Most Common L2L and Remote Access IPSec VPN Troubleshooting Solutions

Document ID: 81824

Introduction

This document contains the most common solutions to IPsec VPN problems. These solutions come directly from service requests that the Cisco Technical Support have solved. Many of these solutions can be implemented prior to the in–depth troubleshooting of an IPsec VPN connection. As a result, this document is presented as a checklist of common procedures to try before you begin to troubleshoot a connection and call Cisco Technical Support.

If you need configuration example documents for the Site to Site VPN and Remote access VPN, refer to the *Remote Access VPN, Site to Site VPN (L2L) with PIX, Site to Site VPN (L2L) with IOS,* and *Site to Site VPN (L2L) with VPN3000* sections of Configuration Examples and TechNotes.

Note: Even though the configuration examples in this document are for use on routers and security appliances, nearly all of these concepts are also applicable to the the VPN 3000 concentrator.

Note: Refer to IP Security Troubleshooting – Understanding and Using debug Commands to provide an explanation of common debug commands that are used to troubleshoot IPsec issues on both the Cisco IOS® Software and PIX.

Note: You can look up any command used in this document with the Command Lookup Tool (registered customers only).

⚠️ **Warning:** Many of the solutions presented in this document can lead to a temporary loss of all IPsec VPN connectivity on a device. It is recommended that these solutions be implemented with caution and in accordance with your change control policy.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- IPsec VPN Configuration on Cisco Devices:

    ♦ Cisco PIX 500 Series Security Appliance
    ♦ Cisco ASA 5500 Series Security Appliance
    ♦ Cisco IOS® Routers
    ♦ Cisco VPN 3000 Series Concentrators (Optional)

Components Used

The information in this document is based on these software and hardware versions:

- Cisco ASA 5500 Series Security Appliance
- Cisco PIX 500 Series Security Appliance
- Cisco IOS

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Conventions

Refer to Cisco Technical Tips Conventions for more information on document conventions.

Problem: An IPsec VPN Configuration Does Not Work

A recently configured or modified IPsec VPN solution does not work.

A current IPsec VPN configuration no longer works.

Solutions

This section contains solutions to the most common IPsec VPN problems. Although they are not listed in any particular order, these solutions can be used as a checklist of items to verify or try before you engage in in−depth troubleshooting and call the TAC. All of these solutions come directly from TAC service requests and have resolved numerous customer issues.

Note: Some of the commands in these sections have been brought down to a second line due to spatial

considerations.

Enable NAT–Traversal (#1 RA VPN Issue)

NAT–Traversal or NAT–T allows VPN traffic to pass through NAT or PAT devices, such as a Linksys SOHO router. If NAT–T is not enabled, VPN Client users often appear to connect to the PIX or ASA without a problem, but they are unable to access the internal network behind the security appliance.

If you do not enable the NAT–T in the NAT/PAT Device, you can receive the `regular translation creation failed for protocol 50 src inside:10.0.1.26 dst outside:10.9.69.4` error message in the PIX/ASA.

Similarly, if you are unable to do simultaneous login from the same IP address, the `Secure VPN connection terminated locally by client. Reason 412: The remote peer is no longer responding.` error message appears. Enable NAT–T in the head end VPN device in order to resolve this error.

Note: With Cisco IOS Software Release 12.2(13)T and later, NAT–T is enabled by default in Cisco IOS.

Here is the command to enable NAT–T on a Cisco Security Appliance. The 20 in this example is the keepalive time (default).

PIX/ASA 7.1 and earlier

```
pix(config)#isakmp nat-traversal 20
```

PIX/ASA 7.2(1) and later

```
securityappliance(config)#crypto isakmp nat-traversal 20
```

The clients need to be modified as well in order for it to work.

In Cisco VPN Client, choose to **Connection Entries** and click **Modify**. It opens a new window where you have to choose the **Transport** tab. Under this tab, choose **Enable Transparent Tunneling** and the **IPSec over UDP (NAT / PAT)** radio button. Then click **Save** and test the connection.

Note: This command is the same for both PIX 6.x and PIX/ASA 7.x.

Note: It is important to allow the UDP 4500 for NAT–T, UDP 500 and ESP ports by the configuration of an ACL because the PIX/ASA acts as a NAT device. Refer to Configuring an IPsec Tunnel through a Firewall with NAT for more information in order to learn more about the ACL configuration in PIX/ASA.

VPN Concentrator

Choose **Configuration > Tunneling and Security >IPSEC >NAT Transparency > Enable:** *IPsec over NAT–T* in order to enable NAT–T on the VPN Concentartor.

Note: NAT–T also lets multiple VPN clients to connect through a PAT device at same time to any headend whether it is PIX, Router or Concentrator.

Test Connectivity Properly

Ideally, VPN connectivity is tested from devices behind the endpoint devices that do the encryption, yet many users test VPN connectivity with the **ping** command on the devices that do the encryption. While the **ping**

generally works for this purpose, it is important to source your ping from the correct interface. If the **ping** is sourced incorrectly, it can appear that the VPN connection has failed when it really works. Take this scenario as an example:
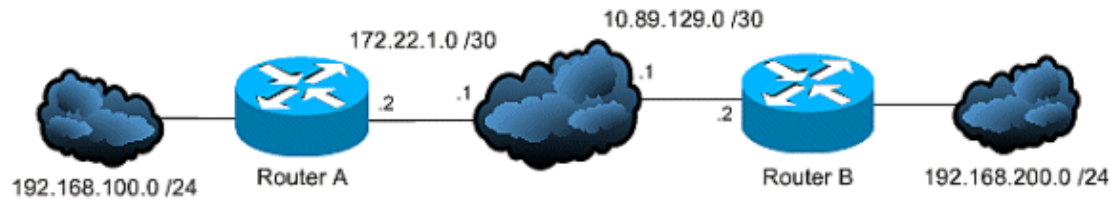
Router A crypto ACL

```
access-list 110 permit ip 192.168.100.0 0.0.0.255 192.168.200.0 0.0.0.255
```

Router B crypto ACL

```
access-list 110 permit ip 192.168.200.0 0.0.0.255 192.168.100.0 0.0.0.255
```

In this situation, a **ping** must be sourced from the "inside" network behind either router. This is because the crypto ACLs are only configured to encrypt traffic with those source addresses. A **ping** sourced from the Internet–facing interfaces of either router are not encrypted. Use the extended options of the **ping** command in privileged EXEC mode to source a ping from the "inside" interface of a router:

```
routerA#ping
Protocol [ip]:
Target IP address: 192.168.200.10
Repeat count [5]:
Datagram size [100]:
Timeout in seconds [2]:
Extended commands [n]: y
Source address or interface: 192.168.100.1
Type of service [0]:
Set DF bit in IP header? [no]:
Validate reply data? [no]:
Data pattern [0xABCD]:
Loose, Strict, Record, Timestamp, Verbose[none]:
Sweep range of sizes [n]:
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.200.1, timeout is 2 seconds:
Packet sent with a source address of 192.168.100.1
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
```

Imagine that the routers in this diagram have been replaced with PIX or ASA security appliances. The **ping** used to test connectivity can also be sourced from the inside interface with the **inside** keyword:

```
securityappliance#ping inside 192.168.200.10
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.200.10, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
```

Note: It is not recommended that you target the inside interface of a security appliance with your **ping**. If you must target the inside interface with your **ping**, you must enable **management–access** on that interface, or the appliance does not reply.

```
securityappliance(config)#management-access inside
```

Enable ISAKMP

If there is no indication that an IPsec VPN tunnel comes up at all, it possibly is due to the fact that ISAKMP has not been enabled. Be sure that you have enabled ISAKMP on your devices. Use one of these commands to enable ISAKMP on your devices:

- Cisco IOS

        router(config)#**crypto isakmp enable**
- Cisco PIX 7.1 and earlier (replace **outside** with your desired interface)

        pix(config)#**isakmp enable outside**
- Cisco PIX/ASA 7.2(1) and later (replace **outside** with your desired interface)

        securityappliance(config)#**crypto isakmp enable outside**

You can also get this error when you enable the ISAKMP on the outside interface:

        UDP: ERROR - socket <unknown> 62465 in used
        ERROR: IkeReceiverInit, unable to bind to port

The cause of the error can be that the Client behind ASA/PIS gets PAT'd to udp port 500 before isakmp can be enabled on the interface. Once that PAT translation is removed (clear xlate), the isakmp is able to be enabled.

Note: Always make sure that UDP 500 and 4500 port numbers are reserved for the negotiation of ISAKMP connections with the peer.

Enable/Disable PFS

In IPsec negotiations, Perfect Forward Secrecy (PFS) ensures that each new cryptographic key is unrelated to any previous key. Either enable or disable PFS on both the tunnel peers; otherwise, the LAN–to–LAN (L2L) IPsec tunnel is not established in the PIX/ASA/IOS router.

PIX/ASA:

PFS is disabled by default. In order to enable PFS, use the **pfs** command with the enable keyword in group–policy configuration mode. In order to disable PFS, enter the disable keyword.

        hostname(config-group-policy)#**pfs {enable | disable}**

In order to remove the PFS attribute from the running configuration, enter the no form of this command. A group policy can inherit a value for PFS from another group policy. Enter the no form of this command in order to prevent inheriting a value.

        hostname(config-group-policy)#**no pfs**

IOS Router:

In order to specify that IPsec must ask for PFS when new Security Associations are requested for this crypto map entry, or that IPsec requires PFS when it receives requests for new Security Associations, use the **set pfs** command in crypto map configuration mode. In order to specify that IPsec must not request PFS, use the no form of this command. By default, PFS is not requested. If no group is specified with this command, group1 is used as the default.

```
set pfs [group1 | group2]
no set pfs
```

For the set pfs command:

- group1 Specifies that IPsec must use the 768–bit Diffie–Hellman prime modulus group when the new Diffie–Hellman exchange is performed.
- group2 Specifies that IPsec must use the 1024–bit Diffie–Hellman prime modulus group when the new Diffie–Hellman exchange is performed.

