

ىلإ لوصول دييقت : PIX/ASA 7.x ASDM لوصول VPN يمدختسمب ةصاخلة كبشلا دعب نع

المحتويات

- [المقدمة](#)
- [المتطلبات الأساسية](#)
- [المتطلبات](#)
- [المكونات المستخدمة](#)
- [المنتجات ذات الصلة](#)
- [الرسم التخطيطي للشبكة](#)
- [الاصطلاحات](#)
- [تكوين الوصول عبر ASDM](#)
- [تكوين الوصول عبر CLI \(واجهة سطر الأوامر\)](#)
- [التحقق من الصحة](#)
- [استكشاف الأخطاء وإصلاحها](#)
- [معلومات ذات صلة](#)

المقدمة

يقدم هذا المستند نموذجاً للتكوين باستخدام مدير أجهزة الأمان المعدلة (ASDM) من Cisco لتقييد ما يمكن لمستخدمي الشبكة الخاصة الظاهرية (VPN) للوصول إليه من الشبكات الداخلية عبر جهاز أمان PIX أو جهاز الأمان القابل للتكيف (ASA). يمكنك تقييد مستخدمي شبكة VPN للوصول عن بعد إلى مناطق الشبكة التي تريد منهم الوصول إليها فقط عندما:

1. إنشاء قوائم الوصول.
 2. إقرانهم بنهج المجموعة.
 3. إقران سياسات هذه المجموعة بمجموعات النفق.
- ارجع إلى [تكوين مركز VPN 3000 من Cisco للحد باستخدام عوامل التصفية وتعيين عامل تصفية RADIUS](#) لمعرفة المزيد حول السيناريو الذي يقوم فيه مركز VPN بحظر الوصول من مستخدمي VPN.

المتطلبات الأساسية

المتطلبات

تأكد من استيفاء المتطلبات التالية قبل أن تحاول إجراء هذا التكوين:

- يمكن تكوين PIX باستخدام ASDM. **ملاحظة:** راجع [السماح بوصول HTTPS لـ ASDM](#) للسماح بتكوين PIX بواسطة ASDM.
- لديك تكوين VPN واحد معروف جيداً للوصول عن بعد. **ملاحظة:** إذا لم يكن لديك أي تكوينات من هذا القبيل،

فارجع إلى [ASA كخادم VPN بعيد باستخدام مثال تكوين ASDM](#) للحصول على معلومات حول كيفية تكوين تكوين تكوين تكوين شبكة VPN جيدة للوصول عن بعد.

المكونات المستخدمة

تستند المعلومات الواردة في هذا المستند إلى إصدارات البرامج والمكونات المادية التالية:

- جهاز الأمان Cisco Secure PIX 500 Series Security Appliance، الإصدار 7.1(1) **ملاحظة:** لا تدعم أجهزة الأمان PIX 501 و 506E الإصدار 7.x.
- Cisco Adaptive Security Device Manager، الإصدار 5.1(1) **ملاحظة:** لا يتوفر ASDM إلا في PIX أو ASA 7.x.

تم إنشاء المعلومات الواردة في هذا المستند من الأجهزة الموجودة في بيئة معملية خاصة. بدأت جميع الأجهزة المستخدمة في هذا المستند بتكوين ممسوح (افتراضي). إذا كانت شبكتك مباشرة، فتأكد من فهمك للتأثير المحتمل لأي أمر.

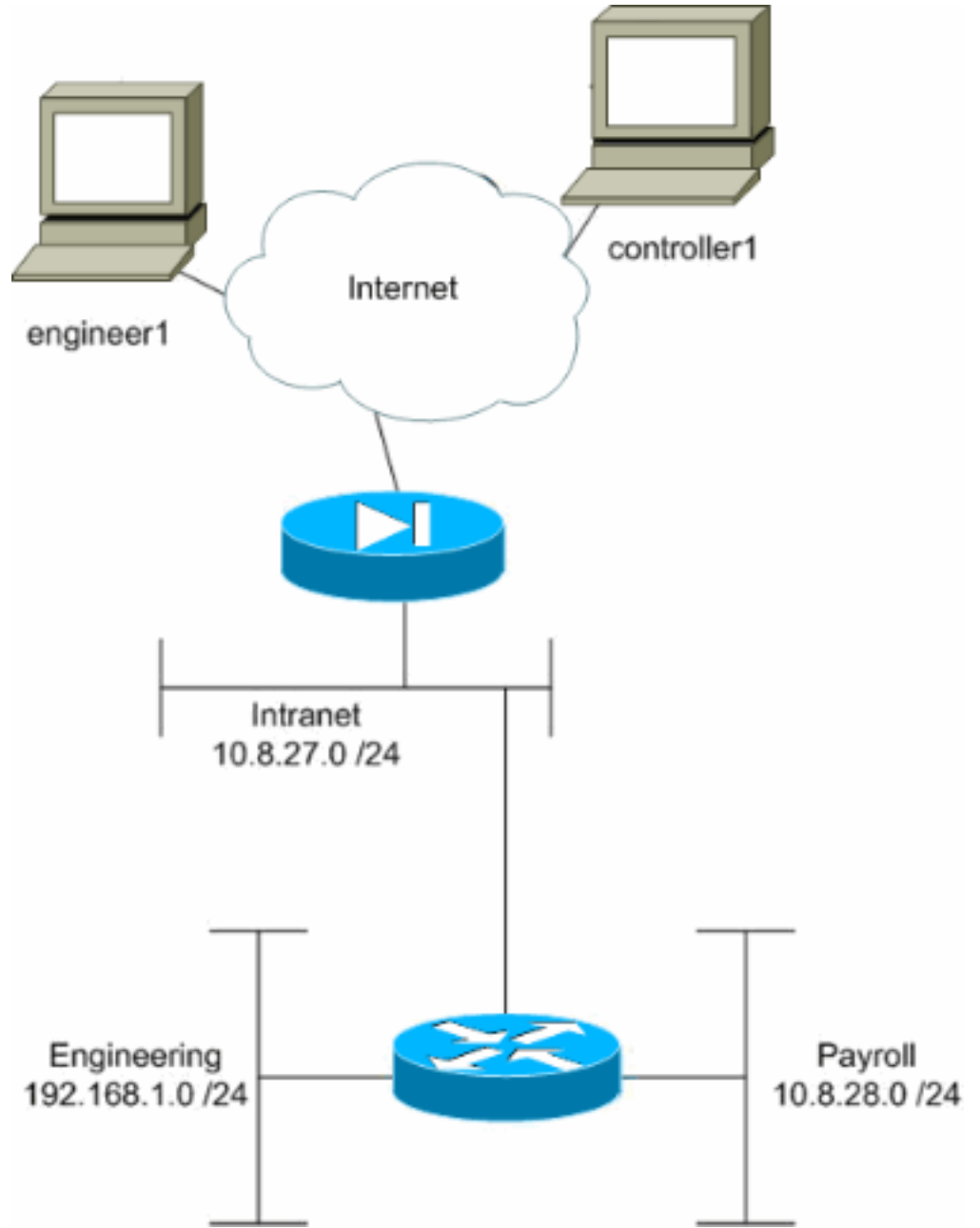
المنتجات ذات الصلة

كما يمكن استخدام هذا التكوين مع إصدارات الأجهزة والبرامج التالية:

- جهاز الأمان القابل للتكيف ASA 5500 Series، الإصدار 7.1(1) من Cisco

الرسم التخطيطي للشبكة

يستخدم هذا المستند إعداد الشبكة التالي:



في مثال التكوين هذا، من المفترض أن تكون شبكة شركة صغيرة بثلاث شبكات فرعية. يوضح هذا المخطط المخطط المخطط الشبكات الفرعية الثلاث هي إنترانت والهندسة وجدول الرواتب. الهدف من مثال التكوين هذا هو السماح لموظفي الرواتب بالوصول عن بعد إلى الشبكات الفرعية للإنترانet وكشوف المرتبات ومنعهم من الوصول إلى الشبكة الفرعية الهندسية. كما يجب أن يكون المهندسون قادرين على الوصول عن بعد إلى الشبكات الفرعية الهندسية والإنترانت، وليس إلى الشبكة الفرعية الخاصة بكشوف المرتبات. مستخدم الرواتب في هذا المثال هو "controller1". المستخدم الهندسي في هذا المثال هو "Engineer1".

