



# Release Notes for Cisco 7000 Family for Cisco IOS Release 12.2(14)SU

---

January 27, 2005

Text Part Number OL-5458-01 B0

These release notes describe changes to the software for the Cisco 7200 series routers for Cisco IOS Release 12.2(14)SU.

## Contents

- [Introduction, page 2](#)
- [System Requirements, page 5](#)
- [New and Changed Information, page 7](#)
- [Caveats, page 8](#)
- [Sample Configuration, page 28](#)
- [Related Documentation, page 31](#)
- [Obtaining Documentation, page 31](#)
- [Documentation Feedback, page 32](#)
- [Cisco Product Security Overview, page 32](#)
- [Obtaining Technical Assistance, page 33](#)
- [Obtaining Additional Publications and Information, page 35](#)
- [Glossary, page 36](#)



---

**Corporate Headquarters:**  
**Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA**

Copyright © 2005 Cisco Systems, Inc. All rights reserved.

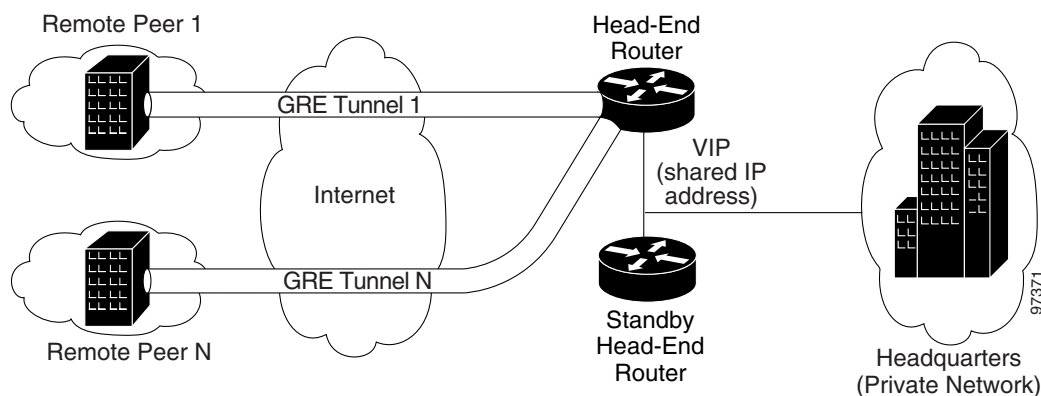
# Introduction

Cisco IOS Software Release 12.2(14)SU features Stateful Failover of IPsec security associations (SAs) for site-to-site VPN (see [Figure 1](#)), storage of encrypted pre-shared keys in the configuration, Cisco 7200 NPE-G1 processor support, and VAM2 crypto card support (DES and 3DES only). Cisco IOS Software Release 12.2(14)SU is based on Cisco IOS Release 12.2(11)YX, which supports Stateful Failover of IPsec SAs for site-to-site VPNs, but not on Cisco 7200 routers with the NPE-G1 processor, and not on VAM2 crypto cards.

[Figure 1](#) shows a sample topology for site-to-site configuration of IPsec Stateful Failover with Generic Routing Encapsulation (GRE), a tunnel interface not tied to specific “passenger” or “transport” protocols.

GRE supports multicast traffic, critical for V3PN applications.

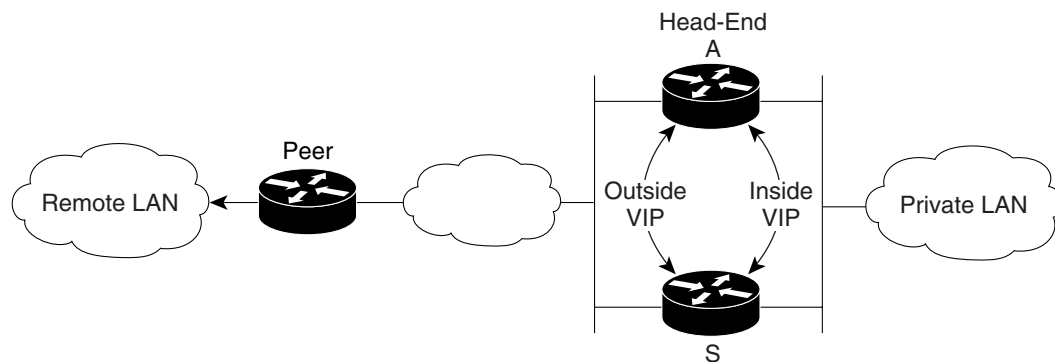
**Figure 1 Site-to-Site VPN Configuration**



There are four possible configurations for the Cisco 7200 series routers using Cisco IOS Release 12.2(14)SU:

- non-GRE High Availability (HA) with a virtual IP (VIP), or redundancy groups, on the outside and a VIP on the inside (see [Figure 2](#))
- non-GRE HA with only VIPs on the outside. The route to the outside is provided by Reverse Route Injection (RRI) (see [Figure 3](#))
- GRE HA, with VIPs on the outside and inside interfaces (see [Figure 4](#))
- GRE HA, with only a VIP on the outside, using RRI to inject routes (see [Figure 5](#))

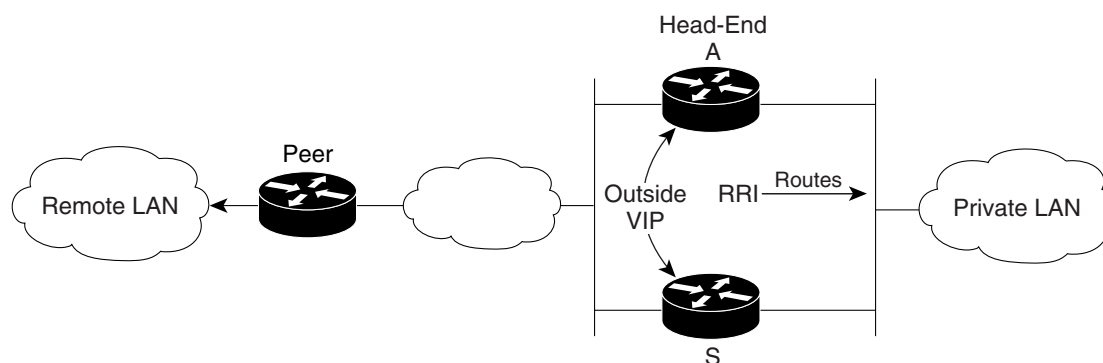
**Figure 2 HSRP VIP on Inside and Outside**



Inside VIP configured as default gateway for route from private LAN to remote LAN

114186

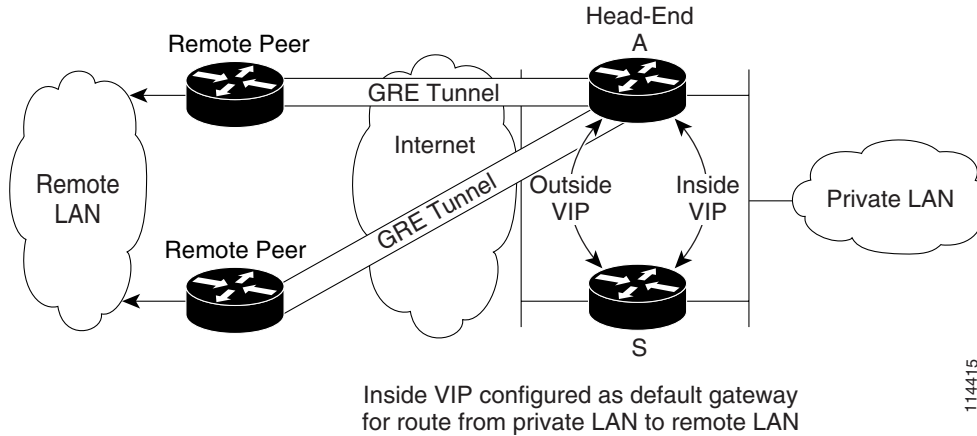
**Figure 3 HSRP VIP on Outside, RRI Injected Routes on Inside**



Reverse Route Injection (RRI) is configured on the head-end router when the tunnel is forming. RRI injects static routes to the remote network.

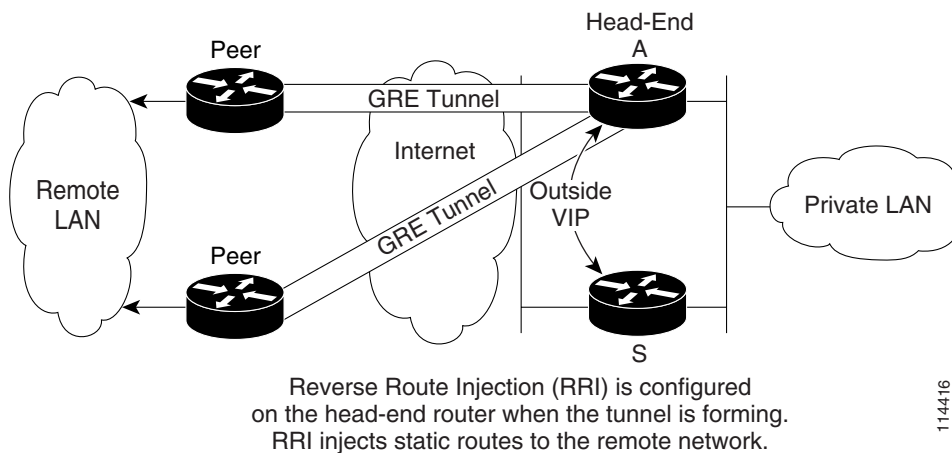
114187

**Figure 4** GRE HA with VIPs on the Outside and Inside Faces



114415

**Figure 5** GRE HA with Only a VIP on the Outside, Using RRI to Inject Routes



114416

## Features

The following features are new to Cisco IOS Release 12.2(14)SU:

- Cisco 7200 router with the NPE-G1 processor
- VPN Acceleration Module (VAM), VPN Acceleration Module 2 (VAM2)
- Encrypted pre-shared key

[Table 1](#) provides a summary of the Cisco IOS Release 12.2(14)SU performance guidelines.



