

# Hinzufügen von AAA-Authentifizierung (Xauth) zu PIX IPSec 5.2 und höher

## Inhalt

[Einführung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Konventionen](#)

[Hintergrundinformationen](#)

[Debugschritte](#)

[Debuggen von Befehlen auf dem PIX](#)

[Clientseitige Fehlerbehebung](#)

[AAA-Serverprofile](#)

[Cisco Secure UNIX TACACS+](#)

[Cisco Secure ACS für Windows TACACS+](#)

[Cisco Secure UNIX RADIUS](#)

[Cisco Secure ACS für Windows RADIUS](#)

[Merit RADIUS \(unterstützt Cisco AV-Paare\)](#)

[Netzwerkdiagramm](#)

[Konfigurierbare RADIUS-Ports \(5.3 und höher\)](#)

[Authentifizierung mit Xauth ohne VPN-Gruppen](#)

[Cisco Secure VPN Client 1.1-Einrichtung - Xauth ohne VPN-Gruppen](#)

[VPN 3000 Client 2.5 oder VPN Client 3.x-Einrichtung - Xauth ohne VPN-Gruppen](#)

[Xauth ohne VPN-Gruppen - PIX-Einrichtung](#)

[Authentifizierung mit Xauth mit VPN-Gruppen](#)

[VPN Client 2.5- oder 3.0-Einrichtung - Xauth mit VPN-Gruppen](#)

[Xauth mit VPN-Gruppen - PIX-Einrichtung](#)

[Xauth mit VPN-Gruppen und benutzerspezifischen herunterladbaren ACLs - ACS-Einrichtung](#)

[Xauth mit VPN-Gruppen und herunterladbaren benutzerspezifischen ACLs - PIX 6.x-Einrichtung](#)

[Xauth mit VPN-Gruppen und benutzerspezifischen herunterladbaren ACLs - ASA/PIX 7.x-Einrichtung](#)

[Konfigurieren von lokalem Xauth für VPN-Clientverbindung](#)

[Hinzufügen von Accounting](#)

[Beispiel für TACACS+-Accounting](#)

[Beispiel für RADIUS-Accounting](#)

[Debug und Show - Xauth ohne VPN-Gruppen](#)

[Debug und Show - Xauth mit VPN-Gruppen](#)

[Debug und Show - Xauth mit benutzerspezifischen herunterladbaren ACLs](#)

[Zugehörige Informationen](#)

## Einführung

Die RADIUS- und TACACS+-Authentifizierung und -Accounting sowie in gewissem Umfang auch die Autorisierung erfolgt für die am PIX terminierten Tunnel des Cisco Secure VPN Client 1.1 und des Cisco VPN 3000 2.5 Hardware Client. Änderungen an PIX 5.2 und einer höheren erweiterten Authentifizierung (Xauth) im Vergleich zu früheren Versionen, die Authentifizierung, Autorisierung und Accounting (AAA)-Zugriffslistenunterstützung umfassen, um zu kontrollieren, auf welche authentifizierten Benutzer Zugriff und Unterstützung für die Xauth-Terminierung des Cisco VPN 3000 Client 2.5 haben. Mit dem Befehl **VPN-Gruppen-Split-Tunneling** kann der VPN 3000-Client gleichzeitig eine Verbindung zum Netzwerk innerhalb des PIX sowie zu anderen Netzwerken (z. B. dem Internet) herstellen. In PIX 5.3 und höher besteht die AAA-Änderung gegenüber früheren Codeversionen darin, dass die RADIUS-Ports konfigurierbar sind. In PIX 6.0 wird die Unterstützung für den VPN Client 3.x hinzugefügt. Dies erfordert Diffie-Hellman-Gruppe 2.

## Voraussetzungen

### Anforderungen

Für dieses Dokument bestehen keine speziellen Anforderungen.

### Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf den folgenden Software- und Hardwareversionen:

- PIX Softwareversion 5.2.1
- Cisco Secure VPN Client 1.1
- Cisco VPN 3000 2.5 Client oder VPN Client 3.x **Hinweis:** Cisco VPN Client Version 3.0.x funktioniert nicht mit PIX-Versionen vor 6.0. Weitere Informationen finden Sie unter [Cisco Hardware- und VPN-Clients, die IPsec/PPTP/L2TP unterstützen](#).