Example:

```
Router(config)#crypto map map 10 ipsec-isakmp
Router(config-crypto-map)#set pfs group2
```

Note: Perfect Forward Secrecy (PFS) is Cisco proprietary and is not supported on third party devices.

Clear Old or Existing Security Associations (Tunnels)

If this error message occurs in the IOS Router, the problem is that the SA has either expired or been cleared. The remote tunnel end device does not know that it uses the expired SA to send a packet (not a SA establishment packet). When a new SA has been established, the communication resumes, so initiate the *interesting* traffic across the tunnel to create a new SA and re–establish the tunnel.

```
%CRYPTO-4-IKMP_NO_SA: IKE message from x.x.x.x  has no SA
```

If you clear ISKAMP (Phase I) and IPsec (Phase II) security associations (SAs), it is the simplest and often the best solution to resolve IPsec VPN problems.

If you clear SAs, you can frequently resolve a wide variety of error messages and strange behaviors without the need to troubleshoot. While this technique can easily be used in any situation, it is almost always a requirement to clear SAs after you change or add to a current IPsec VPN configuration. Moreover, while it is possible to clear only specific security associations, the most benefit can come from when you clear SAs globally on the device.

Note: Once the Security Associations have been cleared, it can be necessary to send traffic across the tunnel to re–establish them.

Warning: Unless you specify which security associations to clear, the commands listed here can clear all security associations on the device. Proceed with caution if other IPsec VPN tunnels are in use.

1. View Security Associations before you clear them

   a. **Cisco IOS**

   ```
   router#show crypto isakmp sa
   router#show crypto ipsec sa
   ```
   b. **Cisco PIX/ASA Security Appliances**

   ```
   securityappliance#show crypto isakmp sa
   securityappliance#show crypto ipsec sa
   ```

   Note: These commands are the same for both Cisco PIX 6.x and PIX/ASA 7.x
2. Clear Security Associations. Each command can be entered as shown in bold or entered with the

options shown with them.

     a. **Cisco IOS**

        a. **ISAKMP (Phase I)**

```
router#clear crypto isakmp ?
  <0 - 32766>  connection id of SA
  <cr>
```
     b. **IPsec (Phase II)**

```
router#clear crypto sa ?
  counters  Reset the SA counters
  map       Clear all SAs for a given crypto map
  peer      Clear all SAs for a given crypto peer
  spi       Clear SA by SPI
  <cr>
```
     b. **Cisco PIX/ASA Security Appliances**

        a. **ISAKMP (Phase I)**

```
securityappliance#clear crypto isakmp sa
```
     b. **IPsec (Phase II)**

```
security appliance#clear crypto ipsec sa ?

  counters  Clear IPsec SA counters
  entry     Clear IPsec SAs by entry
  map       Clear IPsec SAs by map
  peer      Clear IPsec SA by peer
  <cr>
```

Verify ISAKMP Lifetime

If the users are frequently disconnected across the L2L tunnel, the problem can be the lesser lifetime configured in ISAKMP SA. If any discrepancy occurs in the ISAKMP lifetime, you can recieve the `%PIX-5-713092: Group = x.x.x.x, IP = x.x.x.x, Failure during phase 1 rekeying attempt due to collision` error message. Configure the same value in both the peers in order to fix it.

The default is 86,400 seconds or 24 hours. As a general rule, a shorter lifetime provides more secure ISAKMP negotiations (up to a point), but, with shorter lifetimes, the security appliance sets up future IPsec SAs more quickly.

A match is made when both policies from the two peers contain the same encryption, hash, authentication, and Diffie−Hellman parameter values, and when the policy of the remote peer specifies a lifetime less than or equal to the lifetime in the compared policy. If the lifetimes are not identical, the shorter lifetime from the policy of the remote peer is used. If no acceptable match is found, the IKE refuses negotiation, and the IKE SA is not established.

Specify the SA lifetime. This examples sets a lifetime of 4 hours (14400 seconds). The default is 86400 seconds (24 hours).

PIX/ASA

```
hostname(config)#isakmp policy 2 lifetime  14400
```

IOS Router

```
R2(config)#crypto isakmp policy 10
R2(config-isakmp)#lifetime 86400
```

If the maximum configured lifetime is exceeded, you receive this error message when the VPN connection is terminated:

```
Secure VPN Connection terminated locally by the Client. Reason 426:
Maximum Configured Lifetime Exceeded.
```

In order to resolve this error message, set the *lifetime* value to *0* in order to set the lifetime of an IKE security association to infinity. The VPN will always be connection and will not terminate.

```
hostname(config)#isakmp policy 2 lifetime 0
```

Enable or Disable ISAKMP Keepalives

If you configure ISAKMP keepalives, it helps prevent sporadically dropped LAN−to−LAN or Remote Access VPN, which includes VPN clients, tunnels and the tunnels that are dropped after a period of inactivity. This feature lets the tunnel endpoint monitor the continued presence of a remote peer and report its own presence to that peer. If the peer becomes unresponsive, the endpoint removes the connection. In order for ISAKMP keepalives to work, both VPN endpoints must support them.

- Configure ISAKMP keepalives in Cisco IOS with this command:

  ```
  router(config)#crypto isakmp keepalive 15
  ```
- Use these commands to configure ISAKMP keepalives on the PIX/ASA Security Appliances:

  ♦ Cisco PIX 6.x

    ```
    pix(config)#isakmp keepalive 15
    ```
  ♦ Cisco PIX/ASA 7.x and later, for the tunnel group named **10.165.205.222**

    ```
    securityappliance(config)#tunnel-group 10.165.205.222
       ipsec-attributes

    securityappliance(config-tunnel-ipsec)#isakmp keepalive
       threshold 15 retry 10
    ```

In some situations, it is necessary to disable this feature in order to solve the problem, for example, if the VPN Client is behind a Firewall that prevents DPD packets.

Cisco PIX/ASA 7.x and later, for the tunnel group named **10.165.205.222**

Disables IKE keepalive processing, which is enabled by default.

```
securityappliance(config)#tunnel-group 10.165.205.222
   ipsec-attributes

securityappliance(config-tunnel-ipsec)#isakmp keepalive disable
```

Disable Keepalive for Cisco VPN Client 4.x

Choose **%System Root% > Program Files > Cisco Systems >VPN Client > Profiles** on the Client PC that experiences the issue in order to disable IKE keepalive, and edit the **PCF file** , where

applicable, for the connection.

Change the **'ForceKeepAlives=0'** (default) to **'ForceKeepAlives=1'**.

Note: Keepalives are Cisco proprietary and are not supported by third party devices.

Re−Enter or Recover Pre−Shared−Keys

In many cases, a simple typo can be to blame when an IPsec VPN tunnel does not come up. For example, on the security appliance, pre−shared keys become hidden once they are entered. This obfuscation makes it impossible to see if a key is incorrect.**Be certain that you have entered any pre−shared−keys correctly on each VPN endpoint.** Re−enter a key to be certain that it is correct; this is a simple solution that can help avoid in−depth troubleshooting.

In Remote Access VPN, check that the valid group name and preshared key are entered in the CiscoVPN Client. You can face this error if the group name/ preshared key are not matched between the VPN Client and the head−end device.

```
 1 12:41:51.900 02/18/06 Sev=Warning/3 IKE/0xE3000056
 The received HASH payload cannot be verified
 2 12:41:51.900 02/18/06 Sev=Warning/2 IKE/0xE300007D
Hash verification failed
3     14:37:50.562  10/05/06  Sev=Warning/2 IKE/0xE3000099
Failed to authenticate peer (Navigator:904)
4     14:37:50.593  10/05/06  Sev=Warning/2 IKE/0xE30000A5
Unexpected SW error occurred while processing Aggressive Mode
negotiator:(Navigator:2202)
5     14:44:15.937  10/05/06  Sev=Warning/2 IKE/0xA3000067
Received Unexpected InitialContact Notify (PLMgrNotify:888)
6     14:44:36.578  10/05/06  Sev=Warning/3 IKE/0xE3000056
The received HASH payload cannot be verified
7     14:44:36.593  10/05/06  Sev=Warning/2 IKE/0xE300007D
Hash verification failed... may be configured with invalid group password.
8     14:44:36.609  10/05/06  Sev=Warning/2 IKE/0xE3000099
Failed to authenticate peer (Navigator:904)
9     14:44:36.640  10/05/06  Sev=Warning/2 IKE/0xE30000A5
Unexpected SW error occurred while processing Aggressive Mode
negotiator:(Navigator:2202)
```

You can also recover a pre−shared key without any configuration changes on the PIX/ASA security appliance. Refer to PIX/ASA 7.x and later: Pre−shared Key Recovery.

Warning: If you remove crypto−related commands, you are likely to bring down one or all of your VPN tunnels. Use these commands with caution and refer to the change control policy of your organization before you follow these steps.