### Note

Performance may vary depending on the actual features enabled, however these guidelines offer general guidelines for stable deployment. Contact Cisco TAC for guidelines outside of these parameters.

**Table 1 Performance Guidelines**

Feature	Description
Number of tunnels	<ul style="list-style-type: none"> <li>2000 tunnels [2000 IKE SA: 4000 IPSec SA] for Cisco 7200 with NPE-G1 or NPE400 with VAM/VAM2</li> <li>500 tunnels for Cisco 7200 with NPE225 with VAM/VAM2</li> </ul>
GRE	1000 GRE/IPSec tunnels

## Limitations

Cisco IOS Release 12.2(14)SU feature limitations include:

- No EzVPN support for Stateful Failover
- Only single VAM/VAM2 support in the high availability (HA) configuration
- IPSec stateful solution is incompatible with old style IKE keepalives but is compatible with DPD (Note: DPD is not a requirement for IPSec stateful HA solution)
- No AES support in Cisco IOS Release 12.2(14)SU or hardware (VAM2)
- No NAT-T features

## System Requirements

This section includes the following topics:

- [Memory Requirements, page 5](#)
- [Hardware Supported, page 6](#)
- [Determining the Software Version, page 6](#)
- [Upgrading to a New Software Release, page 6](#)
- [Feature Set Tables, page 7](#)

## Memory Requirements

[Table 2](#) lists the software images and corresponding memory requirements for the Cisco 7200 series routers in Cisco IOS Release 12.2(14)SU.



### Note

For a complete list of the minimum memory recommendations for the Cisco 7200 series of routers in Cisco IOS Release 12.2, go to the following URL:

<http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122reInt/xprn122/122feats.htm#55814>



### Note

It is recommended that you upgrade your boot image with the c7200-kboot-mz boot helper image when using Cisco IOS Release 12.2(14)SU.

**Table 2** Software Images and Memory Recommendations for Cisco IOS Release 12.2(14)SU

Platform	Feature Set	Image Name	Flash Memory Required	Minimum DRAM
Cisco 7200	Cisco IOS IP/FW/IDS/IPSec 3DES	c7200-ik9o3s-mz	64 MB	256 MB
	Cisco IOS IP Plus/IPSec 3DES	c7200-ik9s-mz	64 MB	256 MB
	Cisco IOS Enterprise/FW/IDS/IPSec 3DES	c7200-jk9o3s-mz	64 MB	256 MB
	Cisco IOS Enterprise/IPSec 3DES	c7200-jk9s-mz	64 MB	256 MB
	Cisco IOS Enterprise IPSec 3DES	c7200-kboot-mz	64 MB	256 MB

## Hardware Supported

Cisco IOS Software Release 12.2(14)SU supports the Cisco 7200 series routers with NPE- 225, NPE-400, and NPE-G1 processors, as well as the VPN Acceleration Module (VAM) and VAM2 crypto cards (DES and 3DES only).



### Note

Cisco IOS Software Release 12.2(14)SU supports only a single VAM/VAM2 in the HA configuration.

For additional information about supported hardware for these platforms, refer to the Hardware/Software Compatibility Matrix in the Cisco Software Advisor at the following URL:

<http://www.cisco.com/cgi-bin/front.x/Support/HWSWmatrix/hswswmatrix.cgi>

## Determining the Software Version

To determine the version of Cisco IOS software running on your router, log in to the router and enter the **show version EXEC** command:



### Note

The following example shows output from the Cisco 7200 series router.

```
router> show version
```

```
Cisco Internetwork Operating System Software
IOS (tm) 7200 series Software c7200-jk9o3s-mz, Version 12.2(14)SU, RELEASE SOFTWARE
```

## Upgrading to a New Software Release

For general information about upgrading to a new software release, refer to *Software Installation and Upgrade Procedures* located at the following URL:

[http://www.cisco.com/warp/public/130/upgrade\\_index.shtml](http://www.cisco.com/warp/public/130/upgrade_index.shtml)

## Feature Set Tables

The Cisco IOS software is packaged in feature sets consisting of software images—depending on the platform. Each feature set contains a specific set of Cisco IOS features.

For a complete list of feature sets supported by the Cisco 7200 series routers in Release 12.2, go to the following URL:

<http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122reInt/xprn122/122reqs.htm#xtocid3>



### Caution

Cisco IOS images with strong encryption (including, but not limited to, 168-bit Triple Data Encryption Standard [3DES] data encryption feature sets) are subject to United States government export controls and have limited distribution. Strong encryption images to be installed outside the United States are likely to require an export license. Customer orders may be denied or subject to delay because of United States government regulations. When applicable, purchaser and user must obtain local import and use authorizations for all encryption strengths. Please contact your sales representative or distributor for more information, or send an E-mail to [export@cisco.com](mailto:export@cisco.com).

## New and Changed Information

This section includes the following topics:

- [New Hardware Features in Cisco IOS Release 12.2\(14\)SU, page 7](#)
- [New Software Features in Cisco IOS Release 12.2\(14\)SU, page 7](#)

### New Hardware Features in Cisco IOS Release 12.2(14)SU

The following hardware features are new to Cisco IOS Release 12.2(14)SU:

- Cisco 7200 router NPE-G1 processor
- VPN Acceleration Module 2 (VAM2)



### Note

Support for Stateful Failover of IPsec security associations (SAs) for site-to-site VPNs was first introduced on Cisco IOS Release 12.2(11)YX, but did not extend to Cisco 7200 routers with the NPE-G1 processor, and VAM2 crypto cards.

### New Software Features in Cisco IOS Release 12.2(14)SU

Encrypted pre-shared key is the new software feature added to Cisco IOS Release 12.2(14)SU.

The following software features were previously introduced in Cisco IOS Release 12.2(11)YX and Cisco IOS Release 12.2(11)YX1, and are also supported in Cisco IOS Release 12.2(14)SU:

- IPsec High Availability with Generic Routing Encapsulation (GRE)—Adds a tunnel interface for each GRE endpoint. Because tunnels are point-to-point links, you must configure a separate tunnel for each link.
- IPsec High Availability—Enables VPN tunnels to fail over from an active unit to a standby unit without reinitiating the VPN tunnels, and without detection by remote devices.

- IKE Acceleration—Reduces VPN tunnel setup time. This feature is useful in network storm situations, when a large number of tunnels need to be set up simultaneously.
- Dead Peer Detection (DPD)—Tracks peer connectivity. When a peer connection is down, it will trigger IKE renegotiation. While similar to IKE keepalive functions, it provides improved scalability and less peer tracking overhead. DPD is the only keepalive supported under stateful HA.
- Multiple redundancy groups (VIPs).

## Caveats

This section lists caveats for the Cisco IOS Release 12.2(14)SU, by tracking number (DDTS #) and release number, and indicates whether the caveat has been corrected. An “O” indicates that the caveat is open in the release; a “C” indicates that the caveat is closed in the release, and an “R” indicates that the caveat is resolved in the release.



**Note**

If you are a registered cisco.com user, view Bug Toolkit on cisco.com at the following website:

[http://www.cisco.com/kobayashi/support/tac/tools\\_trouble.shtml](http://www.cisco.com/kobayashi/support/tac/tools_trouble.shtml)

To become a registered cisco.com user, go to the following website:

<http://tools.cisco.com/RPF/register/register.do>

Table 3 lists the caveats for the Cisco IOS Release 12.2(14)SU.

**Table 3** *Caveats for Cisco IOS Release 12.2(14)SU*

Cisco IOS Software Release 12.2(14)SU	
DDTS Number	Status
<a href="#">CSCdt38138</a>	R
<a href="#">CSCdu14815</a>	R
<a href="#">CSCdu27522</a>	R
<a href="#">CSCdu83902</a>	R
<a href="#">CSCdv02381</a>	R
<a href="#">CSCdy23784</a>	R
<a href="#">CSCdz28836</a>	R
<a href="#">CSCdz41087</a>	R
<a href="#">CSCdz45785</a>	R
<a href="#">CSCdz55602</a>	R
<a href="#">CSCdz66009</a>	R
<a href="#">CSCdz84583</a>	R
<a href="#">CSCdz90291</a>	R
<a href="#">CSCea04725</a>	R
<a href="#">CSCea19885</a>	R

**Table 3** *Caveats for Cisco IOS Release 12.2(14)SU (continued)*

<b>Cisco IOS Software Release 12.2(14)SU</b>	
<b>DDTS Number</b>	<b>Status</b>
<a href="#">CSCea26142</a>	R
<a href="#">CSCea32240</a>	R
<a href="#">CSCea33065</a>	R
<a href="#">CSCea36231</a>	R
<a href="#">CSCea46342</a>	R
<a href="#">CSCea51030</a>	R
<a href="#">CSCea51076</a>	R
<a href="#">CSCea51108</a>	R
<a href="#">CSCea54851</a>	R
<a href="#">CSCea66198</a>	R
<a href="#">CSCea72586</a>	R
<a href="#">CSCea73184</a>	R
<a href="#">CSCea80003</a>	R
<a href="#">CSCea89248</a>	R
<a href="#">CSCeb10232</a>	R
<a href="#">CSCeb16876</a>	R
<a href="#">CSCeb26495</a>	R
<a href="#">CSCeb38634</a>	R
<a href="#">CSCeb47002</a>	R
<a href="#">CSCeb56909</a>	R
<a href="#">CSCeb68105</a>	R
<a href="#">CSCec21593</a>	R
<a href="#">CSCec24217</a>	R
<a href="#">CSCec33454</a>	R
<a href="#">CSCec33664</a>	R
<a href="#">CSCec48816</a>	R
<a href="#">CSCec84331</a>	R
<a href="#">CSCec85977</a>	R
<a href="#">CSCec88024</a>	R
<a href="#">CSCed09248</a>	R
<a href="#">CSCed11518</a>	R
<a href="#">CSCed13751</a>	R
<a href="#">CSCed16994</a>	R
<a href="#">CSCed18933</a>	R
<a href="#">CSCed19230</a>	R

**Table 3** *Caveats for Cisco IOS Release 12.2(14)SU (continued)*

<b>Cisco IOS Software Release 12.2(14)SU</b>	
<b>DDTS Number</b>	<b>Status</b>
CSCed19428	R
CSCed19587'	R
CSCed22494	R
CSCed22795	R
CSCed27956	R
CSCed28138	R
CSCed31869	R
CSCed31890	R
CSCed32403	R
CSCed33591	R
CSCed33762	R
CSCed33770	R
CSCed34652	R
CSCed34670	R
CSCed35253	
CSCed35796	R
CSCed36090	R
CSCed36105	R
CSCed36412	R
CSCed36440	R
CSCed36440	R
CSCed38527	R
CSCed40933	R
CSCed44981	R
CSCed46460	R
CSCed47133	R
CSCed47856	R
CSCed48389	R
CSCec48816	R
CSCed49592	R
CSCed54904	R
CSCed58110	R
CSCed59558	R
CSCed61928	R
CSCed65825	R

**Table 3** Caveats for Cisco IOS Release 12.2(14)SU (continued)

Cisco IOS Software Release 12.2(14)SU	
DDTS Number	Status
<a href="#">CSCed73109</a>	R
<a href="#">CSCed73415</a>	R
<a href="#">CSCed76298</a>	R
<a href="#">CSCed80460</a>	R
<a href="#">CSCed84283</a>	R
<a href="#">CSCed96004</a>	R
<a href="#">CSCee00041</a>	R
<a href="#">CSCee24950</a>	R
<a href="#">CSCee67450</a>	R

In this section, the following information is provided for each caveat:

- Symptoms—A description of what is observed when the caveat occurs.
- Conditions—The conditions under which the caveat has been known to occur.
- Workaround—Solutions, if available, to counteract the caveat.

**Note**

If you have an account with Cisco.com, you can use Bug Navigator II to find caveats of any severity for any release. To reach Bug Navigator II, log in to Cisco.com and click **Software Center: Cisco IOS Software: Bug Toolkit: Bug Navigator II**. Another option is to go to [http://www.cisco.com/cgi-bin/Support/Bugtool/launch\\_bugtool.pl](http://www.cisco.com/cgi-bin/Support/Bugtool/launch_bugtool.pl).

The caveats section includes the following subsections:

- [Open Caveats—Cisco IOS Release 12.2\(14\)SU, page 11](#)
- [Resolved Caveats—Cisco IOS Release 12.2\(14\)SU, page 12](#)

## Open Caveats—Cisco IOS Release 12.2(14)SU

This section describes possibly unexpected behavior by Cisco IOS Release 12.2(14)SU. All the caveats listed in this section are open in Cisco IOS Release 12.2(14)SU. This section describes severity 1 and 2 caveats and select severity 3 caveats.

**Note**

Many caveats that apply to Cisco IOS Release 12.2 also apply to Cisco IOS Release 12.2(11)S. For information on severity 1 and 2 caveats in Cisco IOS Release 12.2, see the *Caveats for Cisco IOS Release 12.2* document located on Cisco.com at the following URL:

<http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122relnt/xprn122/index.htm>

- CSCed20668

**Symptom:** On the standby device, you may see the following IPsec security association (SA) insertion failure message:

```
%CRYPTO_HA-3-IPSECADENTRYFAIL: (VIP=80.0.0.200) IPSEC SA entry insertion on standby device failed
```

**Condition:** This occurs when Quality of Service (QoS) is enabled, and 64 bytes packets of voice data are being sent. At rekey time, we may run into this problem; no failover attempt is needed to trigger this.

**Workaround:** Do not send small size packets.

- CSCed31869

**Symptom:** During rekey we may see the following Invalid Packet message:

```
%VPN_HW-1-PACKET_ERROR: slot: 6 Packet Encryption/Decryption error, Invalid Packet
```

**Condition:** At rekey time, we may run into this problem; no failover attempt is needed to trigger this.

**Workaround:** There is no workaround.

## Resolved Caveats—Cisco IOS Release 12.2(14)SU

This section describes caveats that have been resolved by Cisco IOS Release 12.2(14)SU.

- CSCdt38138

**Symptom:** A Cisco 7200 series router configured for IPsec may reboot with a bus error. This occurs due to a race condition in rare circumstances. Often, reloading helps continue operations until the code is upgraded.

**Workaround:** There is no workaround.

- CSCdu14815

**Symptoms:** In a multiple crypto peer and tunnel environment, packets may be encrypted with the wrong security associations and delivered to the wrong peers. This symptom may coincide with the following error on the unintended crypto peers:

```
%CRYPTO-4-RECVD_PKT_INV_IDENTITY: identity doesn't match negotiated identity
```

**Conditions:** This symptom is observed if the encryption router is a Cisco 7100 series or a Cisco 7200 series that is configured with an Integrated Service Adapter (ISA), an Integrated Service Module (ISM), a Virtual Private Network (VPN) Acceleration Module (VAM), an IP Security (IPsec) accelerator module and that is running Cisco Express Forwarding (CEF) switching.

**Workaround:** Use fast switching instead of CEF switching.

- CSCdu27522

**Symptoms:** A simple data encryption standard (DES) encrypted mechanism is needed to set a configuration password.

**Workaround:** A configuration password can be set using:

```
key config-key encrypted-password <minimum 8 chars password>
```


This password is stored in private NVRAM and can not be viewed. This same password should be used for a DES encryption (and subsequent decryption).



**Note** This DDTS has been incorporated in Cisco IOS Release 12.2(14)SU as a feature.

- CSCdu83902  
**Symptom:** A Simple Network Management Protocol (SNMP) query for cips3DesCapable may return an incorrect value.  
**Workaround:** There is no workaround.
  - CSCdv02381  
Duplicate (see [CSCdu83902](#)).
  - CSCdv40576  
**Symptoms:** Entering the **show ip rsvp neighbor**, **show ip rsvp listeners**, or **show ip rsvp sender** command line interface (CLI) commands does not provide protection against the deletion of the current state on the router console when, for example, the output pauses in the More state. This situation may cause the router to reload.  
**Conditions:** This symptom is observed on a router that is configured with Resource Reservation Protocol (RSVP).  
**Workaround:** There is no workaround.
  - CSCdy23784  
**Symptom:** A Cisco 7204VXR router with a VAM card running Cisco IOS Release 12.1(12)CE and configured for IPsec generates an error message (“Error coming back 0004”). The IPsec tunnel stays up and traffic passes without any problem.  
**Workaround:** There is no workaround.
  - CSCdz28836  
**Symptom:** When using the **no crypto engine accelerator[<slot>]** command to disable the hardware encryption adapter, the command does not appear in the running configuration, nor is it saved in the startup configuration. After reboot, the adapter is re-enabled.  
**Workaround:** If necessary, remove the adapter from the chassis.
  - CSCdz41087  
**Symptom:** In a router running Enhanced IGRP (EIGRP), after reload, the subnet of the gig interface which is covered under EIGRP as a passive interface, does not appear in the topology table.  
**Workaround:** Perform a shut/no shut on the interface, or configure an “event-buffer” under the interface configuration mode for the affected interfaces:

```
interface Ethernet1/0
  event-buffer
```

Then, copy the running configuration to the startup configuration and perform a shut/no shut on the interface.
- 
-  **Note** This command need not be configured under subinterfaces, and is not available under subinterfaces.
- 

- CSCdz45785  
**Symptoms:** The **protocol ppp virtual-template number** interface configuration command may not function.  
**Conditions:** This symptom is platform independent and is observed in an environment that uses permanent virtual circuits (PVCs) or switched virtual circuits (SVCs).  
**Workaround:** There is no workaround.

- CSCdz55602
 

**Symptoms:** A Cisco router may reload unexpectedly when you enter the **crypto card shutdown**<slot> global configuration command, followed by the **crypto card enable**<slot> global configuration command while traffic is flowing.

**Conditions:** This symptom is observed on a Cisco 7200 series router that is configured with a VPN Accelerator Module (VAM).

**Workaround:** Shut down the input interface before you enter the **crypto card shutdown** <slot> global configuration command followed by the **crypto card enable** <slot> global configuration command.
- CSCdz66009
 

**Symptom:** All IKE/IPSec security associations (SAs) on a VAM2 card failed after running for 48 hours.

**Workaround:** There is no workaround.
- CSCdz84583
 

Duplicate (see [CSCed27956](#)).
- CSCdz90291
 

**Symptom:** Routers using a crypto accelerator will print CPUHOG messages when those crypto accelerators are disabled. When all crypto accelerators are disabled, the Cisco IOS software switches to software crypto and as part of this transition will attempt a DOA clean-up, which is CPU intensive.

**Workaround:** There is no workaround.
- CSCea04725
 

**Symptom:** The counter '#pkts decompress failed' updates when decompressing 100 byte packets instead of showing '#pkts decompressed'.