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

### Konventionen

Weitere Informationen zu Dokumentkonventionen finden Sie unter [Cisco Technical Tips Conventions](#) (Technische Tipps zu Konventionen von Cisco).

## Hintergrundinformationen

PIX Firewall Software Version 6.2 unterstützt das Herunterladen von Zugriffskontrolllisten (Access Control Lists, ACLs) von einem Zugriffssteuerungsserver (ACS) auf die PIX-Firewall. Dadurch können benutzerspezifische ACLs auf einem AAA-Server konfiguriert werden, um eine benutzerspezifische ACL-Autorisierung bereitzustellen. Sie kann dann über den ACS auf die PIX-Firewall heruntergeladen werden. Diese Funktion wird nur für RADIUS-Server unterstützt. Es wird nicht für TACACS+-Server unterstützt.

## Debugschritte

Gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass die PIX Xauth-Konfiguration funktioniert, bevor Sie AAA-Authentifizierung hinzufügen. Wenn Sie den Datenverkehr nicht weiterleiten können, bevor Sie AAA implementieren, können Sie ihn anschließend nicht mehr weiterleiten.
2. Aktivieren Sie eine Protokollierung in PIX: Führen Sie den Befehl **zum Debuggen der Protokollierungskonsole** nicht auf einem stark ausgelasteten System aus. Der Befehl **zum Debuggen der Protokollierung** kann ausgegeben werden. Führen Sie dann den Befehl **show logging aus**. Die Protokollierung kann auch an einen Syslog-Server (System Message Log) gesendet und überprüft werden.
3. Aktivieren Sie das Debuggen auf den TACACS+- oder RADIUS-Servern. Diese Option steht allen Servern zur Verfügung.

## Debuggen von Befehlen auf dem PIX

- **debug crypto ipsec sa**: Dieser Debugbefehl zeigt IPsec-Ereignisse an.
- **debug crypto isakmp sa**: Dieser Debugbefehl zeigt Meldungen über IKE-Ereignisse (Internet Key Exchange) an.
- **debug crypto isakmp engine** - Dieser Debugbefehl zeigt Meldungen über IKE-Ereignisse an.

## Clientseitige Fehlerbehebung

Aktivieren Sie die Protokollanzeige, um die clientseitigen Debugging in Cisco Secure 1.1 oder VPN 3000 Client 2.5 anzuzeigen.

## AAA-Serverprofile

### 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 für Windows TACACS+

Die noacl-, 3000full- und 3000partiellen Benutzer benötigen in Cisco Secure ACS für Windows nur einen Benutzernamen und ein Kennwort. Der pixb-Benutzer benötigt einen Benutzernamen, ein Kennwort, eine Shell/exec-Zugriffsgruppe, eine aktivierte Zugriffskontrollliste und 115 im Feld.

## 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 für Windows RADIUS

RADIUS/Cisco ist der Gerätetyp. Die noacl-, 3000full- und 3000partiellen Benutzer benötigen in Cisco Secure ACS für Windows nur einen Benutzernamen und ein Kennwort. Der pixb-Benutzer benötigt einen Benutzernamen, ein Kennwort und ein Häkchen und ein "acl=115" im rechteckigen Feld Cisco/RADIUS, in dem 009\001 AV-Pair (anbieterspezifisch) steht.

**Hinweis:** Sie benötigen das anbieterattribut für die ACL. Attribut 11, Filter-ID, ist ungültig. Dieses Problem wird mit der Cisco Bug-ID [CSCdt50422](#) (nur [registrierte](#) Kunden) behandelt. Es wurde in PIX Software Version 6.0.1 behoben.

