

Troubleshooting Connection Problems on the VPN 3000 Concentrator

Document ID: 23840

Introduction

Prerequisites

- Requirements

- Components Used

- Conventions

Configure the Public Interface for Secure HTTPS Access

Set Up Debugging

- General Configuration

- Classes

View Logs on the VPN 3000 Concentrator Through the GUI

- Live Event Log

- Filterable Event Log

Debugs

- Good Debug (Remote Access)

- Bad Debugs

Known Issues when you use Kerberos between a VPN 3000 Concentrator and a Windows Active Directory (AD) Server

NetPro Discussion Forums – Featured Conversations

Related Information

Introduction

This document provides troubleshooting tips you can use in order to resolve connectivity issues with the Cisco VPN 3000 Concentrator.

Prerequisites

Requirements

There are no specific requirements for this document.

Components Used

The information in this document is based on VPN 3000 Concentrator software version 4.1.7A and later.

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

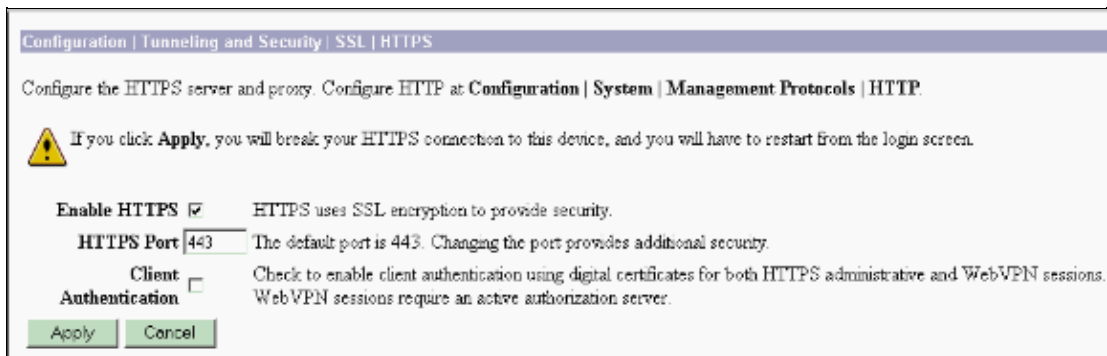
Conventions

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

Configure the Public Interface for Secure HTTPS Access

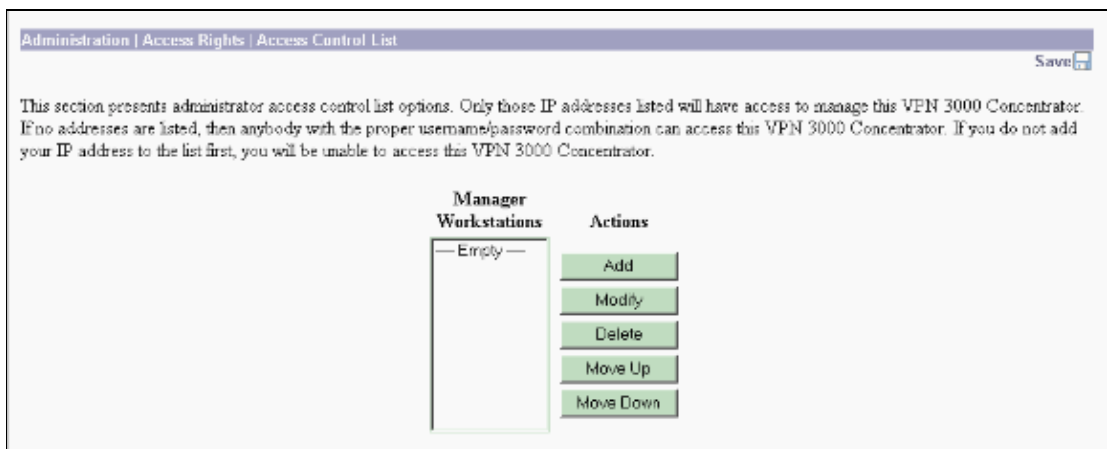
Complete these steps in order to open secure access to the VPN Concentrator so that you can troubleshoot with a Cisco Technical Support engineer.

1. Select **Configuration > Interfaces**. Ensure that the public filter is on the public interface and the private filter is on the private interface.
2. Select **Configuration > Policy Management > Traffic Management > Filters**. Choose the public filter and click **Assign Rules to Filter**. Under Available Rules, select **Incoming HTTPS In (forward/in)** and click **Add**. Then select **Incoming HTTPS Out (forward/out)** and click **Add**.
3. Select **Configuration > Tunneling and Security > SSL > HTTPS** and ensure that **HTTPS** is enabled as this window shows.



4. Select **Administration > Access Rights > Access Control List**.

If the list is empty, leave it alone. If the list contains entries, add the IP address of the Technical Support engineer who assists you.



5. Select **Administration > Certificate Management**. Under SSL Certificate, ensure that there is a valid certificate with the subject "at Cisco Systems, Inc.".

If the IP address is incorrect, or if the certificate says "Altiga Networks" instead of "Cisco Systems", delete the certificate and generate a new certificate. In order to do this, click on the appropriate links.

Refer to the Certificate Management documentation for the VPN 3000 Concentrator for more information on how to generate the SSL certificate.

Note: If you are unable to generate a certificate the first time, or if you get an error, try again a few times. Also, ensure that you do not have TCP port 443 (HTTPS) traffic blocked in front of the VPN Concentrator by an access list or any sort of firewall. This prevents access.

Administration | Certificate Management Sunday, 27 February 2006 22:23:05
Refresh

This section lets you view and manage certificates on the VPN 3000 Concentrator.

- [Click here to enroll with a Certificate Authority](#)
- [Click here to install a certificate](#)

Certificate Authorities [[View All CRL Caches](#) | [Clear All CRL Caches](#)] (current: 1, maximum: 20)

Subject	Issuer	Expiration	SCEP Issuer	Actions
cisco1.ccie.com L=Chennai C=Ind...	cisco1.ccie.com L=Chennai C=Ind...	02/12/2006	Yes	View Configure Delete SCEP

Identity Certificates (current: 1, maximum: 20)

Subject	Issuer	Expiration	Actions
VPN3K at CODC	cisco1.ccie.com L=Chennai C=Ind...	09/01/2005	View Renew Delete

SSL Certificates

Interface	Subject	Issuer	Expiration	Actions
Private	10.1.1.2 at Cisco Systems, Inc.	10.1.1.2 at Cisco Systems, Inc.	02/12/2008	View Renew Delete Export Generate Enroll Import
Public	120.10.10.2 at Cisco Systems, Inc.	120.10.10.2 at Cisco Systems, Inc.	02/12/2008	View Renew Delete Export Generate Enroll Import

SSH Host Key

Key Size	Key Type	Date Generated	Actions
512 bits	RSA	02/12/2005	Generate

Enrollment Status [[Remove All](#) | [Expired](#) | [Timed-Out](#) | [Rejected](#) | [Cancelled](#) | [In Progress](#)] (current: 0 available: 19)

Subject	Issuer	Date	Use	Reason	Method	Status	Actions
No Enrollment Requests							

Set Up Debugging

General Configuration

Select **Configuration > System > Events > General**. There are multiple options you can use in order to configure the event logs and where the logs need to be sent. Refer to the Events documentation for the VPN 3000 Concentrator for details on Save Log on Wrap and other options.

Configuration | System | Events | General

This section lets you configure default event handling.

Save Log on Wrap Check to save the event log to a file on wrap.
Save Log Format Select the format of the saved log files.
 FTP Saved Log on Wrap Check to automatically FTP the saved log to a remote destination.
E-mail Source Address Enter the e-mail address that appears in the **From:** field.
Syslog Format Select the format of Syslog messages.
Events to Log Select the events to enter in the log.
Events to Console Select the events to display on the console.
Events to Syslog Select the events to send to a Syslog Server.
Events to E-mail Select the events to send to an E-mail Recipient.
Events to Trap Select the events to send to an SNMP Trap Destination.

Event List
Enter as: Event Class/List of Event IDs, SEV(#)
Example: IKE/1, 13-45, SEV(3)

- Set the *Event Class* to any of the predefined event classes or **ALL** for all event classes
- Set the *List of Event IDs* to
 - a range of numbers
 - a comma-separated list of numbers
 - or a combination of both (e.g. 2,5,8,13-45)
- Set Event Severities to *SEV(levels)* where *levels* can be a single number or a range of numbers

Classes

Select **Configuration > System > Events > Classes > Add**. You can configure the default options shown in this window for classes that you want to monitor.

Configuration | System | Events | Classes | Add

This screen lets you add and configure an event class for special handling.

Class Name Select the event class to configure.
Enable Check to enable special handling of this class.

If one of the following values has been set to *Use Event List*, the Event List can be seen by viewing **Configuration | System | Events | General**. Changing a value set to *Use Event List* will override the sections of the Event List referring to this event class.

Events to Log Select the events to enter in the log.
Events to Console Select the events to display on the console.
Events to Syslog Select the events to send to a Syslog Server.
Events to E-mail Select the events to send to an E-mail Recipient.
Events to Trap Select the events to send to an SNMP Trap Destination.

In order to configure a class to monitor in the logs, select a class name, ensure that you check the **Enable** option, and set Severity to Log at **1–13** (in order to capture all events). This severity level can be set lower if you want less verbosity. If you use a syslog server and want to collect the debugs, you can set the Severity to Syslog value to **1–13**. This is because the default level of **1–5** sometimes does not indicate all the events that lead to an error or problem. Refer to Event Severity Level for an explanation on what each level of Severity means.

You can also add more classes based on the types of problems that you experience. This table shows a few specific problems and the related classes that you can add.

Note: You cannot simultaneously select multiple classes. You need to individually configure each class.

If you experience this problem...	...then add these classes
Authentication issue	AUTH AUTHDBG
Issues in first phase IPsec	IKE IKEDBG
Issues in second phase IPsec	IPSEC IPSECDBG
Cannot tell where in the process the connection fails	AUTH AUTHDBG IKE IKEDBG IPSEC IPSECDBG

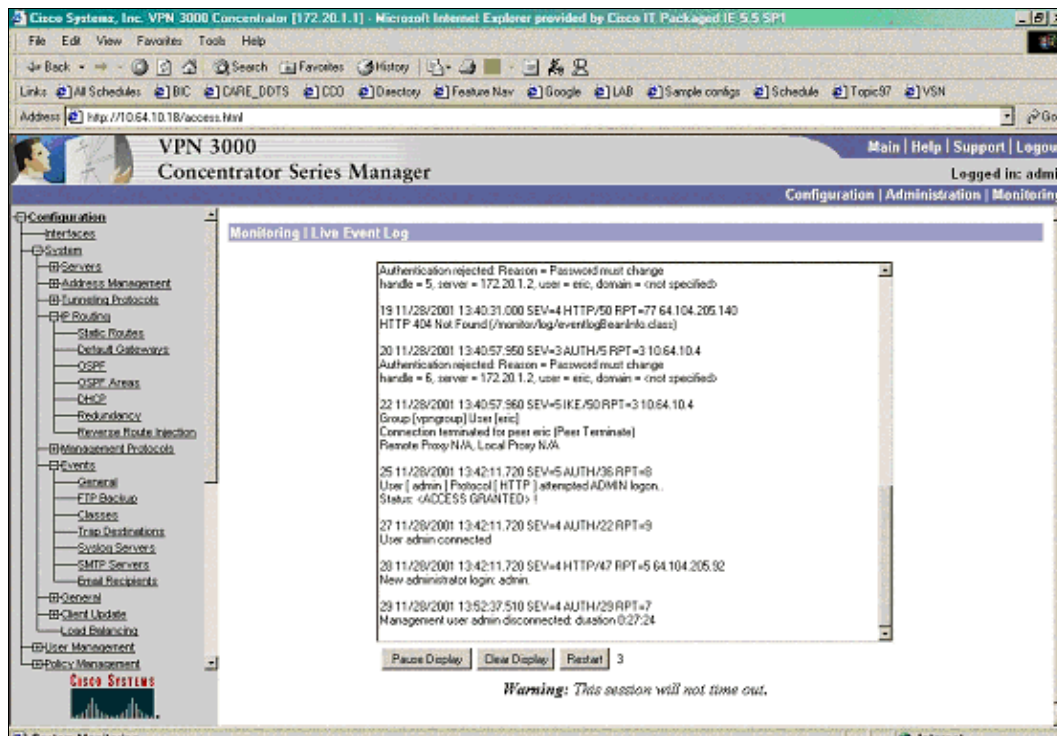
If the problem relates to other areas of performance, you can set up additional classes, such as Point-to-Point Tunneling Protocol (PPTP), Virtual Router Redundancy Protocol (VRRP), LBSSF (load balancing), and Dynamic Host Configuration Protocol (DHCP). Refer to Event Class. for a complete list of classes available.

View Logs on the VPN 3000 Concentrator Through the GUI

There are two ways in order to view event logs with the use of the VPN Concentrator GUI.

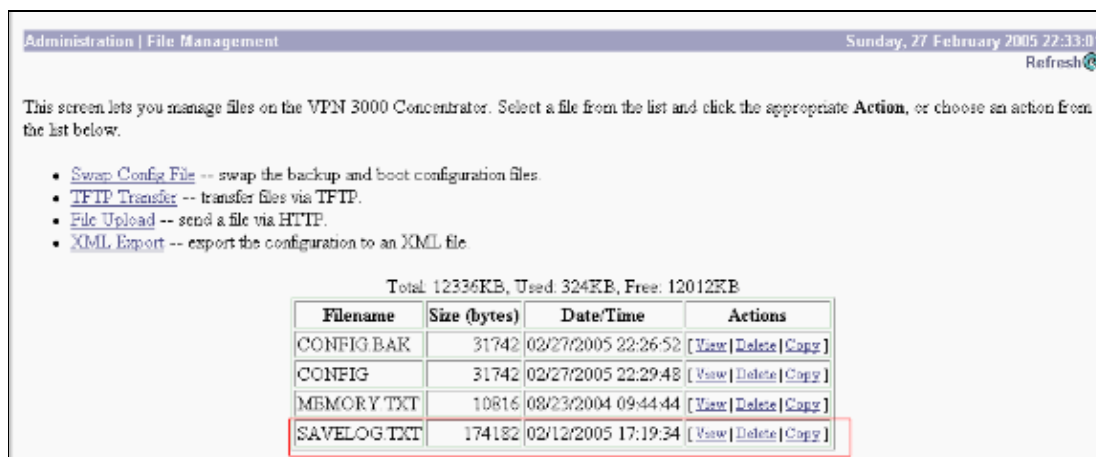
Live Event Log

Select **Monitoring > Live Event Log** to view logs while events occur.

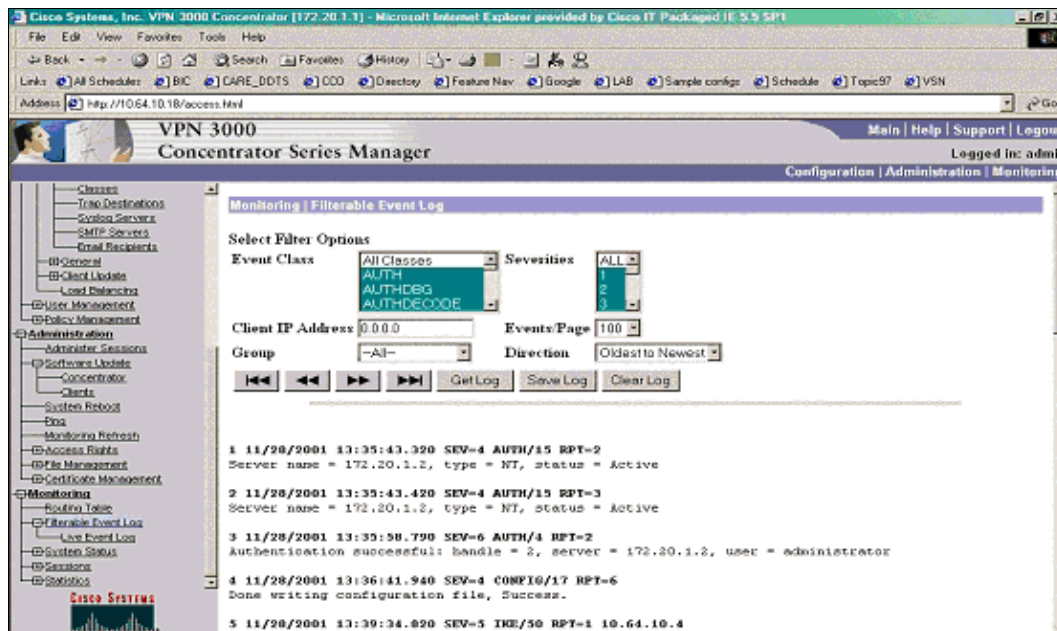


Filterable Event Log

In order to view the logs generated after an event, select **Administration** > **File Management** > **Savelog** in order to view older log files (after a crash, for instance) as this window shows.



You can also select **Monitoring** > **Filterable Event Log**, as this window shows.



Click **Get Log** so that you can scroll through all the log events on one page. Copy the log events to a text file that you can transfer by e-mail or FTP to get the log file without access to the VPN Concentrator. Each entry (record) in the event log consists of several fields:

1. A sequence number
2. Date and Time
3. Event severity level
4. Event class and number
5. Event repetition count
6. Event IP address (only for certain events)
7. Description string

Debugs

Good Debug (Remote Access)

```
1568 11/29/2001 16:20:17.860 SEV=9 IKEDBG/0 RPT=527 64.104.205.92
Group [ciscogroup] User [ciscouser]
constructing blank hash
```

```
1569 11/29/2001 16:20:17.860 SEV=9 IKEDBG/20 RPT=2 64.104.205.92
Group [ciscogroup] User [ciscouser]
construct_cfg_set: default domain = bechtel.com
```

```
1571 11/29/2001 16:20:17.860 SEV=9 IKEDBG/0 RPT=528 64.104.205.92
0000: 00010004 C0A80101 00030004 9301098B .....
0010: 00040004 93013001 F0010000 7002000B .....0....p...
0020: 62656368 74656C2E 636F6DF0 052710F0 bechtel.com..'..
0030: 070000 .....
```

```
1575 11/29/2001 16:20:17.860 SEV=9 IKEDBG/0 RPT=529 64.104.205.92
Group [ciscogroup] User [ciscouser]
constructing qm hash
```

```
1576 11/29/2001 16:20:17.860 SEV=8 IKEDBG/0 RPT=530 64.104.205.92
SENDING Message (msgid=f4d3c42c) with payloads :
HDR + HASH (8) ... total length : 107
```

```
1583 11/29/2001 16:20:18.480 SEV=9 IKEDBG/21 RPT=2 64.104.205.92
```

Group [ciscogroup] User [ciscouser]
Delay Quick Mode processing, Cert/Trans Exch/RM DSID in progress

1585 11/29/2001 16:20:18.480 SEV=4 AUTH/21 RPT=11
User ciscouser connected

1586 11/29/2001 16:20:18.480 SEV=7 IKEDBG/22 RPT=2 64.104.205.92
Group [ciscogroup] User [ciscouser]
Resume Quick Mode processing, Cert/Trans Exch/RM DSID completed

1588 11/29/2001 16:20:18.480 SEV=4 IKE/119 RPT=2 64.104.205.92
Group [ciscogroup] User [ciscouser]
PHASE 1 COMPLETED

1589 11/29/2001 16:20:18.480 SEV=6 IKE/121 RPT=2 64.104.205.92
Keep-alive type for this connection: DPD

1590 11/29/2001 16:20:18.480 SEV=7 IKEDBG/0 RPT=531 64.104.205.92
Group [ciscogroup] User [ciscouser]
Starting phase 1 rekey timer: 73440000 (ms)

1591 11/29/2001 16:20:18.480 SEV=9 IKEDBG/0 RPT=532 64.104.205.92
Group [ciscogroup] User [ciscouser]
sending notify message

1592 11/29/2001 16:20:18.480 SEV=9 IKEDBG/0 RPT=533 64.104.205.92
Group [ciscogroup] User [ciscouser]
constructing blank hash

1593 11/29/2001 16:20:18.480 SEV=9 IKEDBG/0 RPT=534 64.104.205.92
Group [ciscogroup] User [ciscouser]
constructing qm hash

1594 11/29/2001 16:20:18.480 SEV=8 IKEDBG/0 RPT=535 64.104.205.92
SENDING Message (msgid=8f18070b) with payloads :
HDR + HASH (8) ... total length : 88

1596 11/29/2001 16:20:18.480 SEV=8 IKEDBG/0 RPT=536 64.104.205.92
RECEIVED Message (msgid=13dc5023) with payloads :
HDR + HASH (8) + SA (1) + NONCE (10) + ID (5) + ID (5) + NONE (0) ...
total length : 792
Group [ciscogroup] User [ciscouser]
processing hash

1600 11/29/2001 16:20:18.480 SEV=9 IKEDBG/0 RPT=538 64.104.205.92
Group [ciscogroup] User [ciscouser]
processing SA payload

1711 11/29/2001 16:20:18.500 SEV=9 IKEDBG/1 RPT=143 64.104.205.92
Group [ciscogroup] User [ciscouser]
processing nonce payload

1712 11/29/2001 16:20:18.500 SEV=9 IKEDBG/1 RPT=144 64.104.205.92
Group [ciscogroup] User [ciscouser]
Processing ID

1713 11/29/2001 16:20:18.500 SEV=5 IKE/25 RPT=3 64.104.205.92
Group [ciscogroup] User [ciscouser]
Received remote Proxy Host data in ID Payload:
Address 192.168.1.1, Protocol 0, Port 0

1716 11/29/2001 16:20:18.500 SEV=9 IKEDBG/1 RPT=145 64.104.205.92
Group [ciscogroup] User [ciscouser]
Processing ID

1717 11/29/2001 16:20:18.500 SEV=5 IKE/24 RPT=2 64.104.205.92

Group [ciscogroup] User [ciscouser]
Received local Proxy Host data in ID Payload:
Address 10.64.10.9, Protocol 0, Port 0

1720 11/29/2001 16:20:18.500 SEV=8 IKEDBG/0 RPT=539
QM IsRekeyed old sa not found by addr

1721 11/29/2001 16:20:18.500 SEV=5 IKE/66 RPT=3 64.104.205.92
Group [ciscogroup] User [ciscouser]
IKE Remote Peer configured for SA: ESP-3DES-MD5

1723 11/29/2001 16:20:18.500 SEV=9 IKEDBG/0 RPT=540 64.104.205.92
Group [ciscogroup] User [ciscouser]
processing IPSEC SA

1730 11/29/2001 16:20:18.500 SEV=8 IKEDBG/0 RPT=541
Proposal # 2, Transform # 1, Type ESP, Id Triple-DES
Parsing received transform:
Phase 2 failure:
Mismatched attr types for class HMAC Algorithm:
Rcv'd: SHA
Cfg'd: MD5

1737 11/29/2001 16:20:18.500 SEV=7 IKEDBG/27 RPT=3 64.104.205.92
Group [ciscogroup] User [ciscouser]
IPSec SA Proposal # 3, Transform # 1 acceptable

1739 11/29/2001 16:20:18.500 SEV=7 IKEDBG/0 RPT=542 64.104.205.92
Group [ciscogroup] User [ciscouser]
IKE: requesting SPI!

1740 11/29/2001 16:20:18.500 SEV=9 IPSECDBG/6 RPT=15
IPSEC key message parse - msgtype 6, len 192, vers 1, pid 00000000, seq 5, err 0
, type 2, mode 0, state 32, label 0, pad 0, spi 00000000, encrKeyLen 0, hashKeyLen 0, ivlen 0, alg 0, hmacAlg 0, lifetype 0, lifetime1 7631924, lifetime2 0, dsid 300

1744 11/29/2001 16:20:18.500 SEV=9 IPSECDBG/1 RPT=43
Processing KEY_GETSPI msg!

1745 11/29/2001 16:20:18.500 SEV=7 IPSECDBG/13 RPT=3
Reserved SPI 296051861

1746 11/29/2001 16:20:18.500 SEV=8 IKEDBG/6 RPT=3
IKE got SPI from key engine: SPI = 0x11a56495

1747 11/29/2001 16:20:18.500 SEV=9 IKEDBG/0 RPT=543 64.104.205.92
Group [ciscogroup] User [ciscouser]
oakley constructing quick mode

1748 11/29/2001 16:20:18.500 SEV=9 IKEDBG/0 RPT=544 64.104.205.92
Group [ciscogroup] User [ciscouser]
constructing blank hash

1749 11/29/2001 16:20:18.500 SEV=9 IKEDBG/0 RPT=545 64.104.205.92
Group [ciscogroup] User [ciscouser]
constructing ISA_SA for ipsec

1750 11/29/2001 16:20:18.500 SEV=5 IKE/75 RPT=3 64.104.205.92
Group [ciscogroup] User [ciscouser]
Overriding Initiator's IPsec rekeying duration from 2147483 to 28800 seconds

1752 11/29/2001 16:20:18.500 SEV=9 IKEDBG/1 RPT=146 64.104.205.92
Group [ciscogroup] User [ciscouser]
constructing ipsec nonce payload

1753 11/29/2001 16:20:18.500 SEV=9 IKEDBG/1 RPT=147 64.104.205.92
Group [ciscogroup] User [ciscouser]
constructing proxy ID

1754 11/29/2001 16:20:18.500 SEV=7 IKEDBG/0 RPT=546 64.104.205.92
Group [ciscogroup] User [ciscouser]
Transmitting Proxy Id:
Remote host: 192.168.1.1 Protocol 0 Port 0
Local host: 10.64.10.9 Protocol 0 Port 0

1758 11/29/2001 16:20:18.500 SEV=7 IKEDBG/0 RPT=547 64.104.205.92
Group [ciscogroup] User [ciscouser]
Sending RESPONDER LIFETIME notification to Initiator

1760 11/29/2001 16:20:18.500 SEV=9 IKEDBG/0 RPT=548 64.104.205.92
Group [ciscogroup] User [ciscouser]
constructing qm hash

1762 11/29/2001 16:20:18.500 SEV=8 IKEDBG/0 RPT=549 64.104.205.92
SENDING Message (msgid=13dc5023) with payloads :
HDR + HASH (8) ... total length : 172

1769 11/29/2001 16:20:18.510 SEV=8 IKEDBG/0 RPT=550 64.104.205.92
RECEIVED Message (msgid=718cb0db) with payloads :
HDR + HASH (8) + SA (1) + NONCE (10) + ID (5) + ID (5) + NONE (0) ...
total length : 796

1772 11/29/2001 16:20:18.510 SEV=9 IKEDBG/0 RPT=551 64.104.205.92
Group [ciscogroup] User [ciscouser]
processing hash

1773 11/29/2001 16:20:18.510 SEV=9 IKEDBG/0 RPT=552 64.104.205.92
Group [ciscogroup] User [ciscouser]
processing SA payload

1884 11/29/2001 16:20:18.520 SEV=9 IKEDBG/1 RPT=148 64.104.205.92
Group [ciscogroup] User [ciscouser]
processing nonce payload

1885 11/29/2001 16:20:18.520 SEV=9 IKEDBG/1 RPT=149 64.104.205.92
Group [ciscogroup] User [ciscouser]
Processing ID

1886 11/29/2001 16:20:18.520 SEV=5 IKE/25 RPT=4 64.104.205.92
Group [ciscogroup] User [ciscouser]
Received remote Proxy Host data in ID Payload:
Address 192.168.1.1, Protocol 0, Port 0

1889 11/29/2001 16:20:18.520 SEV=9 IKEDBG/1 RPT=150 64.104.205.92
Group [ciscogroup] User [ciscouser]
Processing ID

1890 11/29/2001 16:20:18.520 SEV=5 IKE/34 RPT=2 64.104.205.92
Group [ciscogroup] User [ciscouser]
Received local IP Proxy Subnet data in ID Payload:
Address 0.0.0.0, Mask 0.0.0.0, Protocol 0, Port 0

1893 11/29/2001 16:20:18.520 SEV=8 IKEDBG/0 RPT=553
QM IsRekeyed old sa not found by addr

1894 11/29/2001 16:20:18.520 SEV=5 IKE/66 RPT=4 64.104.205.92
Group [ciscogroup] User [ciscouser]
IKE Remote Peer configured for SA: ESP-3DES-MD5

1896 11/29/2001 16:20:18.520 SEV=9 IKEDBG/0 RPT=554 64.104.205.92
Group [ciscogroup] User [ciscouser]

processing IPSEC SA

1903 11/29/2001 16:20:18.520 SEV=8 IKEDBG/0 RPT=555
Proposal # 2, Transform # 1, Type ESP, Id Triple-DES
Parsing received transform:

Phase 2 failure:

Mismatched attr types for class HMAC Algorithm:

Rcv'd: SHA

Cfg'd: MD5

1910 11/29/2001 16:20:18.520 SEV=7 IKEDBG/27 RPT=4 64.104.205.92
Group [ciscogroup] User [ciscouser]
IPSec SA Proposal # 3, Transform # 1 acceptable

1912 11/29/2001 16:20:18.520 SEV=7 IKEDBG/0 RPT=556 64.104.205.92
Group [ciscogroup] User [ciscouser]
IKE: requesting SPI!

1913 11/29/2001 16:20:18.520 SEV=9 IPSECDBG/6 RPT=16
IPSEC key message parse - msgtype 6, len 192, vers 1, pid 00000000, seq 6, err 0
, type 2, mode 0, state 32, label 0, pad 0, spi 00000000, encrKeyLen 0, hashKeyLen 0, ivlen 0, alg 0, hmacAlg 0, lifetype 0, lifetime1 7633504, lifetime2 0, dsID 300

1917 11/29/2001 16:20:18.520 SEV=9 IPSECDBG/1 RPT=44
Processing KEY_GETSPI msg!

1918 11/29/2001 16:20:18.520 SEV=7 IPSECDBG/13 RPT=4
Reserved SPI 1959748726

1919 11/29/2001 16:20:18.520 SEV=8 IKEDBG/6 RPT=4
IKE got SPI from key engine: SPI = 0x74cf6476

1920 11/29/2001 16:20:18.530 SEV=9 IKEDBG/0 RPT=557 64.104.205.92
Group [ciscogroup] User [ciscouser]
oakley constructing quick mode

1921 11/29/2001 16:20:18.530 SEV=9 IKEDBG/0 RPT=558 64.104.205.92
Group [ciscogroup] User [ciscouser]
constructing blank hash

1922 11/29/2001 16:20:18.530 SEV=9 IKEDBG/0 RPT=559 64.104.205.92
Group [ciscogroup] User [ciscouser]
constructing ISA_SA for ipsec

1923 11/29/2001 16:20:18.530 SEV=5 IKE/75 RPT=4 64.104.205.92
Group [ciscogroup] User [ciscouser]
Overriding Initiator's IPsec rekeying duration from 2147483 to 28800 seconds

1925 11/29/2001 16:20:18.530 SEV=9 IKEDBG/1 RPT=151 64.104.205.92
Group [ciscogroup] User [ciscouser]
constructing ipsec nonce payload

1926 11/29/2001 16:20:18.530 SEV=9 IKEDBG/1 RPT=152 64.104.205.92
Group [ciscogroup] User [ciscouser]
constructing proxy ID

1927 11/29/2001 16:20:18.530 SEV=7 IKEDBG/0 RPT=560 64.104.205.92
Group [ciscogroup] User [ciscouser]
Transmitting Proxy Id:
Remote host: 192.168.1.1 Protocol 0 Port 0
Local subnet: 0.0.0.0 mask 0.0.0.0 Protocol 0 Port 0

1931 11/29/2001 16:20:18.530 SEV=7 IKEDBG/0 RPT=561 64.104.205.92
Group [ciscogroup] User [ciscouser]
Sending RESPONDER LIFETIME notification to Initiator

1933 11/29/2001 16:20:18.530 SEV=9 IKEDBG/0 RPT=562 64.104.205.92
Group [ciscogroup] User [ciscouser]
constructing qm hash

1935 11/29/2001 16:20:18.530 SEV=8 IKEDBG/0 RPT=563 64.104.205.92
SENDING Message (msgid=718cb0db) with payloads :
HDR + HASH (8) ... total length : 176

1941 11/29/2001 16:20:18.530 SEV=8 IKEDBG/0 RPT=564 64.104.205.92
RECEIVED Message (msgid=13dc5023) with payloads :
HDR + HASH (8) + NONE (0) ... total length : 48

1943 11/29/2001 16:20:18.530 SEV=9 IKEDBG/0 RPT=565 64.104.205.92
Group [ciscogroup] User [ciscouser]
processing hash

1944 11/29/2001 16:20:18.530 SEV=9 IKEDBG/0 RPT=566 64.104.205.92
Group [ciscogroup] User [ciscouser]
loading all IPSEC SAs

1945 11/29/2001 16:20:18.530 SEV=9 IKEDBG/1 RPT=153 64.104.205.92
Group [ciscogroup] User [ciscouser]
Generating Quick Mode Key!

1946 11/29/2001 16:20:18.530 SEV=9 IKEDBG/1 RPT=154 64.104.205.92
Group [ciscogroup] User [ciscouser]
Generating Quick Mode Key!

1947 11/29/2001 16:20:18.540 SEV=7 IKEDBG/0 RPT=567 64.104.205.92
Group [ciscogroup] User [ciscouser]
Loading host:
 Dst: 10.64.10.9
 Src: 192.168.1.1

1949 11/29/2001 16:20:18.540 SEV=4 IKE/49 RPT=3 64.104.205.92
Group [ciscogroup] User [ciscouser]
Security negotiation complete for User (ciscouser)
Responder, Inbound SPI = 0x11a56495, Outbound SPI = 0xb17718a5

1952 11/29/2001 16:20:18.540 SEV=9 IPSECDBG/6 RPT=17
IPSEC key message parse - msgtype 1, len 608, vers 1, pid 00000000, seq 0, err 0
, type 2, mode 1, state 64, label 0, pad 0, spi b17718a5, encrKeyLen 24, hashKey
Len 16, ivlen 8, alg 2, hmacAlg 3, lifetype 0, lifetime1 7633504, lifetime2 0, d
sId 0

1956 11/29/2001 16:20:18.540 SEV=9 IPSECDBG/1 RPT=45
Processing KEY_ADD msg!

1957 11/29/2001 16:20:18.540 SEV=9 IPSECDBG/1 RPT=46
key_msghdr2secassoc(): Enter

1958 11/29/2001 16:20:18.540 SEV=9 IPSECDBG/1 RPT=47
KeyProcessAdd: Enter

1959 11/29/2001 16:20:18.540 SEV=8 IPSECDBG/1 RPT=48
KeyProcessAdd: Adding outbound SA

1960 11/29/2001 16:20:18.540 SEV=8 IPSECDBG/1 RPT=49
KeyProcessAdd: src 10.64.10.9 mask 0.0.0.0, dst 192.168.1.1 mask 0.0.0.0

1961 11/29/2001 16:20:18.540 SEV=8 IPSECDBG/1 RPT=50
KeyProcessAdd: FilterIpssecAddIkeSa success

1962 11/29/2001 16:20:18.540 SEV=9 IPSECDBG/6 RPT=18

IPSEC key message parse - msgtype 3, len 328, vers 1, pid 00000000, seq 0, err 0
, type 2, mode 1, state 32, label 0, pad 0, spi 11a56495, encrKeyLen 24, hashKey
Len 16, ivlen 8, alg 2, hmacAlg 3, lifetype 0, lifetime1 7631924, lifetime2 0, d
sId 0

1966 11/29/2001 16:20:18.540 SEV=9 IPSECDBG/1 RPT=51
Processing KEY_UPDATE msg!

1967 11/29/2001 16:20:18.540 SEV=9 IPSECDBG/1 RPT=52
Update inbound SA addresses

1968 11/29/2001 16:20:18.540 SEV=9 IPSECDBG/1 RPT=53
key_msghdr2secassoc(): Enter

1969 11/29/2001 16:20:18.540 SEV=9 IPSECDBG/1 RPT=54
KeyProcessUpdate: Enter

1970 11/29/2001 16:20:18.540 SEV=8 IPSECDBG/1 RPT=55
KeyProcessUpdate: success

1971 11/29/2001 16:20:18.540 SEV=8 IKEDBG/7 RPT=3
IKE got a KEY_ADD msg for SA: SPI = 0xb17718a5

1972 11/29/2001 16:20:18.540 SEV=8 IKEDBG/0 RPT=568
pitcher: rcv KEY_UPDATE, spi 0x11a56495

1973 11/29/2001 16:20:18.540 SEV=4 IKE/120 RPT=3 64.104.205.92
Group [ciscogroup] User [ciscouser]
PHASE 2 COMPLETED (msgid=13dc5023)

1978 11/29/2001 16:20:19.100 SEV=8 IKEDBG/0 RPT=569 64.104.205.92
RECEIVED Message (msgid=718cb0db) with payloads :
HDR + HASH (8) + NONE (0) ... total length : 48

1980 11/29/2001 16:20:19.100 SEV=9 IKEDBG/0 RPT=570 64.104.205.92
Group [ciscogroup] User [ciscouser]
processing hash

1981 11/29/2001 16:20:19.100 SEV=9 IKEDBG/0 RPT=571 64.104.205.92
Group [ciscogroup] User [ciscouser]
loading all IPSEC SAs

1982 11/29/2001 16:20:19.100 SEV=9 IKEDBG/1 RPT=155 64.104.205.92
Group [ciscogroup] User [ciscouser]
Generating Quick Mode Key!

1983 11/29/2001 16:20:19.110 SEV=9 IKEDBG/1 RPT=156 64.104.205.92
Group [ciscogroup] User [ciscouser]
Generating Quick Mode Key!

1984 11/29/2001 16:20:19.110 SEV=7 IKEDBG/0 RPT=572 64.104.205.92
Group [ciscogroup] User [ciscouser]
Loading subnet:
 Dst: 0.0.0.0 mask: 0.0.0.0
 Src: 192.168.1.1

1986 11/29/2001 16:20:19.110 SEV=4 IKE/49 RPT=4 64.104.205.92
Group [ciscogroup] User [ciscouser]
Security negotiation complete for User (ciscouser)
Responder, Inbound SPI = 0x74cf6476, Outbound SPI = 0x82b07c35

1989 11/29/2001 16:20:19.110 SEV=9 IPSECDBG/6 RPT=19
IPSEC key message parse - msgtype 1, len 608, vers 1, pid 00000000, seq 0, err 0
, type 2, mode 1, state 64, label 0, pad 0, spi 82b07c35, encrKeyLen 24, hashKey
Len 16, ivlen 8, alg 2, hmacAlg 3, lifetype 0, lifetime1 7633504, lifetime2 0, d
sId 0

1993 11/29/2001 16:20:19.110 SEV=9 IPSECDBG/1 RPT=56
Processing KEY_ADD msg!

1994 11/29/2001 16:20:19.110 SEV=9 IPSECDBG/1 RPT=57
key_msghdr2secassoc(): Enter

1995 11/29/2001 16:20:19.110 SEV=9 IPSECDBG/1 RPT=58
KeyProcessAdd: Enter

1996 11/29/2001 16:20:19.110 SEV=8 IPSECDBG/1 RPT=59
KeyProcessAdd: Adding outbound SA

1997 11/29/2001 16:20:19.110 SEV=8 IPSECDBG/1 RPT=60
KeyProcessAdd: src 0.0.0.0 mask 255.255.255.255, dst 192.168.1.1 mask 0.0.0.0

1998 11/29/2001 16:20:19.110 SEV=8 IPSECDBG/1 RPT=61
KeyProcessAdd: FilterIpssecAddIkeSa success

1999 11/29/2001 16:20:19.110 SEV=9 IPSECDBG/6 RPT=20
IPSEC key message parse - msgtype 3, len 328, vers 1, pid 00000000, seq 0, err 0
, type 2, mode 1, state 32, label 0, pad 0, spi 74cf6476, encrKeyLen 24, hashKey
Len 16, ivlen 8, alg 2, hmacAlg 3, lifetype 0, lifetime1 7631924, lifetime2 0, d
sId 0

2003 11/29/2001 16:20:19.110 SEV=9 IPSECDBG/1 RPT=62
Processing KEY_UPDATE msg!

2004 11/29/2001 16:20:19.110 SEV=9 IPSECDBG/1 RPT=63
Update inbound SA addresses

2005 11/29/2001 16:20:19.110 SEV=9 IPSECDBG/1 RPT=64
key_msghdr2secassoc(): Enter

2006 11/29/2001 16:20:19.110 SEV=9 IPSECDBG/1 RPT=65
KeyProcessUpdate: Enter

2007 11/29/2001 16:20:19.110 SEV=8 IPSECDBG/1 RPT=66
KeyProcessUpdate: success

2008 11/29/2001 16:20:19.110 SEV=8 IKEDBG/7 RPT=4
IKE got a KEY_ADD msg for SA: SPI = 0x82b07c35

2009 11/29/2001 16:20:19.120 SEV=8 IKEDBG/0 RPT=573
pitcher: rcv KEY_UPDATE, spi 0x74cf6476

2010 11/29/2001 16:20:19.120 SEV=4 IKE/120 RPT=4 64.104.205.92
Group [ciscogroup] User [ciscouser]
PHASE 2 COMPLETED (msgid=718cb0db)

2011 11/29/2001 16:20:19.150 SEV=7 IPSECDBG/1 RPT=67
IPSec Inbound SA has received data!

2012 11/29/2001 16:20:19.150 SEV=8 IKEDBG/0 RPT=574
pitcher: recv KEY_SA_ACTIVE spi 0x74cf6476

2013 11/29/2001 16:20:19.150 SEV=8 IKEDBG/0 RPT=575
KEY_SA_ACTIVE no old rekey centry found with new spi 0x74cf6476, mess_id 0x0

2016 11/29/2001 16:20:19.490 SEV=7 IPSECDBG/1 RPT=68
IPSec Inbound SA has received data!

2017 11/29/2001 16:20:19.490 SEV=8 IKEDBG/0 RPT=576
pitcher: recv KEY_SA_ACTIVE spi 0x11a56495

2018 11/29/2001 16:20:19.490 SEV=8 IKEDBG/0 RPT=577

KEY_SA_ACTIVE no old rekey centry found with new spi 0x11a56495, mess_id 0x0

Bad Debugs

- Remote peer no longer responds.
- Failure to establish a secure connection to the security gateway.
- User authentication fails (incorrect user name).
- User authentication fails (incorrect user password).
- User authentication fails – misconfiguration in choosing server type (Internal or External)
- User authentication fails – mismatch in group name letter case (Case Sensitive)
- Problem in authenticating VPN Client with certificates due to time synchronization between VPN Concentrator and CA server
- Remote peer terminates the connection.
- GET post-validation Bad Value error on aIEventInclusionListData.1.
- User receives the "Failure during phase 1 rekeying attempt due to collision" error message.
- User receives the Received non-routine Notify message: Invalid ID info (18) log message on the Cisco VPN 3000 Concentrator
- SEV=3 CAPI/0 RPT=877 CAPI IPsec Authentication Error : No decompression performed

Remote peer no longer responds.

This message on the client indicates that the group name is incorrect.

```
236 11/28/2001 15:20:07.030 SEV=9 IKEDBG/23 RPT=3 10.64.10.6
Starting group lookup for peer 10.64.10.6

237 11/28/2001 15:20:07.030 SEV=4 IKE/22 RPT=2 10.64.10.6
No Group found matching cisCogroup for Pre-shared key peer 10.64.10.6

238 11/28/2001 15:20:07.030 SEV=9 IKEDBG/0 RPT=136 10.64.10.6
Group [cisCogroup]
IKE SA AM:88a549ad terminating:
flags 0x0000c001, refcnt 0, tuncnt 0

240 11/28/2001 15:20:07.030 SEV=9 IKEDBG/0 RPT=137
sending delete message
```

Failure to establish a secure connection to the security gateway.

This message on the client indicates that the group password is incorrect.

```
293 11/28/2001 15:23:53.990 SEV=9 IKEDBG/0 RPT=175 10.64.10.6
Group [ciscogroup]
Processing Notify payload

294 11/28/2001 15:23:53.990 SEV=8 IKEDECODE/0 RPT=263 10.64.10.6
Notify Payload Decode :
  DOI           :      IPSEC (1)
  Protocol      :      ISAKMP (1)
  Message       :      Invalid hash info (23)

  Length       :      12

298 11/28/2001 15:23:53.990 SEV=5 IKE/68 RPT=1 10.64.10.6
Group [ciscogroup]
Received non-routine Notify message: Invalid hash info (23)
```

User authentication fails (incorrect user name).

This message on the client indicates that the user name is incorrect.

```
411 11/28/2001 15:30:48.680 SEV=3 AUTH/5 RPT=2 10.64.10.6
Authentication rejected: Reason = User was not found
handle = 6, server = Internal, user = Ciscouser, domain =
```

User authentication fails (incorrect user password).

This message on the client indicates that the user password is incorrect.

```
819 11/28/2001 16:20:27.770 SEV=3 AUTH/5 RPT=4 10.64.10.6
Authentication rejected: Reason = Invalid password
handle = 9, server = Internal, user = ciscouser, domain =
```

User authentication fails – misconfiguration in choosing server type (Internal or External).

This message on the VPN 3000 Concentrator indicates that the server type chosen for user authentication is incorrect. For example, if the VPN Concentrator uses the Kerberos protocol to communicate with an external authentication server, choose the authentication server type as **External** (Kerberos) under the IPsec tab.

```
26779 10/16/2006 15:58:24.160 SEV=4 AUTH/15 RPT=15
Server name = gw-pr01, type = KERBEROS,
group = IT, status = Active
```

```
26780 10/16/2006 15:58:57.260 SEV=5 IKEDBG/64 RPT=18 192.168.1.25
IKE Peer included IKE fragmentation capability flags:
Main Mode: True
Aggressive Mode: False
```

```
!--- When you try to authenticate the user
!--- 'vpnuser1', the VPN Concentrator attempts to authenticate internally.
```

```
26782 10/16/2006 15:59:00.800 SEV=3 AUTH/5 RPT=26 192.168.1.25
Authentication rejected: Reason = User was not found
handle = 846, server = Internal, user = vpnuser1, domain = <not specified>
```

```
26784 10/16/2006 15:59:03.940 SEV=3 AUTH/5 RPT=27 192.168.1.25
Authentication rejected: Reason = User was not found
handle = 847, server = Internal, user = vpnuser1, domain = <not specified>
```

```
26786 10/16/2006 15:59:06.300 SEV=3 AUTH/5 RPT=28 192.168.1.25
Authentication rejected: Reason = User was not found
handle = 848, server = Internal, user = vpnuser1, domain = <not specified>
```

```
26788 10/16/2006 15:59:06.310 SEV=4 IKE/167 RPT=6 192.168.1.25
Group [IT] User [vpnuser1]
Remote peer has failed user authentication -
check configured username and password
```

```
26791 10/16/2006 15:59:06.320 SEV=5 IKE/194 RPT=10 192.168.1.25
Group [IT] User [vpnuser1]
Sending IKE Delete With Reason message: No Reason Provided.
```

```
26793 10/16/2006 15:59:38.350 SEV=4 CONFIG/17 RPT=6
Done writing configuration file, Success.
```

User authentication fails – mismatch in group name letter case (case sensitive).

VPN group names are **case sensitive**. This means that user authentication fails if the group name specified in the VPN Concentrator and the group name in the "OU=" field of an MS RADIUS server or on the client are different in terms of letter case (upper or lower case).

For example, when you enter the group name as **VPNGroup** in one device and **vpngroup** in another device, the device does not work.

Problem in authenticating the VPN Client with certificates due to time synchronization between the VPN Concentrator and CA server.

On a VPN Concentrator that uses a CA server for the authentication of VPN Clients, this message indicates that the VPN Client is not authenticated even if the certification validation is successful. This is because the time on the VPN Concentrator and the time on the CA server are too far out of sync.

```
1407 10/18/2006 15:09:56.900 SEV=5 IKE/79 RPT=13 10.1.1.28
Group [ipseccert]
Validation of certificate successful
(CN=client2, SN=040DF7E8000000000010)

1409 10/18/2006 15:09:56.900 SEV=7 IKEDBG/0 RPT=9259 10.1.1.28
Group [ipseccert]
peer ID type 9 received (DER_ASN1_DN)
```

Solution: Ensure that the time is configured properly on both the VPN Concentrator and the CA server. The use of NTP on both the VPN Concentrator and the CA server allows you to keep time in sync.

Remote peer terminates the connection.

This message on the client indicates that no address pool is configured or no assignment mode is checked.

```
815 11/28/2001 16:22:43.630 SEV=6 IKE/0 RPT=10
TM received unexpected event EV_START_XAUTH in state TM_START

826 11/28/2001 16:22:48.640 SEV=7 IKEDBG/42 RPT=1 10.64.10.6
Group [ciscogroup] User [ciscouser]
IKE received response of type [FAILED] to a request from the IP address utility

828 11/28/2001 16:22:48.640 SEV=5 IKE/132 RPT=1 10.64.10.6
Group [ciscogroup] User [ciscouser]
Cannot obtain an IP address for remote peer

846 11/28/2001 16:22:48.640 SEV=6 IKE/38 RPT=2 10.64.10.6
Header invalid, missing SA payload! (next payload = 8)

847 11/28/2001 16:22:48.640 SEV=8 IKEDBG/0 RPT=339
SENDING Message (msgid=0) with payloads :
HDR + NOTIFY (11) ... total length : 68

856 11/28/2001 16:22:48.640 SEV=6 IKE/38 RPT=3 10.64.10.6
Header invalid, missing SA payload! (next payload = 8)
```

GET post-validation Bad Value error on aIEventInclusionListData.1

Check to see if **Save Log on Wrap** is selected under **Configuration > System > Events > General**. If this option is selected, look under **Administration > File Management** for a large number of old log files. These log files take up lot of memory on the Cisco VPN 3000 Concentrator and can cause it to crash. Uncheck **Save Log on Wrap** and delete all the old log files to overcome this issue. If you need to keep old logs, setup either

a syslog server or FTP backup.

User receives the "Failure during phase 1 rekeying attempt due to collision" error message.

This error message means that the ISAKMP lifetime on both the VPN Concentrator and the remote site (VPN) does not match. The default ISAKMP lifetime on the VPN Concentrator is 86400 seconds. Therefore, you need to check this ISAKMP lifetime on both the VPN Concentrator and the remote VPN device to make sure that they match.

User receives the Received non-routine Notify message: Invalid ID info (18) log message on the Cisco VPN 3000 Concentrator

Complete these steps in order to resolve this issue:

1. Examine the specific reason information. Many notify messages indicate a configuration setting that the peer does not accept.

Most often, this error message is seen when there is a misconfiguration, for example, some attributes are not matched, for a LAN-to-LAN VPN tunnel between the Cisco VPN 3000 Concentrator and a third-party PIX Firewall.

2. Check the network lists (Access Control Lists [ACLs]) on both ends of this VPN tunnel.

They have to be identical mirrors of each other.

Refer to these documents for more information:

- [Configuring an IPSec Tunnel – Cisco VPN 3000 Concentrator to Checkpoint 4.1 Firewall](#)
- Refer to the [Configuration | Policy Management | Traffic Management | Network Lists](#) section of [Policy Management](#) for instructions on how to configure network lists on the VPN 3000 Concentrator.

SEV=3 CAPI/0 RPT=877 CAPI IPsec Authentication Error : No decompression performed

These message indicates that:

- Corrupted frames are dropped before they enter the compression engine. These were previously used to pass these errored frames into the decompressor, which results in the 100 percent CPU hang that IPsec compression causes.
- Frames received by the concentrator cannot be decrypted because the hash is failing. This is typically caused by a PAT device.
- Therefore, there is a PAT device somewhere either in front of the concentrator or the VPN clients that causes the message to be appeared.

You can create a different group for broadband users and have LZS compression off since these options are only useful for dial-in users. Go to the **Group Configuration** and then the **IPSEC** tab in order to find this option. You can set the Compression option to **none**.

Known Issues when you use Kerberos between a VPN 3000 Concentrator and a Windows Active Directory (AD) Server

There are a few known issues when you use Kerberos between a VPN 3000 Concentrator and a Windows AD server:

1. Microsoft KB article 829074 describes a bug in Windows 2003: Users Cannot Connect to a Windows Server 2003 Domain by Using a VPN Connection

The solution for this is to install the hotfix from Microsoft referenced in the article.

2. Most other problems are related to the fact that the server tries to switch to TCP instead of UDP if the Kerberos packets get larger than a certain size.

There are two things that can be done about this:

- ◆ The solution is to update (on the AD server) the subkey in HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Kdc MaxDatagramReplySize to 32000 (decimal), and reboot the server.

This registry key is also explained in MS Knowledge base article 837361 .

- ◆ In the Active Directory server, on the Account tab of the User Properties of the failing user, you should see this check box:

Do not require kerberos pre-authentication

If this check box is unchecked, check it and try to authenticate again with this user.

NetPro Discussion Forums – Featured Conversations

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

NetPro Discussion Forums – Featured Conversations for VPN
Service Providers: VPN Service Architectures
Service Providers: Network Management
Virtual Private Networks: General

Related Information

- [Cisco VPN 3000 Series Configuration Guide Release 4.7](#)
- [Cisco VPN 3000 Series Concentrators](#)
- [Cisco VPN 3002 Hardware Clients](#)
- [IPsec Negotiation/IKE Protocols](#)
- [Technical Support & Documentation – Cisco Systems](#)

All contents are Copyright © 2006–2007 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

Updated: Nov 30, 2006

Document ID: 23840