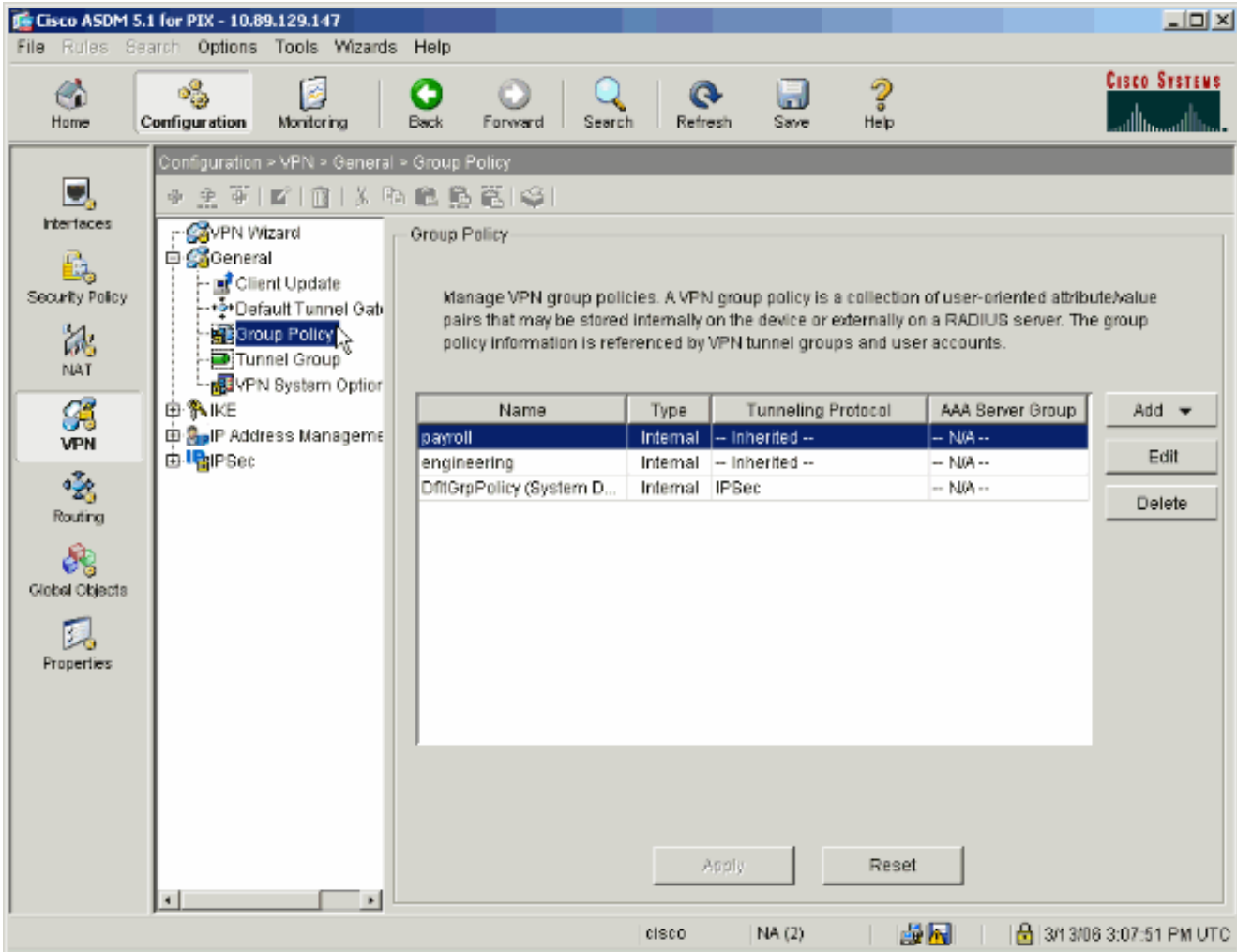
الاصطلاحات

راجع [اصطلاحات تلميحات Cisco التقنية للحصول على مزيد من المعلومات حول اصطلاحات المستندات.](#)

تكوين الوصول عبر ASDM

أكمل الخطوات التالية لتكوين جهاز أمان PIX باستخدام ASDM:

1. حدد تشكيل < VPN < عام < نهج المجموعة.



2. استنادا إلى الخطوات التي تم إتخاذها لتكوين مجموعات النفق على PIX، قد تكون نهج المجموعة موجودة بالفعل لمجموعات الأنفاق التي ترغب في تقييد استخدامها. في حالة وجود نهج مجموعة مناسب بالفعل، قم باختياره وانقر فوق تحرير. وإلا، انقر فوق إضافة واختر نهج المجموعة الداخلي....

Cisco ASDM 5.1 for PIX - 10.89.129.147

File Rules Search Options Tools Wizards Help

Home Configuration Monitoring Back Forward Search Refresh Save Help

Configuration > VPN > General > Group Policy

VPN Wizard
 General
 Client Update
 Default Tunnel Group
 Group Policy
 Tunnel Group
 VPN System Option
 IKE
 IP Address Management
 IPsec

Group Policy

Manage VPN group policies. A VPN group policy is a collection of user-oriented attribute/value pairs that may be stored internally on the device or externally on a RADIUS server. The group policy information is referenced by VPN tunnel groups and user accounts.

Name	Type	Tunneling Protocol	AAA Server Group
payroll	Internal	-- Inherited --	-- N/A --
engineering	Internal	-- Inherited --	-- N/A --
DfltGrpPolicy (System D...	Internal	IPsec	-- N/A --

Add Edit Delete

Apply Reset

disco NA (2) 3/13/08 3:08:31 PM UTC

3. إذا لزم الأمر، قم بإدخال أو تغيير اسم "نهج المجموعة" في أعلى الإطار الذي يتم فتحه.
4. في علامة التبويب "عام" قم بإلغاء تحديد مربع **Inherit** المجاور للتصفية ثم انقر فوق إدارة.

Edit Internal Group Policy: payroll

Name:

General | IPsec | Client Configuration | Client Firewall | Hardware Client

Check an Inherit checkbox to let the corresponding setting take its value from the default group policy.

Tunneling Protocols: Inherit IPsec

Filter: Inherit

Connection Settings

Access Hours: Inherit

Simultaneous Logins: Inherit

Maximum Connect Time: Inherit Unlimited minutes

Idle Timeout: Inherit Unlimited minutes

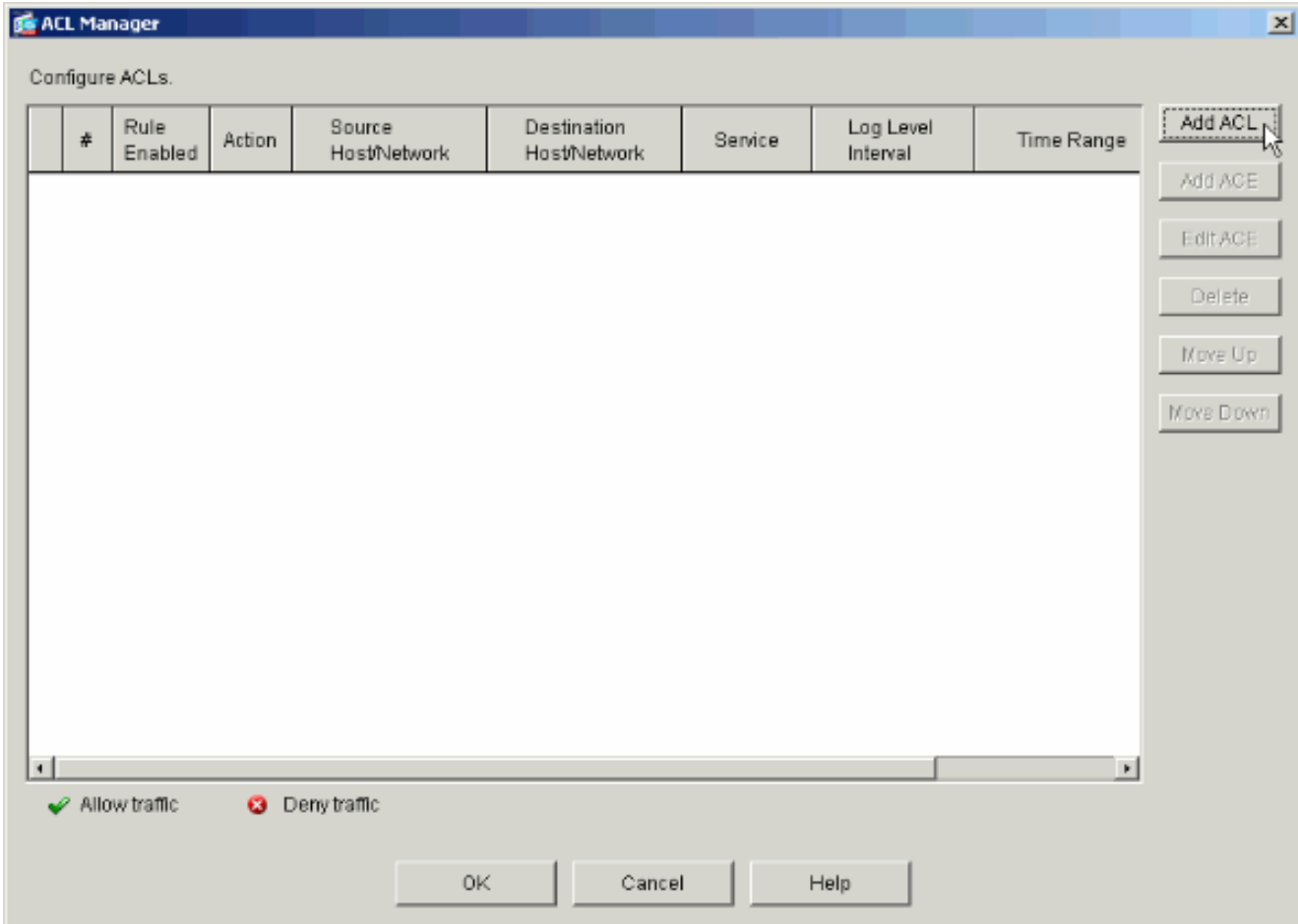
Servers

DNS Servers: Inherit Primary: Secondary:

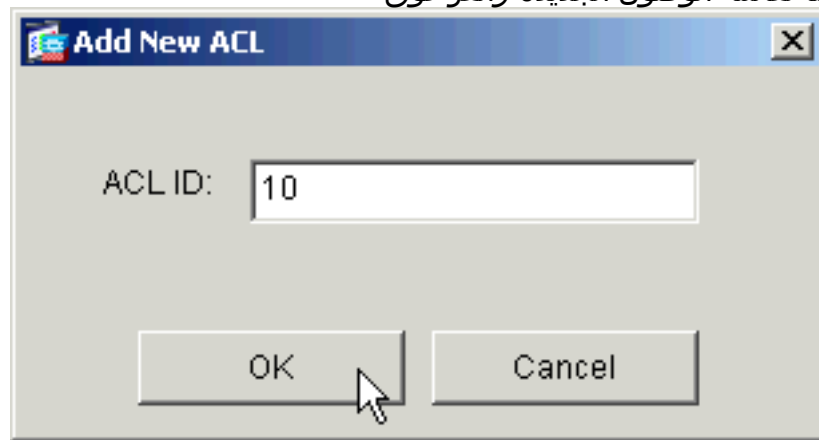
WINS Servers: Inherit Primary: Secondary:

DHCP Scope: Inherit

5. انقر على إضافة قائمة التحكم في الوصول (ACL) لإنشاء قائمة وصول جديدة في نافذة إدارة قائمة التحكم في الوصول (ACL) التي تظهر.