- Use these commands to remove and re−enter the pre−shared−key **secretkey** for the peer **10.0.0.1** or the group **vpngroup** in IOS:

    ♦ Cisco LAN−to−LAN VPN

    ```
    router(config)#no crypto isakmp key secretkey
       address 10.0.0.1
    router(config)#crypto isakmp key secretkey
       address 10.0.0.1
    ```
    ♦ Cisco Remote Access VPN

```
router(config)#crypto isakmp client configuration
    group vpngroup
router(config-isakmp-group)#no key secretkey
router(config-isakmp-group)#key secretkey
```

- Use these commands to remove and re–enter the pre–shared–key **secretkey** for the peer **10.0.0.1** on PIX/ASA Security Appliances:

    ♦ Cisco PIX 6.x

    ```
    pix(config)#no isakmp key secretkey address 10.0.0.1
    pix(config)#isakmp key secretkey address 10.0.0.1
    ```
    ♦ Cisco PIX/ASA 7.x and later

    ```
    securityappliance(config)#tunnel-group 10.0.0.1
        ipsec-attributes
    securityappliance(config-tunnel-ipsec)#no pre-shared-key
    securityappliance(config-tunnel-ipsec)#pre-shared-key
        secretkey
    ```

Remove and Re–apply Crypto Maps

When you clear security associations, and it does not resolve an IPsec VPN issue, remove and reapply the relevant crypto map in order to resolve a wide variety of issues that includes intermittent dropping of VPN tunnel.

Warning: If you remove a crypto map from an interface, it **definitely** brings down any IPsec tunnels associated with that crypto map. Follow these steps with caution and consider the change control policy of your organization before you proceed.

- Use these commands to remove and replace a crypto map in Cisco IOS:

    Begin with the removal of the crypto map from the interface. Use the no form of the **crypto map** command.

    ```
    router(config-if)#no crypto map mymap
    ```

    Continue to use the **no** form to remove an entire crypto map.

    ```
    router(config)#no crypto map mymap 10
    ```

    Replace the crypto map on interface Ethernet0/0 for the peer **10.0.0.1**. This example shows the minimum required crypto map configuration:

    ```
    router(config)#crypto map mymap 10 ipsec-isakmp
    router(config-crypto-map)#match address 101
    router(config-crypto-map)#set transform-set mySET
    router(config-crypto-map)#set peer 10.0.0.1
    router(config-crypto-map)#exit
    router(config)#interface ethernet0/0
    router(config-if)#crypto map mymap
    ```
- Use these commands to remove and replace a crypto map on the PIX or ASA:

    Begin with the removal of the crypto map from the interface. Use the no form of the **crypto map** command.

    ```
    securityappliance(config)#no crypto map mymap interface outside
    ```

Continue to use the **no** form to remove the other crypto map commands.

```
securityappliance(config)#no crypto map mymap 10 match
   address 101
securityappliance(config)#no crypto map mymap set
   transform-set mySET
securityappliance(config)#no crypto map mymap set
   peer 10.0.0.1
```

Replace the crypto map for the peer **10.0.0.1**. This example shows the minimum required crypto map configuration:

```
securityappliance(config)#crypto map mymap 10 ipsec-isakmp
securityappliance(config)#crypto map mymap 10
   match address 101
securityappliance(config)#crypto map mymap 10 set
   transform-set mySET
securityappliance(config)#crypto map mymap 10 set
   peer 10.0.0.1
securityappliance(config)#crypto map mymap interface outside
```

Note: If you remove and reapply the crypto map, this also resolves the connectivity issue if the IP address of head end has been changed.

Verify that sysopt Commands are Present (PIX/ASA Only)

The commands **sysopt connection permit–ipsec** and **sysopt connection permit–vpn** allow packets from an IPsec tunnel and their payloads to bypass interface ACLs on the security appliance. IPsec tunnels that are terminated on the security appliance are likely to fail if one of these commands is not enabled.

In Security Appliance Software Version 7.0 and earlier, the relevant sysopt command for this situation is **sysopt connection permit–ipsec**.

In Security Appliance Software Version 7.1(1) and later, the relevant sysopt command for this situation is **sysopt connection permit–vpn**.

In PIX 6.x, this functionality is **disabled** by default. With PIX/ASA 7.0(1) and later, this functionality is **enabled** by default. Use these show commands to determine if the relevant **sysopt** command is enabled on your device:

1. Cisco PIX 6.x

```
pix# show sysopt
no sysopt connection timewait
sysopt connection tcpmss 1380
sysopt connection tcpmss minimum 0
no sysopt nodnsalias inbound
no sysopt nodnsalias outbound
no sysopt radius ignore-secret
no sysopt uauth allow-http-cache
no sysopt connection permit-ipsec

!--- sysopt connection permit-ipsec is disabled

no sysopt connection permit-pptp
no sysopt connection permit-l2tp
no sysopt ipsec pl-compatible
```
2. Cisco PIX/ASA 7.x

```
securityappliance# show running-config sysopt
no sysopt connection timewait
sysopt connection tcpmss 1380
sysopt connection tcpmss minimum 0
no sysopt nodnsalias inbound
no sysopt nodnsalias outbound
no sysopt radius ignore-secret
sysopt connection permit-vpn

!--- sysopt connection permit-vpn is enabled
!--- This device is running 7.2(2)
```

Use these commands in order to enable the correct **sysopt** command for your device:

- Cisco PIX 6.x and PIX/ASA 7.0

  ```
  pix(config)#sysopt connection permit-ipsec
  ```
- Cisco PIX/ASA 7.1(1) and later

  ```
  securityappliance(config)#sysopt connection permit-vpn
  ```

Note: If you do not wish to use the **sysopt connection** command, then you must explicitly permit the required traffic, which is interesting traffic from source to destination, for example, from LAN of remote device to LAN of local device and "UDP port 500" for outside interface of remote devie to outside interface of local device, in outside ACL.

Verify the ISAKMP Identity

If the IPsec VPN tunnnel has failed within the IKE negotiation, the failure can be due to either the PIX or the inability of its peer to recognize the identity of its peer.When two peers use IKE to establish IPsec security associations, each peer sends its ISAKMP identity to the remote peer. It sends either its IP address or host name dependent upon how each has its ISAKMP identity set. By default, the ISAKMP identity of the PIX Firewall unit is set to the IP address. As a general rule, set the security appliance and the identities of its peers in the same way to avoid an IKE negotiation failure.

In order to set the Phase 2 ID to be sent to the peer, use the **isakmp identity** command in global configuration mode

```
crypto isakmp identity address

!--- If the RA or L2L (site-to-site) VPN tunnels connect
!--- with pre-shared key as authentication type
```

OR

```
crypto isakmp identity auto

!--- If the RA or L2L (site-to-site) VPN tunnels connect
!--- with ISAKMP negotiation by connection type; IP address for
!--- preshared key or cert DN for certificate authentication.
```

OR

```
crypto isakmp identity hostname

!--- Uses the fully-qualified domain name of
```

```
                !--- the host exchanging ISAKMP identity information (default).
                !--- This name comprises the hostname and the domain name.
```

Note: The **isakmp identity** command was deprecated from the software version 7.2(1). Refer to the Cisco Security Appliance Command Reference, Version 7.2 for more information.

Verify Idle/Session Timeout

If the idle timeout is set to 30 minutes (default), it means that it drops the tunnel after 30 minutes of no traffic passes through it. The VPN client gets disconnected after 30 minutes regardless of the setting of idle timeout and encounters the PEER_DELETE−IKE_DELETE_UNSPECIFIED error.

Configure **idle timeout** and **session timeout** as **none** in order to make the tunnel always be **up** and so that the tunnel is never dropped.

PIX/ASA 7.x and later

Enter the **vpn−idle−timeout** command in group−policy configuration mode or in username configuration mode in order to configure the user timeout period:

```
hostname(config)#group-policy DfltGrpPolicy attributes
hostname(config-group-policy)#vpn-idle-timeout none
```

Configure a maximum amount of time for VPN connections with the **vpn−session−timeout** command in group−policy configuration mode or in username configuration mode:

```
hostname(config)#group-policy DfltGrpPolicy attributes
hostname(config-group-policy)#vpn-session-timeout none
```

Cisco IOS Router

Use the **crypto ipsec security−association idle−time** command in global configuration mode or crypto map configuration mode in order to configure the IPsec SA idle timer. By default IPsec SA idle timers are disabled.

```
crypto ipsec security-association idle-time
seconds
```

Time is in *seconds*, which the idle timer allows an inactive peer to maintain an SA. Valid values for the seconds argument range from 60 to 86400.

Verify that ACLs are Correct

There are two access lists used in a typical IPsec VPN configuration. One access list is used to exempt traffic that is destined for the VPN tunnel from the NAT process. The other access list defines what traffic to encrypt; this includes a crypto ACL in a LAN−to−LAN setup or a split−tunneling ACL in a Remote Access configuration. When these ACLs are incorrectly configured or missing, traffic might only flow in one direction across the VPN tunnel, or it might not be sent across the tunnel at all.

Be sure that you have configured all of the access lists necessary to complete your IPsec VPN configuration and that those access lists define the correct traffic. This list contains simple things to check when you suspect that an ACL is the cause of problems with your IPsec VPN.

- Make sure that your NAT Exemption and crypto ACLs specify the correct traffic.

- If you have multiple VPN tunnels and multiple crypto ACLs, make sure that those ACLs do not overlap.
- Do not use ACLs twice. Even if your NAT Exemption ACL and crypto ACL specify the same traffic, use two different access lists.
- For remote access configuration, do not use access−list for interesting traffic with the dynamic crypto map. This can cause the VPN client to be unable to connect to the head end device. If you mistakenly configured the crypto ACL for Remote access VPN, you can get the `%ASA−3−713042: IKE Initiator unable to find policy: Intf 2` error message.

   Refer to PIX/ASA 7.x and Cisco VPN Client 4.x with Windows 2003 IAS RADIUS (Against Active Directory) Authentication Configuration Example for a sample configuration that shows how to set up the remote access VPN connection between a Cisco VPN Client and the PIX/ASA.
- Make sure that your device is configured to use the NAT Exemption ACL. On a router, this means that you use the **route−map** command. On the PIX or ASA, this means that you use the **nat (0)** command. A NAT exemption ACL is required for both LAN−to−LAN and Remote Access configurations.

   ♦ Here, an IOS router is configured to exempt traffic that is sent between **192.168.100.0 /24** and **192.168.200.0 /24** or **192.168.1.0 /24** from NAT. Traffic destined for anywhere else is subject to NAT overload:

   ```
   access-list 110 deny ip 192.168.100.0 0.0.0.255
      192.168.200.0 0.0.0.255
   access-list 110 deny ip 192.168.100.0 0.0.0.255
      192.168.1.0 0.0.0.255
   access-list 110 permit ip 192.168.100.0 0.0.0.255 any

   route-map nonat permit 10
     match ip address 110

   ip nat inside source route-map nonat interface FastEthernet0/0 overload
   ```
   ♦ Here, a PIX is configured to exempt traffic that is sent between **192.168.100.0 /24** and **192.168.200.0 /24** or **192.168.1.0 /24** from NAT. For example, all other traffic is subject to NAT overload:

   ```
   access-list noNAT extended permit ip 192.168.100.0
      255.255.255.0 192.168.200.0 255.255.255.0
   access-list noNAT extended permit ip 192.168.100.0
      255.255.255.0 192.168.1.0 255.255.255.0

   nat (inside) 0 access-list noNAT
   nat (inside) 1 0.0.0.0 0.0.0.0

   global (outside) 1 interface
   ```

   Note: NAT exemption ACLs work only with the IP address or IP networks, such as those examples mentioned (access−list noNAT), and must be identical to the crypto map ACLs. The NAT exemption ACLs do not work with the port numbers (for instance, 23, 25, etc.).

   Note: You can get the error message as shown if there is misconfiguration in NAT exemption (nat 0) ACLs.

   ```
   %PIX-3-305005: No translation group
   found for icmp src outside:192.168.100.41 dst
   inside:192.168.200.253 (type 8, code 0)
   ```

   Note: Incorrect Example:

```
access-list noNAT extended permit ip 192.168.100.0
    255.255.255.0 192.168.200.0 255.255.255.0 eq 25
```

If NAT exemption (nat 0) does not work, then try to remove it and issue the **NAT 0** command in order for it to work.

- Make sure that your ACLs are not backwards and that they are the right type.

  ◆ Crypto and NAT exemption ACLs for LAN−to−LAN configurations must be written from the perspective of the device on which the ACL is configured. This means that the ACLs must **mirror** each other. In this example, a LAN−to−LAN tunnel is set up between **192.168.100.0 /24** and **192.168.200.0 /24**.
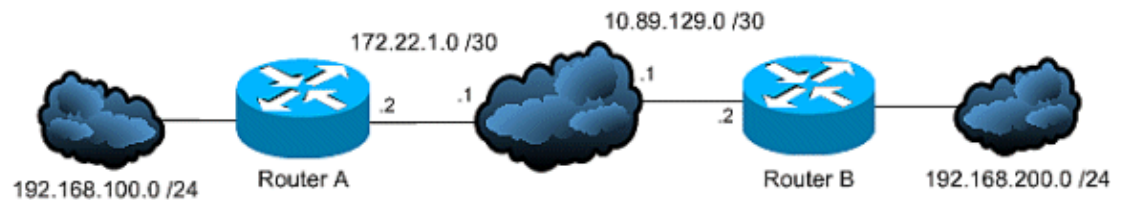
Router A crypto ACL

```
access-list 110 permit ip 192.168.100.0 0.0.0.255
    192.168.200.0 0.0.0.255
```

Router B crypto ACL

```
access-list 110 permit ip 192.168.200.0 0.0.0.255
    192.168.100.0 0.0.0.255
```

Note: Although it is not illustrated here, this same concept applies to the PIX and ASA Security Appliances, as well.

  ◆ Split−tunnel ACLs for Remote Access configurations must be **standard** access lists that permit traffic to the network to which the VPN clients need access.

Note: In the extended access list, to use **'any'** at the source in the split tunneling ACL is similar to disable split tunneling. Use only the source networks in the extended ACL for split tunneling.

Note: Correct Example:

```
access-list 140 permit ip 10.1.0.0 0.0.255.255 10.18.0.0 0.0.255.255
```

Note: Incorrect Example:

```
access-list 140 permit ip any 10.18.0.0 0.0.255.255
```


  ◊ Cisco IOS

```
router(config)#access-list 10 permit ip 192.168.100.0
router(config)#crypto isakmp client configuration group MYGROUP
```

```
                    router(config-isakmp-group)#acl 10
        ◊ Cisco PIX 6.x

                    pix(config)#access-list 10 permit 192.168.100.0
                       255.255.255.0
                    pix(config)#vpngroup MYGROUP split-tunnel 10
        ◊ Cisco PIX/ASA 7.x

                    securityappliance(config)#access-list 10 standard
                       permit 192.168.100.0 255.255.255.0
                    securityappliance(config)#group-policy MYPOLICY internal
                    securityappliance(config)#group-policy MYPOLICY attributes
                    securityappliance(config-group-policy)#split-tunnel-policy
                       tunnelspecified
                    securityappliance(config-group-policy)#split-tunnel-network-list
                       value 10
```

Verify the ISAKMP Policies

If the IPsec tunnel is not UP, check that the ISAKMP policies match with the remote peers. This ISAKMP policy is applicable to both the Site–to–Site (L2L) and Remote Access IPsec VPN.

If the Cisco VPN Clients or the Site–to–Site VPN are not able establish the tunnel with the remote–end device, check that **the two peers contain the same encryption, hash, authentication, and Diffie–Hellman parameter values** and when the remote peer policy specifies a lifetime less than or equal to the lifetime in the policy that the initiator sent. If the lifetimes are not identical, the security appliance uses the shorter lifetime. If no acceptable match exists, ISAKMP refuses negotiation, and the SA is not established.

```
    "removing peer from peer table failed − no match"
```

This message usually appears due to mismatched ISAKMP policies or a missing NAT 0 statement.

If the Cisco VPN Client is unable to connect the head−end device, the problem can be the mismatch of ISAKMP Policy. The head−end device must match with one of the IKE Proposals of the Cisco VPN Client.

Note: For the ISAKMP policy and IPsec Transform−set that is used on the PIX/ASA, the Cisco VPN client cannot use a policy with a combination of DES and SHA. If you use DES, you need to use MD5 for the hash algorithm, or you can use the other combinations, 3DES with SHA and 3DES with MD5.

Verify that Routing is Correct

Routing is a critical part of almost every IPsec VPN deployment. Be certain that your encryption devices such as Routers and PIX or ASA Security Appliances have the proper routing information to send traffic over your VPN tunnel. Moreover, if other routers exist behind your gateway device, be sure that those routers know how to reach the tunnel and what networks are on the other side.

One key component of routing in a VPN deployment is Reverse Route Injection (RRI). RRI places dynamic entries for remote networks or VPN clients in the routing table of a VPN gateway. These routes are useful to the device on which they are installed, as well as to other devices in the network because routes installed by RRI can be redistributed through a routing protocol such as EIGRP or OSPF.

- In a LAN−to−LAN configuration, it is important for each endpoint to have a route or routes to the networks for which it is supposed to encrypt traffic. In this example, Router A must have routes to the networks behind Router B through **10.89.129.2**. Router B must have a similar route to **192.168.100.0 /24**:
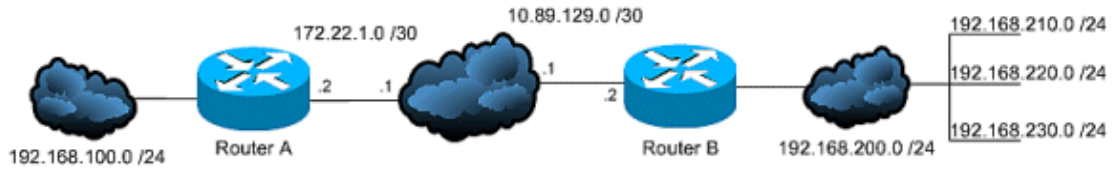
♦ The first way to ensure that each router knows the appropriate route(s) is to configure static routes for each destination network. For example, Router A can have these route statements configured:

```
ip route 0.0.0.0 0.0.0.0 172.22.1.1
ip route 192.168.200.0 255.255.255.0 10.89.129.2
ip route 192.168.210.0 255.255.255.0 10.89.129.2
ip route 192.168.220.0 255.255.255.0 10.89.129.2
ip route 192.168.230.0 255.255.255.0 10.89.129.2
```

If Router A was replaced with a PIX or ASA, the configuration can look like this:

```
route outside 0.0.0.0 0.0.0.0 172.22.1.1
route outside 192.168.200.0 255.255.255.0 10.89.129.2
route outside 192.168.200.0 255.255.255.0 10.89.129.2
route outside 192.168.200.0 255.255.255.0 10.89.129.2
route outside 192.168.200.0 255.255.255.0 10.89.129.2
```

♦ If a large number of networks exists behind each endpoint, the configuration of static routes becomes difficult to maintain. Instead, it is recommended that you use Reverse Route Injection, as described. RRI places into the routing table routes for all of the remote networks listed in the crypto ACL. For example, the crypto ACL and crypto map of Router A can look like this:

```
access-list 110 permit ip 192.168.100.0 0.0.0.255
   192.168.200.0 0.0.0.255
access-list 110 permit ip 192.168.100.0 0.0.0.255
   192.168.210.0 0.0.0.255
access-list 110 permit ip 192.168.100.0 0.0.0.255
   192.168.220.0 0.0.0.255
access-list 110 permit ip 192.168.100.0 0.0.0.255
   192.168.230.0 0.0.0.255

crypto map myMAP 10 ipsec-isakmp
 set peer 10.89.129.2
 reverse-route
 set transform-set mySET
 match address 110
```

If Router A was replaced by a PIX or ASA, the configuration can look like this:

```
access-list cryptoACL extended permit ip 192.168.100.0
   255.255.255.0 192.168.200.0 255.255.255.0
access-list cryptoACL extended permit ip 192.168.100.0
   255.255.255.0 192.168.210.0 255.255.255.0
access-list cryptoACL extended permit ip 192.168.100.0
   255.255.255.0 192.168.220.0 255.255.255.0
access-list cryptoACL extended permit ip 192.168.100.0
   255.255.255.0 192.168.230.0 255.255.255.0

crypto map myMAP 10 match address cryptoACL
crypto map myMAP 10 set peer 10.89.129.2
crypto map myMAP 10 set transform-set mySET
crypto map mymap 10 set reverse-route
```

• In a Remote Access configuration, routing changes are not always necessary. Yet, if other routers exist behind the VPN gateway router or Security Appliance, those routers need to learn the path to the

VPN clients somehow. In this example, suppose that the VPN clients are given addresses in the range of **10.0.0.0 /24** when they connect.
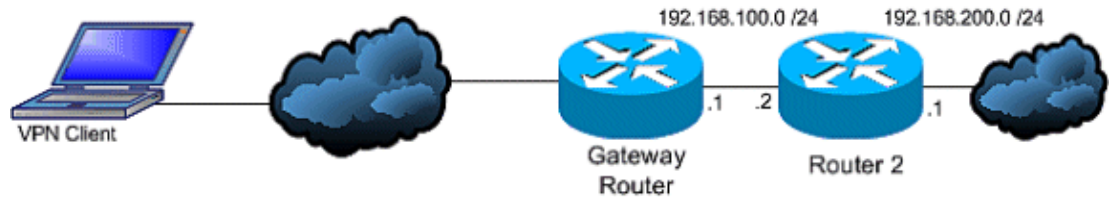
If no routing protocol is in use between the gateway and the other router(s), static routes can be used on routers such as Router 2:

```
ip route 10.0.0.0 255.255.255.0 192.168.100.1
```

If a routing protocol such as EIGRP or OSPF is in use between the gateway and other routers, it is recommended that Reverse Route Injection be used as described. RRI automatically adds routes for the VPN client to the routing table of the gateway. These routes can then be distributed to the other routers in the network.

- ◆ Cisco IOS Router:

```
crypto dynamic-map dynMAP 10
 set transform-set mySET
 reverse-route

crypto map myMAP 60000 ipsec-isakmp dynamic dynMAP
```
- ◆ Cisco PIX or ASA Security Appliance:

```
crypto dynamic-map dynMAP 10 set transform-set mySET
crypto dynamic-map dynMAP 10 set reverse-route

crypto map myMAP 60000 ipsec-isakmp dynamic dynMAP
```

Note: The routing issue occurs if the pool of IP addresses assigned for the VPN clients are overlaps with internal networks of the head−end device. For further information, refer to the Overlapping Private Networks section .

Vertify that Transform−Set is Correct

Make sure that the IPsec encryption and hash algorithms to be used by the transform set on the both ends are the same. Refer to the Command reference section of the Cisco Security Appliance configuration guide for more information.

Note: For the ISAKMP policy and IPsec Transform−set that is used on the PIX/ASA, the Cisco VPN client cannot use a policy with a combination of DES and SHA. If you use DES, you need to use MD5 for the hash algorithm, or you can use the other combinations, 3DES with SHA and 3DES with MD5.

Verify Crypto Map Sequence Numbers and Name

If static and dynamic peers are configured on the same crypto map, the order of the crypto map entries is very important. The sequence number of the dynamic crypto map entry **must be** higher than all of the other static crypto map entries. If the static entries are numbered higher than the dynamic entry, connections with those peers fail and the debugs as shown appears.

```
IKEv1]: Group = x.x.x.x, IP = x.x.x.x, QM FSM error (P2 struct &0x49ba5a0, mess id 0xcd600
```

```
[IKEv1]: Group = x.x.x.x, IP = x.x.x.x, Removing peer from correlator table failed, no mat
```

Note: Only one Dynamic Crypto−map is allowed for each interface in the Security Appliance.

Here is an example of a properly numbered crypto map that contains a static entry and a dynamic entry. Note that the dynamic entry has the highest sequence number and room has been left to add additional static entries:

```
crypto dynamic-map cisco 20 set transform-set myset
crypto map mymap 10 match address 100
crypto map mymap 10 set peer 172.16.77.10
crypto map mymap 10 set transform-set myset
crypto map mymap interface outside
crypto map mymap 60000 ipsec-isakmp dynamic cisco
```

Note: Crypto map names are case−sensitive.

Note: Verify the Crypto map is applied in the right interface in which the IPsec tunnel start/end.

In the scenarios where multiple VPN tunnels to be terminated in the same interface, we need to create crypto map with same name (only one crypto map is allowed per interface) but with a different sequence number. This holds true for the router, PIX, and ASA.

Refer to Configuring IPsec Between Hub and Remote PIXes with VPN Client and Extended Authentication for more information in order to learn more about the hub PIX configuration for the same crypto map with the different sequence numbers on the same interface. Similarly, refer to PIX/ASA 7.X : Add a New Tunnel or Remote Access to an Existing L2L VPN for more information in order to learn more about the crypto map configuration for both L2L and Remote Access VPN scenarios.

Verify the Peer IP Address is Correct

For a PIX/ASA Security Appliance 7.x LAN−to−LAN (L2L) IPsec VPN configuration, you must specify the **<name>** of the tunnel group as the**Remote peer IP Address**(remote tunnel end) in the **tunnel−group <name> type ipsec−l2l** command for the creation and management of the database of connection−specific records for IPsec. The peer IP address must match in **tunnel group name** and the **Crypto map set address** commands. While you configure the VPN with ASDM, it generated the tunnel group name automatically with right peer IP address. If the peer IP Address is not configured properly, the logs can contain this message, which can be resolved by proper configuration of the **Peer IP Address**.

```
[IKEv1]: Group = DefaultL2LGroup, IP = x.x.x.x,
ERROR, had problems decrypting packet, probably due to mismatched pre-shared key. Aborting
```

In PIX 6.x LAN−to−LAN (L2L) IPsec VPN configuration, the Peer IP address (remote tunnel end) must match **isakmp key address** and the **set peer** command in crypto map for a successful IPsec VPN connection.

Verify the Tunnel Group and Group Names

```
%PIX|ASA-3-713206: Tunnel Rejected: Conflicting protocols specified by
tunnel-group and group-policy
```

The message appears when a tunnel is dropped because the allowed tunnel specified in the group policy is different than the allowed tunnel in the tunnel−group configuration.

```
group-policy hf_group_policy attributes
  vpn-tunnel-protocol l2tp-ipsec

username hfremote attributes
  vpn-tunnel-protocol l2tp-ipsec
```

```
        Both lines should read:
           vpn-tunnel-protocol ipsec l2tp-ipsec
```

Enable IPSec In Default Group policy to the already Existing Protocols In Default Group Policy .

```
        group-policy DfltGrpPolicy attributes
            vpn-tunnel-protocol L2TP-IPSec IPSec webvpn
```

Disable XAUTH for L2L Peers

If a LAN−to−LAN tunnel and a Remote Access VPN tunnel are configured on the same crypto map, the LAN−to−LAN peer is prompted for XAUTH information, and the LAN−to−LAN tunnel fails.

Note: This issue only applies to Cisco IOS and PIX 6.x. whereas PIX/ASA 7.x is not affected by this issue since it uses tunnel−groups.

Use the **no−xauth** keyword when you enter the isakmp key, so the device does not prompt the peer for XAUTH information (username and password). This keyword disables XAUTH for static IPsec peers. Enter a command similar to this on the device that has both L2L and RA VPN configured on the same crypto map:

```
        router(config)#crypto isakmp key cisco123 address
            172.22.1.164 no-xauth
```

In the scenario where the PIX/ASA 7.x acts as the Easy VPN Server, the easy VPN client is unable to connect to headend because of the Xauth issue. Disable the user authentication in the PIX/ASA in order to resolve the issue as shown:

```
        ASA(config)#tunnel-group example-group type ipsec-ra
        ASA(config)#tunnel-group example-group ipsec-attributes
        ASA(config-tunnel-ipsec)#isakmp ikev1-user-authentication none
```

See the Miscellaneous section of this document in order to know more about the **isakmp ikev1−user−authentication** command.

Problem: VPN Clients are Unable to Connect with ASA/PIX

Cisco VPN Clients are unable to authenticate when the X−auth is used with the Radius server.

Solution

The problem can be that the xauth times out. Increase the timeout value for AAA server in order to resolve this issue.

For example:

```
        Hostname(config)#aaa-server test protocol radius
        hostname(config-aaa-server-group)#aaa-server test host 10.2.3.4
        hostname(config-aaa-server-host)#timeout 10
```

Problem: VPN Client Drops Connection Frequently on First Attempt or "Security VPN Connection terminated by tier. Reason 433."

Cisco VPN Client users might receive this error when they attempt the connection with the head end VPN device.

"Attempted to assign network or broadcast IP address, removing (x.x.x.x) from pool" or "VPN client drops connection frequently on first attempt" or "Security VPN Connection terminated by tier. Reason 433."

Solution

The problem might be with the IP pool assignment either through ASA/PIX or Radius server. Use the **debug crypto** command in order to verify that the netmask and IP addresses are correct. Also, verify that the pool does not include the network address and the broadcast address. Radius servers must be able to assign the proper IP addresses to the clients.

Problem: Remote Access and EZVPN Users Connect to VPN but Cannot Access External Resources

Remote access users have no Internet connectivity once they connect to the VPN.

Remote access users cannot access resources located behind other VPNs on the same device.
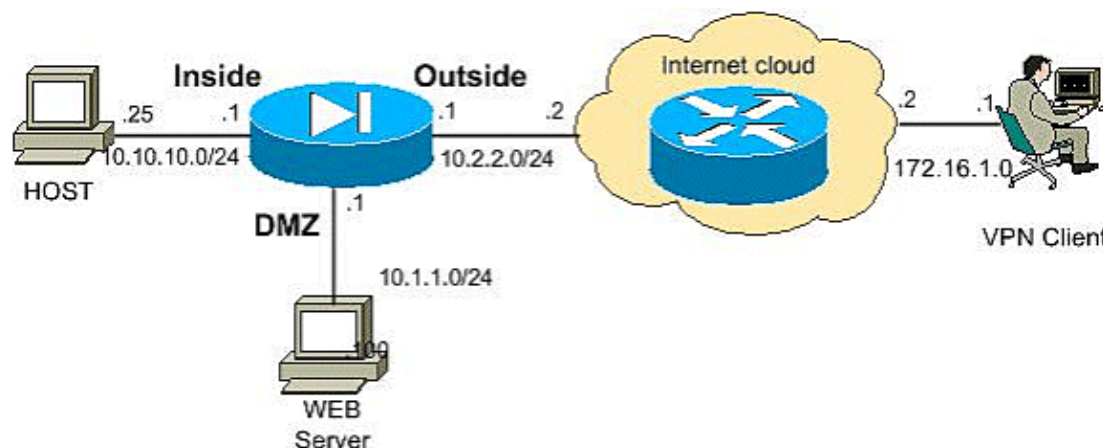
Remote access users can only access the local network.

Solutions

Unable to Access the Servers in DMZ

Once the VPN Client is established the IPsec tunnel with the VPN head−end device (PIX/ASA/IOS Router), the VPN Client users are able to access the INSIDE network (10.10.10.0/24) resources, but they are unable to access the DMZ network (10.1.1.0/24). .

Diagram 1 :

Check that the Split Tunnel, NO NAT configuration is added in the head−end device to access the resources in the DMZ network.

Example 1:

ASA/PIX

```
ciscoasa#show running-config


!--- Split tunnel for the inside network access

access-list vpnusers_spitTunnelAcl permit ip 10.10.10.0 255.255.0.0 any


!--- Split tunnel for the DMZ network access

access-list vpnusers_spitTunnelAcl permit ip 10.1.1.0 255.255.0.0 any


!--- Create a pool of addresses from which IP addresses are assigned
!--- dynamically to the remote VPN Clients.

ip local pool vpnclient 192.168.1.1-192.168.1.5


!--- This access list is used for a nat zero command that prevents
!--- traffic which matches the access list from undergoing NAT.

!--- No Nat for the DMZ network.


access-list nonat-dmz permit ip  10.1.1.0 255.255.255.0  192.168.1.0 255.255.255.0


!--- No Nat for the Inside network.

access-list nonat-in permit ip  10.10.10.0 255.255.255.0  192.168.1.0 255.255.255.0


!--- NAT 0 prevents NAT for networks specified in the ACL nonat

.
nat (DMZ) 0 access-list nonat-dmz
nat (inside) 0 access-list nonat-in
```
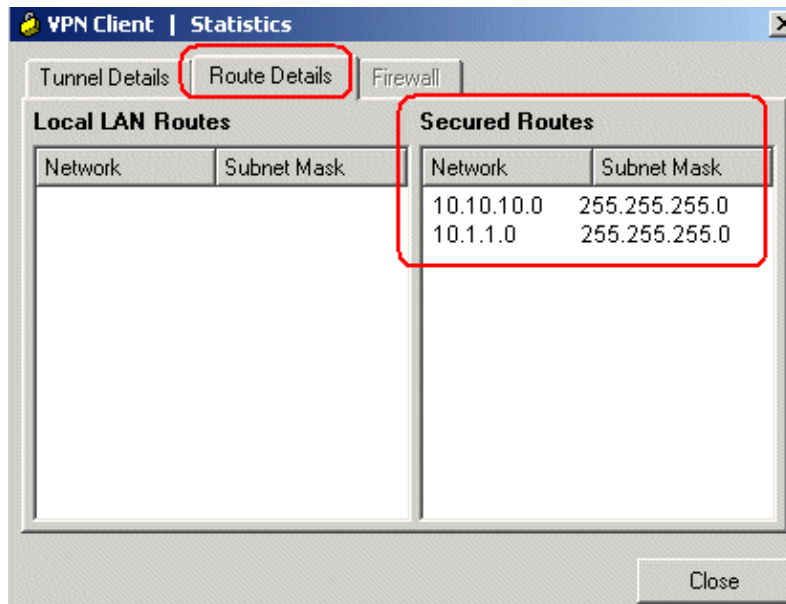
After you add a new entry for the NAT configuration, clear the Nat translation.

```
        Clear xlate
        Clear local
```

Verify :

If the tunnel has been established, go to the **Cisco VPN Client** and choose **Status > Route Details** to check that the secured routes are shown for both the DMZ and INSIDE networks.

Refer to PIX/ASA 7.x: Mail Server Access on the DMZ Configuration Example for more information on how to set up the PIX Firewall for access to a mail server located on the Demilitarized Zone (DMZ) network.

Refer to PIX/ASA 7.x : Add a New Tunnel or Remote Access to an Existing L2L VPN in order to provide the steps required to add a new VPN tunnel or a remote access VPN to a L2L VPN configuration that already exists.

Refer to PIX/ASA 7.x: Allow Split Tunneling for VPN Clients on the ASA Configuration Example ↗ in order to provide step−by−step instructions on how to allow VPN Clients access to the Internet while they are tunneled into a Cisco Adaptive Security Appliance (ASA) 5500 Series Security Appliance.

Refer to PIX/ASA 7.x and Cisco VPN Client 4.x with Windows 2003 IAS RADIUS (Against Active Directory) Authentication Configuration Example for more information on how to set up the remote access VPN connection between a Cisco VPN Client (4.x for Windows) and the PIX 500 Series Security Appliance 7.x.

VPN Clients Unable to Resolve DNS

After the tunnel has been established, if the VPN Clients are unable to resolve the DNS, the problem can be the DNS Server configuration in the head−end device (ASA/PIX). Also check the connectivity between the VPN Clients and the DNS Server. The DNS Server configuration must be configured under the group policy and applied under the the group policy in the tunnel−group general attributes, for example:

```
!--- Create the group policy named vpn3000 and
!--- specify the DNS server IP address(172.16.1.1)
!--- and the domain name(cisco.com) in the group policy.

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


!--- Associate the group policy(vpn3000) to the tunnel group
!--- using the default-group-policy.

tunnel-group vpn3000 general-attributes
 default-group-policy vpn3000
```

VPN clients unable to connect internal servers by name

The VPN client is unable to ping the hosts or servers of the remote or head end internal network by name. You need to enable the split−dns configure on ASA in order to resolve this issue.

Split−tunnel Unable to access Internet or excluded networks

Split tunneling lets remote−access IPsec clients conditionally direct packets over the IPsec tunnel in encrypted form or direct packets to a network interface in cleartext form, decrypted, where they are then routed to a final destination. Split−tunneling is disabled by default, which is `tunnelall` traffic.

        split-tunnel-policy {tunnelall | tunnelspecified | excludespecified}

Note: The option *excludespecified* is supported only for Cisco VPN clients, not EZVPN clients.

        ciscoasa(config-group-policy)#**split-tunnel-policy excludespecified**

Refer to these documents for detailed configuration examples of split−tunneling:

- PIX/ASA 7.x: Allow Split Tunneling for VPN Clients on the ASA Configuration Example
- Router Allows VPN Clients to Connect IPsec and Internet Using Split Tunneling Configuration Example
- Split Tunneling for VPN Clients on the VPN 3000 Concentrator Configuration Example

Hairpinning

This feature is useful for VPN traffic that enters an interface but is then routed out of that same interface. For example, if you have a hub and spoke VPN network, where the security appliance is the hub and remote VPN networks are spokes, in order for one spoke to communicate with another spoke, traffic must go into the security appliance and then out again to the other spoke.

Use the **same−security−traffic** configuration to allow traffic to enter and exit the same interface.

        securityappliance(config)# **same-security-traffic permit intra-interface**

Local LAN Access

Remote access users connect to the VPN and are able to connect to local network only.

For a more detailed configuration example, refer to PIX/ASA 7.x: Allow local LAN access for VPN clients.

Overlapping Private Networks

Problem

If you are unable to access the internal network after the tunnel establishment, check the IP address assigned to the VPN client that overlaps with the internal network behind the head−end device.

Solution 1

Always make sure that the IP addresses in the pool to be assigned for the VPN clients, the internal network of the head−end device and the VPN Client internal network must be in different networks. You can assign the same major network with different subnets, but sometimes the routing issues occur.

For further examples, refer to Diagram 1 and Example 1 of the Unable to Access the Servers in DMZ section.

Problem: Unable to Connect More Than Three VPN Client Users

Only three VPN clients can connect to ASA/PIX; connection for the fourth client fails. Upon failure, this error message is displayed:

```
Secure VPN Connection terminated locally by the client.
        Reason 413: User Authentication failed.

tunnel rejected; the maximum tunnel count has been reached
```

Solutions

In most cases, this issue is related to a simultaneous login setting within group policy and the maximum session−limit. For more information, refer to the Configuring Group Policies section of Selected ASDM VPN Configuration Procedures for the Cisco ASA 5500 Series, Version 5.2.
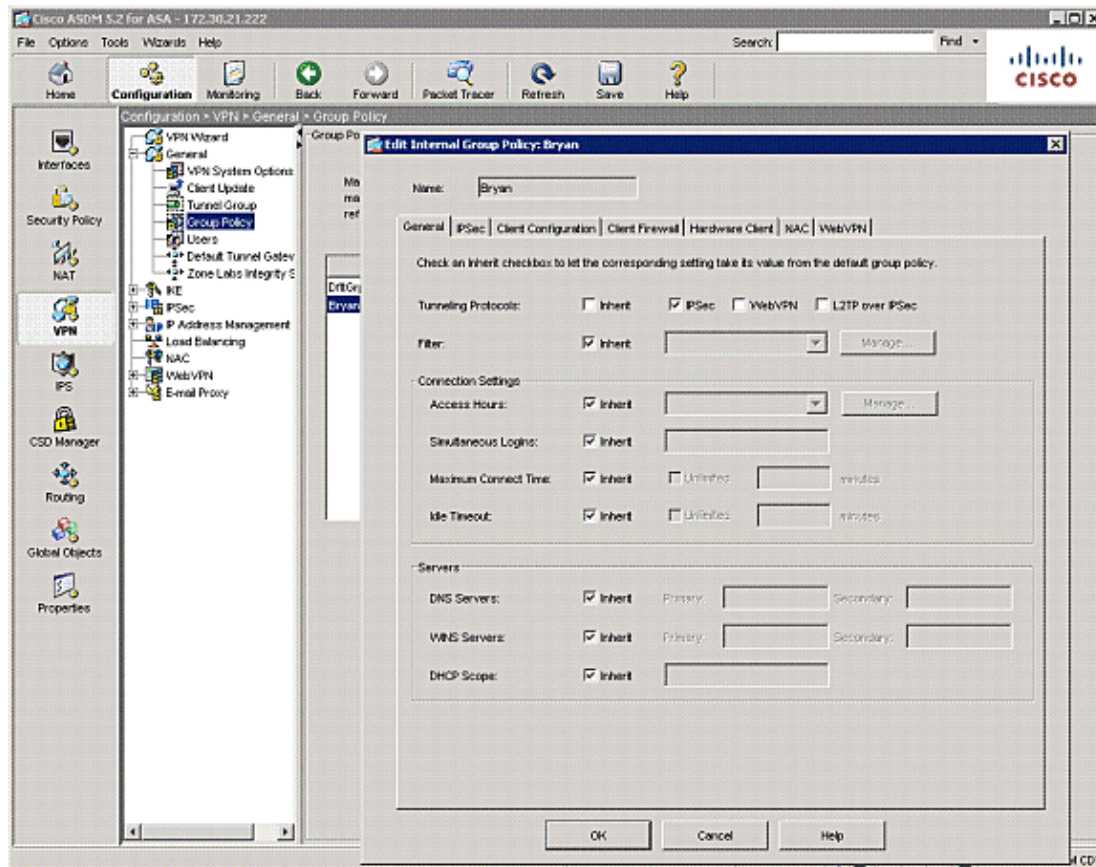
Configure Simultaneous Logins

If the **Inherit** check box is chosen in ASDM, only the default number of simultaneous logins is allowed for the user. The default value for simultaneous logins is three.

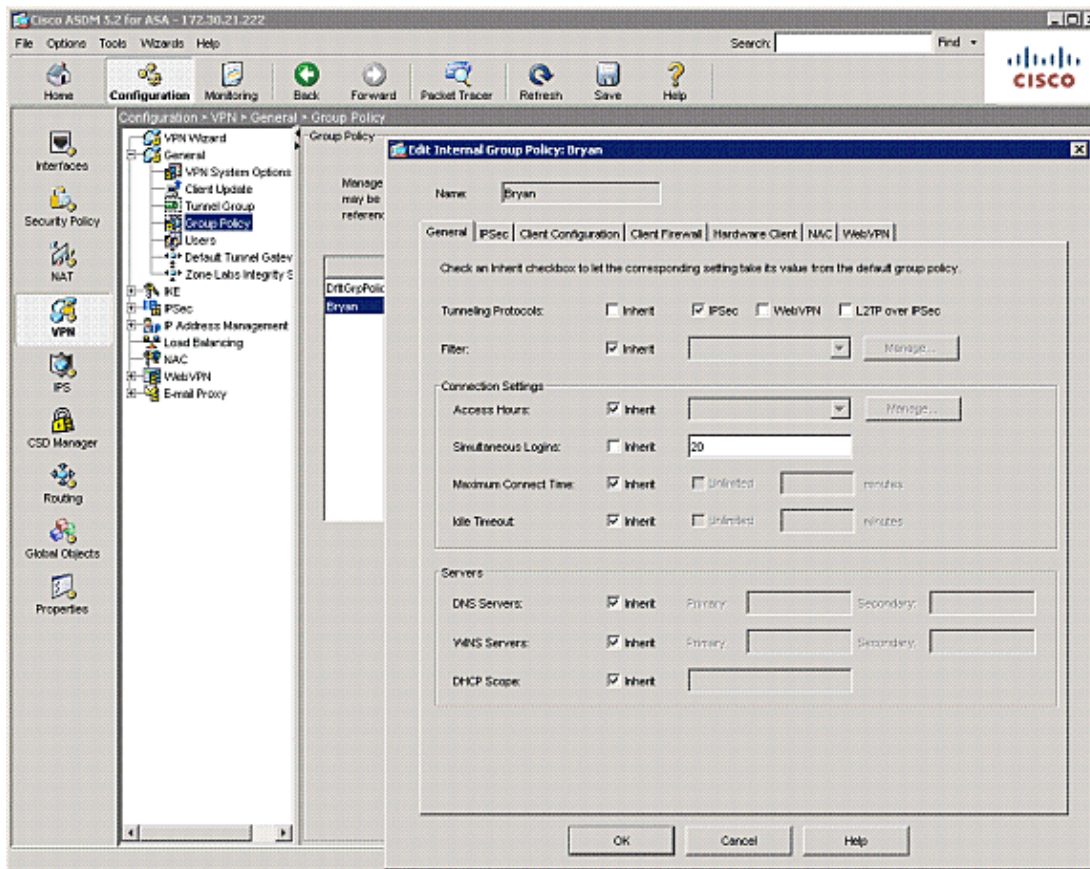In order to resolve this issue, increase the value for simultaneous logins.

Launch ASDM and then navigate to **Configuration > VPN > Group Policy**.
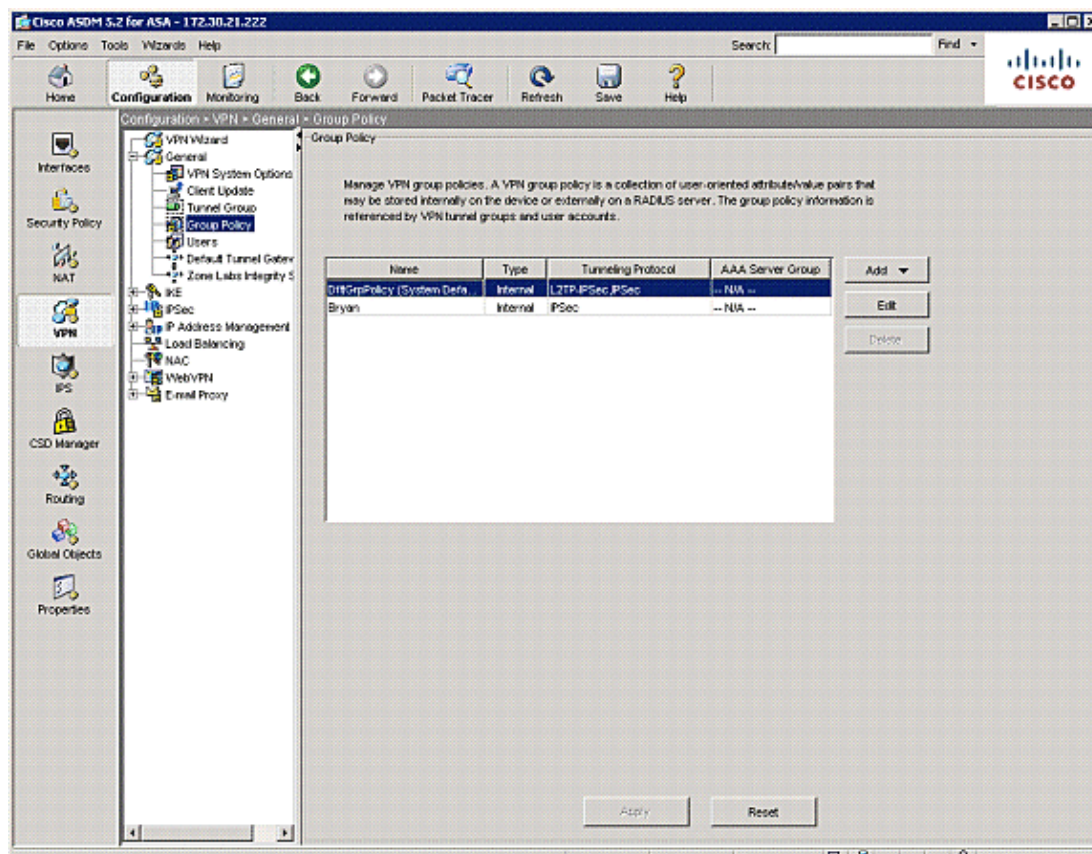
Choose the appropriate **Group** and click the **Edit** button.

Once in the **General** tab, undo the **Inherit** check box for **Simultaneous Logins** under **Connection Settings**. Choose an appropriate value in the field.

Note: The minimum value for this field is 0, which disables login and prevents user access.

Configure the ASA/PIX with CLI

Complete these steps in order to configure the desired number of simultaneous logins. In this example, 20 was chosen as the desired value.

```
ciscoasa(config)#group-policy Bryan attributes
ciscoasa(config-group-policy)#vpn-simultaneous-logins 20
```

In order to learn more about this command, refer to Cisco Security Appliance Command Reference, Version 7.2.

Use the **vpn−sessiondb max−session−limit** command in global configuration mode in order to limit VPN sessions to a lower value than the security appliance allows. Use the `no` version of this command in order to remove the session limit. Use the command again in order to overwrite the current setting.

```
vpn-sessiondb max-session-limit {session-limit}
```

This example shows how to set a maximum VPN session limit of 450:

```
hostname#vpn-sessiondb max-session-limit 450
```

Configure Concentrator

Error Message

```
20932 10/26/2007 14:37:45.430 SEV=3 AUTH/5 RPT=1863 10.19.187.229
Authentication rejected: Reason = Simultaneous logins exceeded for user
```

```
handle = 623, server = (none), user = 10.19.187.229, domain = <not
specified>
```

Solution

Complete these steps in order to configure the desired number of simultaneous logins. You can also try to set the Simultaneous Logins to 5 for this SA:

Choose **Configuration > User Management > Groups > Modify 10.19.187.229 > General > Simultaneouts Logins** and change the number of logins to **5**.

Problem: Unable to Initiate the Session or an Application and Slow transfer after the Tunnel Establishment

After the IPsec tunnel establishment, the application or the session does not initiate across the tunnel.

Solutions

Use the **ping** command to check the network or find whether the application server is reachable from your network. It can be a problem with the maximum segment size (MSS) for transient packets that traverse a router or PIX/ASA device, specifically TCP segments with the SYN bit set.

Cisco IOS Router Change the MSS Value in the Outside Interface (Tunnel End Interface) of the Router

Run these commands in order to change the MSS value in the outside interface (tunnel end interface) of the router:

```
Router>enable
Router#configure terminal
Router(config)#interface ethernet0/1
Router(config-if)#ip tcp adjust-mss 1300
Router(config-if)#end
```

These messages show the debug output for TCP MSS:

```
Router#debug ip tcp transactions

Sep 5 18:42:46.247: TCP0: state was LISTEN -> SYNRCVD [23 -> 10.0.1.1(38437)]
Sep 5 18:42:46.247: TCP: tcb 32290C0 connection to 10.0.1.1:38437, peer MSS 1300, MSS is
1300
Sep 5 18:42:46.247: TCP: sending SYN, seq 580539401, ack 6015751
Sep 5 18:42:46.247: TCP0: Connection to 10.0.1.1:38437, advertising MSS 1300
Sep 5 18:42:46.251: TCP0: state was SYNRCVD -> ESTAB [23 -> 10.0.1.1(38437)]
```

The MSS gets adjusted to 1300 on the router as configured.

For more information, refer to PIX/ASA 7.x and IOS: VPN Fragmentation.

PIX/ASA 7.X Refer to PIX/ASA Documentation

There is an inability to access the Internet properly or slow transfer through the tunnel because it gives the MTU size error message and MSS issues. Refer to these documents in order to resolve the issue:

- PIX/ASA 7.x and IOS: VPN Fragmentation
- PIX/ASA 7.0 Issue: MSS Exceeded – HTTP Clients Cannot Browse to Some Web Sites

Problem: Unable to Initiate VPN Tunnel from ASA/PIX

You are unable to initiate the VPN tunnel from ASA/PIX interface, and after the tunnel establishment, the remote end/VPN Client is unable to ping the inside interface of ASA/PIX on the VPN tunnel. For example, the pn client can be unable to initiate a SSH or HTTP connection to ASA's inside interface over VPN tunnel.

Solution

The inside interface of the PIX cannot be pinged from the other end of the tunnel unless the **management–access** command is configured in the global configuration mode.

```
PIX-02(config)#management-access inside

PIX-02(config)#show management-access
management-access inside
```

Note: This command also helps in initiating a ssh or http connection to inside interface of ASA through a VPN tunnel.

Note: This infomation holds true for DMZ interface as well., for example, if you want to ping the DMZ interface of PIX/ASA or want to initiate a tunnel from DMZ interface, then the **management–access DMZ** command is required.

```
PIX-02(config)#management-access DMZ
```

Note: If the VPN client is unable to connect, then make sure ESP and UDP ports are open, however if those ports are not open then try to connect on TCP 10000 with the selection of this port under the VPN client connection entry. Right click **modify > transport tab > IPsec over TCP**.

Problem: Error :– %ASA–5–713904: Group = DefaultRAGroup, IP = x.x.x.x, Client is using an unsupported Transaction Mode v2 version.Tunnel terminated.

The `%ASA-5-713904: Group = DefaultRAGroup, IP = 99.246.144.186, Client is using an unsupported Transaction Mode v2 version.Tunnel terminated` error message appears.

Solution

The reason for the `Transaction Mode v2` error message is that ASA supports only IKE Mode Config V6 and not the old V2 mode version. So use the IKE Mode Config V6 version in order to resolve this error.

Problem: Error:– %ASA–6–722036: Group client–group User xxxx IP x.x.x.x Transmitting large packet 1220 (threshold 1206)

The `%ASA-6-722036: Group < client-group > User < xxxx > IP < x.x.x.x>`
`Transmitting large packet 1220 (threshold 1206)` error message appears in the logs of
ASA. What does this log means and how this can be resolved?

Solution

This log message states that a large packet was sent to the client. The source of the packet is not aware of the
MTU of the client. This can also be due to compression of non–compressible data. The workaround is to turn
off the SVC compression with the **svc compression none** command. This resolves the issue.

Problem: ERROR: The authentication–server–group none command has been deprecated

If you transfer the VPN configuration from the PIX/ASA that runs Version 7.0.x to the another security
appliance that runs 7.2.x, you receive this error message:

```
ERROR: The authentication-server-group none command has been deprecated.
The "isakmp ikev1-user-authentication none" command in the ipsec-attributes should be used
instead.
```

Solution

The command **authentication–server–group** is no longer supported in 7.2(1) and later. This command was
deprecated and moved to tunnel–group general–attributes configuration mode.

Refer to the isakmp ikev1–user–authentication section of the command reference for more information about
this command.

Problem: Error Message when QoS is Enabled in one End of the VPN Tunnel

If you enabled QoS in one end of the VPN Tunnel, you might receive this error message:

```
IPSEC: Received an ESP packet (SPI= 0xDB6E5A60, sequence number= 0x7F9F) from
10.18.7.11 (user= ghufhi) to 172.16.29.23 that failed anti-replay checking
```

Solution

This message is normally caused when one end of the tunnel is doing QoS. This happens when a packet is
detected as being out of order. You can disable QoS to stop this but it can be ignored as long as traffic is able
to traverse the tunnel.

Problem: WARNING: crypto map entry will be incomplete

When you enter this command, you can get the error message as shown in the output.

```
ciscoasa(config)#crypto map mymap 20 ipsec-isakmp
WARNING: crypto map entry will be incomplete
```

Solution

This is a usual warning when you define a new crypto map, a reminder that parameters such as access–list (match address), transform set and peer address must be configured before it can work. It is also normal that the first line you type in order to define the crypto map does not show in the configuration.

Problem: Error:– %ASA–4–400024: IDS:2151 Large ICMP packet from to on interface outside

Unable to pass large ping packet across the vpn tunnel.When we try to pass large ping packets we get the error `%ASA-4-400024: IDS:2151 Large ICMP packet from to on interface outside`

Solution

This issue can be resolved by disabling the signatures 2150 and 2151.Once the signatures are disabled ping works fine.Use the following commands to disable the signatures:

ASA(config)# ip audit signature 2151 disable

ASA(config)# ip audit signature 2150 disable

Problem: Error:– %PIX|ASA–4–402119: IPSEC: Received a protocol packet (SPI=spi, sequence number= seq_num) from remote_IP (username) to local_IP that failed anti–replay checking.

I received this error in the log messages of the ASA:

```
Error:- %PIX|ASA-4-402119: IPSEC: Received a protocol packet (SPI=spi,
sequence number= seq_num) from remote_IP (username) to local_IP that
failed anti-replay checking.
```

Solution

In order to resolve this error, use the **crypto ipsec security–association replay window–size** command in order to vary the window size.

```
        hostname(config)#crypto ipsec security-association replay window-size 1024
```

Note: Cisco recommends that you use the full 1024 window size to eliminate any anti–replay problems.

Miscellaneous

AG_INIT_EXCH Message Appears in the "show crypto isakmp sa" and "debug" Commands Output

If the tunnel does not get initiated, the `AG_INIT_EXCH` message appears in output of the **show crypto isakmp sa** command and in **debug** output as well. The reason can be due to mismatching isakmp policies or if

port udp 500 gets blocked on the way.

Debug Message "Received an IPC message during invalid state" Appears

This error has nothing to do with the disconnection of the VPN tunnel and is more like an informational message.

NetPro Discussion Forums – Featured Conversations

Networking Professionals Connection is a forum for networking professionals to share questions, suggestions, and information about networking solutions, products, and technologies. The featured links are some of the most recent conversations available in this technology.

NetPro Discussion Forums – Featured Conversations for Security
Security: Intrusion Detection [Systems]
Security: AAA
Security: General
Security: Firewalling

Related Information

- **PIX/ASA 7.0 Issue: MSS Exceeded – HTTP Clients Cannot Browse to Some Web Sites**
- **PIX/ASA 7.x and IOS: VPN Fragmentation**
- **Cisco ASA 5500 Series Security Appliances**
- **Cisco PIX 500 Series Security Appliances**
- **IPsec Negotiation/IKE Protocols**
- **Cisco VPN 3000 Series Concentrators**
- **Technical Support & Documentation – Cisco Systems**

Updated: Apr 28, 2009   Document ID: 81824