

# PIX/ASA 7.x и последующие версии / FWSM: Пример настройки времени ожидания соединения SSH/Telnet/HTTP с использованием MPF

ID документа: 68332

Обновлено : 16 октября 2008



[Загрузка PDF](#)



[Печать](#)

[Обратная связь](#)

## Родственные продукты

- [Диспетчер адаптивных устройств защиты Cisco \(Cisco Adaptive Security Device Manager\)](#)
- [Cisco ASA 5500-X Series межсетевые экраны следующего поколения](#)
- [Cisco PIX 500 Series Security Appliances](#)

## Содержание

[Введение](#)

[Предварительные условия](#)

[Требования](#)

[Используемые компоненты](#)

[Условные обозначения](#)

[Настройка](#)

[Схема сети](#)

[!-- конфигурацию](#)

[Таймаут Ebrionic](#)

[Проверка](#)

[Устранение неполадок](#)

[Дополнительные сведения](#)

[Соответствующие дискуссии сообщества технической поддержки Cisco](#)

## Введение

Этот документ предоставляет пример конфигурации для PIX 7.1 (1) и позже таймаута, который является определенным для конкретного приложения, такого как SSH/Telnet/HTTP, в противоположность тому, который применяется ко всем приложениям. Этот пример конфигурации использует новую Модульную Систему политик, представленную в PIX 7.0.

См. [Использование Модульной Системы политик](#) для получения дополнительной информации.

В этом примере конфигурации Межсетевой экран PIX настроен для разрешения рабочей станции (10.77.241.129) Telnet/SSH/HTTP к удаленному серверу (10.1.1.1) позади маршрутизатора. Таймаут отдельного подключения к TELNET/SSH/ТРАФИКУ HTTP также настроен. Весь другой Трафик TCP продолжает привязывать значение таймаута обычного подключения к **1:00:00 времени ожидания соединения**.

См. [AASA 8.3 и Позже: Подайте Таймаут SSH/TELNET/СОЕДИНЕНИЯ HTTP с помощью Примера Конфигурации MPF](#) для получения дополнительной информации об одинаковой конфигурации с помощью ASDM с устройством адаптивной защиты Cisco (ASA) с версией 8.3 и позже.

## Предварительные условия

### Требования

Для этого документа отсутствуют особые требования.

### Используемые компоненты

Сведения в этом документе основываются на Версии программного обеспечения 7.1 (1) Устройства безопасности PIX/ASA Cisco с Менеджером устройств адаптивной безопасности (ASDM) (ASDM) 5.1.

Сведения, представленные в этом документе, были получены от устройств, работающих в специальной лабораторной среде. Все устройства, описанные в этом документе, были запущены с чистой (стандартной) конфигурацией. В рабочей сети необходимо изучить потенциальное воздействие всех команд до их использования.

### Условные обозначения

[Более подробную информацию о применяемых в документе обозначениях см. в описании условных обозначений, используемых в технической документации Cisco.](#)

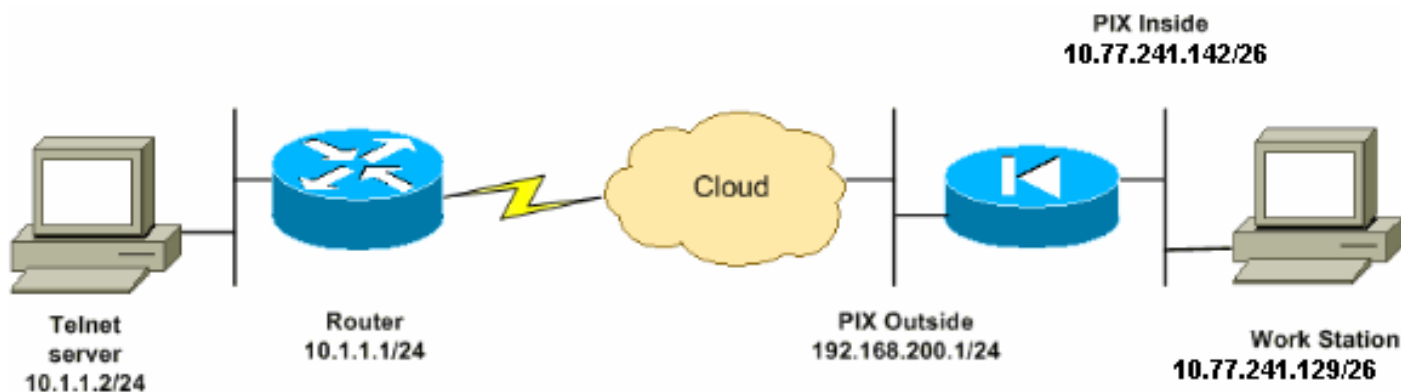
## Настройка

В этом разделе содержатся сведения о настройке функций, описанных в этом документе.

**Примечание:** [Чтобы получить подробные сведения о командах в данном документе, используйте Средство поиска команд \(только для зарегистрированных клиентов\).](#)

### Схема сети

В настоящем документе используется следующая схема сети:



**Примечание:** Схемы IP-адресации, которые использованы в данной конфигурации, не поддерживаются официальной маршрутизацией в Интернете. Это адреса RFC 1918, используемые в лабораторной среде.

## !--- конфигурацию

В данном документе используется следующая конфигурация:

**Примечание:** Они CLI и конфигурации ASDM применимы к Модулю Сервиса межсетевое экрана (FWSM)

Конфигурация интерфейса командой строки CLI:

Конфигурация PIX
<pre> 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 </pre>

```

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
esmtplib 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

```

## Настройка посредством ASDM:

Выполните эти шаги для устанавливания таймаута TCP - подключения для трафика Telnet на основе access-list, который использует ASDM как показано.

**Примечание:** См. [документ Разрешение HTTPS-доступа для ASDM](#) для базовых параметров для доступа к PIX/ASA через ASDM.

1. **Настройте интерфейсы** Выберите **Configuration> Interfaces> Add** для настройки interface ethernet0 (снаружи) и Ethernet1 (внутри) как показано.

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:

Нажмите кнопку  
OK.

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

Эквивалентная конфигурация CLI как показано:

```

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. **Настройте NAT** Выберите **Configuration > NAT > Translation Exemption Rules > Add**, чтобы позволить трафику от сети 10.77.241.128/26 обращаться к Интернету без любой трансляции.

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:

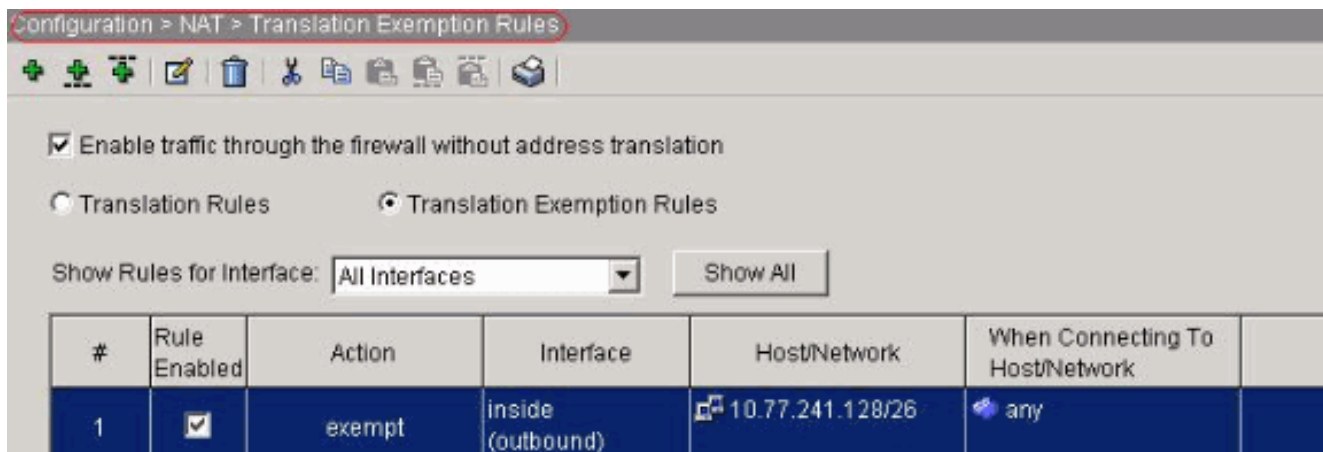
Rule Flow Diagram

Rule applied to traffic incoming to source interface

Please enter the description below (optional):

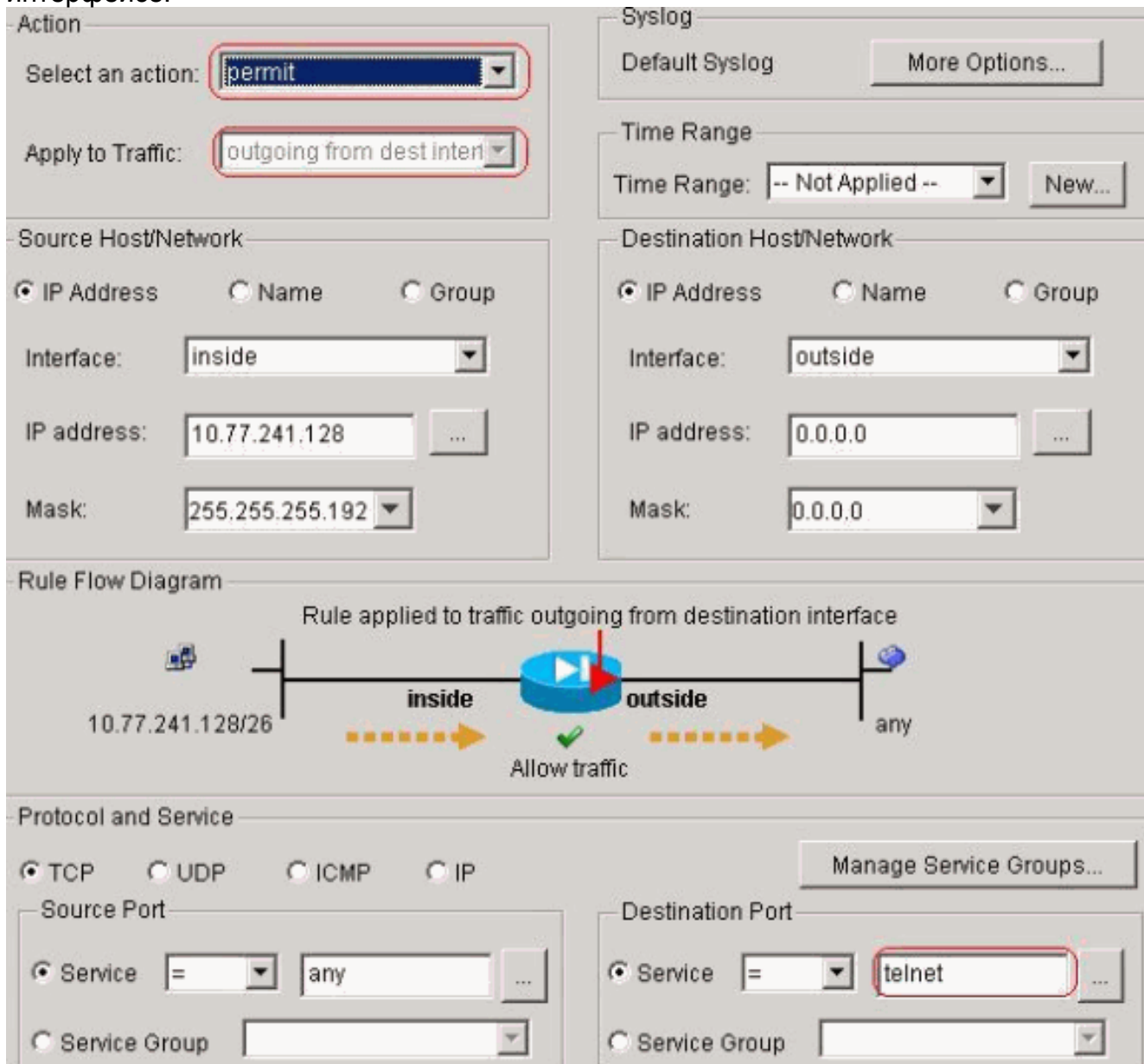
OK Cancel Help

Нажмите кнопку  
OK.



Эквивалентная конфигурация CLI как показано:  
`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. **Настройте ACL** Выберите **> Security Configuration Политика > Правила Доступа** для настройки ACL как показано. **Нажмите Add** для настройки ACL 101, который позволяет трафик Telnet, инициируемый из сети 10.77.241.128/26 к любой сети назначения, и примените его для исходящего трафика на внешнем интерфейсе.



**Нажмите кнопку OK.** Так же для ssh и трафика



HTTP:

Action

Select an action:

Apply to Traffic:

Source Host/Network

IP Address  Name  Group

Interface:

IP address:  ...

Mask:

Destination Host/Network

IP Address  Name  Group

Interface:

IP address:  ...

Mask:

Syslog

Default Syslog

Time Range

Time Range:

Rule Flow Diagram

Rule applied to traffic outgoing from destination interface

The diagram shows a central router with a play button icon. To the left, a source network '10.77.241.128/26' is connected to an 'inside' interface. A dashed orange arrow points from the source network through the 'inside' interface to the router. To the right, the router is connected to an 'outside' interface, which is then connected to a destination 'any'. Another dashed orange arrow points from the router through the 'outside' interface to the destination. A green checkmark and the text 'Allow traffic' are positioned below the router.

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  
  
 10.77.241.128/26 — inside —> [Router] —> outside —> any  
 Allow traffic

**Protocol and Service**  
 TCP  UDP  ICMP  IP

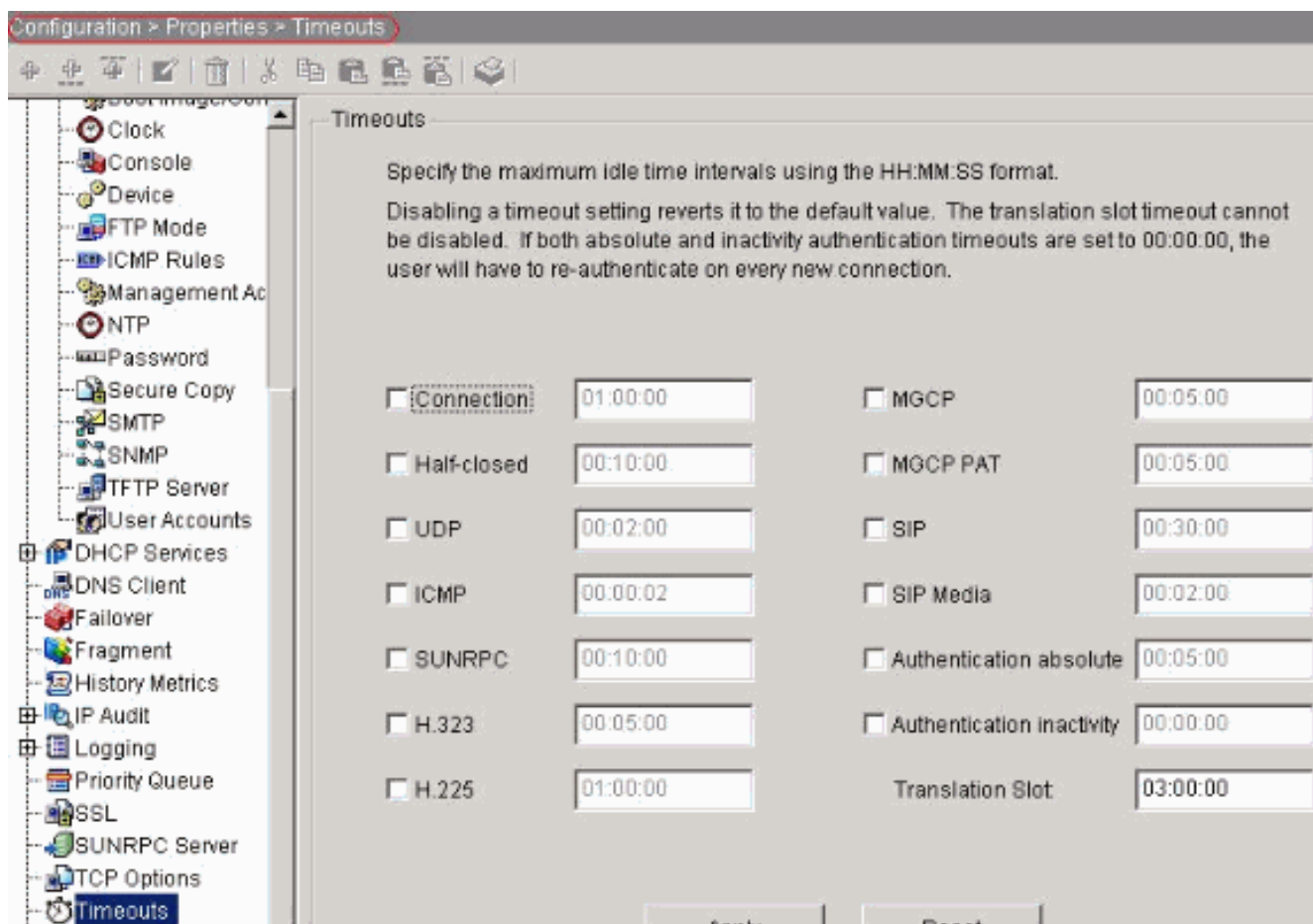
**Source Port**  
 Service =    
 Service Group

**Destination Port**  
 Service =    
 Service Group

Эквивалентная конфигурация CLI как показано:  

```
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. **Настройте таймауты** Выберите **Configuration > Properties > Timeouts** для настройки различных таймаутов. В этом сценарии поддержите значение по умолчанию для всех таймаутов.



Эквивалентная конфигурация CLI как показано: `timeout conn 1:00:00 half-closed 0:10:00  
udp 0:02:00 icmp 0:00:02`

5. Настройте правила политики обслуживания. Выберите > **Security Configuration Политика**>, **Правила Политики обслуживания**> **Добавляют**, чтобы настроить карту классов, карту политик для устанавливания таймаута TCP - подключения как 10 минут, и применить политику обслуживания на внешний интерфейс как показано. Выберите кнопку с зависимой фиксацией **Interface** для выбора **снаружи** - (**создайте новую политику обслуживания**), который должен быть создан, и назначать **telnet** как название политики.

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

Нажмите кнопку **Next**. Создайте **telnet** названия карты классов и выберите **IP - адрес источника и получателя (ACL использования)** флажок в условиях соответствия Трафика.

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.

Нажмите кнопку **Next**. Создайте ACL, чтобы совпасть с трафиком Telnet, инициируемым из сети 10.77.241.128/26 к любой сети назначения, и применить его к telnet

класса.

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

Нажмите кнопку Next. Так же для ssh и трафика HTTP:



**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] --> O[outside]; O --> R((Router)); R --> I[inside]; I --> D[any];
```

**Protocol and Service**  
 TCP  UDP  ICMP  IP

**Source Port**  
 Service =    
 Service Group


**Destination Port**  
 Service =    
 Service Group

**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 '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'. A red arrow points to the router from the right, labeled 'any'. Below the router, a red arrow points to the router, labeled 'match'. Dashed orange arrows indicate traffic flow from left to right.

**Protocol and Service**  
 TCP  UDP  ICMP  IP

**Source Port**  
 Service =    
 Service Group

**Destination Port**  
 Service =    
 Service Group

Выберите **Connection Settings**, чтобы установить Таймаут TCP - подключения как 10 минут, и также выбрать сброс **Send** к оконечным точкам TCP перед флажком таймаута.

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

Нажмите кнопку

Finish.

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

Эквивалентная конфигурация CLI как показано: 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



## Таймаут Ebrionic

Неустановившееся соединение является соединением, которое полуоткрыто или, например, трехэтапное установление связи не было завершено для него. Это определено как время ожидания SYN на ASA; по умолчанию время ожидания SYN на ASA составляет 30 секунд. Это - способ настроить Начальный Таймаут:

```
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
```

## Проверка

Этот раздел позволяет убедиться, что конфигурация работает правильно.

[Средство Output Interpreter \(OIT\) \(только для зарегистрированных клиентов\) поддерживает определенные команды show.](#) Используйте OIT для просмотра анализа выходных данных команды show.

Выполните команду **show service-policy interface outside** для проверки конфигураций.

```
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
```

Выполните команду [потока show service-policy](#), чтобы проверить, что отдельный трафик совпадает с конфигурациями политики обслуживания.

Эти выходные данные команды показывают пример:

```
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
```

## Устранение неполадок

Если вы находите, что время ожидания соединения не работает с Модульной системой политик (MPF), то проверьте соединение инициирования TCP. Проблема может быть реверсированием IP - адреса источника и получателя, или IP-адрес неверна настроенного в списке доступа не совпадает в MPF, чтобы установить новое значение таймаута или изменить время ожидания по умолчанию для приложения. Создайте запись списка доступа (источник и назначение) в соответствии с инициированием соединения для установки времени ожидания соединения с MPF.

## Дополнительные сведения

- [Cisco PIX 500 Series Security Appliances](#)

- [CISCO ASA 5500 SERIES ADAPTIVE SECURITY APPLIANCES](#)
- [Замечания о выпуске устройства защиты Cisco PIX](#)
- [Cisco PIX Firewall Software](#)
- [Справочники по командам для межсетевого экрана PIX Cisco Secure](#)
- [Уведомления о дефектах продуктов по безопасности \(включая PIX\)](#)
- [Запросы комментариев \(RFC\)](#)
- [Cisco Systems – техническая поддержка и документация](#)

Был ли этот документ полезен? [Да](#) [нет](#)

Спасибо за ваш отзыв.

[Адресовать вопрос техподдержке \(требуется контракт сервиса Cisco.\)](#)

## **Соответствующие дискуссии сообщества технической поддержки Cisco**

[Сообщество технической поддержки Cisco является форумом, в котором можно задавать вопросы и получать ответы, обмениваться предложениями и сотрудничать со своими равноправными коллегами.](#)

[См. Условные обозначения технических советов Cisco для получения информации по условным обозначениям, которые используются в данном документе.](#)

Обновлено : 16 октября 2008

ID документа: 68332