## Merit RADIUS (unterstützt Cisco AV-Paare)

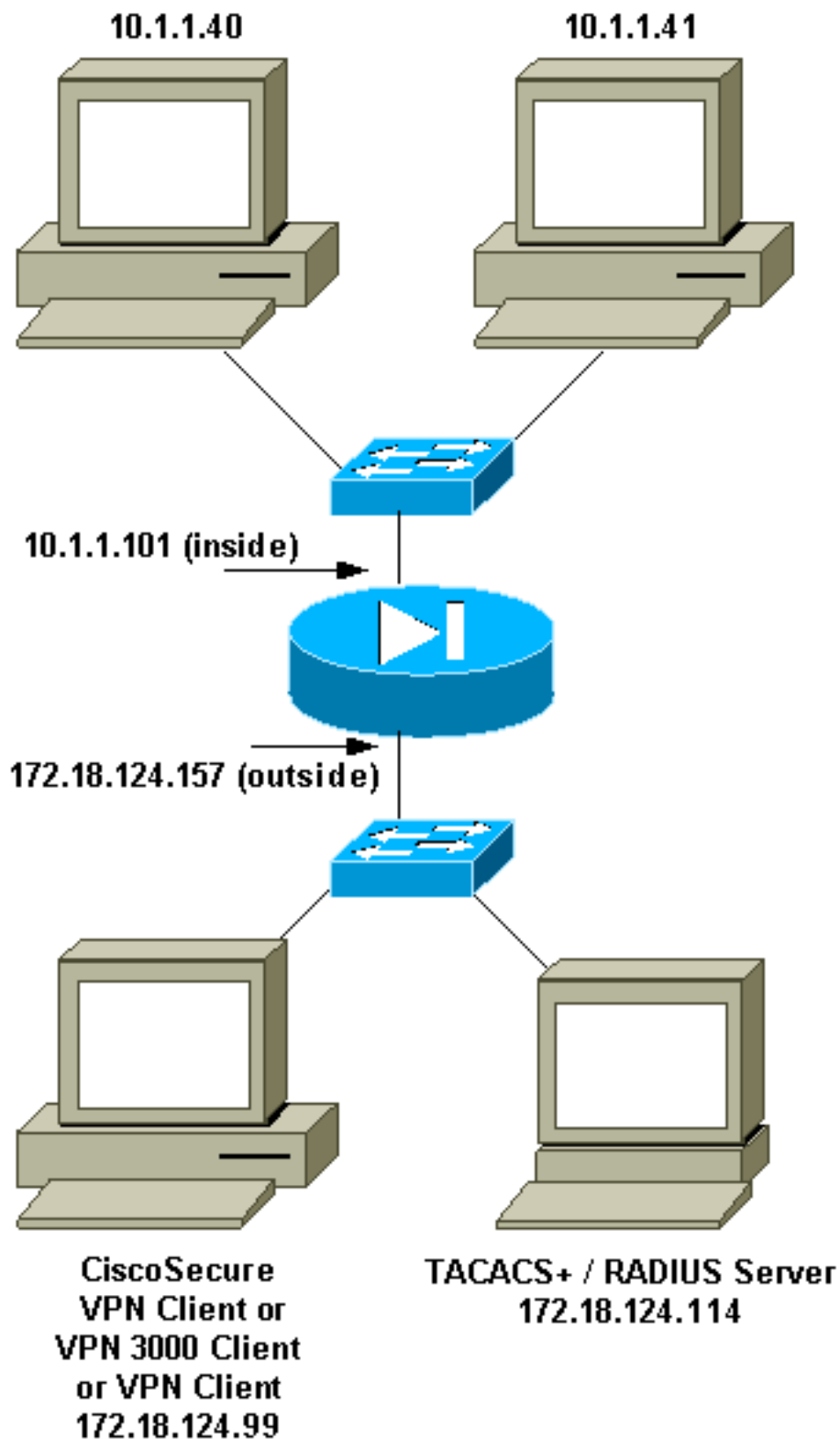
```
noacl Password= "noacl"

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

3000full Password= "3000full"

3000partial Password= "3000partial"
```

## Netzwerkdiagramm



## Konfigurierbare RADIUS-Ports (5.3 und höher)

Einige RADIUS-Server verwenden andere RADIUS-Ports als 1645/1646 (in der Regel 1812/1813). In PIX 5.3 und höher können die RADIUS-Authentifizierungs- und Accounting-Ports mithilfe der folgenden Befehle in andere Ports als den Standard 1645/1646 geändert werden:

- `aa-server radius-authport #`
- `aa-server radius-acctport #`

## Authentifizierung mit Xauth ohne VPN-Gruppen

In diesem Beispiel werden alle drei VPN-Clients mit Xauth authentifiziert. Die VPN-Clients können jedoch nur auf das Netzwerk innerhalb des PIX zugreifen, da Split-Tunneling nicht verwendet wird. Weitere Informationen [zum Split-Tunneling](#) finden Sie [unter Authentifizieren von Xauth mit VPN-Gruppen](#). Vom AAA-Server übergebene ACLs gelten für alle VPN-Clients. In diesem Beispiel soll die Benutzeranschrift eine Verbindung mit allen Ressourcen innerhalb des PIX herstellen und auf diese zugreifen. Benutzer-Pixb stellt eine Verbindung her, aber da die ACL 115 während des Xauth-Prozesses vom AAA-Server heruntergeladen wird, kann der Benutzer nur auf 10.1.1.40 zugreifen. Der Zugriff auf 10.1.1.41 und alle anderen IP-Adressen im Gerät wird verweigert.

**Hinweis:** Für die Unterstützung von VPN Client 3.0 ist PIX Software Release 6.0 erforderlich.

## Cisco Secure VPN Client 1.1-Einrichtung - Xauth ohne VPN-Gruppen

```
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
```

Öffnen Sie ein Denial of Service (DoS)-Fenster, und geben Sie den Befehl **ping -t #####** ein. Wenn das Fenster Xauth angezeigt wird, geben Sie den Benutzernamen und das Kennwort ein, die mit dem auf dem AAA-Server übereinstimmen.

## VPN 3000 Client 2.5 oder VPN Client 3.x-Einrichtung - Xauth ohne VPN-Gruppen

Gehen Sie wie folgt vor:

1. Wählen Sie **Optionen > Eigenschaften > Authentifizierung > Gruppennamen** aus.
2. Der Gruppenname lautet don't\_care, und das Passwort stimmt mit dem auf PIX im **isakmp key**-Befehl überein. Der Hostname lautet 172.18.124.157.
3. Klicken Sie auf **Verbinden**.
4. Wenn das Fenster Xauth angezeigt wird, geben Sie den Benutzernamen und das Kennwort ein, die mit dem auf dem AAA-Server übereinstimmen.

## Xauth ohne VPN-Gruppen - PIX-Einrichtung

```
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]

```

## Authentifizierung mit Xauth mit VPN-Gruppen

In diesem Beispiel kann der VPN 300 Client 2.5 oder VPN Client 3.0 mit Xauth authentifiziert werden, und Split-Tunneling ist in Kraft. Aufgrund der VPN-Gruppenmitgliedschaft wird eine ACL vom PIX an den VPN 3000-Client übergeben. Sie legt fest, dass nur das Netzwerk innerhalb des PIX über einen verschlüsselten Tunnel verfügt. Andere Zugriffe (möglicherweise ins Internet) werden nicht verschlüsselt.

In diesem Beispiel greift ein VPN-Client mit dem Benutzernamen 3000full (auf dem AAA-Server) in der Gruppe vpn3000-all (auf dem PIX) gleichzeitig mit dem Internet auf das gesamte 10.1.1.X-Netzwerk im PIX zu. Der VPN-Client erhält Win-Server-, DNS-Server- und Domännennamen-Informationen. Der andere VPN-Client mit dem Benutzernamen 3000partial (auf dem AAA-Server) in der Gruppe vpn3000-41 (auf dem PIX) greift aufgrund des Gruppenprofils auf nur eine IP-Adresse innerhalb des Netzwerks zu (10.1.1.40). Dieser VPN-Client empfängt keine Win- und DNS-Server-Informationen, führt aber weiterhin Split-Tunneling durch.

