

如何向PIX IPSec 5.2及更高版本新增AAA身份驗證(Xauth)

目錄

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[慣例](#)

[背景資訊](#)

[調試步驟](#)

[PIX上的Debug命令](#)

[客戶端調試](#)

[AAA伺服器設定檔](#)

[Cisco安全UNIX TACACS+](#)

[適用於Windows TACACS+的Cisco安全ACS](#)

[Cisco安全UNIX RADIUS](#)

[適用於Windows RADIUS的Cisco安全ACS](#)

[Merit RADIUS \(支援Cisco AV對 \)](#)

[網路圖表](#)

[可配置的RADIUS埠 \(5.3及更高版本 \)](#)

[如何在不使用VPN組的情況下使用Xauth進行身份驗證](#)

[Cisco安全VPN客戶端1.1設定 — 不帶VPN組的Xauth](#)

[VPN 3000客戶端2.5或VPN客戶端3.x設定 — 不帶VPN組的Xauth](#)

[不帶VPN組的Xauth - PIX設定](#)

[如何使用VPN組的Xauth進行驗證](#)

[VPN客戶端2.5或3.0設定 — 帶VPN組的Xauth](#)

[帶VPN組的Xauth - PIX設定](#)

[含VPN群組和每個使用者可下載ACL的Xauth - ACS設定](#)

[帶VPN組和每個使用者可下載ACL的Xauth - PIX 6.x設定](#)

[帶VPN組和可按使用者下載的ACL的Xauth - ASA/PIX 7.x設定](#)

[如何為VPN客戶端連線配置本地Xauth](#)

[如何新增記帳](#)

[TACACS+計費範例](#)

[RADIUS計費範例](#)

[Debug and Show — 不帶VPN組的Xauth](#)

[調試和顯示 — 使用VPN組的Xauth](#)

[Debug and Show - Xauth \(具有按使用者下載的ACL \)](#)

[相關資訊](#)

簡介

RADIUS和TACACS+身份驗證和記帳，以及在某種程度上，授權是在PIX終止的Cisco Secure VPN Client 1.1和Cisco VPN 3000 2.5硬體客戶端隧道完成的。PIX 5.2及更高版本的擴展身份驗證(Xauth)與先前版本相比的更改，後者包括身份驗證、授權和記帳(AAA)訪問清單支援，以控制經過身份驗證的使用者可以訪問哪些內容以及對Cisco VPN 3000 Client 2.5 Xauth終止的支援。**vpn group split-tunneling**命令使VPN 3000客戶端能夠同時連線到PIX內的網路以及其他網路（例如，網際網路）。在PIX 5.3及更高版本中，AAA與先前代碼版本相比的變化是RADIUS埠是可配置的。在PIX 6.0中，新增了對VPN客戶端3.x的支援。這需要Diffie-Hellman群組2。

必要條件

需求

本文件沒有特定需求。

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- PIX軟體版本5.2.1
- Cisco安全VPN使用者端1.1
- Cisco VPN 3000 2.5使用者端或VPN使用者端3.x**注意**：Cisco VPN客戶端3.0.x版不能與低於6.0的PIX版本配合使用。有關詳細資訊，請參閱[支援IPsec/PPTP/L2TP的Cisco硬體和VPN客戶端](#)。

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路正在作用，請確保您已瞭解任何指令可能造成的影響。

慣例

如需文件慣例的詳細資訊，請參閱[思科技術提示慣例](#)。

背景資訊

PIX防火牆軟體版本6.2支援從訪問控制伺服器(ACS)將訪問控制清單(ACL)下載到PIX防火牆。這樣，在AAA伺服器上配置每使用者ACL即可提供每使用者ACL授權。然後可以通過ACS將其下載到PIX防火牆。僅RADIUS伺服器支援此功能。TACACS+伺服器不支援此功能。

調試步驟

完成以下調試步驟：

1. 在新增AAA身份驗證之前，請確保PIX Xauth配置工作正常。如果在實施AAA之前無法傳遞流量，則之後無法執行。
2. 在PIX中啟用某種日誌記錄：不要在負載較重的系統上發出**logging console debugging**命令。可以發出**logging buffered debugging**命令。然後發出**show logging**命令。日誌記錄還可以傳送

到系統消息日誌(syslog)伺服器並進行檢查。

3. 開啟TACACS+或RADIUS伺服器的調試。所有伺服器均具有此選項。

PIX上的Debug命令

- `debug crypto ipsec sa` — 此debug命令顯示IPsec事件。
- `debug crypto isakmp sa` — 此debug命令顯示有關Internet金鑰交換(IKE)事件的消息。
- `debug crypto isakmp engine` — 此debug命令顯示有關IKE事件的消息。

客戶端調試

啟用日誌檢視器以檢視Cisco Secure 1.1或VPN 3000 Client 2.5中的客戶端調試。

AAA伺服器設定檔

Cisco安全UNIX TACACS+

```
user = noacl{
password = clear "*****"
service=shell {
}
}
user = pixb{
  password = clear "*****"
  service=shell {
  set acl=115
  }
}
user = 3000full{
  password = clear "*****"
  service=shell {
  }
}
user = 3000partial{
  password = clear "*****"
  service=shell {
  }
}
```

適用於Windows TACACS+的Cisco安全ACS

Noacl、3000full和3000partial使用者在Cisco Secure ACS for Windows中只需要使用者名稱和密碼。pixb使用者需要使用者名稱、密碼、檢查的shell/exec組、檢查的ACL和框中的115。

Cisco安全UNIX RADIUS

```
user = noacl{
password = clear "*****"
}
user = pixb{
  password = clear "*****"
  radius=Cisco {
  reply_attributes= {
```

```
9,1="acl=115"  
}  
}  
}  
user = 3000full{  
  password = clear "*****"  
}  
user = 3000partial{  
  password = clear "*****"  
}
```

[適用於Windows RADIUS的Cisco安全ACS](#)

RADIUS/Cisco是裝置型別。Noacl、3000full和3000partial使用者在Cisco Secure ACS for Windows中只需要使用者名稱和密碼。pixb使用者需要在Cisco/RADIUS矩形框中的使用者名稱、密碼和檢查和acl=115，其中顯示009\001 AV配對（特定於供應商）。

注意：您需要該ACL的供應商屬性。屬性11(filter-id)無效。此問題已指派為Cisco錯誤ID [CSCdt50422](#)(僅限註冊客戶)。已在PIX軟體版本6.0.1中修復。

[Merit RADIUS \(支援Cisco AV對 \)](#)

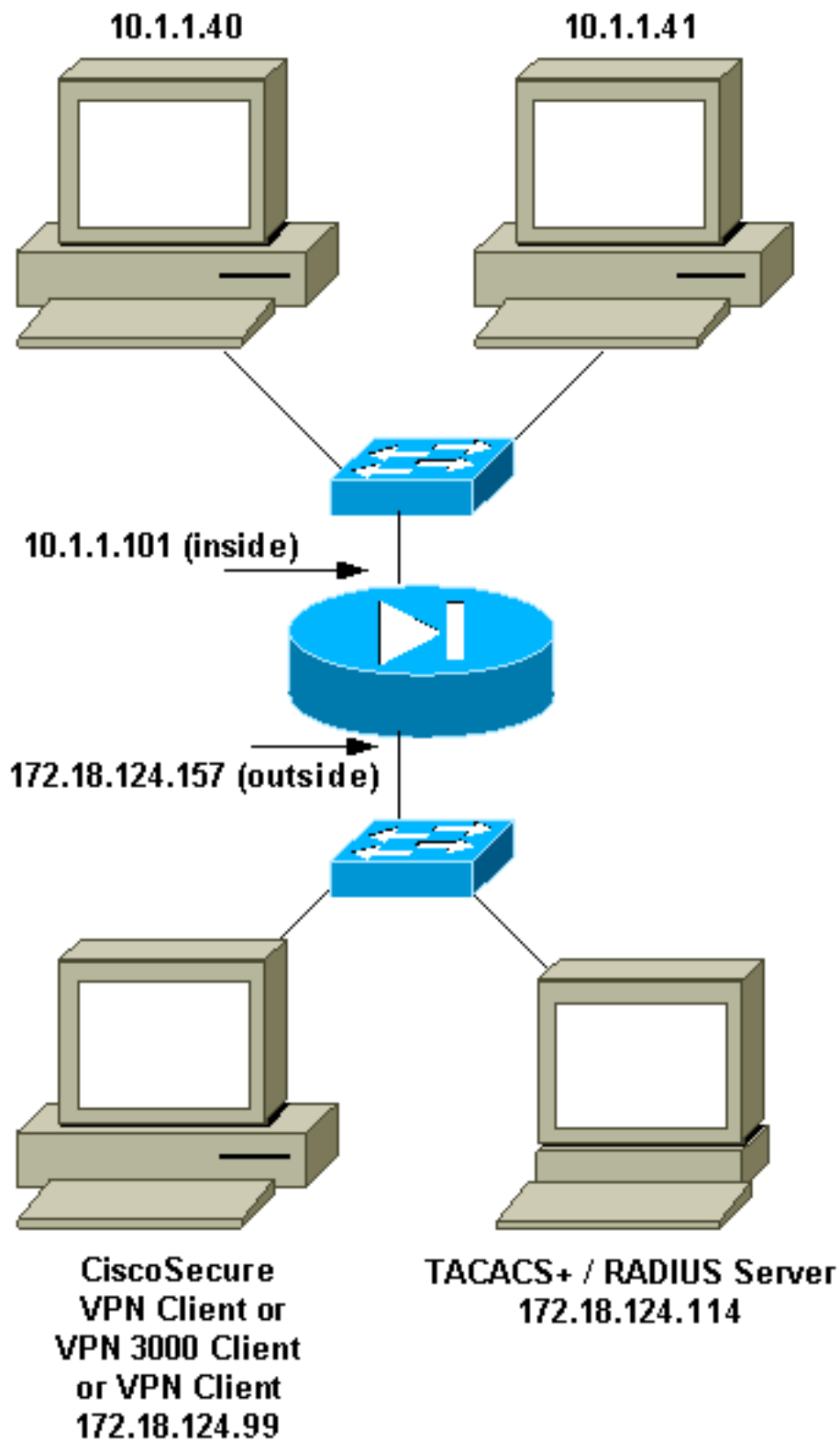
```
noacl Password= "noacl"
```

```
pixb Password= "pixb"  
cisco-avpair = "acl=115"
```

```
3000full Password= "3000full"
```

```
3000partial Password= "3000partial"
```

[網路圖表](#)



可配置的RADIUS埠 (5.3及更高版本)

某些RADIUS伺服器使用RADIUS連線埠而不是1645/1646 (通常為1812/1813)。在PIX 5.3及更高版本中，可以使用以下命令將RADIUS身份驗證和記帳埠更改為除預設1645/1646之外的埠：

