

# Troubleshoot Common L2L and Remote Access IPsec VPN Issues

## Contents

---

[Introduction](#)

[Background Information](#)

[Prerequisites](#)

[IPsec VPN Configuration Does Not Work](#)

[VPN Clients are Unable to Connect with ASA](#)

[VPN Client Drops Connection Frequently on First Attempt or "Security VPN Connection terminated by peer. Reason 433." or "Secure VPN Connection terminated by Peer Reason 433:\(Reason Not Specified by Peer\)"](#)

[Remote Access and EZVPN Users Connect to VPN but Cannot Access External Resources](#)

[Unable to Connect More Than Three VPN Client Users](#)

[Unable to Initiate the Session or an Application and Slow Transfer after the Tunnel Establishment](#)

[Unable to Initiate VPN Tunnel from ASA](#)

[Unable to Pass Traffic Across VPN Tunnel](#)

[Configure Backup peer for vpn tunnel on same crypto map](#)

[Disable/Restart VPN Tunnel](#)

[Some Tunnels not Encrypted](#)

[Error:- %ASA-5-713904: Group = DefaultRAGroup, IP = x.x.x.x, ...unsupported Transaction Mode v2 version.Tunnel terminated.](#)

[Error:- %ASA-6-722036: Group client-group User xxxx IP x.x.x.x Transmitting large packet 1220 \(threshold 1206\)](#)

[Error Message when QoS is Enabled in one End of the VPN Tunnel](#)

[WARNING: crypto map entryincomplete](#)

[Error:- %ASA-4-400024: IDS:2151 Large ICMP packet from to on interface outside](#)

[Error:- %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 check.](#)

[Error Message - %ASA-4-407001: Deny traffic for local-host interface name:inside address, license limit of number exceeded](#)

[Error Message - %VPN HW-4-PACKET ERROR:](#)

[Error message: Command rejected: delete crypto connection between VLAN XXXX and XXXX, first.](#)

[Error Message - % FW-3-RESPONDER WND\\_SCALE\\_INI\\_NO\\_SCALE: Dropped packet - Invalid Window Scale option for session x.x.x.x:27331 to x.x.x.x:23 \[Initiator\(flag 0,factor 0\) Responder \(flag 1, factor 2\)\]](#)

[%ASA-5-305013: Asymmetric NAT rules matched for forward and reverse . Please update this issue flows](#)

[%ASA-5-713068: Received non-routine Notify message: notify\\_type](#)

[%ASA-5-720012: \(VPN-Secondary\) Failed to update IPsec failover runtime data on the standby unit \(or\) %ASA-6-720012: \(VPN-unit\) Failed to update IPsec failover runtime data on the standby unit](#)

[Error:- %ASA-3-713063: IKE Peer address not configured for destination 0.0.0.0](#)

---

[Error: %ASA-3-752006: Tunnel Manager failed to dispatch a KEY\\_ACQUIRE message.](#)

[Error: %ASA-4-402116: IPSEC: Received an ESP packet \(SPI= 0x99554D4E, sequence number= 0x9E\) from XX.XX.XX.XX \(user= XX.XX.XX.XX\) to YY.YY.YY.YY](#)

[Failed to launch 64-bit VA installer to enable the virtual adapter due to error 0xffffffff](#)

[Cisco VPN Client Does Not Work with Data Card on Windows 7](#)

[Alert: "VPN functionality may not work at all"](#)

[IPSec Padding error](#)

[VPN tunnel gets disconnected after every 18 hours](#)

[Traffic flow is not maintained after the LAN to LAN tunnel is re-negotiated](#)

[Error message states that Bandwidth reached for the Crypto functionality](#)

[Problem: Outbound encryption traffic in an IPsec tunnel fails, even if inbound decryption traffic works.](#)

[Miscellaneous](#)

[Related Information](#)

---

## Introduction

This document describes the most common solutions to IPsec VPN problems.

## Background Information

The solutions described here come directly from service requests that the Cisco Technical Support have solved.

Many of these solutions are implemented prior to the in-depth troubleshooting of an IPsec VPN connection.

This document provides a summary of common procedures to try before you begin to troubleshoot a connection.

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

Refer to [IP Security Troubleshooting - Understanding and Using debug Commands](#) for an explanation of common debug commands that are used to troubleshoot IPsec issues on both the Cisco IOS<sup>®</sup> software and .

**Note:** ASA does not pass multicast traffic over IPsec VPN tunnels.

**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 knowledge of IPsec VPN configuration on these Cisco devices:

- Cisco ASA 5500 Series Security Appliance
- Cisco IOS® Routers

## Components Used

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

- Cisco ASA 5500 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, ensure that you understand the potential impact of any command.

## Conventions

Refer to [Cisco Technical Tips Conventions](#) for more information on document conventions.

# IPsec VPN Configuration Does Not Work

## Problem

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 remediation.

All of these solutions come directly from TAC service requests and have resolved numerous issues.

- [Enable NAT-Traversal \(#1 RA VPN Issue\)](#)
- [Test Connectivity Properly](#)
- [Enable ISAKMP](#)
- [Enable/Disable PFS](#)
- [Clear Old or Existing Security Associations \(Tunnels\)](#)
- [Verify ISAKMP Lifetime](#)
- [Enable or Disable ISAKMP Keepalives](#)
- [Re-Enter or Recover Pre-Shared-Keys](#)
- [Mismatched Pre-shared Key](#)

- [Remove and Re-apply Crypto Maps](#)
- [Verify that sysopt Commands are Present \(/ASA Only\)](#)
- [Verify the ISAKMP Identity](#)
- [Verify Idle/Session Timeout](#)
- [Verify that ACLs are Correct and are Bound to Crypto Map](#)
- [Verify the ISAKMP Policies](#)
- [Verify that Routing is Correct](#)
- [Verify that Transform-Set is Correct](#)
- [Verify Crypto Map Sequence Numbers and Name](#)
- [Verify the Peer IP Address is Correct](#)
- [Verify the Tunnel Group and Group Names](#)
- [Disable XAUTH for L2L Peers](#)
- [VPN Pool Getting Exhausted](#)
- [Issues with latency for VPN client traffic](#)

**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 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 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 twenty (20) in this example is the keepalive time (default).

**ASA**

```
<#root>
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, navigate to **Connection Entries** and click **Modify**. It opens a new window where you have to choose the **Transport** tab.

Under this tab, click **Enable Transparent Tunneling** and the **IPSec over UDP ( NAT / PAT )** radio button. Then click **Save** and test the connection.

It is important to allow the UDP 4500 for NAT-T, UDP 500 and ESP ports by the configuration of an ACL because the 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 ASA.

## 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. This is one 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, **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.

**ping** sourced from the outside 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:

```
<#root>
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 ASA security appliances. The **ping** which is used to test connectivity can also be sourced from the inside interface with the **inside** keyword:

```

<#root>

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

```

It is not recommended to 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.

```

<#root>

securityappliance(config)#

management-access inside

```

When a problem exists with the connectivity, even phase one (1) of VPN does not function.

On the ASA, if connectivity fails, the SA output is similar to this example, which indicates a possible

incorrect crypto peer configuration and/or incorrect ISAKMP proposal configuration:

```
<#root>

Router#

show crypto isakmp sa

1  IKE Peer: XX.XX.XX.XX
   Type      : L2L                Role      : initiator
   Rekey     : no                 State     : MM_WAIT_MSG2
```

The state can be from **MM\_WAIT\_MSG2** to **MM\_WAIT\_MSG5**, which denotes failure of concerned state exchange in **Main Mode (MM)**.

**Crypto SA** output when the phase 1 is up is similar to this example:

```
<#root>

Router#

show crypto isakmp sa

1  IKE Peer: XX.XX.XX.XX
   Type      : L2L                Role      : initiator
   Rekey     : no                 State     : MM_ACTIVE
```

## Enable ISAKMP

If there is no indication that an IPsec VPN tunnel works, it possible 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®

```
<#root>

router(config)#

crypto isakmp enable
```

Cisco ASA (replace **outside** with your desired interface)

```
<#root>

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 gets PAT 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.

Verify that UDP 500 and 4500 port numbers are reserved for the negotiation of ISAKMP connections with the peer.

When the ISAKMP is not enabled on the interface, the VPN client shows an error message similar to this message:

```
Secure VPN connection terminated locally by client.
Reason 412: The remote peer is no longer responding
```

In order to resolve this error, enable the ISAKMP on the crypto interface of the VPN gateway.

## 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 ASA / Cisco IOS® router.

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

### 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.

```
<#root>
hostname(config-group-policy)#
pfs {enable | disable}
```

In order to remove the PFS attribute from the 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 transfer of a value.

```
<#root>
hostname(config-group-policy)#
no pfs
```

### Cisco IOS® Router:

In order to specify that IPsec must ask for PFS when new **Security Associations** are requested for this crypto map entry, use the **set pfs** command in crypto map configuration mode.

In order to specify 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:

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

### Clear Old or Current Security Associations (Tunnels)

If this error message occurs in the Cisco 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.

```
<#root>
```

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

If you clear ISAKMP (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.

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 Cisco IOS®

```
<#root>
router#
show crypto isakmp sa
router#
show crypto ipsec sa
```

### b. Cisco ASA Security Appliances

```
<#root>
securityappliance#
show crypto isakmp sa
securityappliance#
show crypto ipsec sa
```

## 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)

```
<#root>
router#
clear crypto isakmp
?
  <0 - 32766> connection id of SA
  <cr>
```

### b. IPsec (Phase II)

```
<#root>
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 ASA Security Appliances

### a. ISAKMP (Phase I)

```
<#root>
securityappliance#
clear crypto isakmp sa
```

### b. IPsec (Phase II)

```
<#root>
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 receive the **%ASA-5-713092: Group = x.x.x.x, IP = x.x.x.x, Failure during phase 1 rekey attempt due to collision** error message in /ASA.

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).

ASA

```
<#root>
hostname(config)#
isakmp policy 2 lifetime 14400
```

Cisco IOS® Router

```
<#root>
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 zero (0) in order to set the lifetime of an IKE security association to infinity. The VPN is always be connected and does not terminate.

```
hostname(config)#isakmp\_policy 2 lifetime 0
```

You can also **disable re-xauth in the group-policy** in order to resolve the issue.

## 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:

```
<#root>  
  
router(config)#  
  
crypto isakmp keepalive 15
```

Use these commands to configure ISAKMP keepalives on the **ASA Security Appliances**:

Cisco ASA for the tunnel group named **10.165.205.222**

```
<#root>  
  
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 ASA, for the tunnel group named **10.165.205.222**

Disable IKE keepalive processing, which is enabled by default.

```

<#root>

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

Navigate to %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.

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

### Re-Enter or Recover Pre-Shared-Keys

In many cases, a simple typographical error can be to blame when an IPsec VPN tunnel does not work. 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 Cisco VPN Client.

You can face this error if the group name or 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... possibly 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)
```

**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 remove crypto-related commands..

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 Cisco IOS®:

#### Cisco LAN-to-LAN VPN

```
<#root>

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

```
<#root>

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 /ASA Security Appliances:

#### Cisco 6.x

```
<#root>
```

```
(config)#
no isakmp key secretkey address 10.0.0.1
(config)#
isakmp key secretkey address 10.0.0.1
```

Cisco /ASA 7.x and later

```
<#root>
securityappliance(config)#
tunnel-group 10.0.0.1
  ipsec-attributes
securityappliance(config-tunnel-ipsec)#
no ikev1 pre-shared-key
securityappliance(config-tunnel-ipsec)#
ikev1

pre-shared-key
  secretkey
```

## Mismatched Pre-shared Key

The initiation of VPN Tunnel gets disconnected. This issue occurs because of a mismatched pre-shared-key during the phase I negotiations.

The **MM\_WAIT\_MSG\_6** message in the **show crypto isakmp sa** command indicates a mismatched pre-shared-key as shown in this example:

```
<#root>
ASA#
show crypto isakmp sa

Active SA: 1
Rekey SA: 0 (A tunnel reports 1 Active and 1 Rekey SA during rekey)
Total IKE SA: 1

1          IKE Peer: 10.7.13.20
           Type : L2L                               Role : initiator
           Rekey : no                               State :

MM_WAIT_MSG_6
```

In order to resolve this issue, re-enter the pre-shared key in both appliances; the pre-shared-key must be

unique and matched. See [Re-Enter or Recover Pre-Shared-Keys](#) for more information.

## 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 drops of VPN tunnel and failure of some VPN sites to come up.

**Warning:** If you remove a crypto map from an interface, it **definitely** brings down any IPsec tunnels associated with that crypto map. Cautiously proceed with these steps 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.

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

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

```
<#root>
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:

```
<#root>
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 ASA:

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

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

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

```
<#root>  
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:

```
<#root>  
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
```

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 (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 6.x, this functionality is **disabled** by default. With /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:

Cisco ASA

```
<#root>  
  
securityappliance#  
  
show running-config all 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 ASA

```
<#root>
securityappliance(config)#
  sysopt connection permit-vpn
```

If you do not wish to use the **sysopt connection** command, explicitly permit the required interesting traffic from source to destination.

For example, from Remote to Local LAN of remote device and "UDP port 500" for outside interface of remote device to outside interface of local device, in outside ACL.

## Verify the ISAKMP Identity

If the IPsec VPN tunnel has failed within the IKE negotiation, the failure can be due to either the 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 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
```

OR

```
crypto isakmp identity auto
!--- If the RA or L2L (site-to-site) VPN tunnels connect !--- with ISAKMP negotiation by connection
```

OR

```
crypto isakmp identity hostname
!--- Uses the fully-qualified domain name of !--- the host exchange ISAKMP identity information (C
```

VPN tunnel fails to come up after a shift of configuration from to ASA with the ASA configuration migration tool; these messages appear in the log:

```
[IKEv1]: Group = x.x.x.x, IP = x.x.x.x, Stale PeerTblEntry found, removing!  
[IKEv1]: Group = x.x.x.x, IP = x.x.x.x, Removing peer from correlator table failed, no match!  
[IKEv1]: Group = x.x.x.x, IP = x.x.x.x, construct_ipsec_delete(): No SPI to identify Phase 2 SA!  
[IKEv1]: Group = x.x.x.x, IP = x.x.x.x, Removing peer from correlator table failed, no match!
```

## 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 idle timeout parameter and encounters the `PEER_DELETE-IKE_DELETE_UNSPECIFIEDERROR`.

Configure **idle timeout** and **session timeout** as **none** in order to make the tunnel always **up**, and so that the tunnel is never dropped even when third party devices are used.

## ASA

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

```
<#root>  
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:

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

When you have **tunnel-all** configured, you do not need to configure **idle-timeout** because, even if you configure VPN-idle timeout, it does not work because all traffic goes through the tunnel (since tunnel-all is

configured).

Therefore, the interesting traffic (or even the traffic generated by the PC) is interesting and does not let Idle-timeout come into action.

## 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.

```
<#root>  
  
crypto ipsec security-association idle-time  
  
seconds
```

Time is measured 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 and Binded to Crypto Map

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-tunnel ACL in a Remote Access configuration.

When these ACLs are incorrectly configured or missed, traffic perhaps flows in one direction across the VPN tunnel, or not sent across the tunnel at all.

Make sure to bind the crypto ACL with crypto map with the **crypto map match address** command in global configuration mode.

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.

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 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, a Cisco 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

```

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,...).

In a VOIP environment, where the voice calls between networks are communicated through the VPN, the voice calls do not work if the NAT 0 ACLs are not properly configured.

Before troubleshooting, it is suggested to check the VPN connectivity status because the problem could be with misconfiguration of NAT exempt ACLs.

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

```

%ASA-3-305005: No translation group found for
udp src Outside:x.x.x.x/p dst Inside:y.y.y.y/p

```

### Incorrect Example:

```

<#root>

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
```

Although it is not illustrated here, this same concept applies to the ASA Security Appliances.

In ASA, 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.

Cisco IOS® routers can use extended ACL for split-tunnel. In the extended access list, to use **'any'** at the source in the split tunnel ACL is similar to disable split tunnel.

Use only the source networks in the extended ACL for split tunnel.

### Correct Example:

```
<#root>
access-list 140 permit ip
10.1.0.0 0.0.255.255
10.18.0.0 0.0.255.255
```

### Incorrect Example:

```
<#root>
access-list 140 permit ip
any
10.18.0.0 0.0.255.255
```

### Cisco IOS®

```
<#root>
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 ASA

```
<#root>

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
```

## NAT exemption configuration in ASA version 8.3 for site-to-site VPN tunnel:

A site-to-site VPN has to be established between HOASA and BOASA with both ASAs with version 8.3. The NAT exemption configuration on HOASA looks similar to this:

```
object network obj-local
subnet 192.168.100.0 255.255.255.0
object network obj-remote
subnet 192.168.200.0 255.255.255.0
nat (inside,outside) 1 source static obj-local obj-local destination static obj-remote objremote
```

## 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 to establish the tunnel with the remote-end device, check that **the two peers contain the same encryption, hash, authentication, and Diffie-Hellman parameter values.**

Verify 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.

```
"Error: Unable to remove Peer TblEntry, Removing peer from peer table failed, no match!"
```

Here is the detailed log message:

```
4|Mar 24 2010 10:21:50|713903: IP = X.X.X.X, Error: Unable to remove PeerTblEntry
3|Mar 24 2010 10:21:50|713902: IP = X.X.X.X, Removing peer from peer table failed,
no match!
3|Mar 24 2010 10:21:50|713048: IP = X.X.X.X, Error processing payload: Payload ID: 1
4|Mar 24 2010 10:21:49|713903: IP = X.X.X.X, Information Exchange processing failed
5|Mar 24 2010 10:21:49|713904: IP = X.X.X.X, Received an un-encrypted
NO_PROPOSAL_CHOSEN notify message, drop
```

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

In addition, this message appears:

```
Error Message %ASA-6-713219: Queueing KEY-ACQUIRE messages to be processed when
P1 SA is complete.
```

This message indicates that Phase 2 messages are in the queue after Phase 1 completes. This error message is due to one of these reasons:

- Mismatch in phase on any of the peers
- ACL blocks the peers from completion of phase 1

This message usually comes after the `Removing peer from peer table failed, no match!` error message.

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.

For the ISAKMP policy and IPsec Transform-set that is used on the 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

Be certain that your encryption devices such as Routers and ASA Security Appliances have the proper routing information to send traffic over your VPN tunnel.

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 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:

```
<#root>
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 an ASA, the configuration can look like this:

```
<#root>
```

```
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:

```

<#root>

crypto dynamic-map dynMAP 10
  set transform-set mySET

reverse-route

crypto map myMAP 60000 ipsec-isakmp dynamic dynMAP

```

Cisco ASA Security Appliance:

```

<#root>

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

```

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 .

## Verify 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.

For the ISAKMP policy and IPsec Transform-set that is used on the 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 and also that the Crypto map is applied in the right interface in which the IPsec tunnel start/end

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 0xcd600011)!

```

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

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:

```
<#root>

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 ciscothe
```

Crypto map names are case-sensitive.

This error message can also be seen when the dynamic crypto map sequence is not correct which causes the peer to hit the wrong crypto map.

This is also caused by a mismatched crypto access list that defines the interesting traffic:  
`%ASA-3-713042: IKE Initiator unable to find policy:`

In a scenario where multiple VPN tunnels to be terminated in the same interface, 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, and ASA.

Similarly, refer to [ASA: Add a New Tunnel or Remote Access to an Existing L2L VPN - Cisco](#) for more information about the crypto map configuration for both the L2L and Remote Access VPN scenario.

## Verify the Peer IP Address is Correct

Create and manage the database of connection-specific records for IPsec.

For a ASA Security Appliance LAN-to-LAN (L2L) IPsec VPN configuration, 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.

The peer IP address must match the `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

When the peer IP address has not been configured properly on the ASA crypto configuration, the ASA is not able to establish the VPN tunnel and hangs in the `MM_WAIT_MSG4` stage only.

In order to resolve this issue, correct the peer IP address in the configuration.

Here is the output of the `show crypto isakmp sa` command when the VPN tunnel hangs at in the `MM_WAIT_MSG4` state.

```
<#root>

hostname#

show crypto isakmp sa

1  IKE Peer: XX.XX.XX.XX
   Type      : L2L           Role      : initiator
   Rekey     : no           State     : MM_WAIT_MSG4
```

## Verify the Tunnel Group and Group Names

```
%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.

```
<#root>

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

username hfremote attributes
  vpn-tunnel-protocol l2tp-ipsec

Both lines 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 with "**CONF\_XAUTH**" in the output of the **show crypto isakmp sa** command.

Here is an example of the SA output:

```
<#root>

Router#

show crypto isakmp sa

IPv4 Crypto ISAKMP SA
dst          src          state          conn-id  slot  status
X.X.X.X      Y.Y.Y.Y      CONF_XAUTH     10223    0     ACTIVE
X.X.X.X      Z.Z.Z.Z      CONF_XAUTH     10197    0     ACTIVE
```

This issue only applies to Cisco IOS® whereas ASA 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:

```
<#root>

router(config)#

crypto isakmp key cisco123 address
  172.22.1.164 no-xauth
```

In the scenario where the ASA acts as the Easy VPN Server, the easy VPN client is unable to connect to head end because of the Xauth issue.

Disable the user authentication in the ASA in order to resolve the issue as shown:

```
<#root>

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.

## VPN Pool Getting Exhausted

When the range of IP addresses assigned to the VPN pool are not sufficient, you can extend the availability of IP addresses in two ways:

1. Remove the existing range, and define the new range. Here is an example:

```
<#root>
CiscoASA(config)#
no ip local pool testvpnpool 10.76.41.1-10.76.41.254
CiscoASA(config)#
ip local pool testvpnpool 10.76.41.1-10.76.42.254
```

2. When discontinuous subnets are to be added to the VPN pool, you can define two separate VPN pools and then specify them in order under the "tunnel-group attributes ". Here is an example:

```
<#root>
CiscoASA(config)#
ip local pool testvpnpoolAB 10.76.41.1-10.76.42.254
CiscoASA(config)#
ip local pool testvpnpoolCD 10.76.45.1-10.76.45.254
CiscoASA(config)#
tunnel-group test type remote-access
CiscoASA(config)#
tunnel-group test general-attributes
CiscoASA(config-tunnel-general)#
address-pool (inside) testvpnpoolAB testvpnpoolCD
CiscoASA(config-tunnel-general)#
exit
```

The order in which you specify the pools is very important because the ASA allocates addresses from these pools in the order in which the pools appear in this command.

The address-pools settings in the group-policy address-pools command always override the local pool settings in the tunnel-group address-pool command.

## Issues with Latency for VPN Client Traffic

When there are latency issues over a VPN connection, verify these conditions in order to resolve this:

1. Verify if the MSS of the packet can be reduced further.
2. If IPsec/tcp is used instead of IPsec/udp, then configure `preserve-vpn-flow`.
3. Re-load the Cisco ASA.

## VPN Clients are Unable to Connect with ASA

### Problem

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:

```
<#root>
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

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

### Solution

Initially, make sure that the authentication works properly. To narrow down the problem, first verify the authentication with local database on ASA.

```
tunnel-group tgroup general-attributes
    authentication-server-group none
    authentication-server-group LOCAL
exit
```

If this works fine, then the problem is related to Radius server configuration.

Verify the connectivity of the Radius server from the ASA. If the ping works without any problem, then check the Radius-related configuration on ASA and database configuration on the Radius server.

You could use the **debug radius** command to troubleshoot radius related issues. For sample **debug radius** output, refer to this [Sample Output](#).

Before you use the **debug** command on the ASA, refer to this documentation: [Warning message](#).

## **VPN Client Drops Connection Frequently on First Attempt or "Security VPN Connection terminated by peer. Reason 433." or "Secure VPN Connection terminated by Peer Reason 433:(Reason Not Specified by Peer)"**

### **Problem**

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

**VPN client drops connection frequently on first attempt**

**Security VPN Connection terminated by peer. Reason 433.**

**Secure VPN Connection terminated by Peer Reason 433:(Reason Not Specified by Peer)**

**Attempted to assign network or broadcast IP address, removing (x.x.x.x) from pool**

### **Solution 1**

The problem can be with the IP pool assignment either through ASA, Radius server, DHCP server or through Radius server which acts as DHCP 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.

### **Solution 2**

This issue also occurs due to the failure of extended authentication. You must check the AAA server to troubleshoot this error.

Check the server authentication password on Server and client. Reload the AAA server can resolve this issue.

### **Solution 3**

Another workaround for this issue is to disable the threat detection feature.

At times when there are multiple re-transmissions for different incomplete **Security Associations (SAs)**, the

ASA with the threat-detection feature enabled thinks that a scanning attack occurred and the VPN ports are marked as the main offender.

Try to disable the threat-detection feature as this can cause a lot of overhead on the processing of ASA. Use these commands in order to disable the threat detection:

```
no threat-detection basic-threat
no threat-detection scanning-threat shun
no threat-detection statistics
no threat-detection rate
```

This can be used as a workaround to verify if this fixes the actual problem.

Make sure that to disable the threat detection on the Cisco ASA actually compromises several security features such as mitigation of the **Scanning Attempts**, **DoS with Invalid SPI**, packets that fail **Application Inspection** , and **Incomplete Sessions**.

## Solution 4

This issue also occurs when a transform set is not properly configured. A proper configuration of the transform set resolves the issue.

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

## Problem

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 access only the local network.

## Solutions

Try these solutions in order to resolve this issue:

- [Unable to Access the Servers in DMZ](#)
- [VPN Clients Unable to Resolve DNS](#)
- [Split-Tunnel—Unable to access Internet or excluded networks](#)
- [Local LAN Access](#)
- [Overlapping Private Networks](#)

### Unable to Access the Servers in DMZ

Once the VPN client is established the IPsec tunnel with the VPN head-end device (ASA / Cisco 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

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

## Example:

### ASA configuration:

This configuration shows how to configure the NAT exemption for the DMZ network in order to enable the VPN users to access the DMZ network:

```
object network obj-dmz
 subnet 10.1.1.0 255.255.255.0
object network obj-vpnpool
 subnet 192.168.1.0 255.255.255.0
 nat (inside,dmz) 1 source static obj-dmz obj-dmz destination static obj-vpnpool obj-vpnpool
```

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 [ASA: Add a New Tunnel or Remote Access to an Existing L2L VPN - Cisco](#) for steps required to add a new VPN tunnel or a remote access VPN to a L2L VPN configuration that already exists.

Refer to [ASA: Allow Split Tunneling for VPN Clients on the ASA Configuration Example](#) for step-by-step instructions on how to allow VPN Clients access to the Internet while tunneled into a **Cisco 5500 Series Adaptive Security Appliance (ASA)**.

## 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).

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:

```
<#root>
```

```
!--- Create the group policy named vpn3000 and !--- specify the DNS server IP address(172.16.1.1)
```

```
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 !--- with 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 tunnel lets remote-access IPsec clients conditionally direct packets over the IPsec tunnel in encrypted form or to a network interface in cleartext form, decrypted, where they are routed to a final destination.

Split-tunnel is disabled by default, which is `tunnel all traffic`.

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

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-tunnel:

- [ASA: 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](#)

## Hairpin solution

This feature is useful for VPN traffic that enters an interface but is then routed out of that same interface.

For example, in a hub and spoke VPN network, where the security appliance is the hub and remote VPN networks are spokes, **spoke-to-spoke** communication 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.

```
<#root>
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 [ASA: 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

Verify 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, are in different networks.

You can assign the same major network with different subnets, but sometimes the routing issues occur.

For further examples, see the *Diagram and Example* of the [Unable to Access the Servers in DMZ](#) section.

## Unable to Connect More Than Three VPN Client Users

### Problem

Only three VPN clients can connect to ASA/; 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.

Try these solutions in order to resolve this issue:

- [Configure Simultaneous Logins](#)
- [Configure the ASA with CLI](#)
- [Configure Configure](#)

## Configure Simultaneous Logins

If the **Inherit** check box in ASDM is checked, only the default number of simultaneous logins is allowed for the user. The default value for simultaneous logins is three (3).

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

1. Launch ASDM and then navigate to **Configuration > VPN > Group Policy**.
2. Choose the appropriate **Group** and click the **Edit** button.
3. Once in the **General** tab, undo the **Inherit** check box for **Simultaneous Logins** under **Connection Settings**. Choose an appropriate value in the field.

The minimum value for this field is zero (0), which disables login and prevents user access.

When you log in with the same user account from a different PC, the current session (the connection established from another PC with the same user account) is terminated, and the new session is established.

This is the default behaviour and is independent to VPN simultaneous logins.

## Configure the ASA with CLI

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

```
<#root>
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](#).

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:

```
<#root>  
hostname#  
vpn-sessiondb max-session-limit 450
```

## Configure

### 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 > Simultaneous Logins**, and change the number of logins to 5.

## Unable to Initiate the Session or an Application and Slow Transfer after the Tunnel Establishment

### Problem

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 /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:

```
<#root>
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:

```
<#root>
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 [ASA and Cisco IOS®: VPN Fragmentation](#).

## **ASA —Refer to /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 this document in order to resolve the issue:

- [ASA and Cisco IOS®: VPN Fragmentation](#)

## **Unable to Initiate VPN Tunnel from ASA Problem**

You are unable to initiate the VPN tunnel from ASA interface, and after the tunnel establishment, the remote end/VPN Client is unable to ping the inside interface of ASA on the VPN tunnel.

For example, the vpn client can be unable to initiate a SSH or HTTP connection to ASAs inside interface over VPN tunnel.

## Solution

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

```
<#root>
ASA-02(config)#
management-access inside

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

This command also helps with ssh initiation or http connection to inside interface of ASA through a VPN tunnel.

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

```
<#root>
ASA-02(config)#
management-access DMZ
```

If the VPN client is unable to connect, then make sure ESP and UDP ports are open.

However, if those ports are not open, 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**.

## Unable to Pass Traffic Across VPN Tunnel

### Problem

You are unable to pass traffic across a VPN tunnel.

### Solution

This issue can also occur when the ESP packets are blocked. In order to resolve this issue, reconfigure the VPN tunnel.

This issue can occur when data is not encrypted, but only decrypted over the VPN tunnel as shown in this output:

```
<#root>
```

```
ASA# sh crypto ipsec sa peer x.x.x.x
peer address: y.y.y.y
  Crypto map tag: IPSec_map, seq num: 37, local addr: x.x.x.x
  access-list test permit ip host xx.xx.xx.xx host yy.yy.yy.yy
  local ident (addr/mask/prot/port): (xx.xx.xx.xx/255.255.255.255/0/0)
  remote ident (addr/mask/prot/port): (yy.yy.yy.yy/255.255.255.255/0/0)
  current_peer: y.y.y.y

#pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
  #pkts decaps: 393, #pkts decrypt: 393, #pkts verify: 393

#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 0, #pkts comp failed: 0, #pkts decomp failed: 0
#pre-frag successes: 0, #pre-frag failures: 0, #fragments created: 0
#PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
#send errors: 0, #recv errors: 0
```

In order to resolve this issue, check for these conditions:

1. If the crypto access-lists match with the remote site, and that NAT 0 access-lists are correct.
2. If routing is correct and traffic does hit outside interface which passes through inside. The sample output shows that decryption is done, but encryption does not occur.
3. If the `sysopt permit connection-vpn` command has been configured on the ASA. If not configured, configure this command because it allows the ASA to exempt the encrypted/VPN traffic from interface ACL Check.

## Configure Backup peer for vpn tunnel on same crypto map

### Problem

You want to use multiple backup peers for a single vpn tunnel.

### Solution

The configuration of multiple peers is equivalent to the provision of a fallback list. For each tunnel, the security appliance attempts to negotiate with the first peer in the list.

If that peer does not respond, the security appliance works its way down the list until either a peer responds or there are no more peers in the list.

The ASA has a crypto map already configured as the primary peer. The secondary peer could be added after the primary one.

This example configuration shows the primary peer as X.X.X.X and backup peer as Y.Y.Y.Y:

```
<#root>
ASA(config)#
crypto map mymap 10 set peer X.X.X.X Y.Y.Y.Y
```

## Disable/Restart VPN Tunnel

### Problem

In order to temporarily disable the VPN tunnel and restart the service, complete the procedure described in this section.

### Solution

Use the **crypto map interface** command in global configuration mode to remove a previously defined crypto map set to an interface.

Use the **no** form of this command in order to remove the crypto map set from the interface.

```
<#root>
hostname(config)#
no crypto map
    map-name
interface
    interface-name
```

This command removes a crypto map set to any active security appliance interface and make the IPsec VPN tunnel inactive in that interface.

To restart the IPsec tunnel on an interface, you must assign a crypto map set to an interface before that interface can provide IPsec services.

```
<#root>
hostname(config)#
crypto map
    map-name
interface
    interface-name
```

## Some Tunnels not Encrypted

### Problem

When a huge number of tunnels are configured on the VPN gateway, some tunnels do not pass traffic. The ASA does not receive encrypted packets for those tunnels.

### Solution

This issue occurs because the ASA fails to pass the encrypted packets through the tunnels. Duplicate encryption rules are created in the ASP table.

**Error:- %ASA-5-713904: Group = DefaultRAGroup, IP = x.x.x.x, ... unsupported Transaction Mode v2 version.Tunnel terminated.**

### Problem

The%ASA-5-713904: Group = DefaultRAGroup, IP = 192.0.2.0,... unsupported Transaction Mode v2 version.Tunnel terminatederror message appears.

### Solution

The reason for theTransaction Mode v2error message is that ASA supports only IKE Mode Config V6 and not the old V2 mode version.

Use the IKE Mode Config V6 version in order to resolve this error.

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

### Problem

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, which resolves the issue.

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

## Problem

If you enabled QoS in one end of the VPN Tunnel, you can 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 check
```

## Solution

This message is normally caused when one end of the tunnel performs QoS. This happens when a packet is detected as 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.

## WARNING: crypto map entry incomplete

### Problem

When you run the `crypto map mymap 20 ipsec-isakmp` command, you can receive this error:

```
WARNING: crypto map entry incomplete
```

For example:

```
<#root>
ciscoasa(config)#
crypto map mymap 20 ipsec-isakmp
WARNING: crypto map entry incomplete
```

### Solution

This is a usual alert 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.

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

### Problem

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

Disable the signatures 2150 and 2151 in order to resolve this issue. Once the signatures are disabled ping works fine.

Use these commands in order to disable the signatures:

```
ASA(config)#ip audit signature 2151 disable
```

```
ASA(config)#ip audit signature 2150 disable
```

**Error:- %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 check.**

## Problem

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

```
Error:- %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 check.
```

## Solution

In order to resolve this error, use the [crypto ipsec security-association replay window-size](#) command in order to vary the window size.

```
<#root>
```

```
hostname(config)#
```

```
crypto ipsec security-association replay window-size 1024
```

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

**Error Message - %ASA-4-407001: Deny traffic for local-host interface\_name:inside\_address, license limit of number exceeded**

## Problem

Few hosts are unable to connect to the Internet, and this error message appears in the syslog:

```
Error Message - %ASA-4-407001: Deny traffic for local-host interface_name:inside_address,
license limit of number exceeded
```

## Solution

This error message is received when the number of users exceeds the user limit of the license used. This error can be resolved by upgrade of the license to a higher number of users.

The user license can include 50, 100, or unlimited users as required.

## **Error Message - %VPN\_HW-4-PACKET\_ERROR:**

### **Problem**

TheError Message - %VPN\_HW-4-PACKET\_ERROR:error message indicates that ESP packet with HMAC received by the router are mismatched. This error can be caused by these issues:

- Defective VPN H/W module
- Corrupt ESP packet

### **Solution**

In order to resolve this error message:

- Ignore the error messages unless there is traffic disruption.
- If there is traffic disruption, replace the module.

## **Error message: Command rejected: delete crypto connection between VLAN XXXX and XXXX, first.**

### **Problem**

This error message appears when you attempt to add an allowed VLAN on the trunk port on a switch:Command rejected: delete crypto connection between VLAN XXXX and VLAN XXXX, first..

The WAN edge trunk cannot be modified to allow additional VLANs. That is, you are unable to add VLANs in theIPSEC VPN SPAtrunk.

This command is rejected because it results in a crypto connected interface VLAN that belongs to the allowed VLAN list, which poses a potential IPsec security breach.

Note that this behavior applies to all trunk ports.

### **Solution**

Instead of the `no switchport trunk allowed vlan (vlanlist)` command, use the `switchport trunk allowed vlan none` command or the `"switchport trunk allowed vlan remove (vlanlist)"` command.

## **Error Message - % FW-3-RESPONDER\_WND\_SCALE\_INI\_NO\_SCALE: Dropped packet - Invalid Window Scale option for session x.x.x.x:27331 to x.x.x.x:23 [Initiator(flag 0, factor 0) Responder (flag 1, factor 2)]**

### **Problem**

This error occurs when you try to telnet from a device on the far end of a VPN tunnel or when you try to

telnet from the router itself:

```
Error Message - % FW-3-RESPONDER_WND_SCALE_INI_NO_SCALE: Dropped packet - Invalid Window Scale option for session x.x.x.x:27331 to x.x.x.x:23 [Initiator(flag 0,factor 0) Responder (flag 1, factor 2)]
```

## Solution

The user license can include 50, 100, or unlimited users as required. Window scale function was added to allow for rapid transmission of data on long fat networks (LFN).

These are typically connections with very high bandwidth, but also high latency.

Networks with satellite connections are one example of an LFN, since satellite links always have high propagation delays but typically have high bandwidth.

To enable window scale function to support LFNs, the TCP window size must be more than 65,535. This error message can be resolved if you increase the TCP window size to be more than 65,535.

## **%ASA-5-305013: Asymmetric NAT rules matched for forward and reverse . Please update this issue flows**

### Problem

This error message appears once the VPN tunnel comes up:

```
%ASA-5-305013: Asymmetric NAT rules matched for forward and reverse . Please update this issue flows
```

### Solution

In order to resolve this issue when not on the same interface as the host with NAT, use the mapped address instead of the actual address to connect to the host.

In addition, enable the `inspect` command if the application embeds the IP address.

## **%ASA-5-713068: Received non-routine Notify message: notify\_type**

### Problem

This error message appears if the VPN tunnel fails to come up:

```
%ASA-5-713068: Received non-routine Notify message: notify_type
```

### Solution

This message occurs due to misconfiguration (that is, when the policies or ACLs are not configured to be the same on peers).

Once the policies and ACLs are matched the tunnel comes up without any problem.

## **%ASA-5-720012: (VPN-Secondary) Failed to update IPsec failover runtime data on the standby unit (or) %ASA-6-720012: (VPN-unit) Failed to update IPsec failover runtime data on the standby unit**

### **Problem**

One of these error messages appear when you try to upgrade the Cisco Adaptive Security Appliance (ASA):

```
%ASA-5-720012: (VPN-Secondary) Failed to update IPsec failover runtime data on the standby unit.
```

```
%ASA-6-720012: (VPN-unit) Failed to update IPsec failover runtime data on the standby unit.
```

### **Solution**

These error messages are informative errors. The messages do not impact functionality of the ASA or the VPN.

These messages appear when the VPN failover subsystem cannot update IPsec-related runtime data because the related IPsec tunnel has been deleted on the standby unit.

In order to resolve these, issue the **wr standby** command on the active unit.

## **Error:- %ASA-3-713063: IKE Peer address not configured for destination 0.0.0.0**

### **Problem**

The **%ASA-3-713063: IKE Peer address not configured for destination 0.0.0.0** error message appears and the tunnel fails to come up.

### **Solution**

This message appears when the IKE peer address is not configured for a L2L tunnel.

This error can be resolved if you change the sequence number of crypto map, then remove and reapply the crypto map.

## **Error: %ASA-3-752006: Tunnel Manager failed to dispatch a KEY\_ACQUIRE message.**

### **Problem**

The **%ASA-3-752006: Tunnel Manager failed to dispatch a KEY\_ACQUIRE message.** Probable mis-configuration of the crypto map or tunnel-group." error message is logged on the Cisco ASA.

### **Solution**

This error message can be caused by a misconfiguration of the crypto map or tunnel group. Ensure that both are configured properly. For more information about this error message, refer to **Error 752006** .

Here are some of the corrective actions:

- Remove the crypto ACL (for example, associated to dynamic map).
- Remove unused IKEv2 related configuration, if any.
- Verify that the crypto ACL matched properly.
- Remove duplicate access-list entries, if any.

## **Error: %ASA-4-402116: IPSEC: Received an ESP packet (SPI=0x99554D4E, sequence number= 0x9E) from XX.XX.XX.XX (user=XX.XX.XX.XX) to YY.YY.YY.YY**

In a LAN-to-LAN VPN tunnel setup, this error is received on one end ASA:

The decapsulated inner packet does not match the negotiated policy in the SA.

The packet specifies its destination as 10.32.77.67, its source as 10.105.30.1, and its protocol as icmp.

The SA specifies its local proxy as 10.32.77.67/255.255.255.255/ip/0 and its remote\_proxy as 10.105.42.192/255.255.255.224/ip/0.

### **Solution**

You need to verify the interesting traffic access-lists defined on both ends of the VPN tunnel. Both must match as exact mirror images.

## **Failed to launch 64-bit VA installer to enable the virtual adapter due to error 0xffffffff**

### **Problem**

The Failed to launch 64-bit VA installer to enable the virtual adapter due to error 0xffffffff log message is received when AnyConnect fails to connect.

### **Solution**

Complete these steps in order to resolve this issue:

1. Go to **System > Internet Communication Management > Internet Communication settings** and make sure that **Turn Off Automatic Root Certificates Update** is disabled.
2. If it is disabled, then disable the entire **Administrative Template** part of the GPO assigned to the affected machine and test again.

Refer to [Turn off Automatic Root Certificates Update](#) for more information.

## **Cisco VPN Client Does Not Work with Data Card on Windows 7**

## Problem

Cisco VPN Client does not work with data card on Windows 7.

## Solution

Cisco VPN Client installed on Windows 7 does not work with 3G connections since data cards are not supported on VPN clients installed on a Windows 7 machine.

## Alert: "VPN functionality may not work at all"

### Problem

During attempts to enable the isakmp on the outside interface of ASA, this alert message is received:

```
ASA(config)# crypto isakmp enable outside
WARNING, system is running low on memory. Performance may start to degrade.
VPN functionality may not work at all.
```

At this point, access to ASA through ssh. HTTPS is stopped and other SSL clients are also affected.

### Solution

This problem is due to memory requirements by different modules such as logger and crypto.

Make sure you do not have the **logging queue 0** command. It makes the queue size set to 8192 and the memory allocation increases.

In platforms such as ASA5505 and ASA5510, this memory allocation tends to memory-starve other modules.

## IPSec Padding error

### Problem

This error message is received:

```
%ASA-3-402130: CRYPTO: Received an ESP packet (SPI =
0XXXXXXXX, sequence number= 0XXXXX) from x.x.x.x (user= user) to y.y.y.y with
incorrect IPsec padding
```

### Solution

The issue occurs because the IPSec VPN negotiates without a hash algorithm. Packet hash ensures integrity check for the ESP channel.

Therefore, without hash, malformed packets are accepted undetected by the Cisco ASA and it attempts to decrypt these packets.

However, because these packets are malformed, the ASA finds flaws during packet decryption. This causes the padding error messages that are seen.

The recommendation is to include a hash algorithm in the transform set for the VPN and to ensure that the link between the peers has minimum packet malformation.

## **VPN tunnel gets disconnected after every 18 hours**

### **Problem**

The VPN tunnel gets disconnected after every 18 hours even though the lifetime is set for 24 hours.

### **Solution**

The lifetime is the maximum time the SA can be used for rekey. The value you enter in the configuration as the lifetime is different from the rekey time of the SA.

Therefore, it is necessary to negotiate a new SA (or SA pair in the case of IPsec) before the current one expires.

The rekey time must always be smaller than the lifetime in order to allow for multiple attempts in case the first rekey attempt fails.

The RFCs do not specify how to calculate the rekey time. This is left to the discretion of the implementers.

Therefore, the time varies with platform. Some implementations can use a random factor to calculate the rekey timer.

For example, if the ASA initiates the tunnel, then it is normal that it rekeys at 64800 seconds = 75% of 86400.

If the router initiates, then the ASA can wait longer to give the peer more time to initiate the rekey.

Thus, it is normal that the VPN session gets disconnected every 18 hours to use another key for the VPN negotiation. This must not cause any VPN drop or problem.

## **Traffic flow is not maintained after the LAN to LAN tunnel is re-negotiated**

### **Problem**

Traffic flow is not maintained after the LAN to LAN tunnel is re-negotiated.

### **Solution**

The ASA monitors every connection that passes through it and maintains an entry in its state table in accordance with the application inspection feature.

The encrypted traffic details that pass through the VPN are maintained in the form of a security association

(SA) database. For LAN to LAN VPN connections, it maintains two different traffic flows.

One is the encrypted traffic between the VPN gateways. The other is the traffic flow between the network resource behind the VPN gateway and the end-user behind the other end.

When the VPN is terminated, the flow details for this particular SA are deleted.

However, the state table entry maintained by the ASA for this TCP connection becomes stale because of no activity, which hampers the download.

This means the ASA still retains the TCP connection for that particular flow while the user application terminates.

However, the TCP connections become stray and eventually timeout after the TCP idle-timer expires.

This problem has been resolved with the introduction of a feature called **Persistent IPSec Tunneled Flows**.

A new command, `sysopt connection preserve-vpn-flows`, has been integrated into the Cisco ASA in order to retain the state table information at the re-negotiation of the VPN tunnel.

By default, this command is disabled. To enable this, the Cisco ASA maintains the TCP state table information when the L2L VPN recovers from the disruption and re-establishes the tunnel.

## Error message states that Bandwidth reached for the Crypto functionality

### Problem

This error message is received on the 2900 Series Router:

```
Error: Mar 20 10:51:29: %CERM-4-TX_BW_LIMIT: Maximum Tx Bandwidth limit of 85000 Kbps reached for Crypto functionality with securityk9 technology package license.
```

### Solution

This is a known issue that occurs because of the strict guidelines issued by the **United States** government.

In accordance, the **securityk9** license can only allow a payload encryption up to rates close to 90Mbps and limit the number of encrypted tunnels/TLS sessions to the device.

For more information about the crypto export restrictions, refer to [Cisco ISR G2 SEC and HSEC Licensing](#).

In case of Cisco devices, it is derived to be less than 85Mbps unidirectional traffic in or out of the ISR G2 router, with a bidirectional total of 170 Mbps.

This requirement applies for the Cisco 1900, 2900, and 3900 ISR G2 platforms. This command helps to view these limitations:

```
<#root>
```

```
Router#
```

```
show platform cerm-information
```

Crypto Export Restrictions Manager(CERM) Information:  
CERM functionality: ENABLED

Resource	Maximum Limit	Available
Tx Bandwidth(in kbps)	85000	85000
Rx Bandwidth(in kbps)	85000	85000
Number of tunnels	225	225
Number of TLS sessions	1000	1000

---Output truncated---

To avoid this problem, purchase a HSECK9 license. An "hseck9" feature license provides enhanced payload encryption functionality with increased VPN tunnel counts and secure voice sessions.

For more information about Cisco ISR Router licensing, refer to [Software Activation](#).

## **Problem: Outbound encryption traffic in an IPsec tunnel fails, even if inbound decryption traffic works.**

### **Solution**

This issue has been observed on an IPsec connection after multiple rekeys, but the trigger condition is not clear.

The presence of this issue can be established if you check the output of the `show asp drop` command and verifying that the Expired VPN context counter increases for each outbound packet sent.

## **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 a mismatch of isakmp policies or if port udp 500 gets blocked on the way.

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

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

## **Related Information**

- [ASA and Cisco IOS®: VPN Fragmentation](#)
- [Cisco ASA 5500 Series Security Appliances](#)
- [IPsec Negotiation/IKE Protocols](#)
- [Technical Support & Documentation - Cisco Systems](#)