如何向 PIX IPSec 5.2 及更高版本添加 AAA 认证 (Xauth)

目录

简介

RADIUS和TACACS+认证和核算，和在某种程度上，授权，为终止在PIX的思科安全VPN客户端1.1和Cisco VPN 3000 2.5硬件客户端隧道完成。在PIX 5.2上的变化在包括验证、授权和统计(AAA)访问列表支持控制的那的及以后扩展认证以前版本什么已认证的用户可以为Cisco VPN 3000客户端2.5 Xauth终端访问和支持。**vpn group split-tunneling命令**使VPN 3000客户端同时连接到网络在PIX以及其他网络里面(例如，互联网)。在PIX 5 3和以后，在以前的版本编码的AAA更改是RADIUS端口可配置。在PIX 6.0中， VPN client 3.x的支持被添加。这要求迪菲–赫尔曼组2。

先决条件

要求

本文档没有任何特定的要求。

使用的组件

本文档中的信息基于以下软件和硬件版本：

- PIX软件版本5.2.1
- Cisco 安全 VPN 客户端 1.1
- Cisco VPN 3000 2.5客户端或VPN client 3.x**注意：** Cisco VPN Client版本3.0.x不与PIX版本一起使用早于6.0。参考支持IPsec/PPTP/L2TP欲知更多信息的Cisco硬件和VPN客户端。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

规则

有关文档规则的详细信息，请参阅 Cisco 技术提示规则。

背景信息

PIX防火墙软件版本6.2可以从访问控制服务器 (ACS)将访问控制列表(ACL) 下载到PIX防火墙。这使每用户ACL的配置在AAA服务器的提供每用户ACL授权。它通过ACS是然后可下载的对PIX防火墙。此功能为仅RADIUS服务器支持。它不为TACACS+服务器支持。

调试步骤

完成这些调试步骤：

1. 在您添加AAA认证前，请确保PIX Xauth配置工作。如果无法通过流量，在您实现AAA前，您不能之后执行它。
2. 启用登陆PIX ：请勿发出**logging console debugging命令**在高负荷系统。**logging buffered debugging命令**可以发出。然后请发出**show logging命令**。记录日志可能也发送到系统信息日志(Syslog)服务器和被检查。
3. 启用调试在TACACS+或RADIUS服务器。所有服务器有此选项。

PIX 上的调试命令

- **debug crypto ipsec sa** —此debug命令显示IPSec事件。
- **debug crypto isakmp sa** —此关于Internet Key Exchange (IKE)事件的debug命令显示消息。
- **debug crypto isakmp engine** —此关于IKE事件的debug命令显示消息。

客户端一侧调试

使日志查看器发现在Cisco Secure 1.1或VPN 3000客户端2.5的客户端一侧调试。

AAA 服务器配置文件

Cisco Secure 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 {
  }
  }
```

Cisco Secure ACS for Windows TACACS+

noacl， 3000full和3000partial用户需要一用户名和仅一个密码在Cisco Secure ACS for Windows。pixb用户需要用户名，密码， shell/exec被检查的组， ACL检查和115在方框。

Cisco Secure 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 "********"
  }
```

Cisco Secure ACS for Windows RADIUS

RADIUS/Cisco是设备类型。noacl， 3000full和3000partial用户需要一用户名和仅一个密码在Cisco Secure ACS for Windows。pixb用户需要一用户名、一个密码和一检查和acl=115在说009\001 AV对的Cisco/RADIUS矩形框(根据厂商的)。

注意： 您需要ACL的供应商属性。属性11，过滤器ID，无效。此问题分配Cisco Bug ID CSCdt50422 (仅限注册用户)。它在PIX软件版本6.0.1修复。

