is a dashed orange arrow pointing right, labeled 'outside'. A red arrow points to the router from the top, labeled 'match'. Below this arrow is a dashed orange arrow pointing right, labeled 'inside'. A red arrow points to the router from the right, labeled 'any'. Below this arrow is a dashed orange arrow pointing right, labeled 'any'.

**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(연결 설정)**를 선택하여 TCP Connection Timeout(TCP 연결 시간 제한)을 10분으로 설정하고 Send reset to **TCP endpoints before timeout(시간 제한 전에 TCP 엔드포인트로 재설정 보내기)** 확인란을 선택합니다

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

마침을 클릭합니다

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 resu

표시된 것과 동일한 CLI 컨피그레이션:

```

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

```



## ebryonic 시간 초과

원시 연결은 절반이 열려 있거나, 예를 들어 3방향 핸드셰이크가 완료되지 않은 연결입니다. ASA에서 SYN 시간 초과로 정의됩니다. 기본적으로 ASA의 SYN 시간 제한은 30초입니다. 이는 원시 시간 제한을 구성하는 방법입니다.

```
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
```

## 다음을 확인합니다.

이 섹션을 사용하여 컨피그레이션이 제대로 작동하는지 확인합니다.

Output [Interpreter 도구\(등록된 고객만 해당\)](#)(OIT)는 특정 **show** 명령을 지원합니다. **show** 명령 출력의 분석을 보려면 OIT를 사용합니다.

컨피그레이션을 확인하려면 **show service-policy interface outside** 명령을 실행합니다.

```
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
```

특정 트래픽이 서비스 정책 컨피그레이션과 일치하는지 확인하려면 [show service-policy flow](#) 명령을 실행합니다.

이 명령 출력은 예를 보여줍니다.

```
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
```

## 문제 해결

연결 시간 제한이 MPF(Modular Policy Framework)에서 작동하지 않는 경우 TCP 시작 연결을 확인합니다. 이 문제는 소스 및 대상 IP 주소를 취소하거나 액세스 목록의 잘못된 구성된 IP 주소가 MPF에서 일치하지 않아 새 시간 초과 값을 설정하거나 애플리케이션의 기본 시간 제한을 변경할 수 있습니다. MPF로 연결 시간 제한을 설정하려면 연결 시작에 따라 액세스 목록 항목(소스 및 대상)을 생성합니다.

## 관련 정보

- [Cisco PIX 500 Series 보안 어플라이언스](#)
- [Cisco ASA 5500 Series Adaptive Security Appliance](#)
- [Cisco PIX 방화벽 소프트웨어](#)
- [Cisco Secure PIX Firewall 명령 참조](#)
- [보안 제품 필드 알림\(PIX 포함\)](#)
- [RFC\(Request for Comments\)](#)