- `aaa-server radius-authport #`
- `aaa-server radius-acctport #`

如何在不使用VPN組的情況下使用Xauth進行身份驗證

在本範例中，所有三個VPN使用者端都使用Xauth進行驗證。但是，VPN客戶端只能訪問PIX內部的網路，因為不使用拆分隧道。如需分割通道的詳細資訊，請參閱[如何使用VPN組驗證Xauth](#)。從AAA伺服器向下傳遞的ACL適用於任何VPN客戶端。在本示例中，目標是讓使用者noacl連線並訪問PIX中的所有資源。使用者pixb連線，但由於ACL 115在Xauth過程中從AAA伺服器向下傳遞，因此使用者只能訪問10.1.1.40。對10.1.1.41和內部所有其他IP地址的訪問被拒絕。

注意：VPN客戶端3.0支援需要PIX軟體6.0版。

[Cisco安全VPN客戶端1.1設定 — 不帶VPN組的Xauth](#)

```
Name of connection:
Remote party address = IP_Subnet = 10.1.1.0, Mask 255.255.255.0
Connect using Secure Gateway Tunnel to 172.18.124.157
My Identity:
Select certificate = None
ID_Type = ip address, pre-shared key and fill in key
('cisco1234') - matches that of pix in 'isakmp key' command
Security policy = defaults
Proposal 1 (Authen) = DES, MD5
Proposal 2 (Key Exchange) = DES, MD5, Tunnel
```

開啟拒絕服務(DoS)視窗，然後發出ping -t #.#.#.# 指令。出現Xauth視窗時，鍵入與AAA伺服器上的使用者名稱和密碼一致的使用者名稱和密碼。

[VPN 3000客戶端2.5或VPN客戶端3.x設定 — 不帶VPN組的Xauth](#)

請完成以下步驟：

1. 選擇Options > Properties > Authentication > Group Name。
2. 組名稱為no_care，密碼與isakmp key命令中PIX上的密碼一致。主機名為172.18.124.157。
3. 按一下「Connect」。
4. 出現Xauth視窗時，鍵入與AAA伺服器上的使用者名稱和密碼一致的使用者名稱和密碼。

[不帶VPN組的Xauth - PIX設定](#)

```
PIX Version 5.2(1)
nameif ethernet0 outside security0
nameif ethernet1 inside security100
enable password 8Ry2YjIyt7RRXU24 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
hostname goss-pixb
fixup protocol ftp 21
fixup protocol http 80
fixup protocol h323 1720
fixup protocol rsh 514
fixup protocol smtp 25
fixup protocol sqlnet 1521
fixup protocol sip 5060
names
access-list 108 permit ip 10.1.1.0 255.255.255.0
192.168.1.0 255.255.255.0
access-list 115 deny ip any host 10.1.1.41
access-list 115 permit ip any host 10.1.1.40
pager lines 24
logging on
```

```
no logging timestamp
no logging standby
logging console debugging
no logging monitor
no logging buffered
logging trap debugging
no logging history
logging facility 20
logging queue 512
interface ethernet0 auto
interface ethernet1 auto
mtu outside 1500
mtu inside 1500
ip address outside 172.18.124.157 255.255.255.0
ip address inside 10.1.1.101 255.255.255.0
ip audit info action alarm
ip audit attack action alarm
ip local pool test 192.168.1.1-192.168.1.5
no failover
failover timeout 0:00:00
failover poll 15
failover ip address outside 0.0.0.0
failover ip address inside 0.0.0.0
arp timeout 14400
global (outside) 1 172.18.124.154
nat (inside) 0 access-list 108
Nat (inside) 1 10.1.1.0 255.255.255.0 0 0
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00
rpc 0:10:00 h323 0:05:00
sip 0:30:00 sip_media 0:02:00
timeout uauth 0:05:00 absolute
AAA-server TACACS+ protocol tacacs+
AAA-server RADIUS protocol radius
AAA-server AuthInbound protocol tacacs+
AAA-server AuthInbound (outside) host 172.18.124.114 cisco timeout 5
no snmp-server location
no snmp-server contact
snmp-server community public
no snmp-server enable traps
floodguard enable
sysopt connection permit-ipsec
no sysopt route dnat
crypto ipsec transform-set myset esp-des esp-md5-hmac
crypto dynamic-map dynmap 10 set transform-set myset
crypto map mymap 10 ipsec-isakmp dynamic dynmap
crypto map mymap client configuration address initiate
crypto map mymap client configuration address respond
crypto map mymap client authentication AuthInbound
crypto map mymap interface outside
isakmp enable outside
isakmp key ***** address 0.0.0.0 netmask 0.0.0.0
isakmp identity address
isakmp client configuration address-pool local test outside
!--- Internet Security Association and Key Management Protocol (ISAKMP) !--- Policy for Cisco
VPN Client 2.5 or !--- Cisco Secure VPN Client 1.1. isakmp policy 10 authentication pre-share
isakmp policy 10 encryption des
isakmp policy 10 hash md5
!--- The 1.1 and 2.5 VPN Clients use Diffie-Hellman (D-H) !--- group 1 policy (PIX default).
isakmp policy 10 group 1
isakmp policy 10 lifetime 86400
!
!--- ISAKMP Policy for VPN Client 3.0 isakmp policy 20 authentication pre-share
isakmp policy 20 encryption des
```

```
isakmp policy 20 hash md5
!--- The VPN 3.0 Clients use D-H group 2 policy !--- and PIX 6.0 code. isakmp policy 20 group 2
isakmp policy 20 lifetime 86400
telnet timeout 5
ssh timeout 5
terminal width 80
Cryptochecksum:05c6a2f3a7d187162c4408503b55affa
: end
[OK]
```

如何使用VPN組的Xauth進行驗證

在本範例中，VPN 3000使用者端2.5或VPN使用者端3.0可以使用Xauth進行驗證，且分割通道生效。由於VPN組成員身份，ACL從PIX傳遞到VPN 3000客戶端。它指定只有PIX內的網路具有加密隧道。其他流量（可能通向Internet）不會加密。

在本示例中，使用者名稱為3000full（在AAA伺服器上）的vpn客戶端在組vpn3000-all（在PIX上）同時訪問PIX內的整個10.1.1.X網路。VPN客戶端接收wins-server、dns-server和域名資訊。使用者名稱為3000partial（在AAA伺服器上）的另一個VPN客戶端在組vpn3000-41（在PIX上）僅通過組配置檔案訪問網路內部的一個IP地址(10.1.1.40)。此VPN客戶端不接收wins和dns伺服器資訊，但仍然執行拆分隧道。

注意：VPN客戶端3.0支援需要PIX軟體6.0版。

VPN客戶端2.5或3.0設定 — 帶VPN組的Xauth

請完成以下步驟：

注意：VPN 2.5或3.0客戶端設定取決於涉及的使用者。

1. 選擇**Options > Properties > Authentication**。
2. 組名稱和組密碼與PIX上的組名稱匹配，如下所示：vpngroup vpn3000-all password *****或vpngroup vpn3000-41 password *****。主機名為172.18.124.157。
3. 按一下「**Connect**」。
4. 出現Xauth視窗時，輸入與AAA伺服器上的使用者名稱和密碼。

在本示例中，使用者3000full通過身份驗證後，它將從vpn3000-all組提取資訊。使用者3000部分從vpn3000-41組獲取資訊。該視窗顯示**協商安全配置檔案**，您的連結現在已安全。

使用者3000full使用組vpn3000-all的密碼。出於分割隧道目的，訪問清單108與該組相關聯。形成通向10.1.1.x網路的隧道。流量未加密流向不在存取清單108中的裝置（例如網際網路）。這是分割通道。

這是使用者3000full的「VPN客戶端連線狀態」視窗的輸出：

	Network	Mask
key	10.1.1.0	255.255.255.0
key	172.18.124.157	255.255.255.255

使用者3000partial使用組vpn3000-41的密碼。出於分割隧道目的，訪問清單125與該組關聯。隧道形成到10.1.1.41裝置。未加密的流量流向不在存取清單125中的裝置（例如網際網路）。但是，流量不會流向10.1.1.40裝置，因為此流量不可路由。未在加密隧道清單中指定它。