MERIT RADIUS（支持 Cisco AV 对）

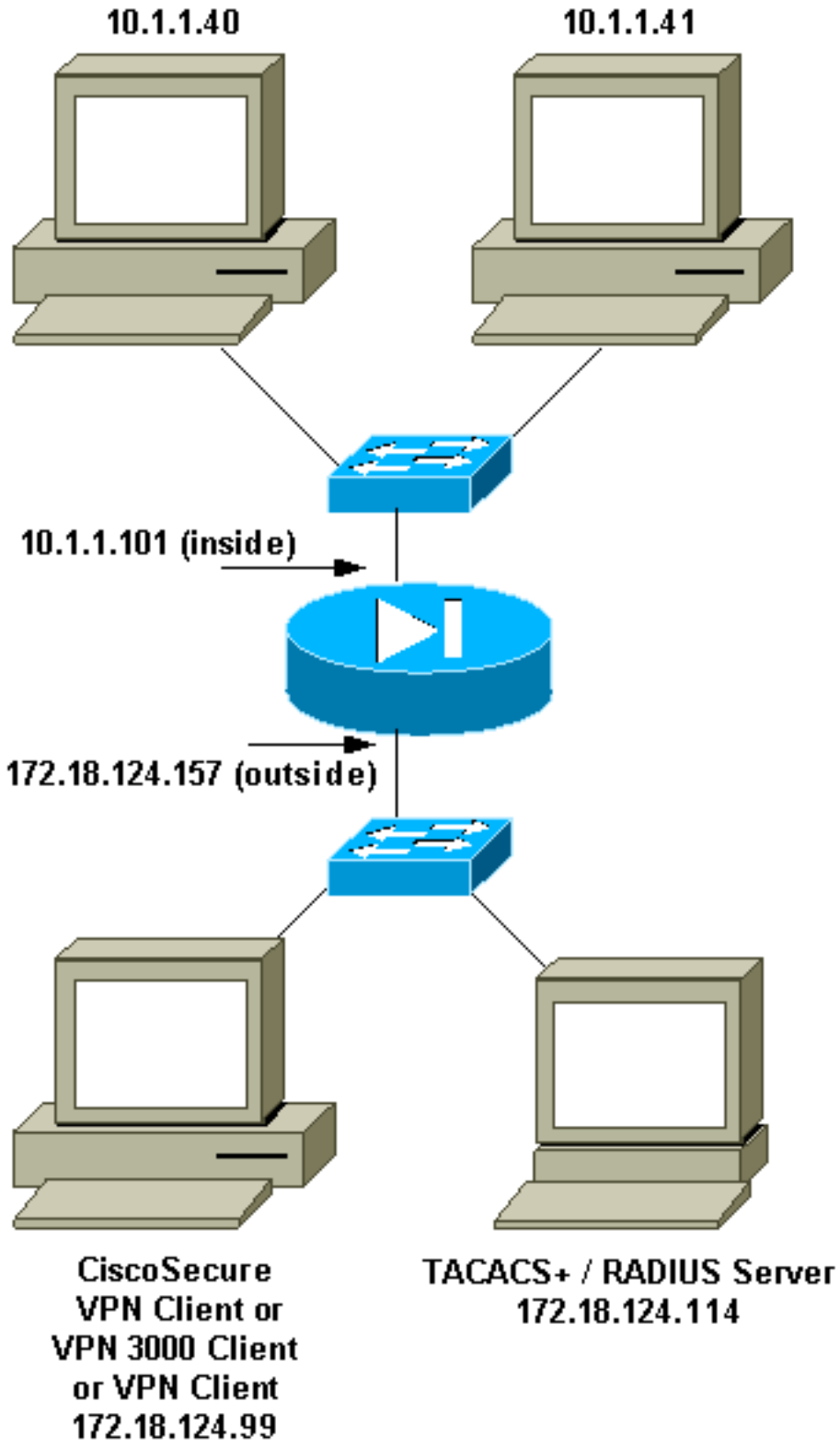
```
noacl Password= "noacl"

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

3000full Password= "3000full"

3000partial Password= "3000partial"
```