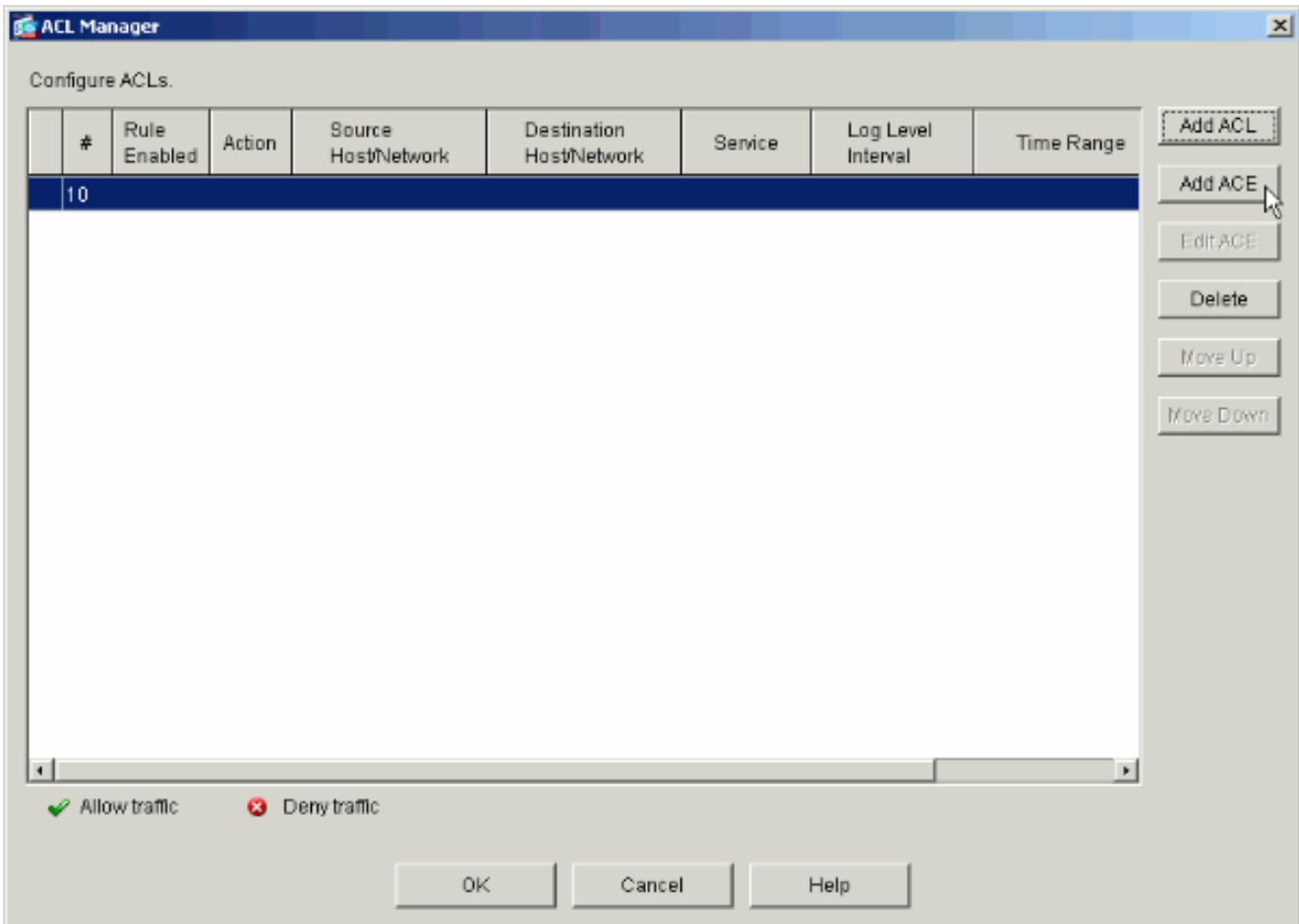


6. أختار رقما لقائمة الوصول الجديدة وانقر فوق



موافق.

7. مع تحديد قائمة التحكم في الوصول (ACL) الجديدة على اليسار، انقر فوق إضافة ACE لإضافة إدخال تحكم في الوصول جديد إلى القائمة.



8. قم بتحديد إدخال التحكم في الوصول (ACE) الذي ترغب في إضافته. في هذا المثال، يسمح إدخال التحكم في الوصول (ACE) الأول في قائمة التحكم في الوصول (ACL) رقم 10 بوصول IP إلى الشبكة الفرعية للرواتب من أي مصدر. **ملاحظة:** بشكل افتراضي، يحدد ASDM بروتوكول TCP فقط كبروتوكول. يجب عليك إختيار IP إذا كنت ترغب في السماح للمستخدمين بالوصول الكامل إلى IP أو رفضه. طقطقت ok عندما أنت إنتهيت.

Add Extended Access List Rule

Action

Permit Deny

Time Range

Time Range: -- Not Applied --

Syslog

Default Syslog

Source Host/Network

IP Address Name Group

IP address: 0.0.0.0

Mask: 0.0.0.0

Destination Host/Network

IP Address Name Group

IP address: 10.8.28.0

Mask: 255.255.255.0

Protocol and Service

TCP UDP ICMP IP

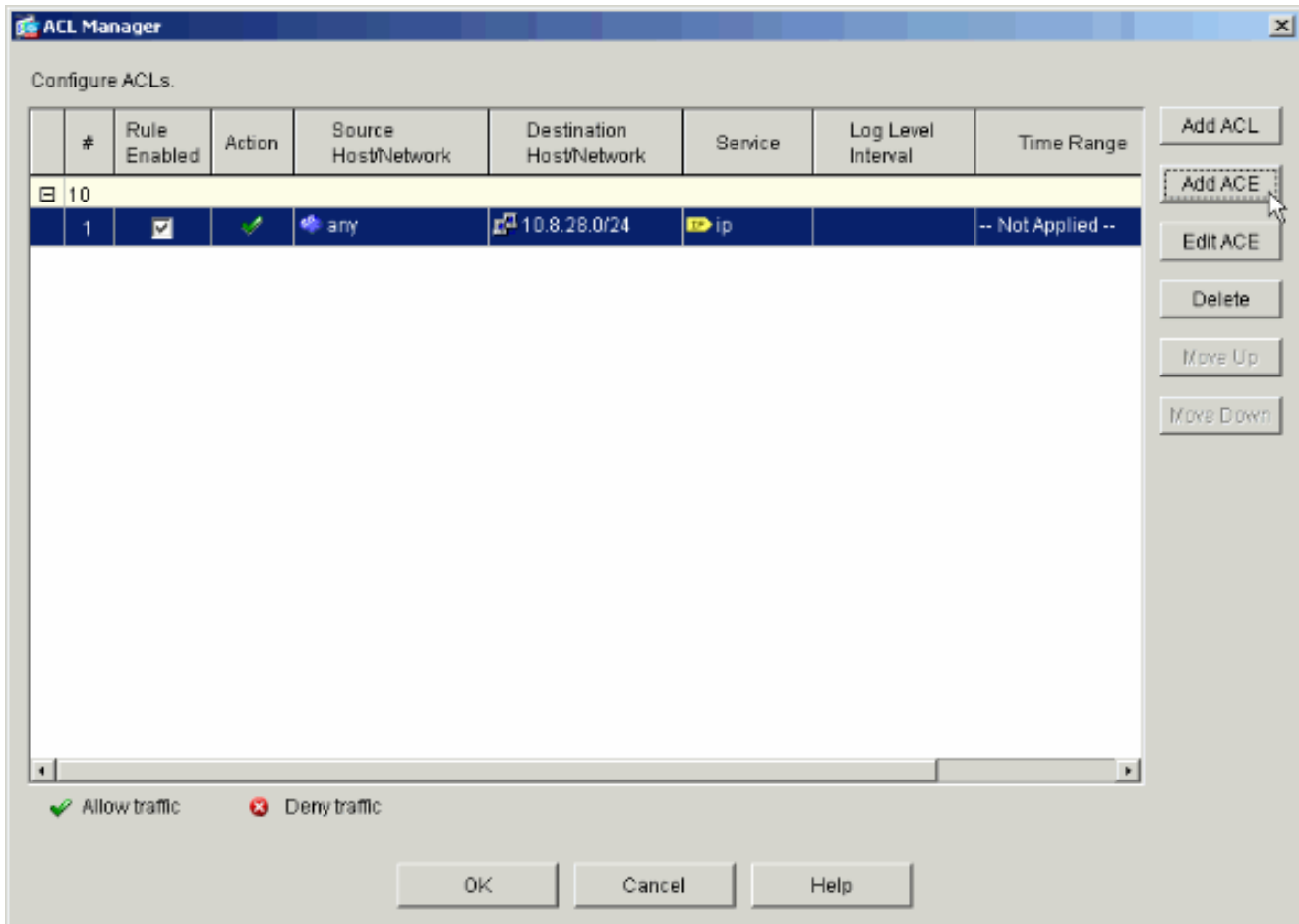
IP Protocol

IP protocol: any

Please enter the description below (optional):

permit IP access from ANY source to the payroll subnet (10.8.28.0 /24)

9. ACE الذي أضفته الآن يظهر في القائمة. أختبر إضافة ACE مرة أخرى لإضافة أي بنود إضافية إلى قائمة الوصول.



في هذا المثال، تتم إضافة إدخال تحكم في الوصول (ACE) ثان إلى قائمة التحكم في الوصول (ACL) 10 للسماح بالوصول إلى الشبكة الفرعية لشبكة الإنترنت.

Add Extended Access List Rule

Action

Permit Deny

Time Range

Time Range: -- Not Applied --

Syslog

Default Syslog

Source Host/Network

IP Address Name Group

IP address: 0.0.0.0

Mask: 0.0.0.0

Destination Host/Network

IP Address Name Group

IP address: 10.8.27.0

Mask: 255.255.255.0

Protocol and Service

TCP UDP ICMP IP

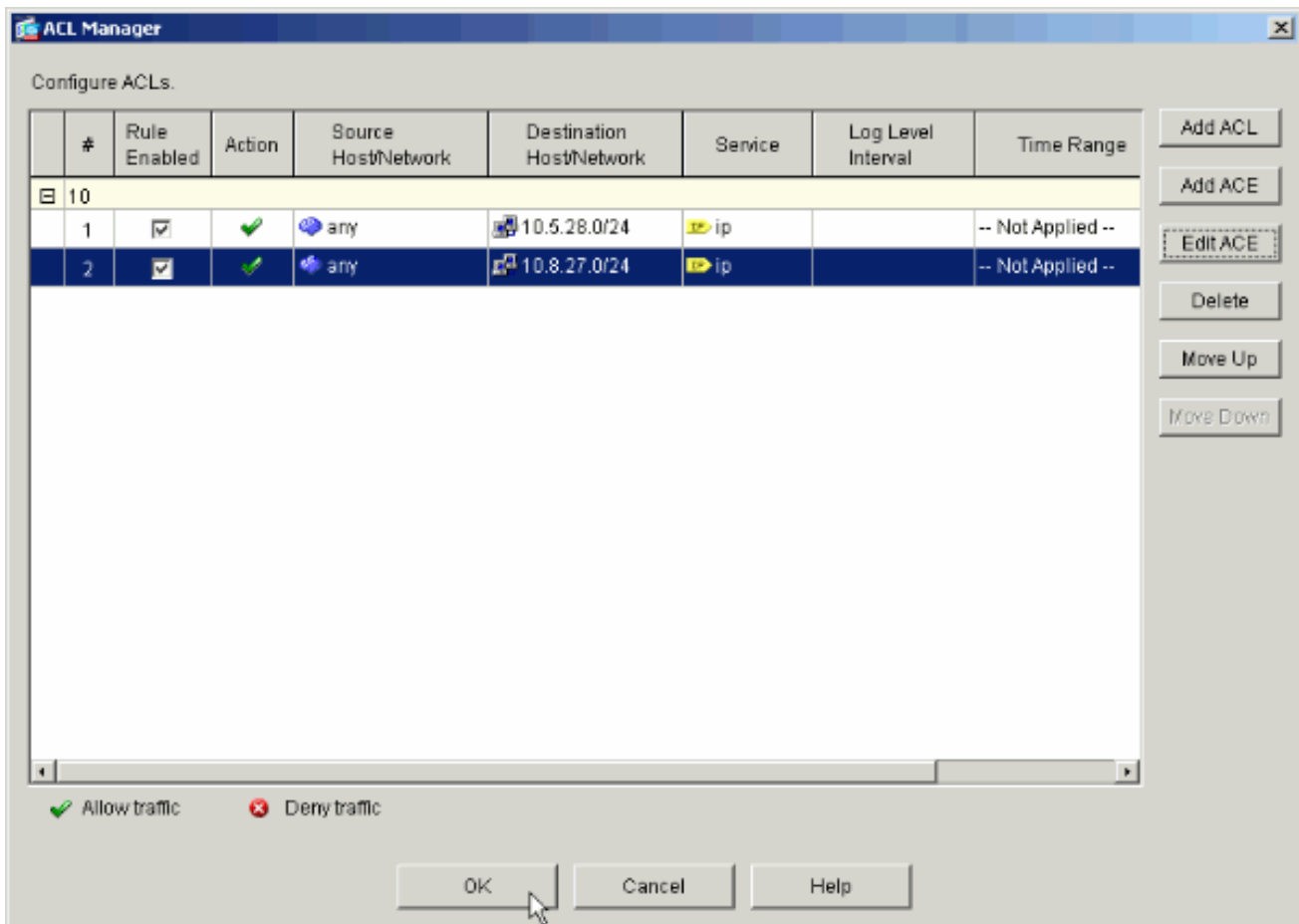
IP Protocol

IP protocol: any

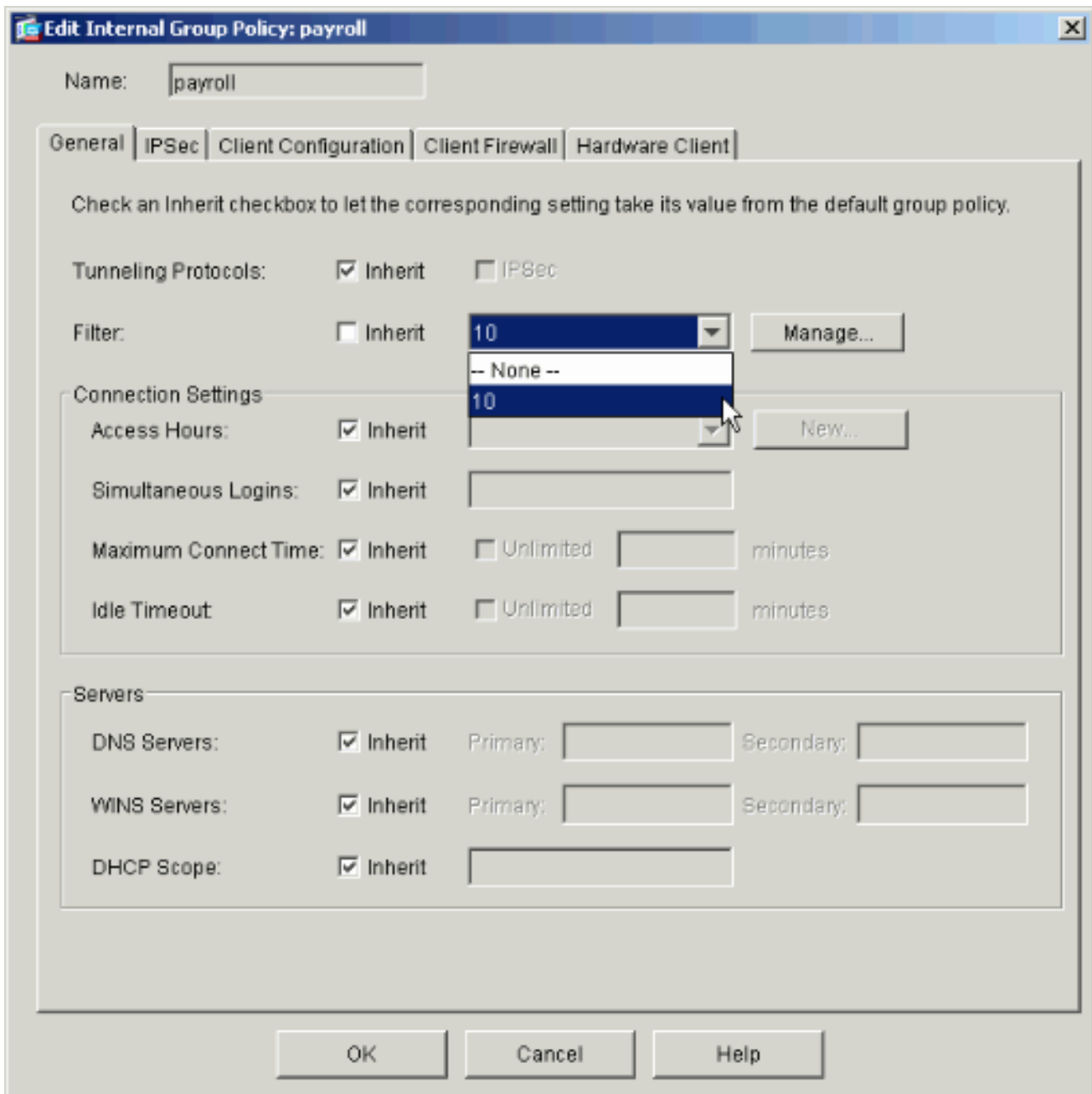
Please enter the description below (optional):

permit IP access from ANY source to the subnet used by all employees (10.8.27.0 /24)