這是使用者3000partial的VPN客戶端連線狀態視窗輸出：

	Network	Mask
key	10.1.1.41	255.255.255.255
key	172.18.124.157	255.255.255.255

帶VPN組的Xauth - PIX設定

注意： Cisco Secure VPN Client 1.1無法使用此功能，因為沒有Internet安全關聯和金鑰管理協定 (ISAKMP)金鑰。新增**isakmp key ***** address 0.0.0.0 netmask 0.0.0.0** 命令使所有VPN客戶端都正常工作。

```
PIX Version 5.2(1)
nameif ethernet0 outside security0
nameif ethernet1 inside security100
enable password 8Ry2YjIyt7RRXU24 encrypted
passwd OnTrBUG1Tp0edmkr encrypted
hostname goss-pixb
fixup protocol ftp 21
fixup protocol http 80
fixup protocol h323 1720
fixup protocol rsh 514
fixup protocol smtp 25
fixup protocol sqlnet 1521
fixup protocol sip 5060
names
access-list 108 permit ip 10.1.1.0 255.255.255.0
192.168.1.0 255.255.255.0
access-list 125 permit ip host 10.1.1.41 any
pager lines 24
logging on
no logging timestamp
no logging standby
logging console debugging
no logging monitor
no logging buffered
logging trap debugging
no logging history
logging facility 20
logging queue 512
interface ethernet0 auto
interface ethernet1 auto
mtu outside 1500
mtu inside 1500
ip address outside 172.18.124.157 255.255.255.0
ip address inside 10.1.1.1 255.255.255.0
ip audit info action alarm
ip audit attack action alarm
ip local pool test 192.168.1.1-192.168.1.5
no failover
failover timeout 0:00:00
failover poll 15
failover ip address outside 0.0.0.0
failover ip address inside 0.0.0.0
arp timeout 14400
global (outside) 1 172.18.124.154
Nat (inside) 0 access-list 108
Nat (inside) 1 10.1.1.0 255.255.255.0 0 0
route outside 0.0.0.0 0.0.0.0 172.18.124.1 1
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00
rpc 0:10:00 h323 0:05:00
```

```

sip 0:30:00 sip_media 0:02:00
timeout uauth 0:05:00 absolute
AAA-server TACACS+ protocol tacacs+
AAA-server RADIUS protocol radius
AAA-server AuthInbound protocol tacacs+
AAA-server AuthInbound (outside) host 172.18.124.111
cisco timeout 5
no snmp-server location
no snmp-server contact
snmp-server community public
no snmp-server enable traps
floodguard enable
sysopt connection permit-ipsec
no sysopt route dnat
crypto ipsec transform-set myset ESP-Des esp-md5-hmac
crypto dynamic-map dynmap 10 set transform-set myset
crypto map mymap 10 ipsec-isakmp dynamic dynmap
crypto map mymap client configuration address initiate
crypto map mymap client configuration address respond
crypto map mymap client authentication AuthInbound
crypto map mymap interface outside
isakmp enable outside
isakmp identity address
isakmp client configuration address-pool local test outside
!--- ISAKMP Policy for Cisco VPN Client 2.5 or !--- Cisco Secure VPN Client 1.1. isakmp policy
10 authentication pre-share
isakmp policy 10 encryption des
isakmp policy 10 hash md5
!--- The 1.1 and 2.5 VPN Clients use Diffie-Hellman (D-H) !--- group 1 policy (PIX default).
isakmp policy 10 group 1
isakmp policy 10 lifetime 86400
!
!--- ISAKMP Policy for VPN Client 3.0 isakmp policy 20 authentication pre-share
isakmp policy 20 encryption des
isakmp policy 20 hash md5
!--- The VPN 3.0 Clients use D-H group 2 policy !--- and PIX 6.0 code. isakmp policy 20 group 2
isakmp policy 20 lifetime 86400
vpngroup vpn3000-all address-pool test
vpngroup vpn3000-all dns-server 10.1.1.40
vpngroup vpn3000-all wins-server 10.1.1.40
vpngroup vpn3000-all default-domain rtp.cisco.com
vpngroup vpn3000-all split-tunnel 108
vpngroup vpn3000-all idle-time 1800
vpngroup vpn3000-all password *****
vpngroup vpn3000-41 address-pool test
vpngroup vpn3000-41 split-tunnel 125
vpngroup vpn3000-41 idle-time 1800
vpngroup vpn3000-41 password *****
telnet timeout 5
ssh timeout 5
terminal width 80
Cryptochecksum:429db0e7d20451fc28074f4d6f990d25
: end

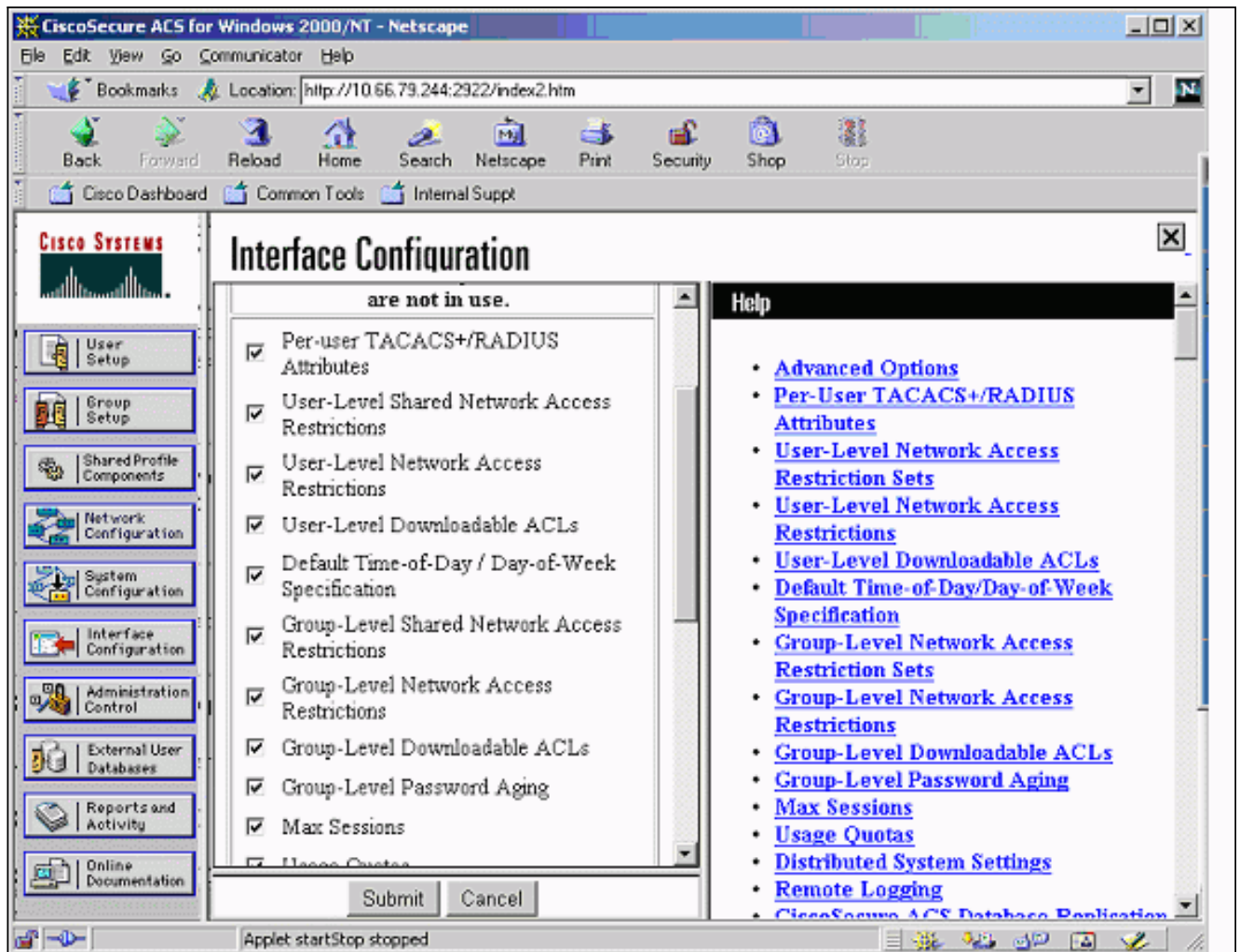
```

[含VPN群組和每個使用者可下載ACL的Xauth - ACS設定](#)

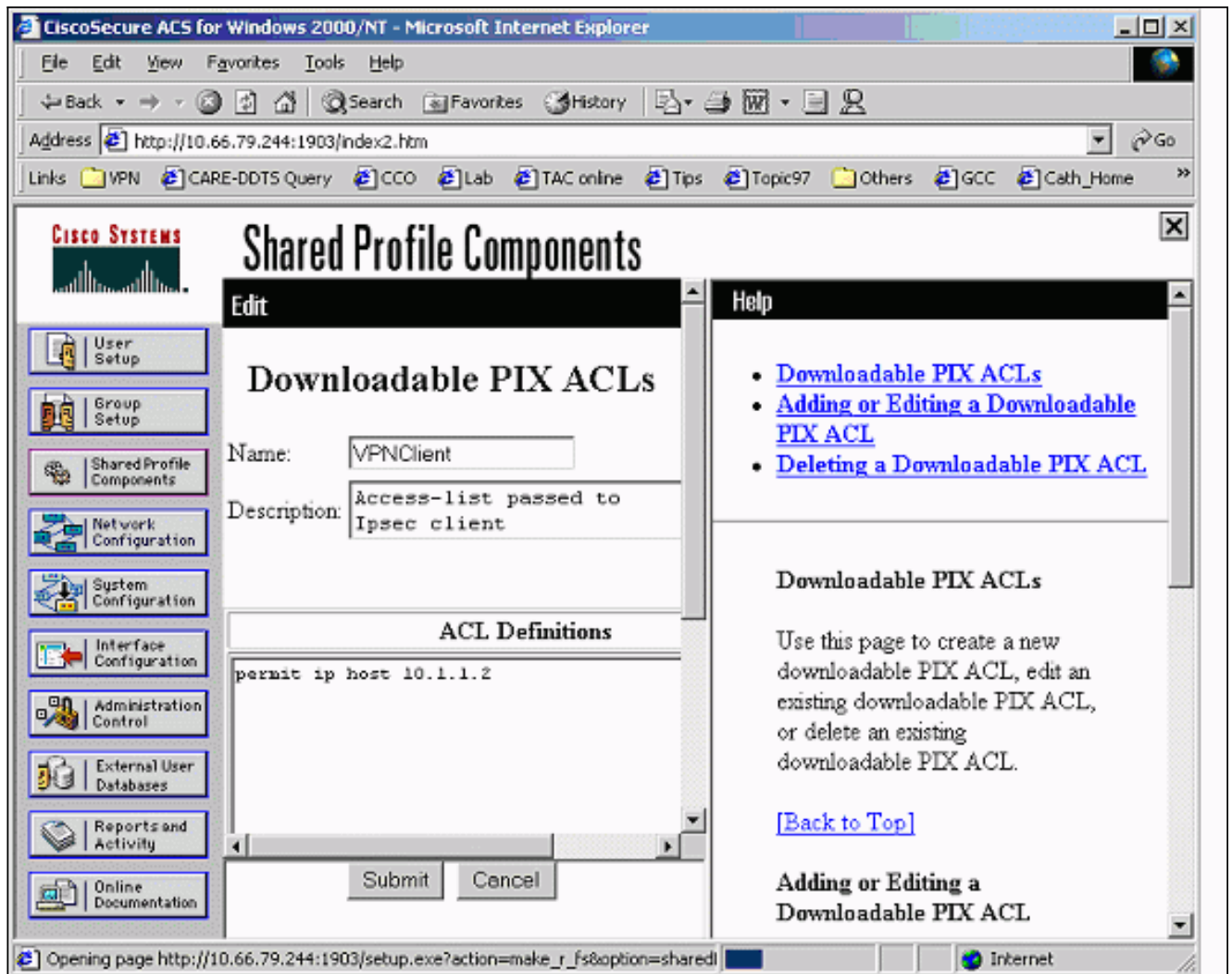
[設定Cisco Secure ACS](#)