**Conditions:** The counter increments with a Cisco 7200 router running a VAM while decompressing 100 byte packets. This problem is not seen for 300, 500, 1400 byte packets.

**Workaround:** There is no workaround. This is a counter issue and there is no functionality change. A 100 byte packet is not decompressed on the IKE responder.
- CSCea19885
 

**Symptoms:** A Cisco 3700 router with a voice feature enabled, such as H.323, may reload because of a bus error at the address 0xD0D0D0B.

**Conditions:** This symptom is observed on a Cisco 3700 series but may also occur on other Cisco routers.

**Workaround:** There is no workaround.
- CSCea26142
 

**Symptoms:** When using a dialer interface, IKE SAs were not being setup.

**Workaround:** There is no workaround.

- CSCea32240

**Symptoms:** Cisco products running Cisco IOS software releases contain vulnerabilities in the processing of H.323 messages, which are typically used in packetized voice or multimedia applications. Features such as NAT and the Cisco IOS Firewall must inspect H.323 messages and may be vulnerable as well. A test suite has been developed by the University of Oulu to target this protocol and identify vulnerabilities.

Support for the H.323 protocol was introduced in Cisco IOS Software Release 11.3T, and all later Cisco IOS releases are affected if configured for various types of Voice/Multimedia Application support. The vulnerabilities can be exploited repeatedly to produce a denial of service (DoS).

**Workaround:** There are workarounds available that may mitigate the impact, but these techniques may not be appropriate for use in all customer networks. This advisory is available at <http://www.cisco.com/warp/public/707/cisco-sa-20040113-h323.shtml>.

- CSCea33065

Duplicate (see [CSCea32240](#)).

- CSCea36231

Duplicate (see [CSCea32240](#)).

- CSCea46342

Duplicate (see [CSCea32240](#)).

- CSCea51030

Duplicate (see [CSCea32240](#)).

- CSCea51076

Duplicate (see [CSCea32240](#)).

- CSCea51108

**Symptom:** A router running Cisco IOS software using the VPN Accelerator Module (VAM) as the hardware crypto engine incorrectly performs anti-replay detection, even though there is no authentication enabled in the IPSec transform set. This is in violation of RFC2406, and it causes out-of-order Encapsulating Security Payload (ESP) packets to be dropped on the receiver.

**Workaround:** The workaround is to either disable the VAM, or to configure the sender such that ESP packets will not be delivered out-of-order.

- CSCea54851

Duplicate (see [CSCea32240](#)).

- CSCea66198

**Symptoms:** A Cisco 7000 series router may encounter a bus error when applying a crypto map on a FDDI interface.

**Conditions:** This symptom is observed on a Cisco 7500 series router that is running Cisco IOS Release 12.2(11)T2, Release 12.2(13)T1, or Release 12.2 (13a). The symptom may also occur in other releases such as Release 12.0 S.

**Workaround:** There is no workaround.

- CSCea72586

Duplicate (see [CSCea66198](#)).

- CSCea73184

**Symptom:** The following messages are seen on the console.

```
15:03:20: ISAKMP: someone is trying to make IKE refcount negative: struct 0x53829B6C
for
declare_sa_dead(), from 0x412BF6CC, last_last is 0x4130FA90last locker 0x412E69F8,
last_last_locker
0x412E69F8
15:03:20: -Traceback= 412EA138 412BF6E4 412BF7E4 412BB254 412BC034
15:03:48: ISAKMP: someone is trying to make IKE refcount negative: struct 0x4B907000
for
declare_sa_dead(), from 0x412BF6CC, last_last is 0x4130FA90last locker 0x412E69F8,
last_last_locker
0x412E7018
15:03:48: -Traceback= 412EA138 412BF6E4 412BF7E4 412BB254 412BC034
15:05:00: %CRYPTO-4-IKMP_NO_SA: IKE message from 101.2.129.1      has no SA and is not
an
initialization offer
15:06:18: ISAKMP: someone is trying to make IKE refcount negative: struct 0x54A6F524
for
declare_sa_dead(), from 0x412BF6CC, last_last is 0x4130FA90last locker 0x412E69F8,
last_last_locker
0x412E69F8
15:06:18: -Traceback= 412EA138 412BF6E4 412BF7E4 412BB254 412BC034
15:07:18: ISAKMP: someone is trying to make IKE refcount negative: struct 0x4BF50C5C
for
declare_sa_dead(), from 0x412BF6CC, last_last is 0x4130FA90last locker 0x412E7018,
last_last_locker
0x412E69F8
15:07:18: -Traceback= 412EA138 412BF6E4 412BF7E4 412BB254 412BC034
```

**Conditions:** These messages can be observed if the standby High Availability (HA) enabled router has a peer that does NAT-T, but no Dead Peer Detection (DPD). Currently, all routers running Cisco IOS software and Cisco VPN Clients that support NAT-T also support DPD.

**Workaround:** Use a DPD enabled router when using NAT-T, or ensure that router is on the public network, i.e. outside the NAT gateway.

- CSCea80003

**Symptom:** Reverse route injection (RRI) routes are not deleted when dynamic crypto maps with reverse-route are enabled. Security associations (SAs) are established, and routes to the remote protected networks are injected. After failing over several times, the routes are not deleted when the active router transitions to the standby router, even though there are no SAs on the router.

**Workaround:** There is no workaround.

- CSCea89248

**Symptom:** IKE will not rekey IKE security associations (SAs) correctly, since for non NAT-T SAs, the peer ports are being set to zero.

**Conditions:** If an IKE SA belongs to a peer that is not using NAT-T, it will not rekey correctly.

**Workaround:** There are no workarounds. Increase IKE SA lifetime as much as possible.

- CSCeb10232
 

**Symptoms:** The counters ‘#pkts encaps’ and ‘#pkts encrypted’ don't match the output of the **show crypto ipsec sa** command.

**Conditions:** A Cisco 7200 series router running a VPN Accelerator Module (VAM) encounters errors while processing packets.

**Workaround:** Disable VAM and use software crypto. Although the counters mismatch, functionality is not affected.
- CSCeb16876
 

**Symptoms:** A Cisco router may generate a “SYS-2-GETBUF” message during the “Tag Input” process and may subsequently reload unexpectedly.

**Conditions:** This symptom is observed when the router fragments a Multiprotocol Label Switching (MPLS) packet.

**Workaround:** There is no workaround.
- CSCeb26495
 

**Symptom:** The Internet Security Association and Key Management Protocol (ISAKMP) security association (SA) establishment might fail when many (>80) SAs are concurrently negotiated to the headend of a Cisco 7200 router with a VPN Accelerator Module (VAM), due to slow processing by the VAM.

**Conditions:** These symptoms occur when:

  - many remote peers are attempting to establish phase 1 SAs to the headend
  - when a Diffie-Hellman group5 configuration occurs in the ISAKMP policy and/or pfs group5

**Workaround:** Use group2 instead of group5.
- CSCeb38634
 

**Symptom:** The SNMP query for “cikeTunHistOutP2SaDelReqs” may return an improper value.

**Workaround:** There is no workaround.
- CSCeb47002
 

**Symptom:** A class map does not match packets that are originated from the router. All packets are classified to class-default.

**Condition:** This problem occurs on Cisco 7200 routers with VAM module when hardware encryption and fast/CEF switching are enabled.

**Workaround:** Turn off hardware encryption.
- CSCeb56909
 

Cisco Routers running Internetwork Operating System (IOS) that supports Multi Protocol Label Switching (MPLS) are vulnerable to a Denial of Service (DoS) attack on MPLS disabled interfaces.

The vulnerability is only present in Cisco IOS release trains based on 12.1T, 12.2, 12.2T, 12.3 and 12.3T. Releases based on 12.1 mainline, 12.1E and all releases prior to 12.1 are not vulnerable.

More details can be found in the security advisory which is posted at <http://www.cisco.com/warp/public/707/cisco-sa-20050126-les.shtml>.

- CSCeb68105
 

**Symptom:** A Cisco 7200 router running Cisco IOS software 12.1(E) crypto image, with dynamic crypto map configuration may drop clear traffic.

**Conditions:** Access lists are not mandatory for dynamic crypto maps. However, if we add an access list and then remove the access list from the dynamic crypto map, the assigned interface will drop clear traffic.

**Workaround:** Reattach the access list or delete the dynamic crypto map configuration and create it again.
- CSCec21593
 

**Symptom:** The Cisco 7200 routers with NPE-G1 processors and VPN Accelerator Module (VAM) cards are not supported.

**Condition:** The IKE tunnel fails to come up with Tunnel End-Point Discovery (TED) configured. The negotiation fails at Peer Discovery.

**Workaround:** A new image has been included in this Cisco IOS software release 12.2(14)SU to support Cisco 7200 routers with NPE-G1 processors and VPN Accelerator Module (VAM) cards.
- CSCec24217
 

Duplicate (see [CSCec21593](#)).
- CSCec33454
 

**Symptom:** When a router is configured to perform IKE/IPSec crypto operations, those operations are handled by the Cisco IOS crypto-software by default. When a router has crypto hardware, crypto operations will be handled by the crypto hardware.

**Condition:** When a failure exists with the crypto hardware or the crypto hardware shuts down, all crypto operations will be switched back to software operations, which can max out the router CPU and potentially disturb normal router operations.

This DDTS introduces a new CLI, which enables the Cisco IOS crypto-software to handle all IKE/IPSec crypto operations. Issue this command to make the router stop handling any IKE/IPSec crypto-operations when there is crypto-hardware failure.