网络图



可配置 RADIUS 端口（5.3 和更高版本）

某些 RADIUS 服务器使用除 1645/1646 之外的 RADIUS 端口（通常为 1812/1813）。在PIX 5 3和以后， RADIUS验证和计费端口可以更改到端口除默认1645/1646之外用这些命令：

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

如何验证与Xauth没有VPN组

在本例中，所有三VPN客户端验证与Xauth。然而，因为分割隧道不是在使用中的， VPN客户端能访问仅网络在PIX里面。请参阅如何验证带VPN组的XAUTH关于分割隧道的更多信息。ACL从AAA服务器通过下来适用于所有VPN客户端。在本例中，目标是为了用户noacl能连接和达到所有资源在PIX里面。pixb联络的用户，但是，因为ACL 115从AAA服务器通过下来在Xauth进程中，用户能只达到10.1.1.40。对10.1.1.41和所有其他IP地址里面的访问拒绝。

注意： PIX软件版本6.0为VPN Client 3.0支持要求。

思科安全VPN客户端1.1设置-没有VPN组的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
```

打开拒绝服务窗口并且发出**ping - t -.-.-.-命令**。当Xauth窗口出现时，请键入同意那个关于AAA服务器的用户名和密码。

设置的VPN 3000客户端2.5或VPN client 3.x -没有VPN组的Xauth

完成这些步骤：

1. 选择**Options > Properties > Authentication > Group Name**。
2. 组名是不_care，并且密码同意那个关于在**isakmp key命令的**PIX。主机名是172.18.124.157。
3. 单击 **Connect**。
4. 当Xauth窗口出现时，键入与AAA服务器相同的用户名和密码。

没有VPN组的Xauth - PIX设定

```
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]
```

如何验证与带VPN组的XAUTH

在本例中， VPN 3000客户端2.5或VPN Client 3.0可以验证与Xauth，并且分割隧道有效。由于VPN组会员， ACL从PIX通过到VPN 3000客户端。它指定仅网络在PIX里面有一加密隧道。其他流量(或许到互联网)没有加密。

在本例中，一VPN客户端，有在组VPN3000所有的用户名的3000full (在AAA服务器)， (在PIX)访问整个10.1.1.X网络在PIX里面在互联网的同时。VPN客户端获得Windows Server， dns-server和域名信息。另一VPN客户端，有在组vpn3000-41的用户名的3000partial (在aaa-server)， (在PIX)由于组配置文件只访问一个IP地址在网络(10.1.1.40)里面。此VPN客户端不获得wins服务器和域名服务器信息，然而仍然执行分割隧道。

注意： PIX软件版本6.0为VPN Client 3.0支持要求。

设置的VPN Client 2.5或3.0 -带VPN组的XAUTH

完成这些步骤：

注意： VPN 2.5或3.0客户端设置依靠用户介入。

1. 选择 **Options > Properties > Authentication**。
2. 组名和组密码匹配在PIX的组名和在：vpngroup VPN3000所有密码********或vpngroup vpn3000-41密码********。主机名是172.18.124.157。
3. 单击 **Connect**。
4. 当Xauth窗口出现时，请输入与AAA服务器相同的用户名和密码。

在本例中，一旦用户3000full验证，它拾起从VPN3000所有组的信息。用户3000partial拾起从vpn3000-41组的信息。窗口表示**协商安全配置文件，并且您的链路当前安全**。

用户3000full使用密码组VPN3000所有。access-list 108关联与分割隧道目的该组。通道形成对10.1.1.x网络。流量以不加密的形式流向访问列表 108 之外的设备（例如 Internet）。这切分通道。

这是VPN客户端连接状态窗口的输出用户的3000full ：

```
        Network         Mask
key     10.1.1.0        255.255.255.0
key     172.18.124.157  255.255.255.255
```

用户3000partial使用密码组vpn3000-41。access-list 125关联与分割隧道目的该组。通道形成到10.1.1.41设备。通信流未加密对设备不在access-list 125 (例如，互联网)。然而，因为此流量不能路由的，流量不流到10.1.1.40设备。它在加密隧道列表没有指定。

这是VPN客户端连接状态窗口的输出用户的3000partial ：

```
        Network         Mask
key     10.1.1.41       255.255.255.255
key     172.18.124.157  255.255.255.255
```

带VPN组的XAUTH - PIX设定

注意： 因为没有互联网安全协会和密钥管理协议(ISAKMP)密钥，思科安全VPN客户端1.1不与此一起使用。添加**isakmp key ********地址0.0.0.0网络屏蔽0.0.0.0**命令使所有VPN客户端工作。

```
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-
```

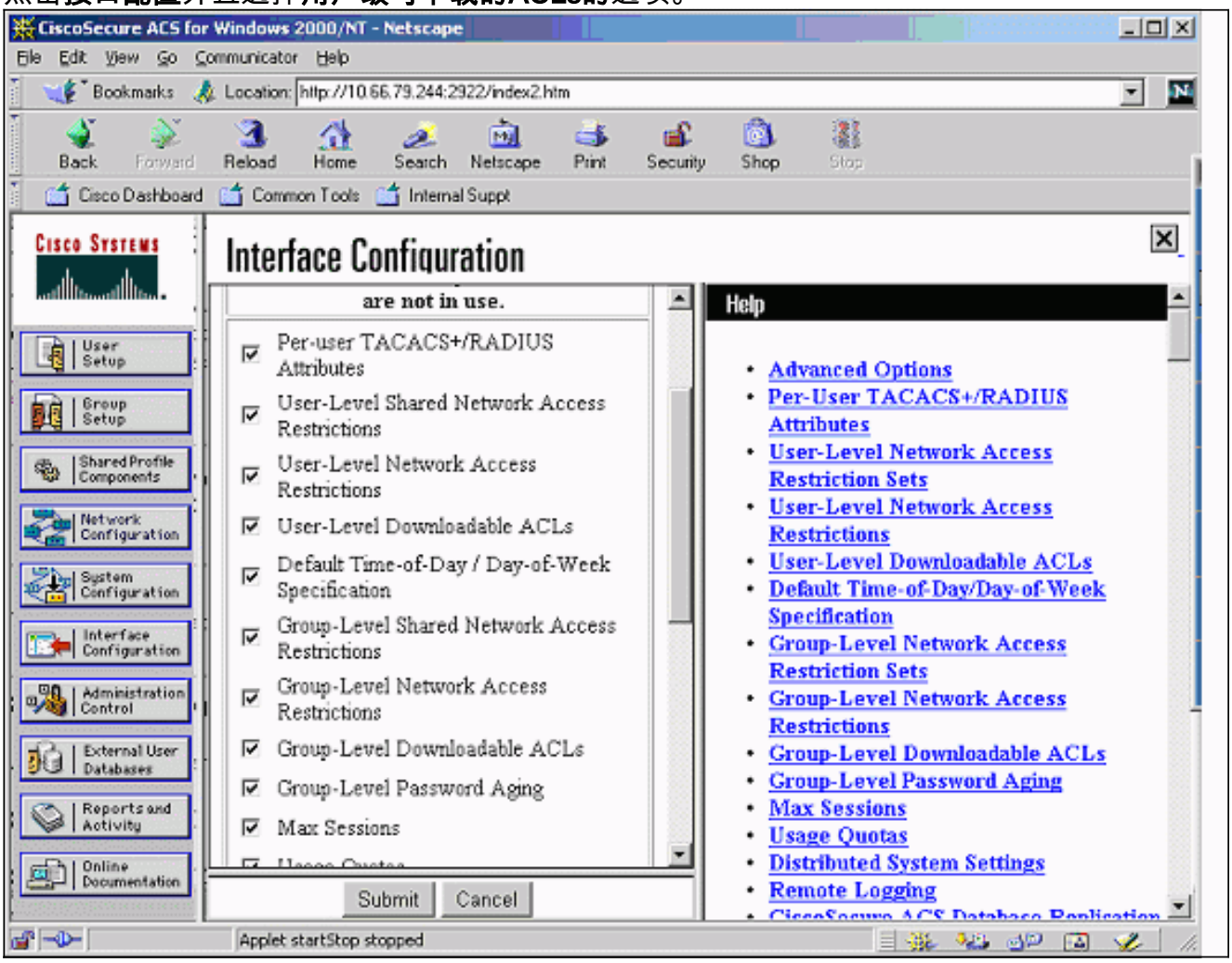
```
tunnel 125 vpngroup vpn3000-41 idle-time 1800 vpngroup vpn3000-41 password ******** telnet
timeout 5 ssh timeout 5 terminal width 80 Cryptochecksum:429db0e7d20451fc28074f4d6f990d25 : end
```

带VPN组的XAUTH和可下载的每用户ACL - ACS设置

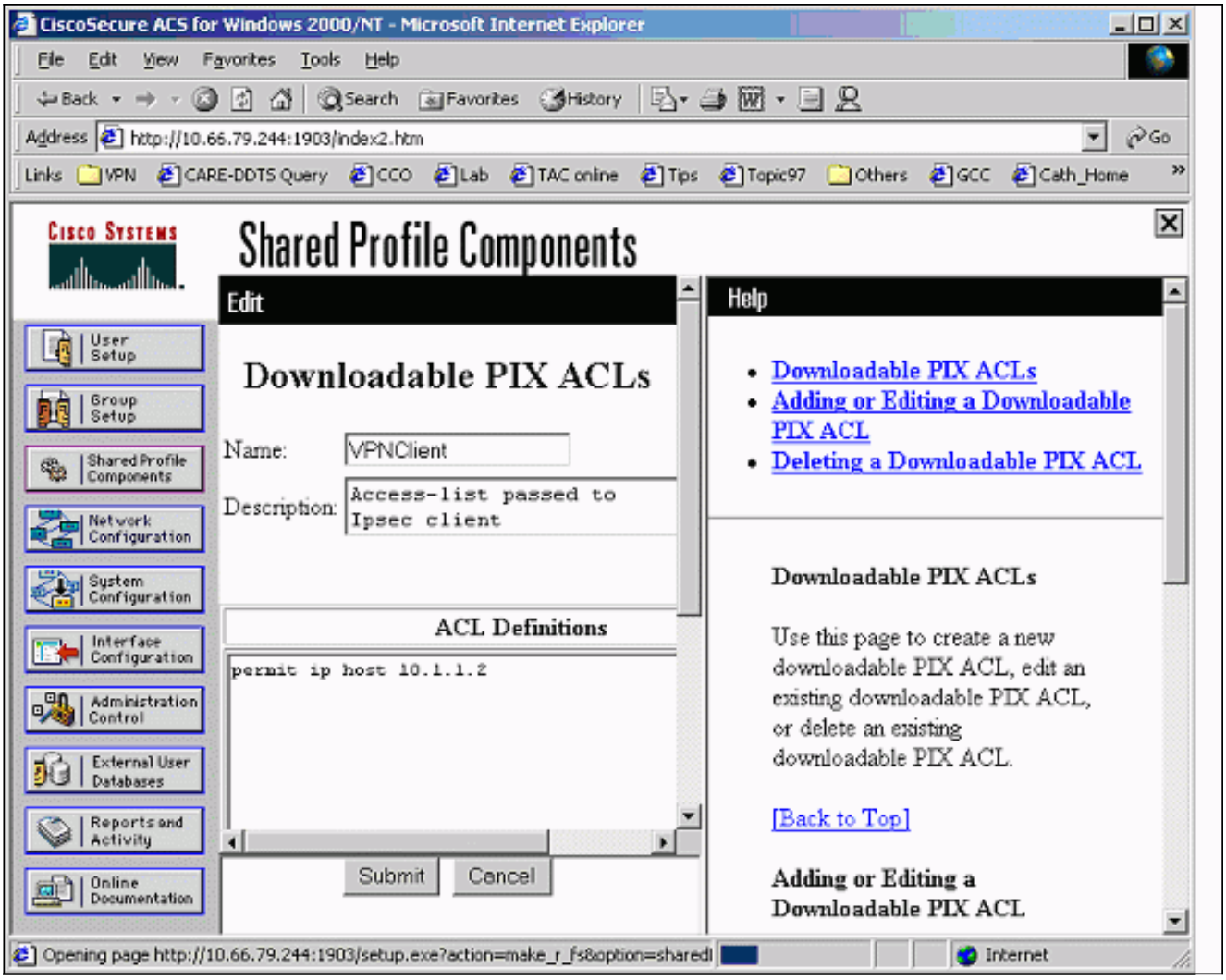
设置Cisco Secure ACS

完成这些步骤：

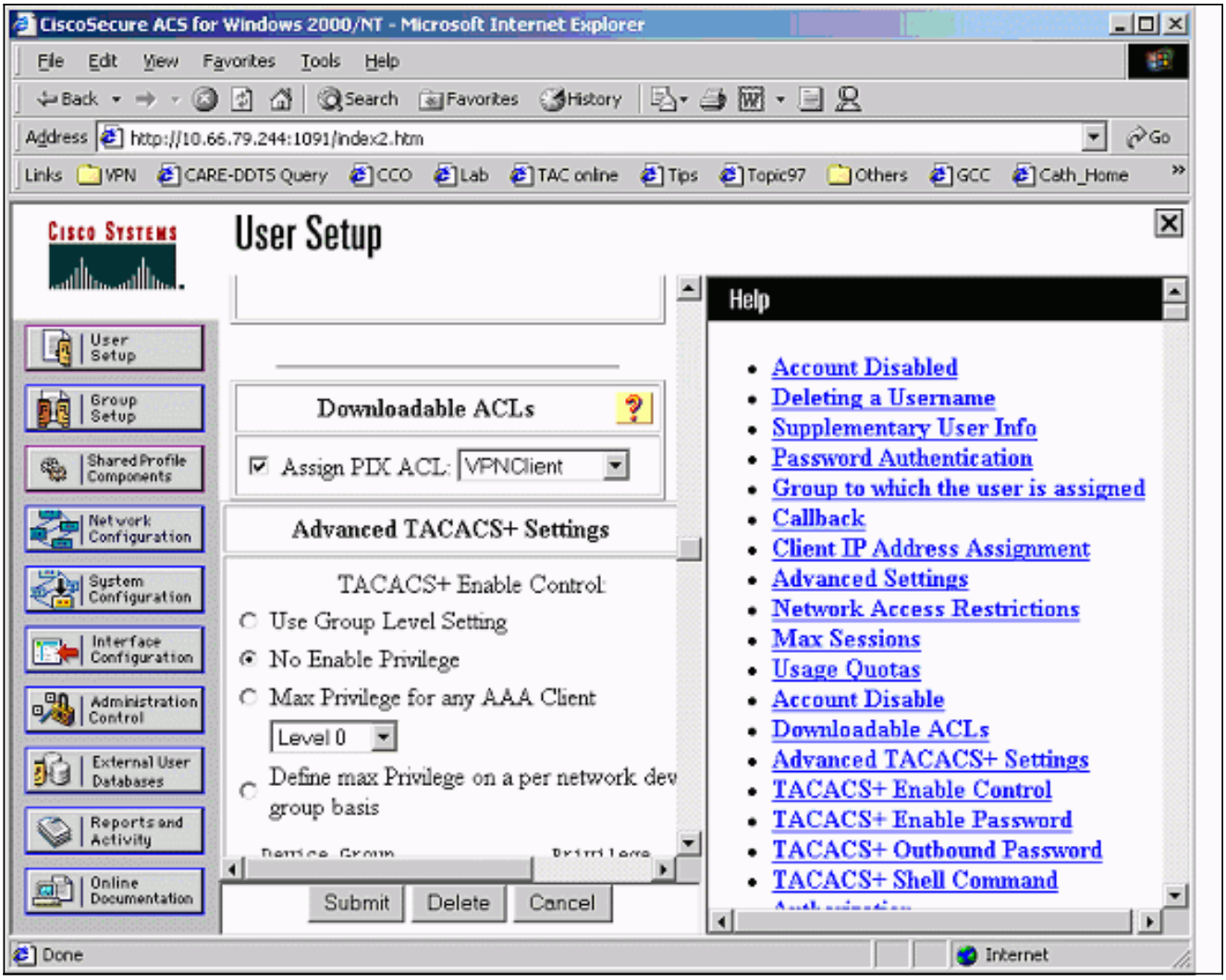
1. 点击**接口配置**并且选择**用户级可下载的ACLs的**选项。



2. 点击**共享配置文件组件**并且定义可下载的ACLs。



3. 点击**用户设置**。选择选项分配**PIX ACL**。从下拉菜单选择正确ACL。



带VPN组的XAUTH和可下载的每用户ACL - PIX 6.x设置

如果要执行授权的一个用户可下载的每用户ACL，请使用PIX防火墙软件版本6.2(2)。参考Cisco Bug ID CSCdx47975 (仅限注册用户)。