請完成以下步驟：

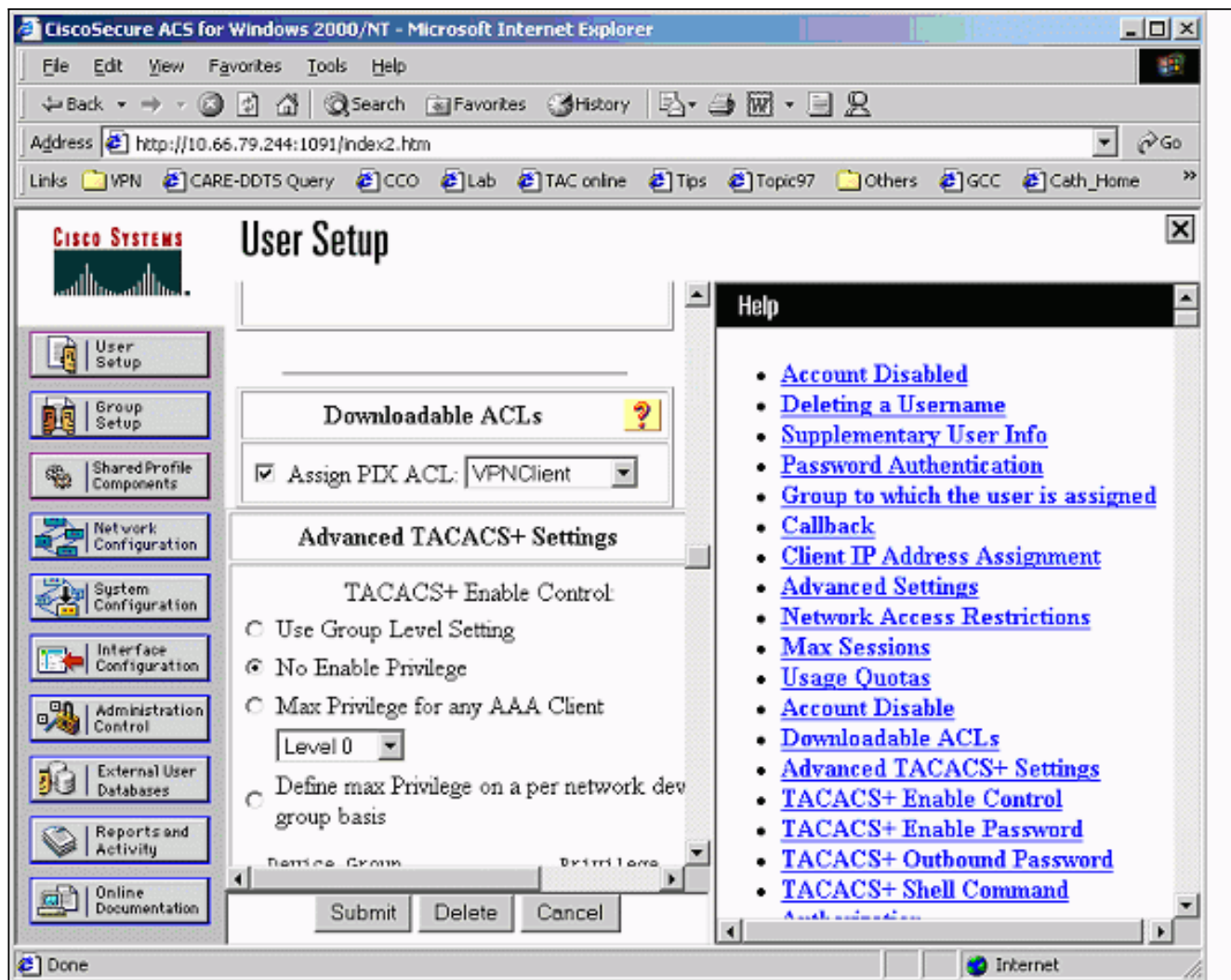
1. 按一下「Interface Configuration」，然後選擇User-Level Downloadable ACLs選項。



2. 按一下**Shared Profile Components**並定義可下載的ACL。



3. 按一下**User Setup**。選擇用於分配**PIX ACL**的選項。從下拉選單中選擇正確的ACL。



帶VPN組和每個使用者可下載ACL的Xauth - PIX 6.x設定

如果要對授權執行使用者每使用者可下載ACL，請使用PIX防火牆軟體版本6.2(2)。請參閱Cisco錯誤ID [CSCdx47975](#)(僅限註冊客戶)。

```

PIX Version 6.2(2)
nameif ethernet0 outside security0
nameif ethernet1 inside security100
enable password 8Ry2YjIyt7RRXU24 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
hostname sv2-4
fixup protocol ftp 21
fixup protocol http 80
fixup protocol h323 h225 1720
fixup protocol h323 ras 1718-1719
fixup protocol ils 389
fixup protocol rsh 514
fixup protocol rtsp 554
fixup protocol smtp 25
fixup protocol sqlnet 1521
fixup protocol sip 5060
fixup protocol skinny 2000
names
access-list 108 permit ip 10.1.1.0 255.255.255.0
192.168.1.0 255.255.255.0
pager lines 24
logging buffered debugging

```

```

interface ethernet0 auto
interface ethernet1 auto
mtu outside 1500
mtu inside 1500
ip address outside 10.66.79.69 255.255.255.224
ip address inside 10.1.1.1 255.255.255.0
ip audit info action alarm
ip audit attack action alarm
ip local pool test 192.168.1.1-192.168.1.5
pdm history enable
arp timeout 14400
nat (inside) 0 access-list 108
conduit permit icmp any any
route outside 0.0.0.0 0.0.0.0 10.66.79.65 1
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00
rpc 0:10:00 h323 0:05:00 sip
0:30:00 sip_media 0:02:00
timeout uauth 0:05:00 absolute
aaa-server TACACS+ protocol tacacs+
aaa-server RADIUS protocol radius
aaa-server LOCAL protocol local
aaa-server AuthInbound protocol radius
aaa-server AuthInbound (outside) host 10.66.79.244 cisco123 timeout 10
no snmp-server location
no snmp-server contact
snmp-server community public
no snmp-server enable traps
floodguard enable
sysopt connection permit-ipsec
no sysopt route dnat
crypto ipsec transform-set myset esp-des esp-md5-hmac
crypto dynamic-map dynmap 10 set transform-set myset
crypto map mymap 10 ipsec-isakmp dynamic dynmap
!--- This commands the router to respond to the VPN 3.x Client. crypto map mymap client
configuration address respond
!--- This tells the router to expect Xauth for the VPN 3.x Client. crypto map mymap client
authentication AuthInbound
crypto map mymap interface outside
isakmp enable outside
isakmp policy 20 authentication pre-share
isakmp policy 20 encryption des
isakmp policy 20 hash md5
isakmp policy 20 group 2
isakmp policy 20 lifetime 86400
!
!--- This is the VPN group configuration. vpngroup vpn3000-all address-pool test
vpngroup vpn3000-all default-domain apt.cisco.com
!--- The split-tunnel mode-config is not used, !--- which enforces authorization on a per-user
basis. vpngroup vpn3000-all idle-time 1800
vpngroup vpn3000-all password *****
!
telnet timeout 5
ssh timeout 5
terminal width 80
Cryptochecksum:7c3d067232f427e7522f4a679e963c58
end:

```

[帶VPN組和可按使用者下載的ACL的Xauth - ASA/PIX 7.x設定](#)

PIX Version 7.1(1)

!

```
hostname PIX
domain-name cisco.com
enable password 9jNfZuG3TC5tCVH0 encrypted
names
!
interface Ethernet0
 nameif outside
 security-level 0
 ip address 10.66.79.69 255.255.255.224
!
interface Ethernet1
 nameif inside
 security-level 100
 ip address 10.1.1.1 255.255.255.0
!
passwd 2KFQnbNIdI.2KYOU encrypted
ftp mode passive
dns domain-lookup inside
dns server-group DefaultDNS
 timeout 30

access-list 108 permit ip 10.1.1.0 255.255.255.0 192.168.1.0 255.255.255.0
pager lines 24
logging buffer-size 500000
logging console debugging
logging monitor errors
mtu outside 1500
mtu inside 1500
ip local pool test 192.168.1.1-192.168.1.5
no failover
icmp permit any outside
icmp permit any inside
no asdm history enable
arp timeout 14400

nat (inside) 0 access-list 108
route outside 0.0.0.0 0.0.0.0 10.66.79.65 1
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
timeout mgcp-pat 0:05:00 sip 0:30:00 sip_media 0:02:00
timeout uauth 0:05:00 absolute

aaa-server AuthInbound protocol radius
aaa-server AuthInbound host 10.66.79.244 key cisco123

group-policy vpn3000 internal
group-policy vpn3000 attributes
 dns-server value 172.16.1.1
 default-domain value cisco.com

username vpn3000 password nPtKy7KDCerzhKeX encrypted
no snmp-server location
no snmp-server contact
snmp-server enable traps snmp authentication linkup linkdown coldstart

crypto ipsec transform-set my-set esp-des esp-md5-hmac

crypto dynamic-map dynmap 10 set transform-set my-set

crypto dynamic-map dynmap 10 set reverse-route

crypto map mymap 10 ipsec-isakmp dynamic dynmap
```



```

crypto map mymap interface outside

isakmp enable outside
isakmp policy 10 authentication pre-share
isakmp policy 10 encryption des
isakmp policy 10 hash md5
isakmp policy 10 group 2
isakmp policy 10 lifetime 1000

isakmp policy 65535 authentication pre-share
isakmp policy 65535 encryption 3des
isakmp policy 65535 hash sha
isakmp policy 65535 group 2
isakmp policy 65535 lifetime 86400

tunnel-group DefaultRAGroup general-attributes
 authentication-server-group (outside) vpn

tunnel-group vpn3000 type ipsec-ra

tunnel-group vpn3000 general-attributes
 address-pool test
 authentication-server-group vpn

tunnel-group vpn3000 ipsec-attributes
 pre-shared-key *

telnet timeout 5
ssh timeout 5
console timeout 0
!
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
!
service-policy global_policy global
Cryptochecksum:ecb58c5d8ce805b3610b198c73a3d0cf
: end

```

[如何為VPN客戶端連線配置本地Xauth](#)

為VPN客戶端連線配置本地Xauth需要以下命令：

- `aaa-server server-tag protocol local`
- `crypto map map-name client authentication aaa-server-name`

發出username命令在PIX上定義本地使用者。

要使用本地PIX防火牆使用者身份驗證資料庫，請為aaa-server命令的server-tag引數輸入LOCAL。使用crypto map命令發出aaa-server命令以建立身份驗證關聯，以便VPN客戶端在訪問PIX防火牆時進行身份驗證。

如何新增記帳

以下是新增記帳的命令的語法：

- `aaa accounting acctg_service [except inbound | outbound | if_name local_ip local_mask foreign_ip foreign_mask tacacs+ | radius;`

或 (5.2中的新功能)：

- `aaa accounting include acctg_service inbound | outbound match server_tag`

在PIX配置中，新增了以下命令：

- `aaa accounting` 包括任何入站 0.0.0.0 0.0.0 0.0.0 0.0.0.0.0 AuthInbound；

或 (5.2中的新功能)：

- `access-list 150 permit ip any any aaa accounting match 150 outside AuthInbound`

注意：xauth記帳需要使用sysopt connection permit-ipsec命令，而不是sysopt ipsec pl-compatible命令。Xauth記帳不只與sysopt ipsec pl-compatible命令一起使用。Xauth記帳對TCP連線有效。它對於網際網路控制訊息通訊協定(ICMP)或使用者資料包通訊協定(UDP)無效。