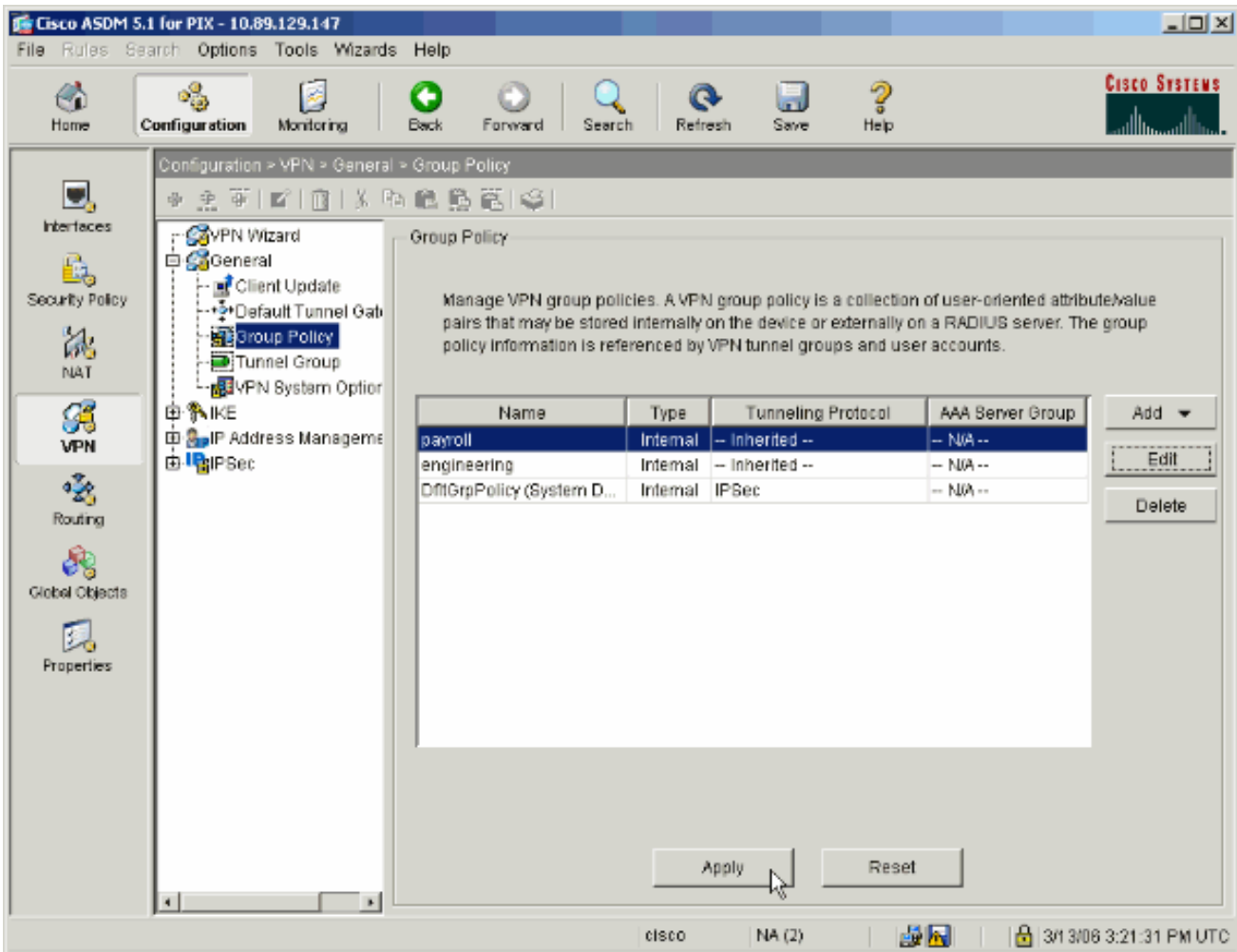
10. طقطقت ok ما إن يكون أنت إنتهيت من إضافة .ACEs



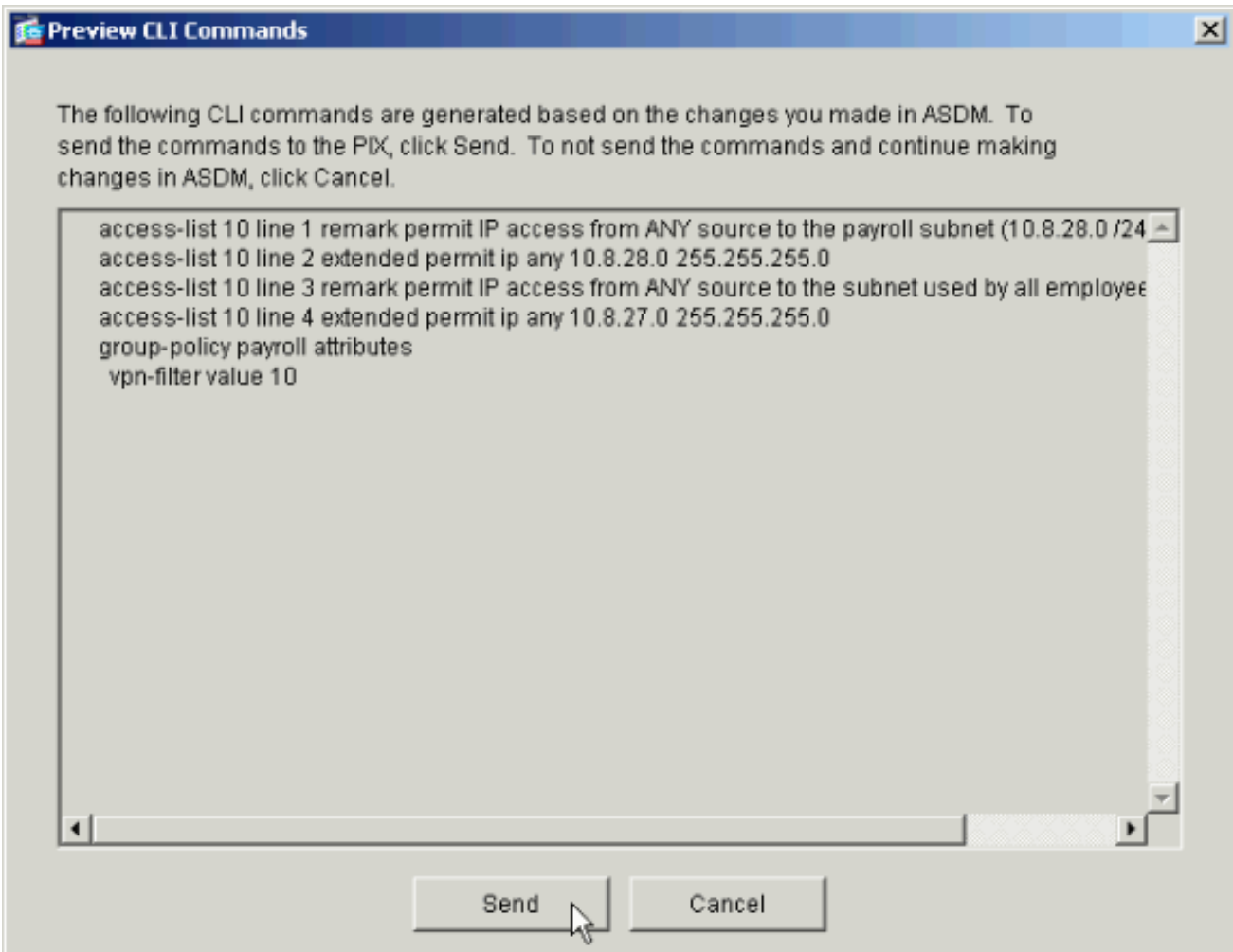
11. حدد قائمة التحكم في الوصول (ACL) التي قمت بتعريفها وتعميمها في الخطوات الأخيرة لتكون المرشح لنهج المجموعة الخاص بك. انقر فوق موافق عند الانتهاء.



12. انقر فوق تطبيق لإرسال التغييرات إلى .PIX



13. إذا قمت بتكوينه ليقوم بذلك ضمن خيارات < تفضيلات، يقوم ASDM بمعاينة الأوامر التي يوشك على إرسالها إلى PIX. طقطقة يرسل.



14. تطبيق "نهج المجموعة" الذي تم إنشاؤه أو تعديله مؤخرا على مجموعة النفق الصحيحة. انقر مجموعة النفق في الإطار الأيسر.

Cisco ASDM 5.1 for PIX - 10.89.129.147

File Rules Search Options Tools Wizards Help

Home Configuration Monitoring Back Forward Search Refresh Save Help

Configuration > VPN > General > Tunnel Group

VPN Wizard
 General
 Client Update
 Default Tunnel Group
 Group Policy
Tunnel Group
 VPN System Options
 IKE
 IP Address Management
 IPsec

Tunnel Group

Manage VPN tunnel groups. A VPN tunnel group represents a connection specific record for a IPsec or WebVPN connection.

Name	Type	Group Policy
payroll	ipsec-ra	payroll
engineering	ipsec-ra	engineering
DefaultIRAGroup	ipsec-ra	DfltGrpPolicy
DefaultL2LGroup	ipsec-l2l	DfltGrpPolicy

Group Delimiter:

Apply Reset

Configuration changes saved successfully. cisco NA (2) 3/13/08 3:22:11 PM UTC

15. أختار مجموعة النفق التي ترغب في تطبيق نهج المجموعة عليها وانقر فوق تحرير.

Cisco ASDM 5.1 for PIX - 10.89.129.147

File Rules Search Options Tools Wizards Help

Home Configuration Monitoring Back Forward Search Refresh Save Help

Configuration > VPN > General > Tunnel Group

VPN Wizard
 General
 Client Update
 Default Tunnel Gab
 Group Policy
Tunnel Group
 VPN System Optor
 IKE
 IP Address Manageme
 IPSec

Tunnel Group

Manage VPN tunnel groups. A VPN tunnel group represents a connection specific record for a IPSec or WebVPN connection.