```
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:

带VPN组的XAUTH和可下载的每用户ACL - ASA/PIX 7.x设置

```
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
```

如何配置VPN客户端连接的本地Xauth

这些命令要求配置VPN客户端连接的本地Xauth ：

- *服务器标记*aaa-server协议*本地*
- 加密映射*aaa-server-name映射名*客户端验证

发出username命令定义PIX的本地用户。

为了使用本地PIX防火墙用户认证数据库，请进入*服务器标记*参数的本地aaa-server命令的。aaa-server命令发出以crypto map命令设立验证关联，以便VPN客户端验证，当他们访问PIX防火墙时。

如何增加记帐功能

这是命令添加核算的语法：

- aaa accounting acctg_service|除了入站|出站*|if_name local_ip local_mask foreign_ip foreign_mask* TACACS+|radius;

或者(新建在5.2) ：

- aaa accounting include acctg_service inbound|出站匹配*server_tag*

在PIX配置中，这是被添加的命令：

- aaa accounting include any inbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 AuthInbound;

或者(新建在5.2) ：

- access-list 150 permit ip任何任何AAA记帐匹配150外部AuthInbound

注意： sysopt connection permit-ipsec命令，不是sysopt ipsec pl-compatible命令，是必要为了Xauth记帐能工作。Xauth记帐不与只sysopt ipsec pl-compatible命令一起使用。Xauth记帐为TCP连接是有效。它为互联网控制消息协议(ICMP)或用户数据报协议(UDP)是无效。

TACACS+ 统计示例

```
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 记帐 示例

```
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 与 Show - 没有 VPN 组时的 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)

Debug与Show -带VPN组的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 pcp 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 pcp 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 pcp 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 pcp sas:

Debug与Show -与可下载的每用户ACL的Xauth

```
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
raidus.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 (0xc1bb3ea1)
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)
```

相关信息

- PIX 支持页
- PIX 命令参考
- 请求注解 (RFC)
- Cisco Secure ACS for UNIX 支持页
- Cisco Secure ACS for Windows 支持页
- TACACS/TACACS+支持页面
- IOS 文档中的 TACACS+
- RADIUS 支持页
- 技术支持和文档 - Cisco Systems