TACACS+計費範例

```
Fri Sep 8 03:48:40 2000 172.18.124.157
pixc PIX 192.168.1.1 start task_id=0x17 foreign_ip=192.168.1.1
  local_ip=10.1.1.40 cmd=telnet
Fri Sep 8 03:48:44 2000 172.18.124.157 pixc PIX 192.168.1.1
  stop task_id=0x17 foreign_ip=192.168.1.1 local_ip=10.1.1.40
  cmd=telnet elapsed_time=4 bytes_in=42 bytes_out=103
Fri Sep 8 03:49:31 2000 172.18.124.157 pixc PIX 192.168.1.1
  start task_id=0x18
foreign_ip=192.168.1.1 local_ip=10.1.1.40 cmd=http
Fri Sep 8 03:49:35 2000 172.18.124.157 pixc PIX 192.168.1.1
  stop task_id=0x18 foreign_ip=192.168.1.1 local_ip=10.1.1.40
  cmd=http elapsed_time=4 bytes_in=242 bytes_out=338
```

RADIUS計費範例

```
Acct-Status-Type = Start
NAS-IP-Address = 172.18.124.157
Login-IP-Host = 10.1.1.40
Login-TCP-Port = 23
Acct-Session-Id = 0x00000003
User-Name = noacl
Vendor-Specific = Source-IP=192.168.1.1
Vendor-Specific = Source-Port=1141
```

```
Vendor-Specific = Destination-IP=10.1.1.40
Vendor-Specific = Destination-Port=23

Acct-Status-Type = Start
NAS-IP-Address = 172.18.124.157
Login-IP-Host = 10.1.1.40
Login-TCP-Port = 80
Acct-Session-Id = 0x00000004
User-Name = noacl
Vendor-Specific = Source-IP=192.168.1.1
Vendor-Specific = Source-Port=1168
Vendor-Specific = Destination-IP=10.1.1.40
Vendor-Specific = Destination-Port=80
```

```
Acct-Status-Type = Stop
NAS-IP-Address = 172.18.124.157
Login-IP-Host = 10.1.1.41
Login-TCP-Port = 80
Acct-Session-Id = 0x00000008
User-Name = noacl
Acct-Session-Time = 4
Acct-Input-Octets = 242
Acct-Output-Octets = 338
Vendor-Specific = Source-IP=192.168.1.1
Vendor-Specific = Source-Port=1182
Vendor-Specific = Destination-IP=10.1.1.41
Vendor-Specific = Destination-Port=80
```

```
Acct-Status-Type = Stop
NAS-IP-Address = 172.18.124.157
Login-IP-Host = 10.1.1.40
Login-TCP-Port = 23
Acct-Session-Id = 0x00000015
User-Name = noacl
Acct-Session-Time = 33
Acct-Input-Octets = 43
Acct-Output-Octets = 103
Vendor-Specific = Source-IP=192.168.1.1
Vendor-Specific = Source-Port=1257
Vendor-Specific = Destination-IP=10.1.1.40
Vendor-Specific = Destination-Port=23
```

[Debug and Show — 不帶VPN組的Xauth](#)

```
goss-pixb#show debug
debug crypto ipsec 1
debug crypto isakmp 1
debug crypto engine
debug fover status
tx Off
rx Off
open Off
cable Off
txdmp Off
rxdmp Off
ifc Off
rxip Off
txip Off
get Off
put Off
verify Off
switch Off
```

```
fail Off
fmsg Off
goss-pixb#terminal monitor
goss-pixb#

crypto_isakmp_process_block: src 172.18.124.99, dest 172.18.124.157
OAK_MM exchange
ISAKMP (0): processing SA payload. message ID = 0

ISAKMP (0): Checking ISAKMP transform 1 against priority 10 policy
ISAKMP: encryption DES-CBC
ISAKMP: hash MD5
ISAKMP: default group 1
ISAKMP: auth pre-share
ISAKMP (0): atts are acceptable. Next payload is 0
ISAKMP (0): SA is doing pre-shared key authentication
using id type ID_IPV4_ADDR
return status is IKMP_NO_ERROR
crypto_isakmp_process_block: src 172.18.124.99, dest 172.18.124.157
OAK_MM exchange
ISAKMP (0): processing KE payload. Message ID = 0

ISAKMP (0): processing NONCE payload. Message ID = 0

ISAKMP (0): processing vendor id payload

ISAKMP (0): processing vendor id payload

return status is IKMP_NO_ERROR
crypto_isakmp_process_block: src 172.18.124.99, dest 172.18.124.157
OAK_MM exchange
ISAKMP (0): processing ID payload. Message ID = 0
ISAKMP (0): processing HASH payload. Message ID = 0
ISAKMP (0): processing NOTIFY payload 24578 protocol 1
spi 0, message ID = 0
ISAKMP (0): processing notify INITIAL_CONTACTIPSEC(key_engine):
got a queue event...
IPSEC(key_engine_delete_sas): rec'd delete notify from ISAKMP
IPSEC(key_engine_delete_sas): delete all SAs shared with 172.18.124.99

ISAKMP (0): SA has been authenticated

ISAKMP (0): ID payload
next-payload : 8
type : 1
protocol : 17
port : 500
length : 8
ISAKMP (0): Total payload length: 12
return status is IKMP_NO_ERROR
crypto_isakmp_process_block: src 172.18.124.99, dest 172.18.124.157
OAK_QM exchange
ISAKMP (0:0): Need XAUTH
ISAKMP/xauth: request attribute XAUTH_TYPE
ISAKMP/xauth: request attribute XAUTH_USER_NAME
ISAKMP/xauth: request attribute XAUTH_USER_PASSWORD
ISAKMP (0:0): initiating peer config to 172.18.124.99.
ID = 2218162690 (0x84367a02)
return status is IKMP_NO_ERROR
crypto_isakmp_process_block: src 172.18.124.99, dest 172.18.124.157
ISAKMP_TRANSACTION exchange
ISAKMP (0:0): processing transaction payload from 172.18.124.99.
Message ID = 2156074032
ISAKMP: Config payload CFG_REPLY
```

```
return status is IKMP_ERR_NO_RETRANS109005: Authentication succeeded
for user 'pixb' from 172.18.124.99/0 to 0.0.0.0/0 on
interface IKE-XAUTH
ISAKMP (0:0): initiating peer config to 172.18.124.99.
ID = 2218162690 (0x84367a02)
109005: Authentication succeeded for user 'pixb' from 172.18.124.157
crypto_isakmp_process_block: src 172.18.124.99, dest 172.18.124.157
ISAKMP_TRANSACTION exchange
ISAKMP (0:0): processing transaction payload from 172.18.124.99.
Message ID = 2156497080
ISAKMP: Config payload CFG_ACK
ISAKMP (0:0): initiating peer config to 172.18.124.99.
ID = 393799466 (0x1778e72a)
return status is IKMP_NO_ERROR
crypto_isakmp_process_block: src 172.18.124.99, dest 172.18.124.157
ISAKMP_TRANSACTION exchange
ISAKMP (0:0): processing transaction payload from 172.18.124.99.
Message ID = 2156156112
ISAKMP: Config payload CFG_ACK
ISAKMP (0:0): peer accepted the address!
return status is IKMP_NO_ERROR.99/0 to 0.0.0.0/0 on
interface IKE-XAUTH

crypto_isakmp_process_block: src 172.18.124.99, dest 172.18.124.157
OAK_QM exchange
oakley_process_quick_mode:
OAK_QM_IDLE
ISAKMP (0): processing SA payload. Message ID = 2323118710

ISAKMP : Checking IPsec proposal 1

ISAKMP: transform 1, ESP_DES
ISAKMP: attributes in transform:
ISAKMP: authenticator is HMAC-MD5
ISAKMP: encaps is 1
ISAKMP (0): atts are acceptable.IPSEC(validate_proposal_request):
proposal part #1,
(key eng. msg.) dest= 172.18.124.157, src= 172.18.124.99,
dest_proxy= 10.1.1.0/255.255.255.0/0/0 (type=4),
src_proxy= 192.168.1.1/255.255.255.255/0/0 (type=1),
protocol= ESP, transform= ESP-Des esp-md5-hmac ,
lifedur= 0s and 0kb,
spi= 0x0(0), conn_id= 0, keysize= 0, flags= 0x4

ISAKMP (0): processing NONCE payload. Message ID = 2323118710

ISAKMP (0): processing ID payload. Message ID = 2323118710
ISAKMP (0): ID_IPV4_ADDR src 192.168.1.1 prot 0 port 0
ISAKMP (0): processing ID payload. Message ID = 2323118710
ISAKMP (0): ID_IPV4_ADDR_SUBNET dst 10.1.1.0/255.255.255.0
prot 0 port 0
IPSEC(key_engine): got a queue event...
IPSEC(spi_response): getting spi 0xeeae8930(4004415792) for SA
from 172.18.124.99 to 172.18.124.157 for prot 3

return status is IKMP_NO_ERROR4
crypto_isakmp_process_block: src 172.18.124.99, dest 172.18.124.157
OAK_QM exchange
oakley_process_quick_mode:
OAK_QM_AUTH_AWAITmap_alloc_entry: allocating entry 1
map_alloc_entry: allocating entry 2

ISAKMP (0): Creating IPsec SAs
inbound SA from 172.18.124.99 to 172.18.124.157
```

```
(proxy 192.168.1.1 to 10.1.1.0)
has spi 4004415792 and conn_id 1 and flags 4
outbound SA from 172.18.124.157 to 172.18.124.99
(proxy 10.1.1.0 to 192.168.1.1)
has spi 1281287211 and conn_id 2 and flags 4
IPSEC(key_engine): got a queue event...
IPSEC(initialize_sas): ,
(key eng. msg.) dest= 172.18.124.157, src= 172.18.124.99,
dest_proxy= 10.1.1.0/255.255.255.0/0/0 (type=4),
src_proxy= 192.168.1.1/0.0.0.0/0/0 (type=1),
protocol= ESP, transform= esp-des esp-md5-hmac ,
lifedur= 0s and 0kb,
spi= 0xeeae8930(4004415792), conn_id= 1, keysize= 0, flags= 0x4
IPSEC(initialize_sas): ,
(key eng. msg.) src= 172.18.124.157, dest= 172.18.124.99,
src_proxy= 10.1.1.0/255.255.255.0/0/0 (type=4),
dest_proxy= 192.168.1.1/0.0.0.0/0/0 (type=1),
protocol= ESP, transform= esp-des esp-md5-hmac ,
lifedur= 0s and 0kb,
spi= 0x4c5ee42b(1281287211), conn_id= 2, keysize= 0, flags= 0x4

return status is IKMP_NO_ERROR02101: decaps: rec'd
IPSEC packet has invalid spi for destaddr=172.18.124.157,
prot=esp, spi=0xeeae8930(0)
602301: sa created, (sa) sa_dest= 172.18.124.157, sa_prot= 50,
sa_spi= 0xeeae8930(4004415792), sa_trans= esp-des esp-md5-hmac,
sa_conn_id= 1

602301: sa created, (sa) sa_dest= 172.18.124.99, sa_prot= 50,
sa_spi= 0x4c5ee42b(1281287211), sa_trans= esp-des esp-md5-hmac,
sa_conn_id= 2

109011: Authen Session Start: user 'pixb', sid 5
109015: Authorization denied (acl=115) for user 'pixb' from
192.168.1.1/0 to 10.1.1.40/8 on interface outside
109015: Authorization denied (acl=115) for user 'pixb' from
192.168.1.1/0 to 10.1.1.40/8 on interface outside
109015: Authorization denied (acl=115) for user 'pixb' from
192.168.1.1/0 to 10.1.1.40/8 on interface outside
109015: Authorization denied (acl=115) for user 'pixb' from
192.168.1.1/0 to 10.1.1.40/8 on interface outside
```

```
goss-pixb#
goss-pixb#show uauth
Current Most Seen
Authenticated Users 1 1
Authen In Progress 0 1
ipsec user 'pixb' at 192.168.1.1, authenticated
access-list 115
goss-pixb#show access-list
access-list 108 permit ip 10.1.1.0 255.255.255.0 192.168.1.0
255.255.255.0 (hitcnt=18)
access-list 125 permit ip host 10.1.1.41 any (hitcnt=0)
access-list dynacl4 permit ip 10.1.1.0 255.255.255.0 host
192.168.1.1 (hitcnt=0)
access-list 115 permit ip any host 10.1.1.41 (hitcnt=0)
access-list 115 deny ip any host 10.1.1.42 (hitcnt=0)
```