Name	Type	Group Policy
payroll	ipsec-ra	payroll
engineering	ipsec-ra	engineering
DefaultRAGroup	ipsec-ra	DfltGrpPolicy
DefaultL2LGroup	ipsec-l2l	DfltGrpPolicy

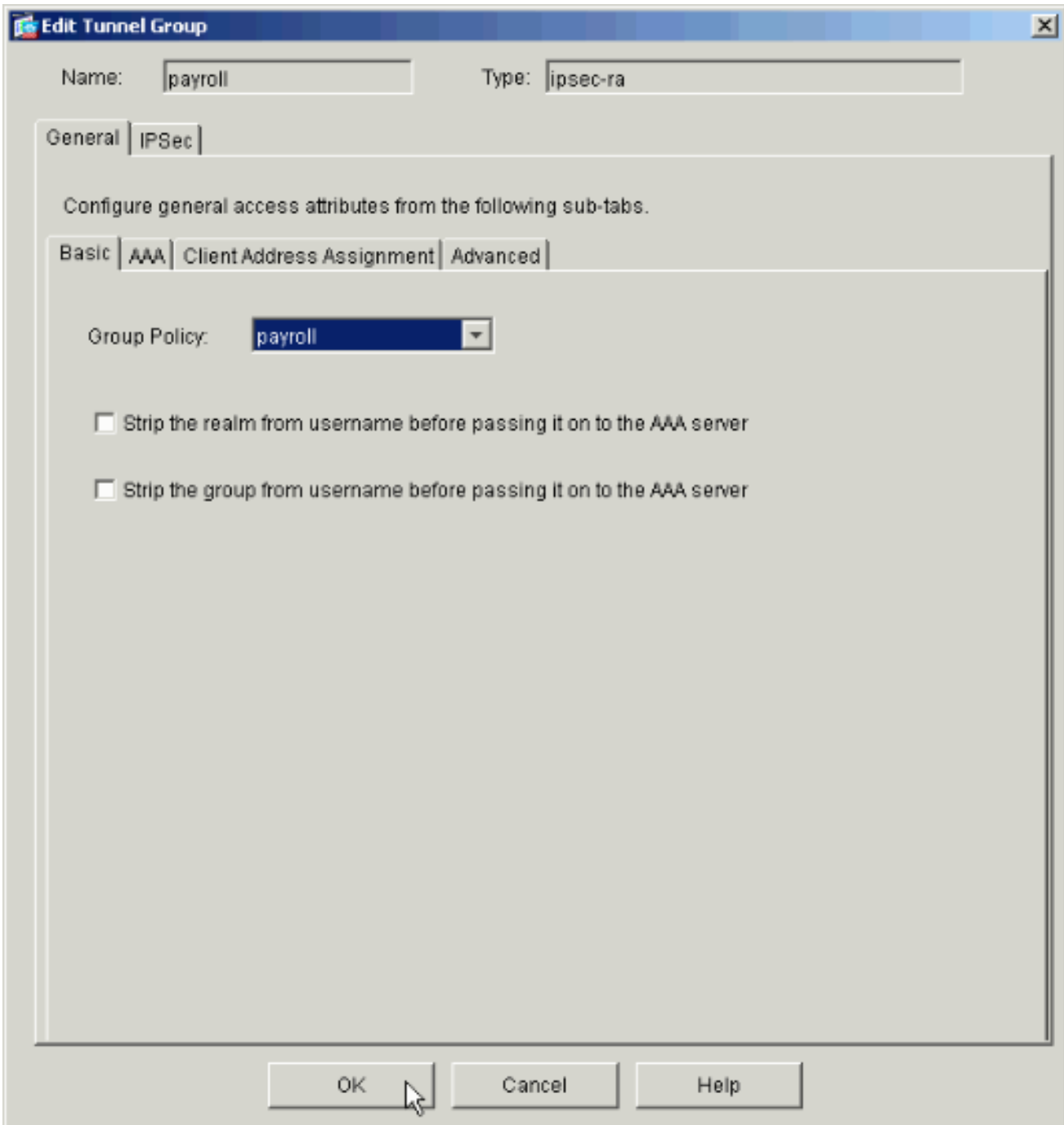
Group Delimiter: -- None --

Apply Reset

Configuration changes saved successfully.

cisco NA (2) 3/13/08 3:22:31 PM UTC

16. إذا تم إنشاء "نهج المجموعة" تلقائياً (راجع الخطوة 2)، فتتحقق من تحديد "نهج المجموعة" الذي قمت بتكوينه للتو في المربع المنسدل. إذا لم يتم تكوين "نهج المجموعة" تلقائياً، فقم بتحديد المربع المنسدل. انقر فوق موافق عند الانتهاء.



17. طقطقة **يطبق**، وإن طلب، **يرسل** أن يضيف التغيير إلى ال PIX تشكيل. في حالة تحديد "نهج المجموعة" بالفعل، قد تتلقى رسالة تقول "لم يتم إجراء أية تغييرات." وانقر فوق OK.
18. كرر الخطوات من 2 إلى 17 لأي مجموعات نفق إضافية تريد إضافة قيود إليها. في مثال التكوين هذا، من الضروري أيضا تقييد وصول المهندسين. ورغم أن الإجراء واحد، فإن هذه مجرد نوافذ قليلة لا تخلو من الاختلافات: قائمة الوصول الجديدة

ACL Manager

Configure ACLs.

#	Rule Enabled	Action	Source Host/Network	Destination Host/Network	Service	Log Level Interval	Time Range
10							
1	<input checked="" type="checkbox"/>	✓	any	10.8.28.0/24	ip		-- Not Applied --
2	<input checked="" type="checkbox"/>	✓	any	10.8.27.0/24	ip		-- Not Applied --
20							
1	<input checked="" type="checkbox"/>	✓	any	192.168.1.0/24	ip		-- Not Applied --
2	<input checked="" type="checkbox"/>	✓	any	10.8.27.0/24	ip		-- Not Applied --

Allow traffic Deny traffic

أختر قائمة الوصول 20 كعامل تصفية في نهج المجموعة الهندسية.

Edit Internal Group Policy: engineering

Name:

General | IPsec | Client Configuration | Client Firewall | Hardware Client

Check an Inherit checkbox to let the corresponding setting take its value from the default group policy.

Tunneling Protocols: Inherit IPsec

Filter: Inherit

Connection Settings

Access Hours: Inherit

Simultaneous Logins: Inherit

Maximum Connect Time: Inherit Unlimited minutes

Idle Timeout: Inherit Unlimited minutes

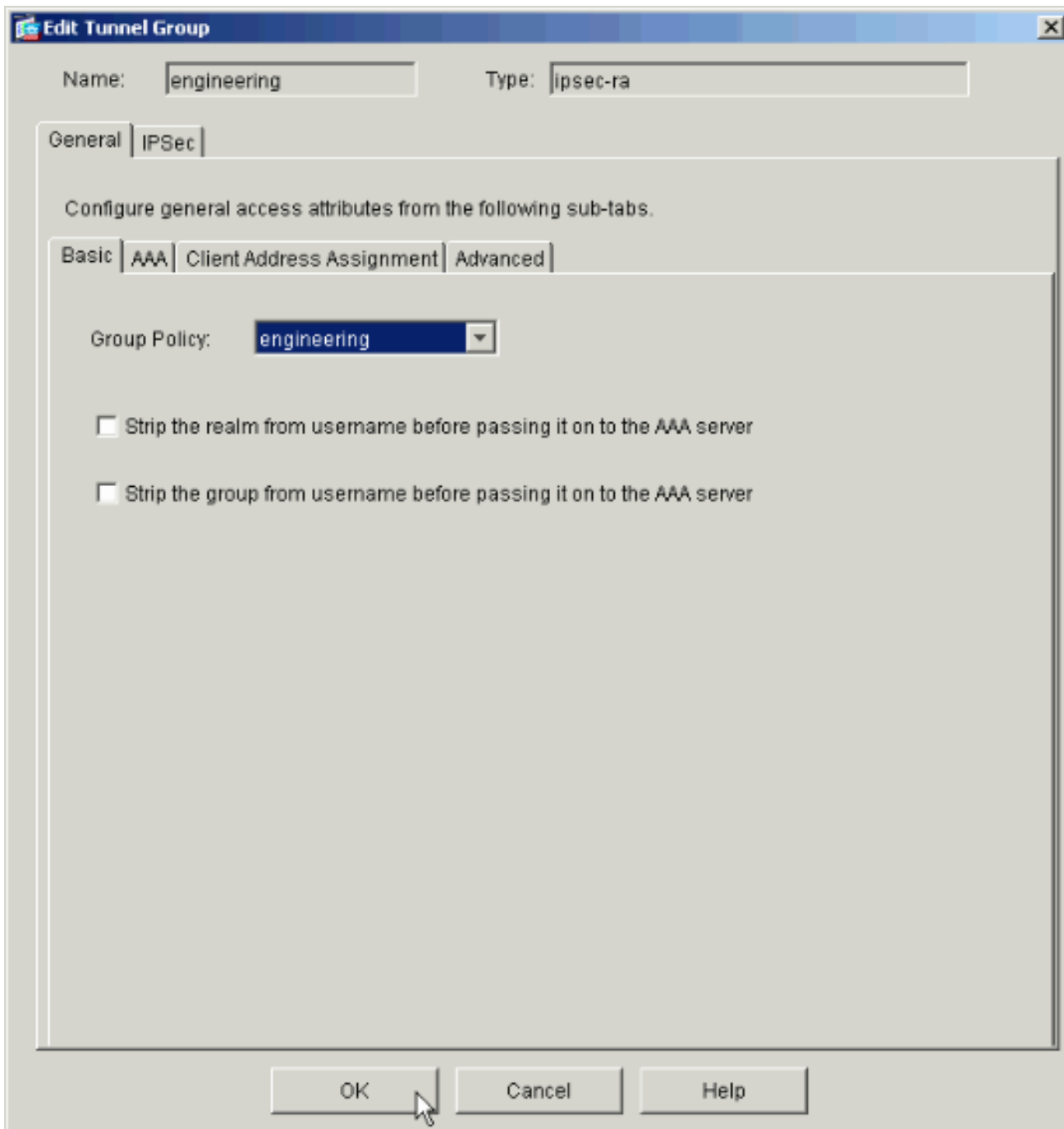
Servers

DNS Servers: Inherit Primary: Secondary:

WINS Servers: Inherit Primary: Secondary:

DHCP Scope: Inherit

تحقق من تعيين نهج المجموعة الهندسية لمجموعة النفق الهندسية.