**Hinweis:** Für die Unterstützung von VPN Client 3.0 ist PIX Software Release 6.0 erforderlich.

## VPN Client 2.5- oder 3.0-Einrichtung - Xauth mit VPN-Gruppen

Gehen Sie wie folgt vor:

**Hinweis:** Die VPN 2.5- oder 3.0-Client-Konfiguration hängt vom jeweiligen Benutzer ab.

1. Wählen Sie **Optionen > Eigenschaften > Authentifizierung aus**.
2. Der Gruppenname und das Gruppenkennwort stimmen mit dem Gruppennamen auf dem PIX wie in überein: vpngroup vpn300-all password \*\*\*\*\* oder vpngroup vpn3000-41 password \*\*\*\*\* Der Hostname lautet 172.18.124.157.
3. Klicken Sie auf **Verbinden**.
4. Wenn das Fenster Xauth angezeigt wird, geben Sie den Benutzernamen und das Kennwort ein, die mit dem auf dem AAA-Server übereinstimmen.

In diesem Beispiel werden die Informationen aus der Gruppe vpn3000-all abgerufen, sobald Benutzer 3000full authentifiziert wurde. Benutzer 3000partieller ruft die Informationen aus der Gruppe vpn3000-41 ab. Das Fenster zeigt die **Aushandlung von Sicherheitsprofilen** an, und Ihr



## Link ist jetzt sicher.

Benutzer 3000full verwendet das Kennwort für die Gruppe vpn3000-all. Die Zugriffsliste 108 ist dieser Gruppe für Split-Tunneling zugeordnet. Der Tunnel wird zum Netzwerk 10.1.1.x geformt. Der Datenverkehr fließt unverschlüsselt zu Geräten, die sich nicht in der Zugriffsliste 108 befinden (z. B. das Internet). Dies ist Split-Tunneling.

Dies ist die Ausgabe für das Verbindungsstatusfenster des VPN-Clients für Benutzer 3000full:

	Network	Mask
key	10.1.1.0	255.255.255.0
key	172.18.124.157	255.255.255.255

Benutzer 3000partial verwendet das Kennwort für die Gruppe vpn3000-41. Die Zugriffsliste 125 ist dieser Gruppe für Split-Tunneling zugeordnet. Der Tunnel wird zum Gerät 10.1.1.41 geformt. Der Datenverkehr fließt unverschlüsselt zu Geräten, die sich nicht in der Zugriffsliste 125 befinden (z. B. das Internet). Der Datenverkehr fließt jedoch nicht zum 10.1.1.40-Gerät, da dieser Datenverkehr nicht routbar ist. Sie ist nicht in der Liste der Verschlüsselungstunnel angegeben.

Dies ist die Ausgabe für das Verbindungsstatusfenster des VPN-Clients für Benutzer 3000partiell:

	Network	Mask
key	10.1.1.41	255.255.255.255
key	172.18.124.157	255.255.255.255

## [Xauth mit VPN-Gruppen - PIX-Einrichtung](#)

**Hinweis:** Der Cisco Secure VPN Client 1.1 funktioniert nicht mit diesem, da es keinen ISAKMP-Schlüssel (Internet Security Association and Key Management Protocol) gibt. Fügen Sie den Befehl **isakmp key \*\*\*\*\* Adresse 0.0.0.0 Netzmaske 0.0.0.0** ein, damit alle VPN-Clients funktionieren.

```
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

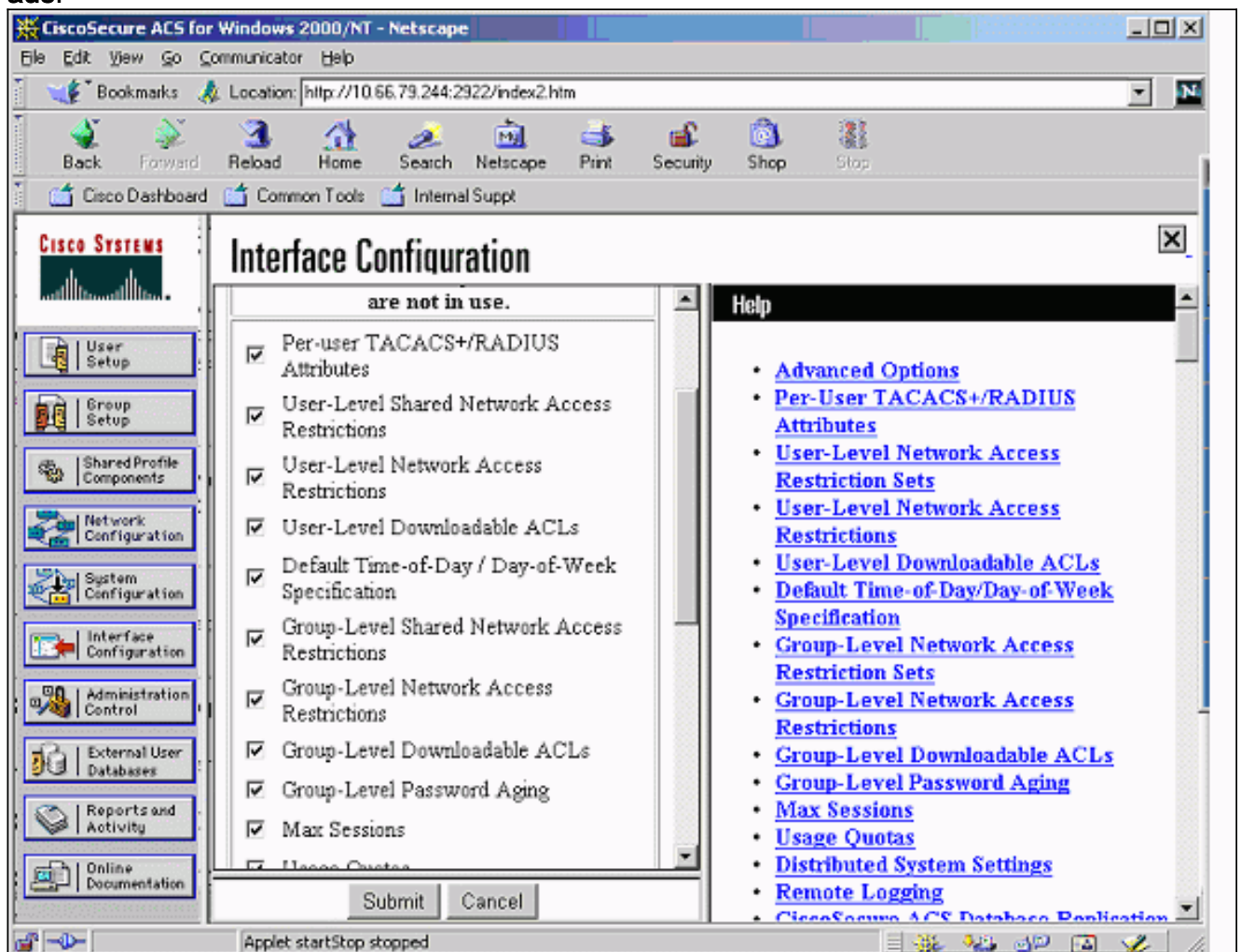
```

## [Xauth mit VPN-Gruppen und benutzerspezifischen herunterladbaren ACLs - ACS-Einrichtung](#)

### [Einrichten des Cisco Secure ACS](#)

Gehen Sie wie folgt vor:

1. Klicken Sie auf **Schnittstellenkonfiguration**, und wählen Sie die Option für herunterladbare ACLs auf Benutzerebene aus.



2. Klicken Sie auf **Komponenten für gemeinsam genutzte Profile**, und definieren Sie eine herunterladbare

## Zugriffskontrollliste.

CiscoSecure ACS for Windows 2000/NT - Microsoft Internet Explorer

Address <http://10.66.79.244:1903/index2.htm>

### Shared Profile Components

**Edit**

#### Downloadable PIX ACLs

Name:

Description:

#### ACL Definitions

```
permit ip host 10.1.1.2
```

#### Help

- [Downloadable PIX ACLs](#)
- [Adding or Editing a Downloadable PIX ACL](#)
- [Deleting a Downloadable PIX ACL](#)