**Workaround:** There is no workaround.
- CSCec33664
 

**Symptom:** When an IPSec crypto card fails, syslog messages are generated which can trigger a syslog SNMP trap when logging it at 'error' level.

**Workaround:** Set logging to 'informational' level, so as to not generate syslog SNMP traps.
- CSCec48816
 

**Symptoms:** A router may reload unexpectedly when removing **network** commands. The crash will not always happen when network commands are removed. There is a small window where this can happen when a network command which covers an interface running OSPF is removed, and there are outstanding packets from this interface in OSPF queue.

**Conditions:** This symptom is observed on a Cisco router that has the **router ospf** global configuration command enabled.

**Workaround:** There is no workaround.

- CSCec84331

**Symptom:** The crypto/ISAKMP subsystem may leak memory related to extended authentication (Xauth) and configuration mode attributes when some ISAKMP security associations (SAs) are not established during Xauth.

**Conditions:** This leak arises under stress or packet loss conditions where either the client or the server declares the SA dead in the middle of Xauth.

**Workaround:** There are no workarounds.

- CSCec85977

**Symptom:** An error 0x4 may occur on a Cisco 7200 router with a VAM.

**Conditions:** The router is configured for a large number of tunnels and has memory fragmentation or low memory conditions.




---

**Note** If there are too many error 0x4 s, after many rekeys, the router will be unable to create IPsec tunnels and reloading the crypto card is the only way out.

---

**Workaround:** Reset the crypto card (VAM), however, this will tear down all the existing tunnels.

- CSCec88024

**Symptom:** The router crashes when the system is running at 100% CPU.

**Condition:** The router crashes when running at 100% CPU with 500 GRE/IPsec tunnels with dead peer detection (DPD).

**Workaround:** The CPU should be running at approximately 50%. The Cisco IOS 12.2(14)SU release is qualified for up to 1000 GRE tunnels.

- CSCed09248

**Symptom:** A Cisco 7200 router running IPsec may crash with tracebacks pointing to mgd\_timer\_set\_exptime\_internal().

**Conditions:** A large number of IPsec tunnels are rekeyed at the same time.

**Workaround:** There is no workaround. Increasing the IPSEC SA life time might help reduce the stress on the router and hence may avoid this race condition.

- CSCed11518

**Symptom:** If the SSP channel between the active and standby router is protected by IPsec (encrypted), the security associations (SAs) will be counted when you perform a **show crypto ipsec ha** command. These should not be included in the list of SAs protected by IPsec Stateful Failover.

**Conditions:** This will happen when there is an SA specifically covering the SSP connection between the redundant head-end pair.

**Workaround:** There is no workaround. This is a cosmetic issue.

- CSCed13751

**Symptom:** A duplicate IKE SA will be created when the link is flapped. This may cause early termination of the IPSEC SAs and potentially stop traffic over the secure link.

**Conditions:** When a PIX501 is connected to a VPNSM as an EzVPN client and a link flap occurs, a duplicate IKE SA may appear on the VPNSM. This is due to a incorrect handling of an Initial Contact message.

**Workaround:** The problem can be rectified by clearing the duplicate IKE SAs and letting the EzVPN client re-establish its IPSEC tunnel.

- CSCed16994
 

**Symptom:** The processor memory usage increases with every console command.

**Condition:** With every console command, the processor memory usage increases.

**Workaround:** This is fixed in the Cisco IOS Release 12.2(14)SU.
- CSCed18933
 

**Symptoms:** During VAM card initialization, The VAM card may fail to come up, with a POST failure being the primary cause for the failure. If the hardware were faulty this might be considered the right behavior, but Statistical RNG POST Failures have also occurred on well-functioning hardware.

**Conditions:** This symptom occurs during VAM card Initialization and then only occasionally when, in accordance with the statistical nature of the RNG Test, happenstance and entropy dictate. It would be quite unusual to see the VAM fail to init from this cause more than once in any given day.

**Workaround:** Use the **microcode reload vam** command to re-attempt initialization.
- CSCed19230
 

**Symptom:** With IPSec, the Inbound Decrypting Counter on the ingress interface is not updated.

**Workaround:** The problem is resolved in the Cisco 12.2(14)SU release.
- CSCed19428
 

**Symptom:** The IPSec card incurs a '0x0006' error occurs when running 2k tunnels.

**Condition:** When running 2k tunnels overnight, rekeying at every 1hr, a '0x0006' error occurs.

**Workaround:** When running up to 2k tunnels, the problem is resolved in the Cisco 12.2(14)SU. With more tunnels, the error is still seen.
- CSCed19587
 

**Symptom:** A '%ISA-1-ERROR' message occurs with a VAM2 in slot 6 of a Cisco 7200 series router. A 'MIPS not ready' message is seen when Online Insertion and Removal (OIR) of the crypto hardware occurs.

**Workaround:** The problem is resolved in the Cisco 12.2(14)SU release.
- CSCed22494
 

**Symptom:** A Reverse Route Injection (RRI) route for the VPN clients is deleted immediately after it is installed.

**Conditions:**

  - presence of the VPN Services Module (VPNSM)
  - the dynamic crypto map entry is added to the already existing crypto map with static entries, without removing the crypto map from the interface

**Workaround:** Remove the crypto map from the interface (this will disconnect all the tunnels) and put it back there again.
- CSCed22795
 

**Symptom:** The following message is seen when issuing a **microcode reload all** command on the router which has thousands of Security Associations (SAs) established:

```
%SCHED-3-THRASHING: Process thrashing at process= Crypto IKMP
```

**Workaround:** The problem is resolved in the Cisco 12.2(14)SU release.

- CSCed27956

A vulnerability in the Transmission Control Protocol (TCP) specification (RFC793) has been discovered by an external researcher. The successful exploitation enables an adversary to reset any established TCP connection in a much shorter time than was previously discussed publicly. Depending on the application, the connection may get automatically re-established. In other cases, a user will have to repeat the action (for example, open a new Telnet or SSH session). Depending upon the attacked protocol, a successful attack may have additional consequences beyond terminated connection which must be considered. This attack vector is only applicable to the sessions which are terminating on a device (such as a router, switch, or computer) and not to the sessions that are only passing through the device (for example, transit traffic that is being routed by a router). In addition, this attack vector does not directly compromise data integrity or confidentiality.

All Cisco products which contain TCP stack are susceptible to this vulnerability.

This advisory is available at:

<http://www.cisco.com/warp/public/707/cisco-sa-20040420-tcp-ios.shtml>, and it describes this vulnerability as it applies to Cisco products that run Cisco IOS® software.

A companion advisory that describes this vulnerability for products that do not run Cisco IOS software is available at

<http://www.cisco.com/warp/public/707/cisco-sa-20040420-tcp-nonios.shtml>.

- CSCed28138

**Symptom:** Running high availability (HA) with repeated failover, the system goes into an infinite loop and the following message flows on the console:

```
 Dropping remainder of this HA IKE SSP message bcoz of infinit
```

**Condition:** Running IPSec/HA rekeying every hour with repeated failover, system goes into an infinite loop.

**Workaround:** The problem is resolved in the Cisco 12.2(14)SU release.

- CSCed31890

**Symptom:** When building one tunnel between the initiator and responder (b5), no rekey occurs. However, sending fixed data traffic (5000pps/64B) causes the CPU to fluctuate between 1-100%.

**Workaround:** There is no workaround.

- CSCed32403

**Symptom:** When an active router CPU is very busy and hello packets are not received by the standby router, two active routers may momentarily occur. On the initiator side we will see the anti-replay error message.

**Conditions:** This symptom occurs when the active router CPU is very high, or short interval failover occur.

**Workaround:** Don't allow the active router CPU to be near 100%, or don't do short interval failover.

- CSCed33591

**Symptom:** When you apply a crypto map before configuring the IP address on an interface, an IPSec Security Association (SA) is not triggered.

**Workaround:** The problem is resolved in the Cisco 12.2(14)SU release.

- CSCed33762  
**Symptom:** The **no shut** command applied to the crypto interface with thousands of subinterfaces and crypto maps attached (initiator) causes a CPUHOG.  
**Workaround:** There is no workaround.
- CSCed33770  
**Symptom:** When the Diffie-Hellman (DH) group5 is configured, the system cannot scale more than 100 tunnels.  
**Condition:** The DH group5 is not scalable. Many 'PAK\_IN\_Q\_TIME\_LIMIT\_EXCEED' messages are seen when trying to build the tunnels as low as 2pps.  
**Workaround:** Use DH-group2 instead.
- CSCed34652  
**Symptom:** The router crashes when the crypto hardware is plugged into a device where the software crypto had already been synchronized with the Active device.  
**Condition:** Inserting the crypto hardware into the router when software crypto is already synchronized with the active device, crashes the box.  
**Workaround:** The problem is resolved in the Cisco 12.2(14)SU release.
- CSCed34670  
**Symptom:** The online insertion and removal (OIR) of the crypto hardware causes multiple instances of controller integrated services adapter (ISA) in the running configuration.  
**Workaround:** The problem is resolved in the Cisco 12.2(14)SU release.
- CSCed35253  
**Symptoms:** A router may reload unexpectedly after it attempts to access a low memory address.  
**Conditions:** This symptom is observed after ACLs have been updated dynamically or after the router has responded dynamically to an IDS signature.  
**Workaround:** Disable IP Inspect and IDS.
- CSCed35796  
**Symptom:** The **clear crypto isa/sa** command on the standby device triggers a state change when the CPU is pegged at 100%.  
**Condition:** With a large number of tunnels, and the CPU running at 90-100%, doing a **clear crypto isa/sa** command on the standby device triggers a state change as hello packets are not exchanged between the active and standby devices.  
**Workaround:** The problem is resolved in the Cisco 12.2(14)SU release. Still it is not recommended that a **clear crypto** command be executed with a high CPU. Maintain the CPU at around 50% and also issue a **clear crypto isa/sa ha standby resync** command if need to be.

- CSCed36090
 

**Symptom:** Online Insertion and Removal (OIR) of the crypto hardware on the standby device causes the router to crash.

**Conditions:** The symptom is seen when the following conditions occur:

  - bring 6000 IPsec security associations (SAs)
  - unplugging the VPN Acceleration Module (VAM) in the standby device causes the router to crash
  - this is not easily reproducible

**Workaround:** This problem is resolved in Cisco IOS Release 12.2(14)SU.
- CSCed36105
 

**Symptom:** Adding the access control list (ACL) to the dynamic crypto map on the fly causes CPUHOG which in turn forces an Hot Standby Router Protocol (HSRP) state change.

**Condition:** When you initially build tunnels with a dynamic crypto map on the hub and no ACL configured, then after the tunnels are up, and you configure the ACL to the dynamic crypto map, CPUHOG is seen and the HSRP state is changed.

**Workaround:** There is no workaround.
- CSCed36412
 

**Symptom:** The processor and IO memory leak may occur while running 6k IPsec security associations (SAs).

**Conditions:** The symptom is seen when the following conditions occur:

  - 6k IPsec SAs, 1k IKE SA, 1k GRE tunnels
  - 1k Enhanced IGRP (EIGRP) neighbors
  - rekey every hour
  - repeated hardware failover

**Workaround:** This problem is resolved in Cisco IOS Release 12.2(14)SU.
- CSCed36440
 

**Symptom:** The following message is seen running high availability (HA) with repeated failover overnight:

```
sa_query_keys_handler: Invalid AVL (0x0, 0x0, 0x0)
```

**Condition:** Invalid AVL messages were seen when running 2k tunnels with repeated failover at one hour rekeys.

**Workaround:** The problem is resolved in the Cisco 12.2(14)SU release and was not seen at 2k tunnels.
- CSCed38527
 

Duplicate (see [CSCed27956](#)).

- CSCed40933  
Cisco Internetwork Operating System (IOS) Software is vulnerable to a Denial of Service (DoS) attack from crafted IPv6 packets when the device has been configured to process IPv6 traffic. This vulnerability requires multiple crafted packets to be sent to the device which may result in a reload upon successful exploitation.  
More details can be found in the security advisory, which is posted at <http://www.cisco.com/warp/public/707/cisco-sa-20050126-ipv6.shtml>.
- CSCed44981  
**Symptom:** A crash occurs at hifn7851\_process\_rx\_packet with repeated hardware failover.  
**Condition:** Running IPSec/HA with repeated crypto hardware failover, the system crashes.  
**Workaround:** The problem is resolved in the Cisco 12.2(14)SU release and was verified at 2k tunnels.
- CSCed46460  
**Symptom:** The **show cry isa key** command doesn't honor terminal length.  
**Workaround:** The problem is resolved in the Cisco 12.2(14)SU release.
- CSCed47133  
**Symptom:** The Cisco 7200 router with a VAM has a DH counter stuck in the output of **show crypto eli** command.  
**Conditions:** The symptom is seen when the following conditions occur:
  - larger number of tunnels all trying to rekey at same time
  - large number of buffer failures
  - large number of IKE negotiation failures due to mismatch in IKE/IPSec policies, ACL, etc.**Workaround:** Restart the crypto engine by issuing **crypto card shut <slot>**, and **crypto card enable <slot>** commands.
- CSCed47856  
**Symptom:** The Security Parameter Index was being displayed as a negative number beyond a specific value.  
**Conditions:** This happens when large number of tunnels are rekeying so that the security parameter index (SPI) value increases to a large value. Once it increases beyond a particular value, the display shows a negative decimal value, although the actual SPI value is still correct.  
**Workaround:** There is no workaround.

- CSCed48389

**Symptom:** When a dynamic crypto map is applied to the crypto end, and during tunnel creation, the dynamic ACL is added to multidimensional tree (mtree). If the process is too busy and can't perform the mtree update, the packets will become decrypted and will fail the mtree identity check.

The following message occurs:

```
%CRYPTO-4-RECV_PKT_INV_IDENTITY_ACL: ipsec check access: identity not allowed by ACL
```

**Conditions:** The symptom is seen when the following conditions occur:

- 2000 IKE/4000 IPSec security associations (SAs)
- a dynamic crypto map is applied to one crypto end (like static to dynamic) or applied to both crypto ends (like TED case)

**Workaround:** This code was fixed in the Cisco 12.2(14)SU release.

- CSCed49592

**Symptom:** The router crashes when disabling the crypto hardware.

**Condition:** When running repeated hardware failover, the router crashes.

**Workaround:** The problem is resolved in the Cisco 12.2(14)SU release and not seen at 2k tunnels.

- CSCed54904

**Symptom:** The router crashes while building tunnels from two initiators.

**Condition:** Building tunnels from two initiators, the active box crashes.

**Workaround:** The problem is resolved in the Cisco 12.2(14)SU release.

- CSCed58110

**Symptom:** When a Catalyst 6500 series router equipped with a VPN Services Module (VPN SM) is serving a large number of EzVPN clients in an unreliable network such that the clients frequently disconnect and reconnect, there can be a memory leak.

The memory leak can be observed by looking at the output of **sh memory allocating-process totals** command over subsequent days. The blocks that are leaked can be identified as Crypto IKMP IKE and Crypto IKMP.

**Conditions:** The problem occurs only in a Catalyst 6500 series device running 12.2(14)SY or its rebuilds. There needs to be a large number of EZVPN client sessions and the network that connects the clients to the server needs to have very intermittent connectivity.

Then customer will see a memory leak of KE messages and malloc'd memory.

**Workaround:** There are no workarounds.

- CSCed59558

**Symptom:** With 1518 bytes packet size, we may run into a situation not all the tunnels are up or none of the tunnels are up.

**Conditions:** This condition is seen only with bigger than MTU packets, and when adjacency entries are not populated.

**Workaround:** Disable cef using the **no ip cef** command and then Enable cef again using the **ip cef** command.

- CSCed61928
 

**Symptom:** When failover occurs, the standby router may take several minutes long to finish the state synchronization process.

**Conditions:** This condition is seen when building a large number of IPsec tunnels/IPsec GRE tunnels/TED tunnels, or when failover is triggered either by “shut/no shut” interface or “no crypto engine accelerator/crypto engine accelerator” for crypto card.

**Workaround:** Do not apply crypto map to the SSP channel. The sync will be fast without encrypted SSP channel.
- CSCed65825
 

**Symptom:** A router running 2k GRE/IPsec tunnels, crashes after a few rekey attempts.

**Workaround:** The problem is resolved in the Cisco 12.2(14)SU release.
- CSCed65827
 

**Symptom:** During failover stateful, security associations (SAs) flap.

**Condition:** When the active device fails before standby is in complete sync, the SAs are torn down and must be renegotiated again.

**Workaround:** It is recommended that the log and counters in the standby router be in complete sync with the active router before failover occurs.
- CSCed73109
 

**Symptom:** With the Rivest, Shamir, and Adelman (RSA) key in the startup configuration, traceback is seen during bootup.

**Workaround:** This problem is resolved in Cisco IOS Release 12.2(14)SU.
- CSCed73415
 

**Symptom:** Boot loader images don't recognize VAM and ISA PAs. When reloading the Cisco 7200 routers with these port adapters (PAs), the loader image would generate error messages which could mislead the user to thinking that these PAs are not supported by this image set.

**Conditions:** The symptom is seen after a router is reloaded.

**Workaround:** There is no workaround at this time except to ignore the error messages and confirm support for these PAs at the Cisco IOS software run-time image level.
- CSCed76298
 

**Symptom:** The Cisco 7200 series router with VAM has the Diffie-Hellman (DH) counter stuck in the output of **show crypto eli** command.

**Conditions:** The symptom is seen when the following conditions occur:

  - larger number of tunnels all trying to rekey at same time
  - large number of buffer failures
  - large number of IKE negotiation failures due to mismatch in IKE/IPsec policies, ACL, etc.

**Workaround:**

  - Restart the crypto engine by issuing the **crypto card shut <slot>** command and the **crypto card enable <slot>** command.

- CSCed80460

**Symptom:** A Cisco 7200 router running a SA-VAM may experience problems if the port adapter bus on which the SA-VAM is installed is close to the 600 bandwidth point limit.

**Conditions:** The SA-VAM was marked as using only 200 bandwidth points when it actually uses 300 bandwidth points. Because of this, the bus may be oversubscribed even if the router does not give a warning that it is.

**Workaround:** If a SA-VAM is used, add 100 bandwidth points to the bus on which it is installed making the bandwidth points for the SA-VAM 300.

- CSCed84283

**Symptom:** During the failover, the following 'ike update entry fail' message may occur:

```
%CRYPTO_HA-6-IKEUPDATEENTRY FAIL: (VIP=80.0.0.200)ISAKMP SA entry update on standby
device failed for src=50 .6.3.165, dst=80.0.0.200
```

**Condition:** Perform several switch overs between the active and standby routers.

**Workaround:** This code was fixed in the Cisco IOS Release 12.2(14)SU.

- CSCed96004

Duplicate (see [CSCee24950](#)).

- CSCed93836

Duplicate (see [CSCed27956](#)).

- CSCee00041

A new vulnerability in the OpenSSL implementation for SSL has been announced on March 17, 2004.

An affected network device running an SSL server based on an affected OpenSSL implementation may be vulnerable to a Denial of Service (DoS) attack. There are workarounds available to mitigate the effects of this vulnerability on Cisco products in the workaround section of this advisory. Cisco is providing fixed software, and recommends that customers upgrade to it when it is available.

This advisory will be posted at

<http://www.cisco.com/warp/public/707/cisco-sa-20040317-openssl.shtml>.

- CSCee24950

**Symptom:** The following message is seen when the router is reloaded:

```
preshare key length exceeds 211 characters. Key not added
```

**Conditions:** A pre-shared key of size 125 or 126 bytes is configured and type 6 password encryption feature is turned on. The key is accepted the first time. But when reloading the router, it is rejected with above message.

**Workaround:** Use a key size smaller than or equal to 124 bytes.

- CSCee67450

A Cisco device running Cisco IOS and enabled for the Border Gateway Protocol (BGP) is vulnerable to a Denial of Service (DoS) attack from a malformed BGP packet. Only devices with the command 'bgp log-neighbor-changes' configured are vulnerable. The BGP protocol is not enabled by default, and must be configured in order to accept traffic from an explicitly defined peer. Unless the malicious traffic appears to be sourced from a configured, trusted peer, it would be difficult to inject a malformed packet.

If a malformed packet is received and queued up on the interface, this bug may also be triggered by other means which are not considered remotely exploitable such as the use of the command 'show ip bgp neighbors' or running the command 'debug ip bgp <neighbor> updates' for a configured bgp neighbor.

Cisco has made free software available to address this problem.

For more details, please refer to this advisory, available at <http://www.cisco.com/warp/public/707/cisco-sa-20050126-bgp.shtml>

## Sample Configuration

The configuration for IPSec Stateful Failover builds on the standard Stateful Failover configuration, but with the addition of a tunnel interface for each GRE endpoint, as shown in [Figure 1](#).

1. The crypto parameters on the Stateful Failover Pair must be the same for:
  - isakmp policy (encryption, authentication, hash, lifetime, group)
  - isakmp key (shared secret with remote peer)
  - IPSec security-association lifetimes
  - IPSec transform set
2. Crypto map has to be applied to the physical interface (not the tunnel). To get traffic to go to the Tunnel interface there should be a route to the Tunnel IP address from the crypto peer.
3. SSP group can be configured with up to 32 redundancy groups, (with 32 Virtual IP Addresses).
4. There must be an access-list for the gre traffic with the VIP as one of the endpoints.

Following is a sample configuration which uses multiple redundancy groups, and multiple GRE tunnels. Note that this isn't necessarily a realistic deployment, but was used in the lab to illustrate the failover of multiple redundancy groups with multiple GRE tunnels. Ethernet sub-interfaces were used to simulate multiple VIPs.

Note that the other redundant router would have the same configuration except that the physical IP addresses will be different, and the SSP remote address will be pointing to the physical IP address of the private interface of the SSP peer.

**Head-end router:**

```

ip cef
!
ssp group 100
  remote 40.0.0.5
  redundancy GRE_1
  redundancy GRE_2
  redundancy PRIVATE

!
crypto isakmp policy 1
  encr 3des
  authentication pre-share
crypto isakmp key gre1 address 20.1.1.1
crypto isakmp key gre2 address 20.1.2.1

```

**Note**


---

The 20.1.+1 addresses are the remote peers.

---

```

crypto isakmp ssp 100
!
!
crypto ipsec security-association lifetime kilobytes 536870912
crypto ipsec security-association lifetime seconds 86400
!
crypto ipsec transform-set HA_TRANSFORM esp-3des
!
crypto map gre_1 1 ipsec-isakmp
  set peer 20.1.1.1
  set transform-set HA_TRANSFORM
  match address gre_1
!
crypto map gre_2 1 ipsec-isakmp
  set peer 20.1.2.1
  set transform-set HA_TRANSFORM
  match address gre_2
!
!
call rsvp-sync
!
!
interface Tunnel1
  ip unnumbered FastEthernet0/0.1
  tunnel source 172.1.1.100
  tunnel destination 20.1.1.1
!
interface Tunnel2
  ip unnumbered FastEthernet0/0.2
  tunnel source 172.1.2.100
  tunnel destination 20.1.2.1
!
!

```

**Note:** Sub-interfaces are used to simulate failover of multiple HSRP groups.

```

interface FastEthernet0/0
  no ip address
  no shutdown
  duplex full
  speed 100
!
interface FastEthernet0/0.1

```

```

encapsulation dot1Q 500
ip address 172.1.1.6 255.255.255.0
standby delay minimum 35 reload 60
standby 1 ip 172.1.1.100
standby timer 1 3
standby 1 preempt
standby 1 name GRE_1
standby 1 track FastEthernet0/1
  crypto map gre_1 ssp 100
!
interface FastEthernet0/0.2
encapsulation dot1Q 501
ip address 172.1.2.6 255.255.255.0
standby delay minimum 35 reload 60
standby 2 ip 172.1.2.100
standby 2 timers 1 3
standby 2 preempt
standby 2 name GRE_2
standby 2 track FastEthernet0/1
  crypto map gre_2 ssp 100
!
!
interface FastEthernet0/1
ip address 40.0.0.6 255.255.255.0

duplex full
speed 100
standby delay minimum 35 reload 60
standby 255 ip 40.0.0.100
standby 255 timers 1 3
standby 255 preempt
standby 255 name PRIVATE
standby 255 track FastEthernet0/0
!
!
ip classless
ip route 10.0.1.1 255.255.255.255 Tunnel1
ip route 10.0.1.2 255.255.255.255 Tunnel2
ip route 20.1.1.0 255.255.255.0 172.1.1.4
ip route 20.1.2.0 255.255.255.0 172.1.2.4
ip route 40.0.1.0 255.255.255.0 40.0.0.13
ip route 40.0.2.0 255.255.255.0 40.0.0.13
ip route 40.0.3.0 255.255.255.0 40.0.0.13
ip route 40.0.4.0 255.255.255.0 40.0.0.13
ip route 40.0.5.0 255.255.255.0 40.0.0.13
ip route 223.255.254.254 255.255.255.255 40.0.0.1
no ip http server
!

```

**Note**


---

Access-lists are needed to permit GRE traffic to flow.

---

```

ip access-list extended gre_1
 permit gre host 172.1.1.100 host 20.1.1.1
ip access-list extended gre_2
 permit gre host 172.1.10.100 host 20.1.2.1

```

## Related Documentation

### Hardware Documents

Cisco 7200 series router hardware documentation is available on cisco.com at this URL:

[http://www.cisco.com/en/US/products/hw/routers/ps341/products\\_product\\_index09186a0080123f5a.html](http://www.cisco.com/en/US/products/hw/routers/ps341/products_product_index09186a0080123f5a.html)

### Cisco IOS Software Documents

Cisco IOS Release 12.2 software documentation is available on cisco.com at this URL:

[http://www.cisco.com/en/US/products/sw/iosswrel/ps1839/products\\_tech\\_note09186a00800941da.shtml](http://www.cisco.com/en/US/products/sw/iosswrel/ps1839/products_tech_note09186a00800941da.shtml)

## Obtaining Documentation

Cisco documentation and additional literature are available on Cisco.com. Cisco also provides several ways to obtain technical assistance and other technical resources. These sections explain how to obtain technical information from Cisco Systems.

### Cisco.com

You can access the most current Cisco documentation at this URL:

<http://www.cisco.com/univercd/home/home.htm>

You can access the Cisco website at this URL:

<http://www.cisco.com>

You can access international Cisco websites at this URL:

[http://www.cisco.com/public/countries\\_languages.shtml](http://www.cisco.com/public/countries_languages.shtml)

### Documentation DVD

Cisco documentation and additional literature are available in a Documentation DVD package, which may have shipped with your product. The Documentation DVD is updated regularly and may be more current than printed documentation. The Documentation DVD package is available as a single unit.

Registered Cisco.com users (Cisco direct customers) can order a Cisco Documentation DVD (product number DOC-DOCDVD=) from the Ordering tool or Cisco Marketplace.

Cisco Ordering tool:

<http://www.cisco.com/en/US/partner/ordering/>

Cisco Marketplace:

<http://www.cisco.com/go/marketplace/>

## Ordering Documentation

You can find instructions for ordering documentation at this URL:

[http://www.cisco.com/univercd/cc/td/doc/es\\_inpk/pdi.htm](http://www.cisco.com/univercd/cc/td/doc/es_inpk/pdi.htm)

You can order Cisco documentation in these ways:

- Registered Cisco.com users (Cisco direct customers) can order Cisco product documentation from the Ordering tool:

<http://www.cisco.com/en/US/partner/ordering/>

- Nonregistered Cisco.com users can order documentation through a local account representative by calling Cisco Systems Corporate Headquarters (California, USA) at 408 526-7208 or, elsewhere in North America, by calling 1 800 553-NETS (6387).

## Documentation Feedback

You can send comments about technical documentation to [bug-doc@cisco.com](mailto:bug-doc@cisco.com).

You can submit comments by using the response card (if present) behind the front cover of your document or by writing to the following address:

Cisco Systems  
Attn: Customer Document Ordering  
170 West Tasman Drive  
San Jose, CA 95134-9883

We appreciate your comments.

## Cisco Product Security Overview

Cisco provides a free online Security Vulnerability Policy portal at this URL:

[http://www.cisco.com/en/US/products/products\\_security\\_vulnerability\\_policy.html](http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html)

From this site, you can perform these tasks:

- Report security vulnerabilities in Cisco products.
- Obtain assistance with security incidents that involve Cisco products.
- Register to receive security information from Cisco.

A current list of security advisories and notices for Cisco products is available at this URL:

<http://www.cisco.com/go/psirt>

If you prefer to see advisories and notices as they are updated in real time, you can access a Product Security Incident Response Team Really Simple Syndication (PSIRT RSS) feed from this URL:

[http://www.cisco.com/en/US/products/products\\_psirt\\_rss\\_feed.html](http://www.cisco.com/en/US/products/products_psirt_rss_feed.html)

## Reporting Security Problems in Cisco Products

Cisco is committed to delivering secure products. We test our products internally before we release them, and we strive to correct all vulnerabilities quickly. If you think that you might have identified a vulnerability in a Cisco product, contact PSIRT:

- Emergencies—[security-alert@cisco.com](mailto:security-alert@cisco.com)
- Nonemergencies—[psirt@cisco.com](mailto:psirt@cisco.com)



**Tip**

We encourage you to use Pretty Good Privacy (PGP) or a compatible product to encrypt any sensitive information that you send to Cisco. PSIRT can work from encrypted information that is compatible with PGP versions 2.x through 8.x.

Never use a revoked or an expired encryption key. The correct public key to use in your correspondence with PSIRT is the one that has the most recent creation date in this public key server list:

<http://pgp.mit.edu:11371/pks/lookup?search=psirt%40cisco.com&op=index&exact=on>

In an emergency, you can also reach PSIRT by telephone:

- 1 877 228-7302
- 1 408 525-6532

## Obtaining Technical Assistance

For all customers, partners, resellers, and distributors who hold valid Cisco service contracts, Cisco Technical Support provides 24-hour-a-day, award-winning technical assistance. The Cisco Technical Support Website on Cisco.com features extensive online support resources. In addition, Cisco Technical Assistance Center (TAC) engineers provide telephone support. If you do not hold a valid Cisco service contract, contact your reseller.

### Cisco Technical Support Website

The Cisco Technical Support Website provides online documents and tools for troubleshooting and resolving technical issues with Cisco products and technologies. The website is available 24 hours a day, 365 days a year, at this URL:

<http://www.cisco.com/techsupport>

Access to all tools on the Cisco Technical Support Website requires a Cisco.com user ID and password. If you have a valid service contract but do not have a user ID or password, you can register at this URL:

<http://tools.cisco.com/RPF/register/register.do>



**Note**

Use the Cisco Product Identification (CPI) tool to locate your product serial number before submitting a web or phone request for service. You can access the CPI tool from the Cisco Technical Support Website by clicking the **Tools & Resources** link under Documentation & Tools. Choose **Cisco Product Identification Tool** from the Alphabetical Index drop-down list, or click the **Cisco Product Identification Tool** link under Alerts & RMAs. The CPI tool offers three search options: by product ID

or model name; by tree view; or for certain products, by copying and pasting **show** command output. Search results show an illustration of your product with the serial number label location highlighted. Locate the serial number label on your product and record the information before placing a service call.

## Submitting a Service Request

Using the online TAC Service Request Tool is the fastest way to open S3 and S4 service requests. (S3 and S4 service requests are those in which your network is minimally impaired or for which you require product information.) After you describe your situation, the TAC Service Request Tool provides recommended solutions. If your issue is not resolved using the recommended resources, your service request is assigned to a Cisco TAC engineer. The TAC Service Request Tool is located at this URL:

<http://www.cisco.com/techsupport/servicerequest>

For S1 or S2 service requests or if you do not have Internet access, contact the Cisco TAC by telephone. (S1 or S2 service requests are those in which your production network is down or severely degraded.) Cisco TAC engineers are assigned immediately to S1 and S2 service requests to help keep your business operations running smoothly.

To open a service request by telephone, use one of the following numbers:

Asia-Pacific: +61 2 8446 7411 (Australia: 1 800 805 227)

EMEA: +32 2 704 55 55

USA: 1 800 553-2447

For a complete list of Cisco TAC contacts, go to this URL:

<http://www.cisco.com/techsupport/contacts>

## Definitions of Service Request Severity

To ensure that all service requests are reported in a standard format, Cisco has established severity definitions.

Severity 1 (S1)—Your network is “down,” or there is a critical impact to your business operations. You and Cisco will commit all necessary resources around the clock to resolve the situation.

Severity 2 (S2)—Operation of an existing network is severely degraded, or significant aspects of your business operation are negatively affected by inadequate performance of Cisco products. You and Cisco will commit full-time resources during normal business hours to resolve the situation.

Severity 3 (S3)—Operational performance of your network is impaired, but most business operations remain functional. You and Cisco will commit resources during normal business hours to restore service to satisfactory levels.

Severity 4 (S4)—You require information or assistance with Cisco product capabilities, installation, or configuration. There is little or no effect on your business operations.

# Obtaining Additional Publications and Information

Information about Cisco products, technologies, and network solutions is available from various online and printed sources.

- Cisco Marketplace provides a variety of Cisco books, reference guides, and logo merchandise. Visit Cisco Marketplace, the company store, at this URL:

<http://www.cisco.com/go/marketplace/>

- *Cisco Press* publishes a wide range of general networking, training and certification titles. Both new and experienced users will benefit from these publications. For current Cisco Press titles and other information, go to Cisco Press at this URL:

<http://www.ciscopress.com>

- *Packet* magazine is the Cisco Systems technical user magazine for maximizing Internet and networking investments. Each quarter, Packet delivers coverage of the latest industry trends, technology breakthroughs, and Cisco products and solutions, as well as network deployment and troubleshooting tips, configuration examples, customer case studies, certification and training information, and links to scores of in-depth online resources. You can access Packet magazine at this URL:

<http://www.cisco.com/packet>

- *iQ Magazine* is the quarterly publication from Cisco Systems designed to help growing companies learn how they can use technology to increase revenue, streamline their business, and expand services. The publication identifies the challenges facing these companies and the technologies to help solve them, using real-world case studies and business strategies to help readers make sound technology investment decisions. You can access iQ Magazine at this URL:

<http://www.cisco.com/go/iqmagazine>

- *Internet Protocol Journal* is a quarterly journal published by Cisco Systems for engineering professionals involved in designing, developing, and operating public and private internets and intranets. You can access the Internet Protocol Journal at this URL:

<http://www.cisco.com/ipj>

- World-class networking training is available from Cisco. You can view current offerings at this URL:

<http://www.cisco.com/en/US/learning/index.html>

# Glossary

**Active**—Active IPsec High Availability router

**DPD**—Dead Peer Detection. DPD allows two IPsec peers to determine if the other is still “alive” during the lifetime of a VPN connection.

**EzVPN**—Cisco Easy Virtual Private Networks (EzVPN) Client on Cisco IOS Software. The Cisco EzVPN client feature can be configured to create IPsec VPN tunnels between a supported router and another Cisco router that supports this form of IPsec encryption/decryption.

**GRE**—Generic Routing Encapsulation. Tunneling protocol developed by Cisco that can encapsulate a wide variety of protocol packet types inside IP tunnels, creating a virtual point-to-point link to Cisco routers at remote points over an IP internetwork.

**HSRP**—Hot Standby Routing Protocol. HSRP provides network redundancy for IP networks, ensuring that user traffic immediately and transparently recovers from first hop failures in network edge devices or access circuits.

**IKE**—Internet Key Exchange. IKE establishes a shared security policy and authenticates keys for services (such as IPsec) that require keys. Before any IPsec traffic can be passed, each router/firewall/host must verify the identity of its peer. This can be done by manually entering pre-shared keys into both hosts or by a CA service.

**IPsec**—IP Security. A framework of open standards that provides data confidentiality, data integrity, and data authentication between participating peers. IPsec provides these security services at the IP layer. IPsec uses IKE to handle the negotiation of protocols and algorithms based on local policy and to generate the encryption and authentication keys to be used by IPsec. IPsec can protect one or more data flows between a pair of hosts, between a pair of security gateways, or between a security gateway and a host.

**SA**—security association. An instance of security policy and keying material applied to a data flow. Both IKE and IPsec use SAs, although SAs are independent of one another. IPsec SAs are unidirectional and they are unique in each security protocol.

**SSP**—State Synchronization Protocol (SSP) is a protocol developed to transfer state information between the active and standby routers.

**Standby**—Standby IPsec High Availability router.

**Stateful Failover**—Feature that enables a backup (standby) router to automatically take over the primary (active) router’s tasks in the event of a active router failure with minimal or no loss of traffic. The remote peer sees no difference between the two routers since it is connected to a virtual end point (VEP), owned by either headend router that shares the same IPsec information.

**V3PN**—Voice and Video Enabled VPN (V3PN), integrates three core technologies: IP Telephony, Quality of Service (QoS), and IP Security (IPsec) VPN to guarantee the timely delivery of latency-sensitive applications such as voice and video.

---

This document is to be used in conjunction with the documents listed in the [“Related Documentation”](#) section on page 31 .

CCSP, the Cisco Square Bridge logo, Follow Me Browsing, and StackWise are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn, and iQuick Study are service marks of Cisco Systems, Inc.; and Access Registrar, Aironet, ASIST, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Empowering the Internet Generation, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, FormShare, GigaDrive, GigaStack, HomeLink, Internet Quotient, IOS, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, LightStream, Linksys, MeetingPlace, MGX, the Networkers logo, Networking Academy, Network Registrar, *Packet*, PIX, Post-Routing, Pre-Routing, ProConnect, RateMUX, ScriptShare, SlideCast, SMARTnet, StrataView Plus, SwitchProbe, TeleRouter, The Fastest Way to Increase Your Internet Quotient, TransPath, and VCO are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0411R)

Copyright © 2005 Cisco Systems, Inc. All rights reserved.