تكوين الوصول عبر CLI (واجهة سطر الأوامر)

أكمل الخطوات التالية لتكوين جهاز الأمان باستخدام CLI (واجهة سطر الأوامر):

ملاحظة: تنزل بعض الأوامر الواردة في هذا الناتج إلى سطر ثان لأسباب مكانية.

قم بإنشاء قائمتين مختلفتين للتحكم في الوصول (15 و 20) يتم تطبيقهما على المستخدمين عند إتصالهم بشبكة VPN الخاصة بالوصول عن بعد. يتم إستدعاء قائمة الوصول هذه لاحقا في التكوين.

```
ASAwCSC-CLI(config)#access-list 15 remark permit IP access from ANY
(source to the payroll subnet (10.8.28.0/24
```

```
ASAwCSC-CLI(config)#access-list 15 extended permit ip
any 10.8.28.0 255.255.255.0
```

```
ASAwCSC-CLI(config)#access-list 15 remark Permit IP access from ANY
(source to the subnet used by all employees (10.8.27.0
```

```
ASAwCSC-CLI(config)#access-list 15 extended permit ip
any 10.8.27.0 255.255.255.0
```

```
ASAwCSC-CLI(config)#access-list 20 remark Permit IP access from ANY
(source to the Engineering subnet (192.168.1.0/24
```

```
ASAwCSC-CLI(config)#access-list 20 extended permit ip
any 192.168.1.0 255.255.255.0
```

```
ASAwCSC-CLI(config)#access-list 20 remark Permit IP access from ANY
(source to the subnet used by all employees (10.8.27.0/24
```

```
ASAwCSC-CLI(config)#access-list 20 extended permit ip
any 10.8.27.0 255.255.255.0
```

2. خلقت إثنان مختلف VPN عنوان بركة. قم بإنشاء واحد للرواتب وآخر للمستخدمين البعيدين لهندسة البيانات.

```
ASAwCSC-CLI(config)#ip local pool Payroll-VPN
mask 255.255.255.0 172.10.1.100-172.10.1.200
```

```
ASAwCSC-CLI(config)#ip local pool Engineer-VPN 172.16.2.1-172.16.2.199
mask 255.255.255.0
```

3. قم بإنشاء سياسات للرواتب التي تنطبق عليهم فقط عند إتصالهم.

```
ASAwCSC-CLI(config)#group-policy Payroll internal
```

```
ASAwCSC-CLI(config)#group-policy Payroll attributes
```

```
ASAwCSC-CLI(config-group-policy)#dns-server value 10.8.27.10
```

```
ASAwCSC-CLI(config-group-policy)#vpn-filter value 15
```

Call the ACL created in step 1 for Payroll. ASAwCSC-CLI(config-group-policy)#vpn- ---!
tunnel-protocol IPSec

```
ASAwCSC-CLI(config-group-policy)#default-domain value payroll.corp.com
```

```
ASAwCSC-CLI(config-group-policy)#address-pools value Payroll-VPN
```

.Call the Payroll address space that you created in step 2 ---!

4. هذه الخطوة هي نفسها الخطوة 3 إلا أنها للمجموعة الهندسية.

```
ASAwCSC-CLI(config)#group-policy Engineering internal
```

```
ASAwCSC-CLI(config)#group-policy Engineering attributes
```

```
ASAwCSC-CLI(config-group-policy)#dns-server value 10.8.27.10
```

```
ASAwCSC-CLI(config-group-policy)#vpn-filter value 20
```

Call the ACL that you created in step 1 for Engineering. ASAwCSC-CLI(config-group- ---!
policy)#vpn-tunnel-protocol IPSec

```
ASAwCSC-CLI(config-group-policy)#default-domain value Engineer.corp.com
```

```
ASAwCSC-CLI(config-group-policy)#address-pools value Engineer-VPN
```

.Call the Engineering address space that you created in step 2 ---!

5. قم بإنشاء مستخدمين محليين وتعيين السمات التي قمت بإنشائها لهؤلاء المستخدمين لتقييد وصولهم إلى الموارد.

```
ASAwCSC-CLI(config)#username engineer password cisco123
```

```
ASAwCSC-CLI(config)#username engineer attributes
```

```

ASAwCSC-CLI(config-username)#vpn-group-policy Engineering

ASAwCSC-CLI(config-username)#vpn-filter value 20

ASAwCSC-CLI(config)#username marty password cisco456

ASAwCSC-CLI(config)#username marty attributes

ASAwCSC-CLI(config-username)#vpn-group-policy Payroll

ASAwCSC-CLI(config-username)#vpn-filter value 15

```

.6 إنشاء مجموعات النفق التي تحتوي على سياسات اتصال لمستخدمي الرواتب.

```

ASAwCSC-CLI(config)#tunnel-group Payroll type ipsec-ra

ASAwCSC-CLI(config)#tunnel-group Payroll general-attributes

ASAwCSC-CLI(config-tunnel-general)#address-pool Payroll-VPN

ASAwCSC-CLI(config-tunnel-general)#default-group-policy Payroll

ASAwCSC-CLI(config)#tunnel-group Payroll ipsec-attributes

ASAwCSC-CLI(config-tunnel-ipsec)#pre-shared-key time1234

```

.7 قم بإنشاء مجموعات النفق التي تحتوي على سياسات اتصال لمستخدمي Engineering.

```

ASAwCSC-CLI(config)#tunnel-group Engineering type ipsec-ra

ASAwCSC-CLI(config)#tunnel-group Engineering general-attributes

ASAwCSC-CLI(config-tunnel-general)#address-pool Engineer-VPN

ASAwCSC-CLI(config-tunnel-general)#default-group-policy Engineering

ASAwCSC-CLI(config)#tunnel-group Engineering ipsec-attributes

ASAwCSC-CLI(config-tunnel-ipsec)#pre-shared-key Engine123

```

ما إن يدخل أنت تشكيل، أنت يستطيع رأيت هذا منطقة مبرزة في تشكيلك:

اسم الجهاز 1
<pre> ASA-AIP-CLI(config)#show running-config (ASA Version 7.2(2 ! hostname ASAwCSC-ASDM domain-name corp.com enable password 9jNfZuG3TC5tCVH0 encrypted names ! interface Ethernet0/0 nameif Intranet security-level 0 ip address 10.8.27.2 255.255.255.0 ! interface Ethernet0/1 nameif Engineer security-level 100 </pre>

```

ip address 192.168.1.1 255.255.255.0
!
interface Ethernet0/2
  nameif Payroll
  security-level 100
  ip address 10.8.28.0
!
interface Ethernet0/3
  no nameif
  no security-level
  no ip address
!
interface Management0/0
  no nameif
  no security-level
  no ip address
!
passwd 2KFQnbNIdI.2KYOU encrypted
ftp mode passive
dns server-group DefaultDNS
domain-name corp.com
access-list Inside_nat0_outbound extended permit ip any
172.10.1.0 255.255.255.0
access-list Inside_nat0_outbound extended permit ip any
172.16.2.0 255.255.255.0
access-list 15 remark permit IP access from ANY source
to the
(Payroll subnet (10.8.28.0/24
access-list 15 extended permit ip any 10.8.28.0
255.255.255.0
access-list 15 remark Permit IP access from ANY source
to the subnet
(used by all employees (10.8.27.0
access-list 15 extended permit ip any 10.8.27.0
255.255.255.0
access-list 20 remark Permit IP access from Any source
to the Engineering
(subnet (192.168.1.0/24
access-list 20 extended permit ip any 192.168.1.0
255.255.255.0
access-list 20 remark Permit IP access from Any source
to the subnet used
(by all employees (10.8.27.0/24
access-list 20 extended permit ip any 10.8.27.0
255.255.255.0
pager lines 24
mtu MAN 1500
mtu Outside 1500
mtu Inside 1500
ip local pool Payroll-VPN 172.10.1.100-172.10.1.200 mask
255.255.255.0
ip local pool Engineer-VPN 172.16.2.1-172.16.2.199 mask
255.255.255.0
no failover
icmp unreachable rate-limit 1 burst-size 1
asdm image disk0:/asdm-522.bin
no asdm history enable
arp timeout 14400
global (Intranet) 1 interface
nat (Inside) 0 access-list Inside_nat0_outbound
nat (Inside) 1 192.168.1.0 255.255.255.0
nat (Inside) 1 10.8.27.0 255.255.255.0
nat (Inside) 1 10.8.28.0 255.255.255.0
route Intranet 0.0.0.0 0.0.0.0 10.8.27.2