調試和顯示 — 使用VPN組的Xauth

```
crypto_isakmp_process_block: src 172.18.124.96,
dest 172.18.124.157
```

```
goss-pixb#show debug
debug crypto ipsec 1
debug crypto isakmp 1
debug crypto engine
debug fover status
tx Off
rx Off
open Off
cable Off
txdmp Off
rxdmp Off
ifc Off
rxip Off
txip Off
get Off
put Off
verify Off
switch Off
fail Off
fmsg Off
goss-pixb#
crypto_isakmp_process_block: src 172.18.124.99, dest 172.18.124.157
OAK_AG exchange
ISAKMP (0): processing SA payload. message ID = 0

ISAKMP (0): Checking ISAKMP transform 1 against priority 10 policy
ISAKMP: encryption DES-CBC
ISAKMP: hash MD5
ISAKMP: default group 1
ISAKMP: auth pre-share
ISAKMP (0): atts are acceptable. Next payload is 3
ISAKMP (0): processing KE payload. message ID = 0

ISAKMP (0): processing NONCE payload. message ID = 0

ISAKMP (0): processing ID payload. message ID = 0
ISAKMP (0): processing vendor id payload

ISAKMP (0): speaking to a VPN3000 client

ISAKMP (0): ID payload
next-payload : 10
type : 1
protocol : 17
port : 500
length : 8
ISAKMP (0): Total payload length: 12
return status is IKMP_NO_ERROR
crypto_isakmp_process_block: src 172.18.124.99, dest 172.18.124.157
OAK_AG exchange
ISAKMP (0): processing HASH payload. message ID = 0
ISAKMP (0): SA has been authenticated
return status is IKMP_NO_ERROR
crypto_isakmp_process_block: src 172.18.124.99, dest 172.18.124.157
OAK_QM exchange
ISAKMP (0:0): Need XAUTH
ISAKMP/xauth: request attribute XAUTH_TYPE
ISAKMP/xauth: request attribute XAUTH_USER_NAME
ISAKMP/xauth: request attribute XAUTH_USER_PASSWORD
ISAKMP (0:0): initiating peer config to 172.18.124.99.
ID = 1396280702 (0x53398d7e)
return status is IKMP_NO_ERROR
crypto_isakmp_process_block: src 172.18.124.99, dest 172.18.124.157
ISAKMP_TRANSACTION exchange
```

```
ISAKMP (0:0): processing transaction payload from 172.18.124.99.
message ID = 2156608344
ISAKMP: Config payload CFG_REPLY
return status is IKMP_ERR_NO_RETRANS10
ISAKMP (0:0): initiating peer config to 172.18.124.99.
ID = 1396280702 (0x53398d7e)9
crypto_isakmp_process_block: src 172.18.124.99, dest 172.18.124.157
ISAKMP_TRANSACTION exchange
ISAKMP (0:0): processing transaction payload from 172.18.124.99.
message ID = 2156115984
ISAKMP: Config payload CFG_ACK
ISAKMP (0:0): peer accepted the address!
ISAKMP (0:0): processing saved QM.
oakley_process_quick_mode:
OAK_QM_IDLE
ISAKMP (0): processing SA payload. message ID = 1697984837

ISAKMP : Checking IPsec proposal 1

ISAKMP: transform 1, ESP_DES
ISAKMP: attributes in transform:
ISAKMP: authenticator is HMAC-MD5
ISAKMP: encaps is 1
ISAKMP (0): atts are acceptable.
IPSEC(validate_proposal_request): proposal part #1,
(key eng. msg.) dest= 172.18.124.157, src= 172.18.124.99,
dest_proxy= 172.18.124.157/255.255.255.255/0/0 (type=1),
src_proxy= 192.168.1.1/255.255.255.255/0/0 (type=1),
protocol= ESP, transform= esp-des esp-md5-hmac ,
lifedur= 0s and 0kb,
spi= 0x0(0), conn_id= 0, keysize= 0, flags= 0x4

ISAKMP (0): processing NONCE payload. message ID = 1697984837

ISAKMP (0): processing ID payload. message ID = 1697984837
ISAKMP (0): ID_IPV4_ADDR src 192.168.1.1 prot 0 port 0
ISAKMP (0): processing ID payload. message ID = 1697984837
ISAKMP (0): ID_IPV4_ADDR dst 172.18.124.157 prot 0 port 0
ISAKMP (0): processing NOTIFY payload 24578 protocol 1
spi 0, message ID = 1697984837
ISAKMP (0): processing notify INITIAL_CONTACTIPSEC(key_engine):
got a queue event...
IPSEC(key_engine_delete_sas): rec'd delete notify from ISAKMP
IPSEC(key_engine_delete_sas): delete all SAs shared with 172.18.124.99
IPSEC(key_engine): got a queue event...
IPSEC(spi_response): getting spi 0x6a9d3f79(1788690297) for SA
from 172.18.124.99 to 172.18.124.157 for prot 3

return status is IKMP_NO_ERROR0
crypto_isakmp_process_block: src 172.18.124.99, dest 172.18.124.157
OAK_QM exchange
oakley_process_quick_mode:
OAK_QM_AUTH_AWAITmap_alloc_entry: allocating entry 1
map_alloc_entry: allocating entry 2

ISAKMP (0): Creating IPsec SAs
inbound SA from 172.18.124.99 to 172.18.124.157
(proxy 192.168.1.1 to 172.18.124.157)
has spi 1788690297 and conn_id 1 and flags 4
outbound SA from 172.18.124.157 to 172.18.124.99
(proxy 172.18.124.157 to 192.168.1.1)
has spi 2854452814 and conn_id 2 and flags 4
IPSEC(key_engine): got a queue event...
IPSEC(initialize_sas): ,
```

```
(key eng. msg.) dest= 172.18.124.157, src= 172.18.124.99,
dest_proxy= 172.18.124.157/0.0.0.0/0/0 (type=1),
src_proxy= 192.168.1.1/0.0.0.0/0/0 (type=1),
protocol= ESP, transform= esp-des esp-md5-hmac ,
lifedur= 0s and 0kb,
spi= 0x6a9d3f79(1788690297), conn_id= 1, keysize= 0, flags= 0x4
IPSEC(initialize_sas): ,
(key eng. msg.) src= 172.18.124.157, dest= 172.18.124.99,
src_proxy= 172.18.124.157/0.0.0.0/0/0 (type=1),
dest_proxy= 192.168.1.1/0.0.0.0/0/0 (type=1),
protocol= ESP, transform= esp-des esp-md5-hmac ,
lifedur= 0s and 0kb,
spi= 0xaa237e4e(2854452814), conn_id= 2, keysize= 0, flags= 0x4

return status is IKMP_NO_ERROR05: Authentication succeeded
for user 'pixc' from 172.18.124.99/0 to 0.0.0.0/0 on interface IKE-XAUTH
602301: sa created, (sa) sa_dest= 172.18.124.157, sa_prot= 50,
sa_spi= 0x6a9d3f79(1788690297), sa_trans= esp-des esp-md5-hmac ,
sa_conn_id= 1

602301: sa created, (sa) sa_dest= 172.18.124.99, sa_prot= 50,
sa_spi= 0xaa237e4e(2854452814), sa_trans= esp-des esp-md5-hmac ,
sa_conn_id= 2

109011: Authen Session Start: user 'pixc', sid 19

crypto_isakmp_process_block: src 172.18.124.99, dest 172.18.124.157
OAK_QM exchange
oakley_process_quick_mode:
OAK_QM_IDLE
ISAKMP (0): processing SA payload. message ID = 3361949217

ISAKMP : Checking IPsec proposal 1

ISAKMP: transform 1, ESP_DES
ISAKMP: attributes in transform:
ISAKMP: authenticator is HMAC-MD5
ISAKMP: encaps is 1
ISAKMP (0): atts are acceptable.
IPSEC(validate_proposal_request): proposal part #1,
(key eng. msg.) dest= 172.18.124.157, src= 172.18.124.99,
dest_proxy= 10.1.1.0/255.255.255.0/0/0 (type=4),
src_proxy= 192.168.1.1/255.255.255.255/0/0 (type=1),
protocol= ESP, transform= esp-des esp-md5-hmac ,
lifedur= 0s and 0kb,
spi= 0x0(0), conn_id= 0, keysize= 0, flags= 0x4

ISAKMP (0): processing NONCE payload. message ID = 3361949217

ISAKMP (0): processing ID payload. message ID = 3361949217
ISAKMP (0): ID_IPV4_ADDR src 192.168.1.1 prot 0 port 0
ISAKMP (0): processing ID payload. message ID = 3361949217
ISAKMP (0): ID_IPV4_ADDR_SUBNET dst 10.1.1.0/255.255.255.0 prot 0 port 0
IPSEC(key_engine): got a queue event...
IPSEC(spi_response): getting spi 0xfec4c3aa(4274308010) for SA
from 172.18.124.99 to 172.18.124.157 for prot 3

return status is IKMP_NO_ERROR4
crypto_isakmp_process_block: src 172.18.124.99, dest 172.18.124.157
OAK_QM exchange
oakley_process_quick_mode:
OAK_QM_AUTH_AWAITmap_alloc_entry: allocating entry 4
map_alloc_entry: allocating entry 3
```



```
ISAKMP (0): Creating IPsec SAs
inbound SA from 172.18.124.99 to 172.18.124.157
(proxy 192.168.1.1 to 10.1.1.0)
has spi 4274308010 and conn_id 4 and flags 4
outbound SA from 172.18.124.157 to 172.18.124.99
(proxy 10.1.1.0 to 192.168.1.1)
has spi 798459812 and conn_id 3 and flags 4
IPSEC(key_engine): got a queue event...
IPSEC(initialize_sas): ,
(key eng. msg.) dest= 172.18.124.157, src= 172.18.124.99,
dest_proxy= 10.1.1.0/255.255.255.0/0/0 (type=4),
src_proxy= 192.168.1.1/0.0.0.0/0/0 (type=1),
protocol= ESP, transform= esp-des esp-md5-hmac ,
lifedur= 0s and 0kb,
spi= 0xfec4c3aa(4274308010), conn_id= 4, keysize= 0, flags= 0x4
IPSEC(initialize_sas): ,
(key eng. msg.) src= 172.18.124.157, dest= 172.18.124.99,
src_proxy= 10.1.1.0/255.255.255.0/0/0 (type=4),
dest_proxy= 192.168.1.1/0.0.0.0/0/0 (type=1),
protocol= ESP, transform= esp-des esp-md5-hmac ,
lifedur= 0s and 0kb,
spi= 0x2f9787a4(798459812), conn_id= 3, keysize= 0, flags= 0x4

return status is IKMP_NO_ERROR02101: decaps: rec'd IPSEC
packet has invalid spi for destaddr=172.18.124.157, prot=esp,
spi=0xfec4c3aa(0)
602301: sa created, (sa) sa_dest= 172.18.124.157, sa_prot= 50,
sa_spi= 0xfec4c3aa(4274308010), sa_trans= esp-des esp-md5-hmac ,
sa_conn_id= 4

602301: sa created, (sa) sa_dest= 172.18.124.99, sa_prot= 50,
sa_spi= 0x2f9787a4(798459812), sa_trans= esp-des esp-md5-hmac ,
sa_conn_id= 3
```

```
goss-pixb#show uauth
Current Most Seen
Authenticated Users 1 1
Authen In Progress 0 1
ipsec user 'pixc' at 192.168.1.1, authenticated
goss-pixb#show crypto ipsec sa
```

```
interface: outside
Crypto map tag: mymap, local addr. 172.18.124.157

local ident (addr/mask/prot/port): (172.18.124.157/255.255.255.255/0/0)
remote ident (addr/mask/prot/port): (192.168.1.1/255.255.255.255/0/0)
current_peer: 172.18.124.99
dynamic allocated peer ip: 192.168.1.1

PERMIT, flags={}
#pkts encaps: 0, #pkts encrypt: 0, #pkts digest 0
#pkts decaps: 0, #pkts decrypt: 0, #pkts verify 0
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 0, #pkts compr. failed: 0,
#pkts decompress failed: 0
#send errors 0, #recv errors 0

local crypto endpt.: 172.18.124.157, remote crypto endpt.: 172.18.124.99
path mtu 1500, ipsec overhead 56, media mtu 1500
current outbound spi: aa237e4e

inbound esp sas:
```

spi: 0x6a9d3f79(1788690297)
transform: esp-des esp-md5-hmac ,
<--- More ---> in use settings ={Tunnel, }
slot: 0, conn id: 1, crypto map: mymap
sa timing: remaining key lifetime (k/sec): (4608000/28519)
IV size: 8 bytes
replay detection support: Y

inbound ah sas:

inbound pcg sas:

outbound esp sas:
spi: 0xaa237e4e(2854452814)
transform: esp-des esp-md5-hmac ,
in use settings ={Tunnel, }
slot: 0, conn id: 2, crypto map: mymap
sa timing: remaining key lifetime (k/sec): (4608000/28510)
IV size: 8 bytes
replay detection support: Y

outbound ah sas:

<--- More --->

outbound pcg sas:

local ident (addr/mask/prot/port): (10.1.1.0/255.255.255.0/0/0)
remote ident (addr/mask/prot/port): (192.168.1.1/255.255.255.255/0/0)
current_peer: 172.18.124.99
dynamic allocated peer ip: 192.168.1.1

PERMIT, flags={}
#pkts encaps: 4, #pkts encrypt: 4, #pkts digest 4
#pkts decaps: 4, #pkts decrypt: 4, #pkts verify 4
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 0, #pkts compr. failed: 0,
#pkts decompress failed: 0
#send errors 0, #recv errors 0

local crypto endpt.: 172.18.124.157, remote crypto
endpt.:172.18.124.99
path mtu 1500, ipsec overhead 56, media mtu 1500
current outbound spi: 2f9787a4

inbound esp sas:
spi: 0xfec4c3aa(4274308010)
<--- More ---> transform: esp-des esp-md5-hmac ,
in use settings ={Tunnel, }
slot: 0, conn id: 4, crypto map: mymap
sa timing: remaining key lifetime (k/sec): (4607999/27820)
IV size: 8 bytes
replay detection support: Y

inbound ah sas:

inbound pcg sas:

```
outbound esp sas:
spi: 0x2f9787a4(798459812)
transform: esp-des esp-md5-hmac ,
in use settings ={Tunnel, }
slot: 0, conn id: 3, crypto map: mymap
sa timing: remaining key lifetime (k/sec): (4607999/27820)
IV size: 8 bytes
replay detection support: Y
```

<--- More ---> outbound ah sas:

```
outbound pcip sas:
```

[Debug and Show - Xauth \(具有按使用者下載的ACL \)](#)

```
crypto_isakmp_process_block: src 10.66.79.229,
dest 10.66.79.69
VPN Peer: ISAKMP: Added new peer: ip:10.66.79.229
Total VPN Peers:1
VPN Peer: ISAKMP: Peer ip:10.66.79.229 Ref cnt incremented to:1
Total VPN Peers:1
OAK_AG exchange
ISAKMP (0): processing SA payload. message ID = 0

ISAKMP (0): Checking ISAKMP transform 1 against priority 20 policy
ISAKMP: encryption 3DES-CBC
ISAKMP: hash SHA
ISAKMP: default group 2
ISAKMP: extended auth pre-share
ISAKMP: life type in seconds
ISAKMP: life duration (VPI) of 0x0 0x20 0xc4 0x9b
ISAKMP (0): atts are not acceptable. Next payload is 3
ISAKMP (0): Checking ISAKMP transform 2 against priority 20 policy
ISAKMP: encryption 3DES-CBC
ISAKMP: hash MD5
ISAKMP: default group 2
ISAKMP: extended auth pre-share
ISAKMP: life type in seconds
ISAKMP: life duration (VPI) of 0x0 0x20 0xc4 0x9b
ISAKMP (0): atts are not acceptable. Next payload is 3
ISAKMP (0): Checking ISAKMP transform 3 against priority 20 policy
ISAKMP: encryption 3DES-CBC
ISAKMP: hash SHA
ISAKMP: default group 2
ISAKMP: auth pre-share
ISAKMP: life type in seconds
ISAKMP: life duration (VPI) of 0x0 0x20 0xc4 0x9b
ISAKMP (0): atts are not acceptable. Next payload is 3
ISAKMP (0): Checking ISAKMP transform 4 against priority 20 policy
ISAKMP: encryption 3DES-CBC
ISAKMP: hash MD5
ISAKMP: default group 2
ISAKMP: auth pre-share
ISAKMP: life type in seconds
ISAKMP: life duration (VPI) of 0x0 0x20 0xc4 0x9b
ISAKMP (0): atts are not acceptable. Next payload is 3
ISAKMP (0): Checking ISAKMP transform 5 against priority 20 policy
ISAKMP: encryption DES-CBC
```

```
ISAKMP: hash SHA
ISAKMP: default group 2
ISAKMP: extended auth pre-share
ISAKMP: life type in seconds
ISAKMP: life duration (VPI) of 0x0 0x20 0xc4 0x9b
ISAKMP (0): atts are not acceptable. Next payload is 3
ISAKMP (0): Checking ISAKMP transform 6 against priority 20 policy
ISAKMP: encryption DES-CBC
ISAKMP: hash MD5
ISAKMP: default group 2
ISAKMP: extended auth pre-share
ISAKMP: life type in seconds
ISAKMP: life duration (VPI) of 0x0 0x20 0xc4 0x9b
ISAKMP (0): atts are acceptable. Next payload is 3
ISAKMP (0): processing KE payload. message ID = 0

ISAKMP (0): processing NONCE payload. message ID = 0

ISAKMP (0): processing ID payload. message ID = 0
ISAKMP (0): processing vendor id payload

ISAKMP (0): received xauth v6 vendor id

ISAKMP (0): processing vendor id payload

ISAKMP (0): remote peer supports dead peer detection

ISAKMP (0): processing vendor id payload

ISAKMP (0): speaking to a Unity client

ISAKMP (0): ID payload
next-payload : 10
type : 2
protocol : 17
port : 500
length : 10
ISAKMP (0): Total payload length: 14
return status is IKMP_NO_ERROR
crypto_isakmp_process_block: src 10.66.79.229, dest 10.66.79.69
OAK_AG exchange
ISAKMP (0): processing HASH payload. message ID = 0
ISAKMP (0): processing NOTIFY payload 24578 protocol 1
spi 0, message ID = 0RADIUS_GET_PASS
RADIUS_REQUEST
raidus.c: rad_mkpkt_authen
attribute:
type 1, length 10, content:
80917fb0: 74 65 73 74 75 73 65 72 | testuser
attribute:
type 4, length 6, content:
80917fb0: 0a 42 | .B
80917fc0: 4f 45 | OE
attribute:
type 5, length 6, content:
80917fd0: 00 00 00 01 | ....

ISAKMP (0): processing notify INITIAL_CONTACTrip 0x80791f00
: chall_state ''
: state 0x7
: timer 0x0
: info 0x5d5ba513
session_id 0x5d5ba513
request_id 0x2
```

```
user 'testuser'
app 0
reason 2
sip 10.66.79.244
type 1
rad_procpkt: ACCEPT
attribute:
type 8, length 6, content:
809186f0: ff ff | ..
80918700: ff ff | ..
RADIUS_RCVD
attribute:
type 26, length 67, content:
Vendor ID 0 0 0 9, type=1, len=61:
80918700: 41 43 53 3a 43 69 | ACS:Ci
80918710: 73 63 6f 53 65 63 75 72 65 2d 44 65 66 69 6e 65
| scoSecure-Define
80918720: 64 2d 41 43 4c 3d 23 41 43 53 41 43 4c 23 2d 50
| d-ACL=#ACSACL#-P
80918730: 49 58 2d 56 50 4e 43 6c 69 65 6e 74 2d 33 64 33
| IX-VPNClient-3d3
80918740: 32 37 38 31 35 | 27815
RADIUS_RCVD
RADIUS_REQUEST
radius.c: rad_mkpkt_authen
attribute:
type 1, length 33, content:
809186d0: 23 41 43 53 41 43 4c 23 2d 50 49 58 | #ACSACL#-PIX
809186e0: 2d 56 50 4e 43 6c 69 65 6e 74 2d 33 64 33 32 37
| -VPNClient-3d327
809186f0: 38 31 35 | 815
attribute:
type 4, length 6, content:
809186f0: 0a 42 4f 45 | .BOE
attribute:
type 5, length 6, content:
80918700: 00 00 00 | ...
80918710: 02 | .
IPSEC(key_engine): got a queue event...rip 0x80791f00
: chall_state ''
: state 0x7
: timer 0x0
: info 0x5d5ba513
session_id 0x5d5ba513
request_id 0x3
user '#ACSACL#-PIX-VPNClient-3d327815'
app 0
reason 2
sip 10.66.79.244
type 1
rad_procpkt: ACCEPT
attribute:
type 26, length 46, content:
Vendor ID 0 0 0 9, type=1, len=40:
80918e20: 69 70 3a 69 6e 61 63 6c 23 31 3d 70 | ip:inacl#1=p
80918e30: 65 72 6d 69 74 20 69 70 20 61 6e 79 20 68 6f 73
| ermit ip any hos
80918e40: 74 20 31 30 2e 31 2e 31 2e 32 | t 10.1.1.2
RADIUS_RCVD
RADIUS_RCVD
RADIUS_ACCESS_ACCEPT:normal termination
RADIUS_DELETE

IPSEC(key_engine_delete_sas): rec'd delete notify from ISAKMP
```

