



# Cisco IOS Software Release 12.2(13)ZG

This product bulletin provides the content and delivery information for Cisco IOS<sup>®</sup> Software Release 12.2(13)ZG. It should be used in conjunction with the Cisco IOS Software 12.2(13)ZG release note for more detailed information. This is a special early-deployment release and supports Cisco 830 Series secure broadband routers and Cisco SOHO 90 Series routers.

New Features in Cisco IOS Software Release 12.2(13)ZG

## IPSec NAT Transparency/NAT Traversal

This feature is in the base image and supports the Cisco 831 Ethernet Broadband Router, the Cisco 837 ADSL Broadband Router, and the Cisco 836 as well as the Cisco SOHO 91 Ethernet Broadband Router, the Cisco SOHO 97 ADSL Broadband Router, and the Cisco SOHO 96.

This feature addresses the IP Security (IPSec) and Network Address Translation (NAT) incompatibilities that have become a major barrier to deploying IPSec in its principal uses.

The incompatibilities that are addressed are as follows:

- *Incompatibility between IPSec Authentication Header and NAT*—Because the Authentication Header security protocol incorporates the IP source and destination addresses in the keyed message integrity check, NAT, or reverse NAT devices making changes to address fields, will invalidate the message integrity check. Because IPSec extended services platform (ESP) does not incorporate the IP source and destination addresses in its keyed message integrity check, this issue does not arise for ESP.
- *Incompatibility between checksums and NAT*—Transmission Control Protocol/User Datagram Protocol (TCP/UDP) checksums have a dependency on the IP source and destination addresses through inclusion of the “pseudo-header” in the calculation. As a result, checksums that are calculated and checked on receipt will be invalidated by passage through a NAT or a reverse NAT device.
- *Incompatibility between fixed Internet Key Exchange (IKE) destination ports and port address translation (PAT)*—When multiple hosts behind the PAT initiate IKE Security Associates (SAs) to the same responder, a mechanism is needed to allow the PAT to demultiplex the incoming IKE packets.
- *Incompatibility between IPSec ESP and PAT*—PAT or reverse PAT devices cannot handle ESP packets. They drop ESP packets if they find legislative IP address and port.



### **Preclassified QoS**

This feature is in the plus image and supports the Cisco 831 Ethernet Broadband Router, the Cisco 837 ADSL Broadband Router, and the Cisco 836 ADSL over ISDN Router.

For Cisco 830 Series secure broadband routers, whenever tunneling or encryption is turned on, the packets are encapsulated by a tunnel or an encryption header. Quality-of-service (QoS) features cannot examine the original packet header to correctly classify the packets.

Preclassification is designed as a feature to be applied on a tunnel interface. A new command-line interface (CLI) command is introduced to allow toggling of preclassification. When the command is enabled, the QoS features on the output interface where the tunnel traverses can classify the packets prior to tunneling or encryption, thus allowing preferential treatment of certain flows within the tunnel.

The following example enables the QoS for virtual private networks (VPNs) feature on tunnel interfaces and virtual templates:

```
Router(config-if)# qos pre-classify
```

The following example enables the QoS for VPNs feature on crypto maps:

```
Router(config-crypto-map)# qos pre-classify
```

Use the no form of this command to disable it.

### **Advanced Encryption Standard Software Support**

This feature is in the plus image and supports the Cisco 831 Ethernet Broadband Router, the Cisco 837 ADSL Broadband Router, and the Cisco 836 ADSL over ISDN Router.

This feature adds support for Advanced Encryption Standard (AES) encryption to IPsec and therefore makes additional IPsec transforms and IKE encryption algorithms available to the user.

This capability adds the following options to the already-existing Data Encryption Standard (DES) and Triple DES (3DES) options in crypto isakmp policy ISAKMP protection suite and crypto ipsec transform IPsec transform definition.

ISAKMP policy:

```
Router(config)#crypto isakmp policy priority
```

Identify the policy to create. (Each policy is uniquely identified by the priority number you assign.) This command puts you into the config-isakmp command mode.

```
encryption encryption algorithm
```



The following options are added to the encryption command.

- aes                    Selecting this option means that encrypted IKE messages protected by this suite will be encrypted using AES with a 128-bit key.
- aes 192                Selecting this option means that encrypted IKE messages protected by this suite will be encrypted using AES with a 192-bit key.
- aes 256                Selecting this option means that encrypted IKE messages protected by this suite will be encrypted using AES with a 256-bit key.

IPSec transform set:

Router(config)# crypto ipsec transform-set transform-set-name transform sets

The IPSec transform set will add the following options within the crypto IPSec transform definition:

- esp-aes                Selecting this option means that IPSec messages protected by this transform will be encrypted using AES with a 128-bit key.
- esp-aes 192            Selecting this option means that IPSec messages protected by this transform will be encrypted using AES with a 192-bit key.
- esp-aes 256            Selecting this option means that IPSec messages protected by this transform will be encrypted using AES with a 256-bit key.

All three options will be treated as ESP encryption transforms.

Note: AES can also be used with Authentication Header security protocol.

### **Intrusion Detection System Signatures**

This feature is in the base image and supports the Cisco 831 Ethernet Broadband Router, the Cisco 837 ADSL Broadband Router, and the Cisco 836 ADSL over ISDN Router.

The Cisco IOS Firewall Intrusion Detection System (IDS) feature supports intrusion detection technology when the Cisco IOS Firewall is present. The Cisco IOS IDS feature statically identifies 100 of the most common network attacks using "signatures" to detect patterns of misuse in network traffic. Statically means that the signatures are part of the compiled Cisco IOS IDS code. They consist of a broad cross-section of intrusion-detection signatures representing severe breaches of network security, the most common network attacks, and information-gathering scans.

Please refer to the following URL for basic configuration of the Cisco IOS Firewall IDS feature.

[http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fsecur\\_c/fttrafwl/scfids.htm](http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fsecur_c/fttrafwl/scfids.htm)

Along with the 58 signatures mentioned in the above URL, 42 signatures were added in this feature.

There are no additional CLI commands to configure these additional signatures. The ip audit signature command will allow the new signatures to be disabled or to apply extended access control lists (ACLs) to individual signatures for filtering out sources of false alarms.



### **Performance Pre-fragmentation Before Encryption**

This feature is in the plus image and supports the Cisco 831 Ethernet Broadband Router, the Cisco 837 ADSL Broadband Router, and the Cisco 836 ADSL over ISDN Router.

Overheads associated with VPN tunnel encapsulations can result in packets exceeding the maximum transmission unit (MTU) threshold of the interface. As a result, data traffic and video-stream traffic can become fragmented after encryption. Fragmentation is done at the Cisco Express Forwarding level in the packet path but reassembly is necessitated on the tunnel end point. This reassembly is done at the process level. All packets that need to be decrypted should first be queued for reassembly, causing a serious decline in encryption performance.

This feature aims at “look ahead fragmentation” where packet size that would result after an impending encryption operation is calculated or checked in advance with the available knowledge of transform sets configured on the IPsec SA. If the packet in addition to this “to be added encapsulation size” exceeds the MTU of output interface, an attempt is made to fragment the packet before encryption. This avoids process-level reassembly before decryption, helping improve decryption performance and overall IPsec throughput.

### **HTTPs for Auth Proxy**

This feature is in the base image and supports the Cisco 831 Ethernet Broadband Router, the Cisco 837 ADSL Broadband Router, and the Cisco 836 ADSL over ISDN Router.

The Cisco IOS Firewall authentication proxy allows network administrators to apply specific network security policies on a per-user basis. Previously, user identity and related authorized access were associated with a user IP address, or a single security policy had to be applied to an entire user group or subnetwork. With authentication proxy, users can be identified and authorized on the basis of their per-user policy. Tailoring access privileges on an individual basis is possible, as opposed to applying a general policy across multiple users.

When authentication proxy is enabled on the Cisco router, users can log in to the network or access the Internet via Hypertext Transfer Protocol (HTTP). When a user initiates an HTTP session through the firewall, the authentication proxy is triggered. The authentication proxy first checks to see if the user has been authenticated. If a valid authentication entry exists for the user, the connection is completed with no further intervention by authentication proxy. If no entry exists, the authentication proxy responds to the HTTP connection request by prompting the user for a username and password. When authenticated, their specific access profiles are automatically retrieved and applied from a Cisco Secure Access Control Server, or another Remote Access Dial-In User Service (RADIUS) or Terminal Access Controller Access Control System (TACACS+) authentication server. The user profiles are active only when there is active traffic from the authenticated users.

This feature encrypts the user ID and password exchanged between the HTTP client and the Cisco IOS router via Secure Sockets Layer (SSL) when the Cisco IOS Firewall authentication proxy is enabled.

### **Web Cache Communications Protocol**

This feature is in the plus image and supports the Cisco 831 Ethernet Broadband Router, the Cisco 837 ADSL Broadband Router, and the Cisco 836 ADSL over ISDN Router.

Web Cache Communications Protocol (WCCP) provides a mechanism to establish and maintain cache clusters, as well as redirect user requests from network components to those clusters in real time. Additionally, WCCP has built-in load-balancing and fault-tolerance features and possesses excellent scaling attributes because it can be implemented in a distributed fashion across the network.



### **Easy VPN Multipeer Group**

This feature is in the base image and supports the Cisco 831 Ethernet Broadband Router, the Cisco 837 ADSL Broadband Router, and the Cisco 836 ADSL over ISDN Router.

Easy VPN will support multiple peer statements. If the negotiation fails while connecting to a peer, Easy VPN should fail over to the next peer. This continues in a round-robin fashion. When the last peer is reached Easy VPN should roll over to the first one. The IKE or IPSec SAs to the previous peer should be deleted. Multiple-set peer statements should work for both IP addresses as well as hostnames. