

نېي عت :FWSM/ثدحأل تارادصلال او PIX/ASA 7.x لاثم مادختساب SSH/Telnet/HTTP لاصتا ةلهم MPF نيوكت

تايوتحملال

[ةمدقملا](#)

[ةيساسأل تابلطتملا](#)

[تابلطتملا](#)

[ةمدختسملا تانوكملا](#)

[تاجالطصالال](#)

[نيوكتلا](#)

[ةكبش ليل يطي طختلا مسرلا](#)

[نيوكتلا](#)

[ةينوي ربا ةلهم](#)

[ةحصلا نم ققحتلا](#)

[اهجالص او عا طخالال فاشكتسا](#)

ةمدقملا

ةدحم نوكت يتلا ةلهملا نم ثدحأل تارادصلال او PIX 7.1(1) ل نيوكت ةني ع دننتمسملال اذه مدقي
عيمج يل ع قبطني يذلا نيوكتلاب ةنراقم ، SSH/Telnet/HTTP لثم نيم قيبطتل
مت يذلا ةيظمنلا ةسايسلل ديدجال لمعل راطا اذه نيوكتلا لاثم مدختسي . تاقيبطتل
نم ديزم يل ع لوصحلل [ةيظمنلا ةسايسلا لمع راطا مادختسا](#) عجار PIX 7.0 يف هميدقت
تامولعمل .

ب (10.77.241.129) لمعلال ةطحمل حامسلل PIX ةيامح راج نيوكت متي ، اذه نيوكتلا جذومن ي
لاصتا ةلهم نيوكت مت امك . هجومل فلخ (10.1.1.1) ديعبال مداخلاب Telnet/SSH/HTTP
يف يرخال TCP رورم تاكرح عيمج رمتست . Telnet/SSH/HTTP تانايب رورم ةكرحل ةلصفنم
conn 1:00:00 ةلهمب ةنرتقملا ةيداعلا لاصتالا ةلهم ءاهتنا ةميقي يل ع لوصحلل .

[لاثم مادختساب SSH/Telnet/HTTP لاصتا ةلهم نېي عت :ثدحأل تارادصلال او ASA 8.3](#) يل ع
عم ASDM مادختساب قباطتملا نيوكتلا لوح تامولعمل نم ديزم يل ع لوصحلل [MPF نيوكت](#)
ثدحأل تارادصلال او 8.3 رادصلال Cisco نم (ASA) فيكتلل لبالل نامال زاھ

ةيساسأل تابلطتملا

تابلطتملا

دننتمسملال اذهل ةصاخ تابلطتم دجوت ال

ةمدختسملا تانوكملا

Cisco PIX/ASA Security Appliance، Adaptive Security Device Manager (ASDM) 5.1 عم 7.1(1) رادصلإا دن تست

ةصاخ ةي لم عم ةئيب يف ةدوجوملا ةزهجالا نم دن تستملا اذه يف ةدراولما تامولعملما عاشنإ مت تناك اذا. (يضارتفا) حوسم نيوكتب دن تستملا اذه يف ةمدختسملا ةزهجالا عيمج تادب رما يال لم تحت حمل ريثاتلل كمهف نم دكأتف ، ةرشابم كتكباش

تاحالطصلا

تاحالطصلا لوح تامولعملما نم ديزم لىع لوصحلل ةينقتلا Cisco تاحيملت تاحالطصلا عجار تادنتسملا

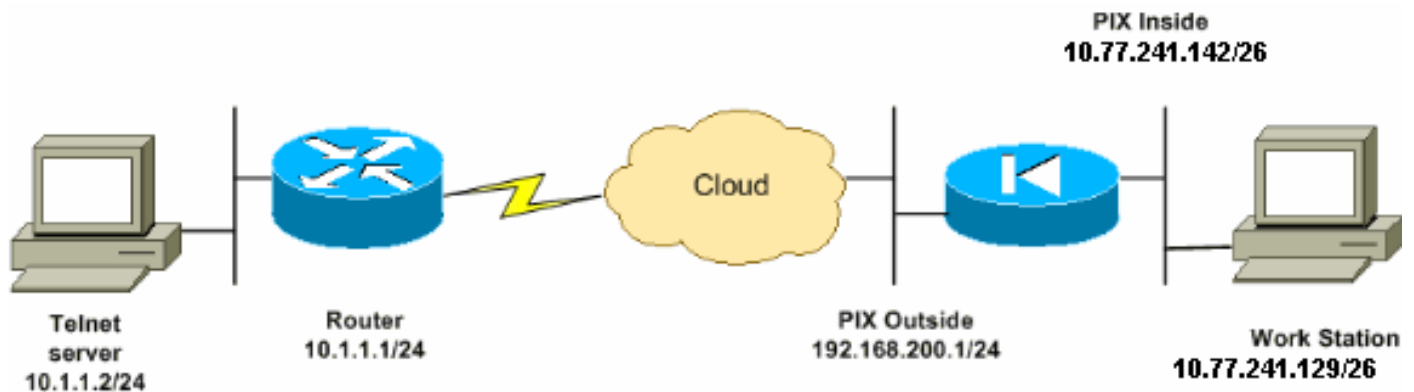
نيوكتلا

دنتسملا اذه يف ةحضوملا تازيملما نيوكت تامولعملما كل مّدقت ، مسقلا اذه يف

نم ديزم لىع لوصحلل (طقف نيولجسملما ءالمعلل) رماوألما ثحب ةادأ مدختسا : ةظحالم مسقلا اذه يف ةمدختسملا رماوألما لوح تامولعملما

ةكبش لىل يطيختلا مسرلا

يلا تلال ةكبشلا دادعا دن تستملا اذه مدختسي



تنرتنإلا لىع routable اينوناق ليكشت اذه يف لمعتسي ةطخ بطاخي سيل ip لىل : ةظحالم ةئيب ربتخم يف تلمعتسا نوكي ىقلتى يا ، ناونع 1918 rfc مه

نيوكتلا

ليكشت اذه ةقيثو اذه لمعتسي

(FWSM) ةيامل رادج ةمدخل ةيظمنلا ةدحولا لىع هذه ASDM و CLI تانيوكت قبطنت : ةظحالم

لىكشت CLI

PIX نيوكت
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 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 نيوكت:

عمىاق ىلإ اءانءسا Telnet ءاناىب رورم ءكرءل TCP لاصءا ءلهم ءاءءل ءاوطءل هذه لمكأ ءضوم وه امك ASDM مءءءسء ءل لوصول.

نم PIX/ASA ىلإ لوصول ءىساسأل ءاءءل ASDM ل [HTTPS لوصول ءامس ل](#) عءار: ءءءءل ASDM.

1. و (جراخ) 0 تي نرث | نراق لا تل ك ش in order to فيضي > نراق > لي ك ش ت ترتخأ ت ا ه اول ا ني وكت .
وه امك (لخاد) 1 تي نرث |
حضورم .

Hardware Port: **Ethernet0** Configure Hardware Properti

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 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:

قوف رقناو

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

حضورم وه امك ئفالم ال CLI نيوكت:

```

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. ترحم سي فيضي > دعاق اناث سا ةم جرت > nat > لي كشت ترتخأ NAT 0 ني وكت
يا نود تنرتن إالا ذفني نأ 10.77.241.128/26 ةكبشلا نم رورم ةكرحلا
ةم جرت.

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**

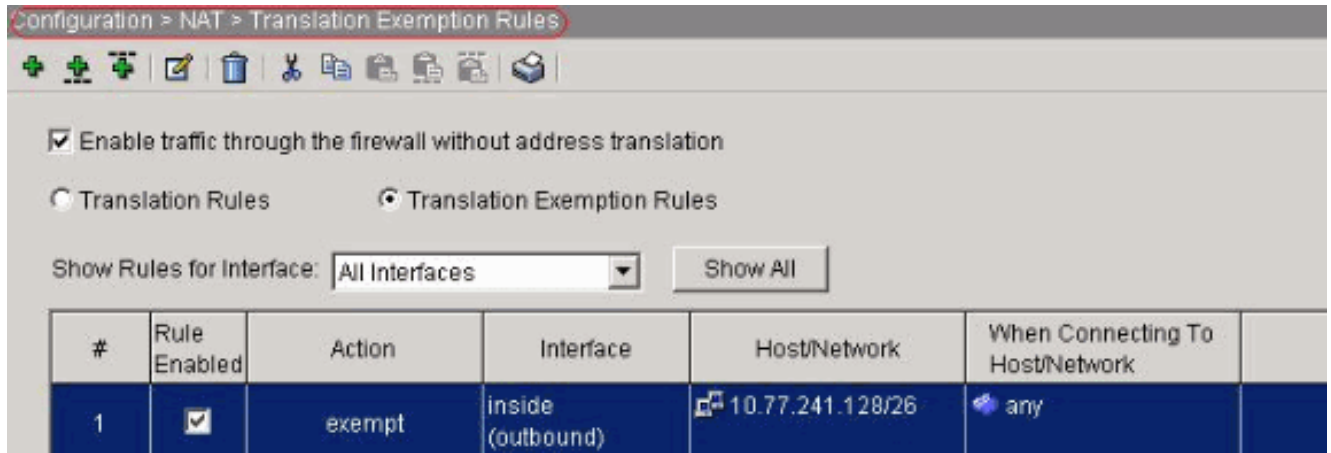
Rule Flow Diagram

Rule applied to traffic incoming to source interface

Please enter the description below (optional):

OK Cancel Help

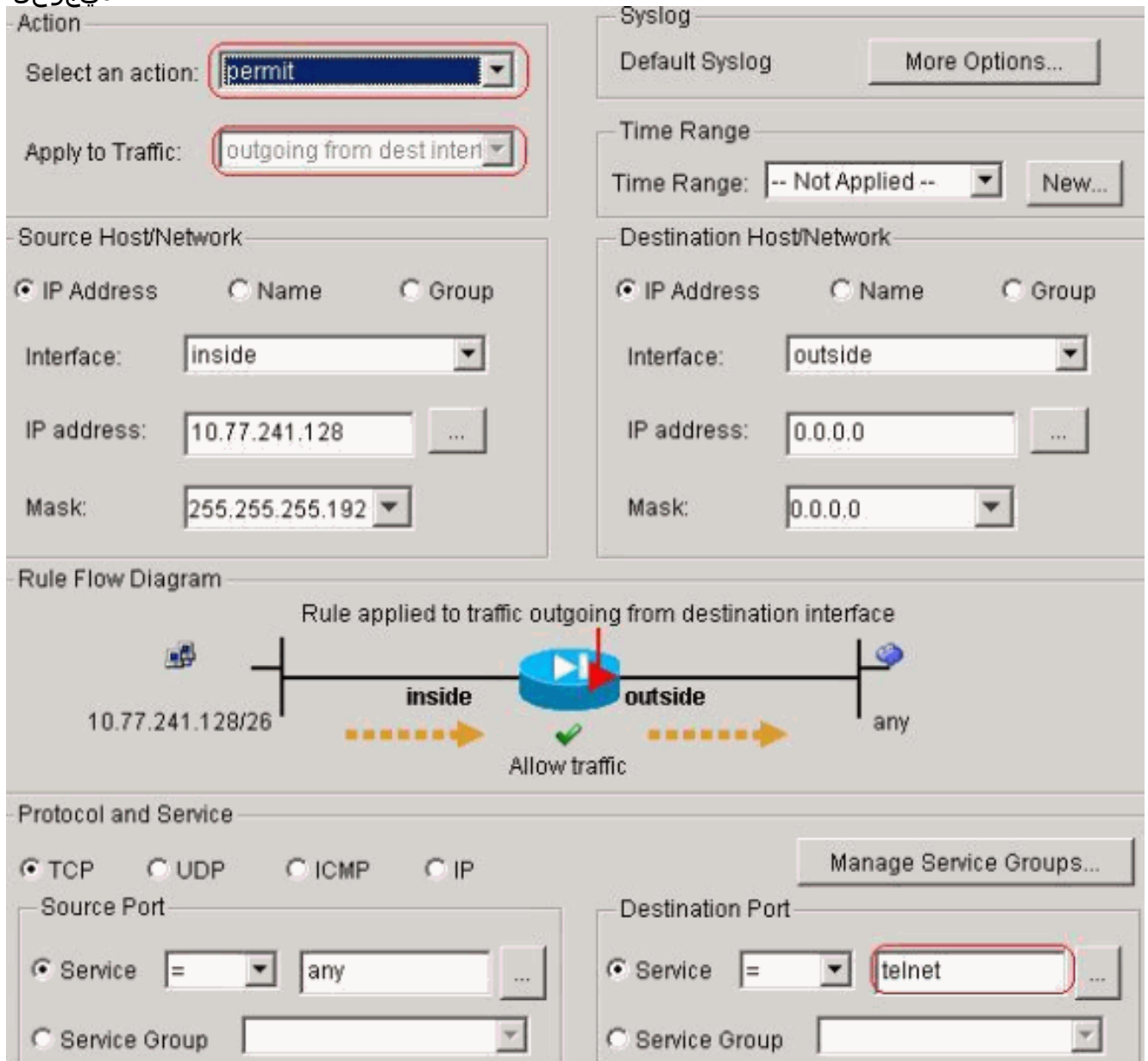
قوف رقناو
OK.



حضوره وه امك ئفالم CLI نيوكت:

```
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. دع اوق > نام الة سايس > نيوكت رتخ ACL لوصولو يف مكحتال مئوق نيوكت
 ةفاضل قوف رقا. حضوره وه امك (ACL) لوصولو يف مكحتال مئوق نيوكتل لوصولو
 Telnet رورم ةكرح عاشن اب حمست يتال 101 (ACL) لوصولو يف مكحتال مئوق نيوكتل
 مرداصل رورم الة كرح لعل اهقبطتو هجو ةكبش يا لى 10.77.241.128/26 ةكبش لى نم
 ةهجالو لى
 ةجراخل.



و SSH رورم ةكحل لثملابو. OK قوف رقناو
http:

Action

Select an action: **permit**

Apply to Traffic: **outgoing from dest inter**

Source Host/Network

IP Address Name Group

Interface: **inside**

IP address: **10.77.241.128**

Mask: **255.255.255.192**

Destination Host/Network

IP Address Name Group

Interface: **outside**

IP address: **0.0.0.0**

Mask: **0.0.0.0**

Syslog

Default Syslog **More Options...**

Time Range

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

Rule Flow Diagram

Rule applied to traffic outgoing from destination interface

10.77.241.128/26 **inside** **outside** any

Allow traffic

Protocol and Service

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

Source Port

Service = **any**

Service Group

Destination Port

Service = **ssh**

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

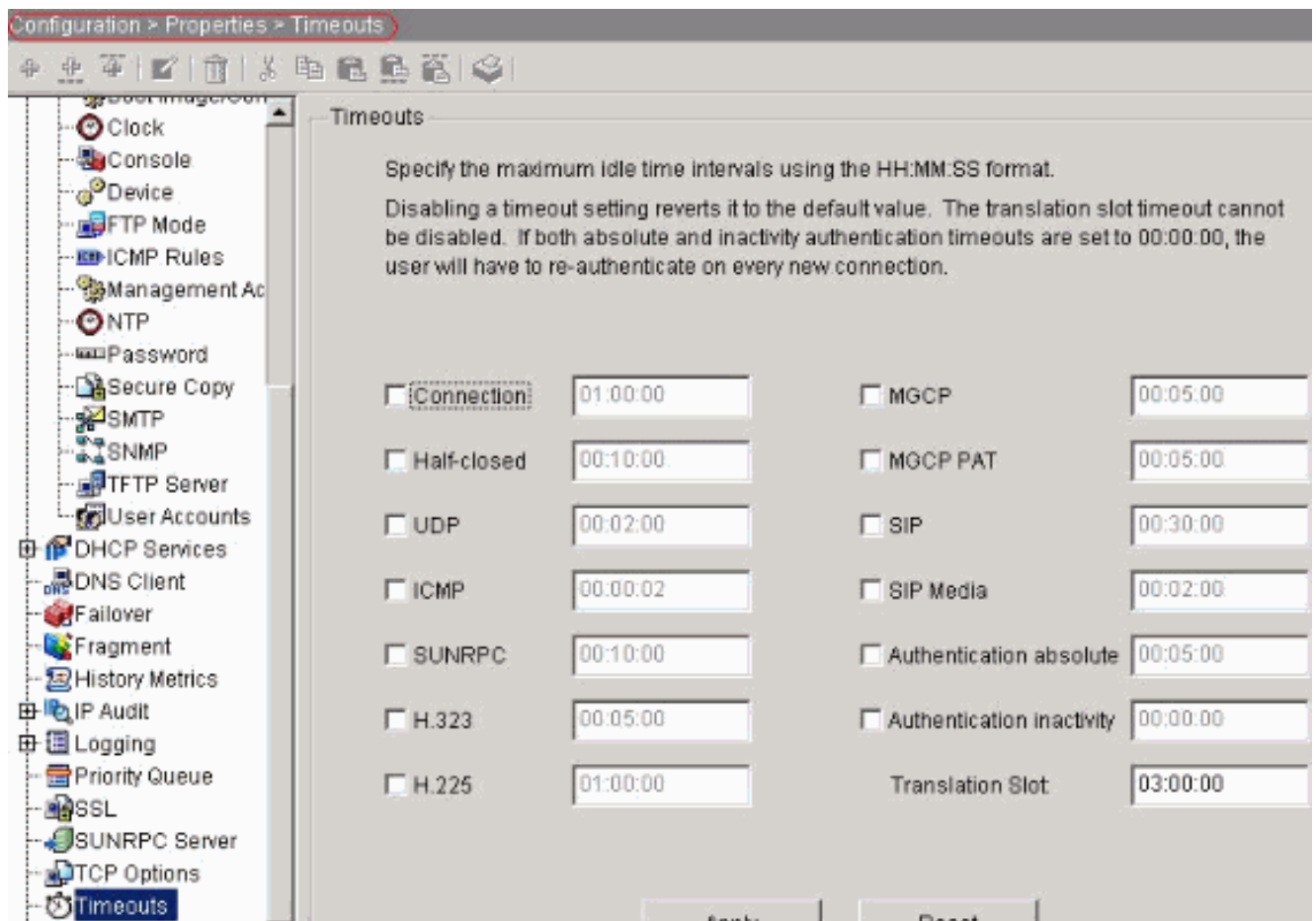
Service =

Service Group

حضوره وه امك ئفالملا CLI نيوكت:

```
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. فلتمل تالكش in order to تقو وخصائصكش تترتخ ألهملا اهاتنا تالاح نيوكت. اهاتنا تالاح عيمل ةيضارتفالا ةمق لابل ظفح، ويراني سالا اذه يف. تقو ةلهملا.



حضوره وه امك ئفالكمل CLI نيوكت

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

5. > ةمدخل ةسايس دعاوق > نامأل ةسايس > نيوكت رتخأ. ةمدخل ةسايس دعاوق نيوكت
 قئاقء 10ك TCP لاصتا ةلهم دادعال ةسايس لاطخم و، ةئفال ةطيرخ نيوكتل ةفاضل
 in ةسايس لراقلا رتخأ. حضوره وه امك ةيجراخل ةهجالا لىل ةمدخل ةسايس قيبطت و
 telnet تنيعو، تقلخ نوئي نأ يا، (ديج ةسايس ةمدخ قلخي) - يجراخ رتخأ
 ةسايس لال
 م سا

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

ردصم لل IP ناو نع رتخاو telnet ةئفلا ةطيخ مسا عاشناب مق.(يلالات) Next قوف رونا ةقباطم ريياعم يف رايتخالال ةناخ (ACL) لوصولا يف مكحتال ةمئاق مدختسي) ةهجولواو ةكح رورملا.

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.

ةكح ةقباطم (ACL) لوصولا يف مكحت ةمئاق عاشناب مق.(يلالات) Next قوف رونا


هجو ةكبش ي ألى | 10.77.241.128/26 ةكبش لى نم اهؤاشن | مت ي تل Telnet رورم
 ةئف لى لى ع اهق ي ب ط و
 Telnet.

Action
 Select an action: **match**

Time Range
 Time Range: -- Not Applied --

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

و SSH رورم ةك رل لثم ل ا ب و . (ي ل ا ل ا) Next قوف ر ق ن ا
 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

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

Protocol and Service
 TCP UDP ICMP IP

Source Port
 Service =
 Service Group

Destination Port
 Service =
 Service Group

رايتخالال ةناخ اضيأ رتخاو ،قئاقود 10ك TCP لاصتا ةلهم دادعإل لاصتالال تاداعإ رتخأ لبق TCP ةياهن طاقن ىلإ نبيعتللا ةداعإ لاسرلا ةلهملا.

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: [Empty Field]

New Edit

قوف رقنا عان.

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...	<input type="checkbox"/>	<input type="checkbox"/>	any	any	default-inspection	inspect (1
Interface: outside, Policy: telnet							
1	telnet	<input checked="" type="checkbox"/>	<input type="checkbox"/>	10.77.241...	any	telnet/tcp	-- Not Appl... connectio send resu

حضورم وه امك ئفالملا CLI نيوكت:

```
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
```


ةينوي رب | ةلم

ةحفاصملا لم تكت مل ، لاثملا ل ي بس ىل ع ، وأ حوتفم فرصن لاصتا وه يني نجل ل لاصتالا SYN ةلم نوكت يضا رتفا لكش بو ؛ ASA ىل ع SYN ةلم هنا ىل ع هف يرت متي . هل ةيثال ل ةينينجل ةلملا ني وكتل ةقيرطلا يه هذ . ةيناث 30 ASA ىل ع :

```
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
```

ةحصلال نم ققحتال

ححص لكش ب ني وكتل ل لمع ديكأتل مسقلا اذ مدختسا

show رم اوأ ضعب (طوقف ني ل ج س م ل اء الم ع ل ل) جارخال ا مجرت م ةادأ معدت OIT in order ل ل تل م عتسا . جاتنا رمأ ضرع نم لي لحت تدهاش to

ةصاخلا تانوي وكتل ل نم ققحتل ل ل ماطنلا جارخ show service-policy interface رمألا رادصاب مقك .

```
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
```

عم ةدحمل رورملا ةكرح قباطت نم ققحتل ل ل show service-policy flow رمألا رادصاب مق ةمدخل ةسايس تانوي وكت .

الاثم هذه رمألا تارخم ضرعت

```
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
```

اهحال صإو ءاطخأل فاشكتسا

نم ققحتف (MPF) "ةيظمنللا تاسايسلا لمع راطا" عم لمعت ال لاصتالا ءلهم نأ تدجو اذإ وأةهول او ردصم لل IP ناونع سكة ءلكشملا نوكت نأ نكمي . TCP لوكتورب ءدب لاصتالا ءميقي نييعتل MPF عم قباطتي ال لوصول ءمئاق يفي ححص ريغ لكشب نوكم IP ناونع لوصول ءمئاق لاخذإ ءاشنإب مق . قيبطتلل ءيضا رتفالا ءلهملا رييغتلا وأةديجلالا ءلهملا MPF ماذختساب لاصتالا ءلهم نييعتل لاصتالا ءدبل اقفو (ةهول او ردصملا)

ءلص تاذا تامولعم

- [Cisco PIX 500 Series Security Appliances نامأالا ءزهأ](#)
- [Cisco ASA 5500 Series Adaptive Security Appliances ءلدعمللا نامأالا ءزهأ](#)
- [Cisco PIX ءيماح رادج جمانب](#)
- [Cisco نم نمأالا PIX ءيماح رادج رماو أءارم](#)
- [\(PIX كلذ يفا ماب\) نامأالا جتنملا ءيناديملا تامالءالا](#)
- [\(RFCs\) تاقيلعتلا تابلط](#)

ةمچرتل هذه ل و ح

ةلأل تاي نقتل ن م ة و مچ م ادخت ساب دن تسم ل ا اذ ه Cisco ت مچرت
م ل ا ل ا ا ن ا ع مچ م ف ن م دخت س م ل م عد و ت م م م دقت ل ة م ش ب ل و
م ك ة ق ي ق د ن و ك ت ن ل ة ل ا ة مچرت ل ض ف ا ن ا ة ظ ح ا ل م م چ ر ي . ة ص ا خ ل م ه ت غ ل ب
Cisco ي ل خ ت . ف ر ت م م مچرت م ا ه م د ق ي ي ت ل ا ة ي ف ا ر ت ح ا ل ا ة مچرت ل ا م ل ا ح ل ا و ه
ل ا ا م ا د ا د ع و چ ر ل ا ب ي ص و ت و ت ا مچرت ل ا ه ذ ه ة ق د ن ع ا ه ت ي ل و ئ س م Cisco
Systems (ر ف و ت م ط ب ا ر ل ا) ي ل ص ا ل ا ي ز ي ل چ ن ا ل ا دن ت س م ل ا