```



```

timeout xlate 3:00:00
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 mgcp-pat 0:05:00
timeout sip 0:30:00 sip_media 0:02:00 sip-invite 0:03:00
                                sip-disconnect 0:02:00
                                timeout uauth 0:05:00 absolute
                                group-policy Payroll internal
                                group-policy Payroll attributes
                                    dns-server value 10.8.27.10
                                    vpn-filter value 15
                                    vpn-tunnel-protocol IPSec
                                default-domain value payroll.corp.com
                                address-pools value Payroll-VPN
                                group-policy Engineering internal
                                group-policy Engineering attributes
                                    dns-server value 10.8.27.10
                                    vpn-filter value 20
                                    vpn-tunnel-protocol IPSec
                                default-domain value Engineer.corp.com
                                address-pools value Engineer-VPN
                                username engineer password LCaPXI.4Xtvclaca encrypted
                                    username engineer attributes
                                    vpn-group-policy Engineering
                                    vpn-filter value 20
                                username marty password 6XmYwQO09tiYnUDN encrypted
                                    privilege 0
                                    username marty attributes
                                    vpn-group-policy Payroll
                                    vpn-filter value 15
                                    no snmp-server location
                                    no snmp-server contact
                                crypto ipsec transform-set ESP-3DES-SHA esp-3des esp-
                                    sha-hmac
                                crypto dynamic-map Outside_dyn_map 20 set pfs
                                crypto dynamic-map Outside_dyn_map 20 set transform-set
                                    ESP-3DES-SHA
                                crypto map Outside_map 65535 ipsec-isakmp dynamic
                                    Outside_dyn_map
                                crypto map Outside_map interface Outside
                                    crypto isakmp enable Outside
                                    crypto isakmp policy 10
                                    authentication pre-share
                                    encryption 3des
                                    hash sha
                                    group 2
                                    lifetime 86400
                                tunnel-group Payroll type ipsec-ra
                                tunnel-group Payroll general-attributes
                                    address-pool vpnpool
                                    default-group-policy Payroll
                                tunnel-group Payroll ipsec-attributes
                                    * pre-shared-key
                                tunnel-group Engineering type ipsec-ra
                                tunnel-group Engineering general-attributes
                                    address-pool Engineer-VPN
                                    default-group-policy Engineering
                                tunnel-group Engineering ipsec-attributes
                                    * pre-shared-key
                                    telnet timeout 5
                                    ssh timeout 5
                                    console timeout 0
                                !

```

```
class-map inspection_default
match default-inspection-traffic
!
!
policy-map type inspect dns migrated_dns_map_1
parameters
message-length maximum 512
policy-map global_policy
class inspection_default
inspect dns migrated_dns_map_1
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
!
service-policy global_policy global
prompt hostname context
Cryptochecksum:0e579c85004dcfb4071cb561514a392b
end :
#(ASA-AIP-CLI(config
```

[التحقق من الصحة](#)

أستخدم إمكانيات مراقبة ASDM للتحقق من التكوين الخاص بك:

1. حدد مراقبة < VPN < إحصائيات VPN < جلسات العمل. أنت ترى النشاط VPN جلسة على ال PIX. حدد جلسة العمل التي تهتم بها وانقر فوق تفاصيل.

Cisco ASDM 5.1 for PIX - 10.89.129.147

File Rules Search Options Tools Wizards Help

Home Configuration Monitoring Back Forward Search Refresh Save Help

Monitoring > VPN > VPN Statistics > Sessions

VPN Connection Graph
IPSec Tunnels
VPN Statistics
Crypto Statistics
Encryption Statistics
Global IKE/IPSec Statistics
Protocol Statistics
Sessions

Sessions

Remote Access	LAN-to-LAN	Total	Total Cumulative
1	0	1	3

Filter By: Remote Access -- All Sessions -- Filter

Username	Group Policy Tunnel Group	Assigned IP Address Public IP Address	Protocol Encryption
controllert	DfltGrpPolicy payroll	10.8.27.50 172.22.1.165	IPSec 3DES

Details
Logout
Ping

To sort VPN sessions, right-click on the above table and select Table Sort Order from popup menu.

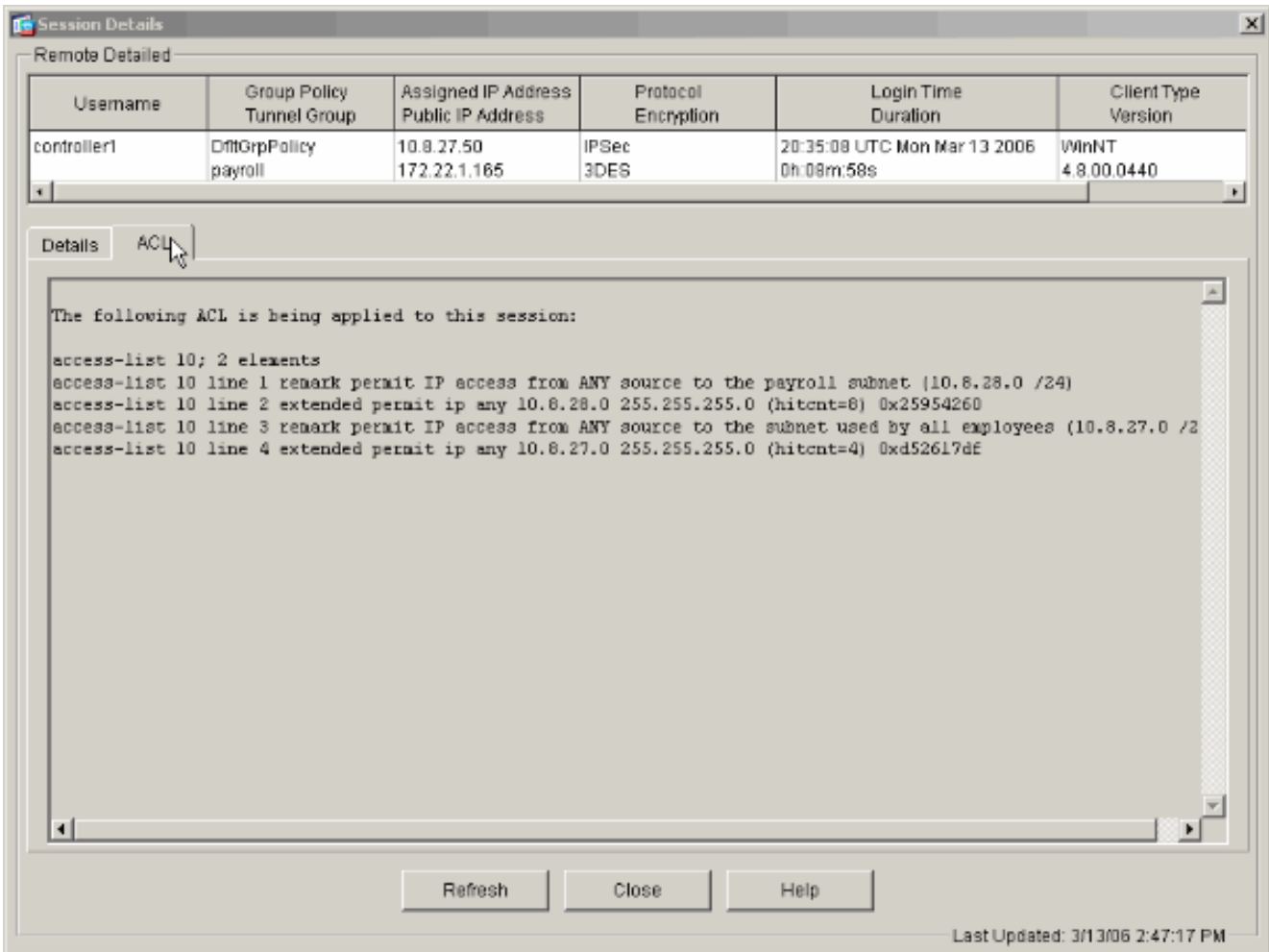
Logout By: -- All Sessions -- Logout Sessions

Refresh

Last Updated: 3/13/06 2:39:33 PM

Data Refreshed Successfully. | cisco | NA (2) | 3/13/06 8:36:34 PM UTC

2. حدد علامة التبويب قائمة التحكم في الوصول (ACL). تعكس قوائم التحكم (ACL) حركة مرور البيانات التي تتدفق عبر النفق من العميل إلى الشبكة (الشبكات) المسموح بها.



استكشاف الأخطاء وإصلاحها

لا تتوفر حاليًا معلومات محددة لاستكشاف الأخطاء وإصلاحها لهذا التكوين.

معلومات ذات صلة

- [أجهزة الأمان المعدلة Cisco ASA 5500 Series Adaptive Security Appliances ASA كخادم VPN بعيد باستخدام مثال تكوين ASDM](#)
- [أمثلة تكوين أجهزة الأمان Cisco PIX 500 Series وإشعارات التقنية](#)
- [أمثلة تكوين أجهزة الأمان المعدلة Cisco ASA 5500 Series Adaptive Security Appliances و TechNotes](#)
- [أمثلة تكوين عميل شبكة VPN والملاحظات التقنية من Cisco](#)
- [الدعم التقني والمستندات - Cisco Systems](#)

ةمچرتل هذه ل و ح

ةلأل تاي نقتل ن م ة و مچ م ادخت ساب دن تسمل اذ ه Cisco ت مچرت
ملاعلاء ان ا عي مچ ي ف ن ي م دخت سمل ل معد ي و تح م مي دقت ل ة ي رش ب ل و
امك ة ق ي قد ن و ك ت ن ل ة ي ل أ ة مچرت ل ض ف أ ن أ ة ظ حال م ي ج ر ي . ة ص ا خ ل م ه ت غ ل ب
Cisco ي ل خ ت . ف ر ت ح 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 ع م ل ا ح ل ا و ه
ي ل ا م ا د ع و ج 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 أ ل ا ي ز ي ل ج ن ا ل ا دن تسمل ا