IPSEC(key_engine_delete_sas): delete all SAs shared with 10.66.79.229

ISAKMP (0): SA has been authenticated
return status is IKMP_NO_ERROR
ISAKMP (0): sending phase 1 RESPONDER_LIFETIME notify
ISAKMP (0): sending NOTIFY message 24576 protocol 1
ISAKMP/xauth: request attribute XAUTH_TYPE
ISAKMP/xauth: request attribute XAUTH_USER_NAME
ISAKMP/xauth: request attribute XAUTH_USER_PASSWORD
ISAKMP (0:0): initiating peer config to 10.66.79.229.
ID = 3250273953 (0xc1bb3eal)
crypto_isakmp_process_block: src 10.66.79.229, dest 10.66.79.69
ISAKMP_TRANSACTION exchange
ISAKMP (0:0): processing transaction payload from 10.66.79.229.
message ID = 2167001532
ISAKMP: Config payload CFG_REPLY
return status is IKMP_ERR_NO_RETRANS
ISAKMP (0:0): initiating peer config to 10.66.79.229.
ID = 1530000247 (0x5b31f377)
crypto_isakmp_process_block: src 10.66.79.229, dest 10.66.79.69
ISAKMP_TRANSACTION exchange
ISAKMP (0:0): processing transaction payload from 10.66.79.229.
message ID = 2167001532
ISAKMP: Config payload CFG_ACK
return status is IKMP_NO_ERROR
crypto_isakmp_process_block: src 10.66.79.229, dest 10.66.79.69
ISAKMP_TRANSACTION exchange
ISAKMP (0:0): processing transaction payload from 10.66.79.229.
message ID = 2167001532
ISAKMP: Config payload CFG_REQUEST
ISAKMP (0:0): checking request:
ISAKMP: attribute IP4_ADDRESS (1)
ISAKMP: attribute IP4_NETMASK (2)
ISAKMP: attribute IP4_DNS (3)
ISAKMP: attribute IP4_NBNS (4)
ISAKMP: attribute ADDRESS_EXPIRY (5)
Unsupported Attr: 5
ISAKMP: attribute APPLICATION_VERSION (7)
Unsupported Attr: 7
ISAKMP: attribute UNKNOWN (28672)
Unsupported Attr: 28672
ISAKMP: attribute UNKNOWN (28673)
Unsupported Attr: 28673
ISAKMP: attribute ALT_DEF_DOMAIN (28674)
ISAKMP: attribute ALT_SPLIT_INCLUDE (28676)
ISAKMP: attribute ALT_PFS (28679)
ISAKMP: attribute UNKNOWN (28680)
Unsupported Attr: 28680
ISAKMP: attribute UNKNOWN (28677)
Unsupported Attr: 28677
ISAKMP (0:0): responding to peer config from 10.66.79.229.
ID = 2397668523
return status is IKMP_NO_ERROR
crypto_isakmp_process_block: src 10.66.79.229, dest 10.66.79.69
OAK_QM exchange
oakley_process_quick_mode:
OAK_QM_IDLE
ISAKMP (0): processing SA payload. message ID = 2858414843

ISAKMP : Checking IPsec proposal 1

ISAKMP: transform 1, ESP_3DES
ISAKMP: attributes in transform:
ISAKMP: authenticator is HMAC-MD5

```
ISAKMP: encaps is 1
ISAKMP: SA life type in seconds
ISAKMP: SA life duration (VPI) of 0x0 0x20 0xc4 0x9b
IPSEC(validate_proposal): transform proposal
(prot 3, trans 3, hmac_alg 1) not supported

ISAKMP (0): atts not acceptable. Next payload is 0
ISAKMP (0): skipping next ANDED proposal (1)
ISAKMP : Checking IPsec proposal 2

ISAKMP: transform 1, ESP_3DES
ISAKMP: attributes in transform:
ISAKMP: authenticator is HMAC-SHA
ISAKMP: encaps is 1
ISAKMP: SA life type in seconds
ISAKMP: SA life duration (VPI) of 0x0 0x20 0xc4 0x9b
IPSEC(validate_proposal): transform proposal
(prot 3, trans 3, hmac_alg 2) not supported

ISAKMP (0): atts not acceptable. Next payload is 0
ISAKMP (0): skipping next ANDED proposal (2)
ISAKMP : Checking IPsec proposal 3

ISAKMP: transform 1, ESP_3DES
ISAKMP: attributes in transform:
ISAKMP: authenticator is HMAC-MD5
ISAKMP: encaps is 1
ISAKMP: SA life type in seconds
ISAKMP: SA life duration (VPI) of 0x0 0x20 0xc4 0x9b IPSEC
(validate_proposal): transform proposal (prot 3, trans 3, hmac_alg 1)
not supported

ISAKMP (0): atts not acceptable. Next payload is 0
ISAKMP : Checking IPsec proposal 4

ISAKMP: transform 1, ESP_3DES
ISAKMP: attributes in transform:
ISAKMP: authenticator is HMAC-SHA
ISAKMP: encaps is 1
ISAKMP: SA life type in seconds
ISAKMP: SA life duration (VPI) of 0x0 0x20 0xc4 0x9b IPSEC
(validate_proposal): transform proposal (prot 3, trans 3, hmac_alg 2)
not supported

ISAKMP (0): atts not acceptable. Next payload is 0
ISAKMP : Checking IPsec proposal 5

ISAKMP: transform 1, ESP_DES
ISAKMP: attributes in transform:
ISAKMP: authenticator is HMAC-MD5
ISAKMP: encaps is 1
ISAKMP: SA life type in seconds
ISAKMP: SA life duration (VPI) of 0x0 0x20 0xc4 0x9b
ISAKMP (0): atts are acceptable.
ISAKMP (0): bad SPI size of 2 octets!
ISAKMP : Checking IPsec proposal 6

ISAKMP: transform 1, ESP_DES
ISAKMP: attributes in transform:
crypto_isakmp_process_block: src 10.66.79.229, dest 10.66.79.69
OAK_QM exchange
crypto_isakmp_process_block: src 10.66.79.229, dest 10.66.79.69
OAK_QM exchange
oakley_process_quick_mode:
```

```
OAK_QM_AUTH_AWAIT
ISAKMP (0): Creating IPsec SAs
sv2-4(config)#
sv2-4(config)#
sv2-4(config)#
sv2-4(config)#
sv2-4(config)#show uauth
Current Most Seen
Authenticated Users 1 1
Authen In Progress 0 1
ipsec user 'testuser' at 192.168.1.1, authenticated
access-list #ACSACL#-PIX-VPNClient-3d327815
sv2-4(config)#show access-list
access-list 108; 1 elements
access-list 108 permit ip 10.1.1.0 255.255.255.0 192.168.1.0
255.255.255.0 (hitcnt=38)
access-list #ACSACL#-PIX-VPNClient-3d327815; 1 elements
access-list #ACSACL#-PIX-VPNClient-3d327815 permit ip any host
10.1.1.2 (hitcnt=15)
access-list dynacl4; 1 elements
access-list dynacl4 permit ip host 10.66.79.69
host 192.168.1.1 (hitcnt=0)
access-list dynacl5; 1 elements
access-list dynacl5 permit ip any host 192.168.1.1 (hitcnt=15)
sv2-4(config)#show access-list
access-list 108; 1 elements
access-list 108 permit ip 10.1.1.0 255.255.255.0
192.168.1.0 255.255.255.0 (hitcnt=42)
access-list #ACSACL#-PIX-VPNClient-3d327815; 1 elements
access-list #ACSACL#-PIX-VPNClient-3d327815 permit ip any
host 10.1.1.2 (hitcnt=17)
access-list dynacl4; 1 elements
access-list dynacl4 permit ip host 10.66.79.69 host
192.168.1.1 (hitcnt=0)
access-list dynacl5; 1 elements
access-list dynacl5 permit ip any host 192.168.1.1 (hitcnt=17)
```

```
sv2-4(config)#show crypto map
```

```
Crypto Map: "mymap" interfaces: { outside }
client configuration address respond
client authentication AuthInbound
```

```
Crypto Map "mymap" 10 ipsec-isakmp
Dynamic map template tag: dynmap
```

```
Crypto Map "mymap" 20 ipsec-isakmp
Peer = 10.66.79.229
access-list dynacl6; 1 elements
access-list dynacl6 permit ip host 10.66.79.69
host 192.168.1.1 (hitcnt=0)
dynamic (created from dynamic map dynmap/10)
Current peer: 10.66.79.229
Security association lifetime: 4608000 kilobytes/28800 seconds
PFS (Y/N): N
Transform sets={ myset, }
```

```
Crypto Map "mymap" 30 ipsec-isakmp
Peer = 10.66.79.229
access-list dynacl7; 1 elements
access-list dynacl7 permit ip any host 192.168.1.1 (hitcnt=0)
dynamic (created from dynamic map dynmap/10)
```


Current peer: 10.66.79.229
Security association lifetime: 4608000 kilobytes/28800 seconds
PFS (Y/N): N
Transform sets={ myset, }
sv2-4(config)

[相關資訊](#)

- [PIX支援頁](#)
- [PIX命令參考](#)
- [要求建議 \(RFC\)](#)
- [Cisco Secure ACS for UNIX支援頁](#)
- [Cisco Secure ACS for Windows支援頁](#)
- [TACACS/TACACS+ 支援頁面](#)
- [IOS 文件中的 TACACS+](#)
- [RADIUS 支援頁面](#)
- [技術支援與文件 - Cisco Systems](#)