**Downloadable PIX ACLs**

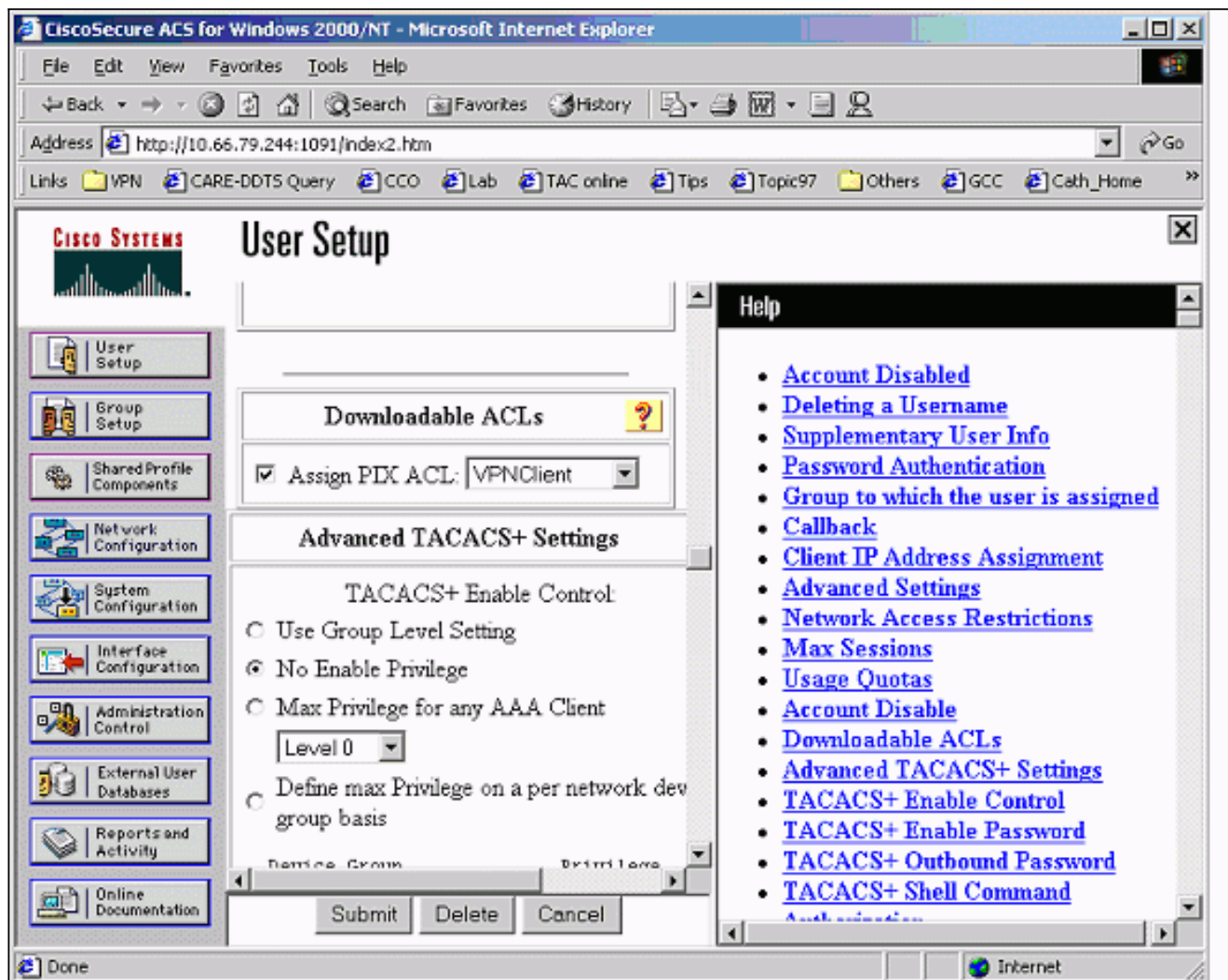
Use this page to create a new downloadable PIX ACL, edit an existing downloadable PIX ACL, or delete an existing downloadable PIX ACL.

[\[Back to Top\]](#)

**Adding or Editing a Downloadable PIX ACL**

Opening page [http://10.66.79.244:1903/setup.exe?action=make\\_r\\_fs&option=shared!](http://10.66.79.244:1903/setup.exe?action=make_r_fs&option=shared!) Internet

3. Klicken Sie auf **Benutzereinrichtung**. Wählen Sie die Option **PIX ACL zuweisen** aus. Wählen Sie die richtige ACL aus der Pulldown-Liste aus.



## [Xauth mit VPN-Gruppen und herunterladbaren benutzerspezifischen ACLs - PIX 6.x-Einrichtung](#)

Wenn Sie eine benutzerspezifische, herunterladbare ACL zur Autorisierung durchführen möchten, verwenden Sie die PIX Firewall-Software Version 6.2(2). Weitere Informationen finden Sie unter Cisco Bug ID [CSCdx47975](#) (nur [registrierte](#) Kunden).

```
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:

```

[Xauth mit VPN-Gruppen und benutzerspezifischen herunterladbaren ACLs - ASA/PIX 7.x-Einrichtung](#)

```
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

```

## [Konfigurieren von lokalem Xauth für VPN-Clientverbindung](#)



Diese Befehle sind erforderlich, um lokale Xauth-Verbindungen für die VPN-Client-Verbindung zu konfigurieren:

- **aaa-server *server-tag*-Protokoll *lokal***
- **crypto map *map-name* client authentication *aa-server-name***

Geben Sie den Befehl **username** ein, um lokale Benutzer auf PIX zu definieren.

Um die lokale PIX Firewall-Benutzerauthentifizierungsdatenbank zu verwenden, geben Sie **LOCAL** für den *Server-Tag*-Parameter für den Befehl **aaa-server** ein. Der **aaa-server**-Befehl wird mit dem Befehl **crypto map** ausgegeben, um eine Authentifizierungszuordnung einzurichten, sodass VPN-Clients authentifiziert werden, wenn sie auf die PIX-Firewall zugreifen.

## Hinzufügen von Accounting

Dies ist die Syntax des Befehls zum Hinzufügen von Accounting:

- **aaa accounting *acctg\_service*|exception inbound|outbound|*if\_name* *local\_ip* *local\_mask* *Foreign\_ip* *Foreign\_mask* tacacs+|radius ;**

oder (neu in 5.2):

- **aaa accounting umfasst *acctg\_service* inbound|outbound match *server\_tag***

In der PIX-Konfiguration wird dieser Befehl hinzugefügt:

- **aaa accounting umfasst alle eingehenden 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 AuthInbound;**

oder (neu in 5.2):

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

**Hinweis:** Der Befehl **sysopt connection permit-ipsec**, nicht der **sysopt ipsec pl-kompatible** Befehl, ist erforderlich, damit Xauth Accounting funktioniert. Xauth Accounting funktioniert nicht nur mit dem **sysopt ipsec pl-kompatiblen** Befehl. Xauth Accounting gilt für TCP-Verbindungen. Sie ist nicht gültig für das Internet Control Message Protocol (ICMP) oder das User Datagram Protocol (UDP).

## Beispiel für TACACS+-Accounting

```
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
```

## Beispiel für RADIUS-Accounting

```
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 und Show - Xauth ohne VPN-Gruppen](#)

```
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
rx dmp 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 und Show - Xauth mit VPN-Gruppen

```
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 pcsp 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 pcsp 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 pcsp 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 pcsp sas:

## [Debug und Show - Xauth mit benutzerspezifischen herunterladbaren ACLs](#)

```
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
radius.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)
```

## Zugehörige Informationen

- [PIX-Support-Seite](#)
- [PIX-Befehlsreferenzen](#)
- [Anforderungen für Kommentare \(RFCs\)](#)
- [Support-Seite für Cisco Secure ACS für UNIX](#)
- [Support-Seite für Cisco Secure ACS für Windows](#)
- [Support-Seite für TACACS/TACACS+](#)
- [TACACS+ in der IOS-Dokumentation](#)
- [RADIUS-Support-Seite](#)
- [Technischer Support und Dokumentation - Cisco Systems](#)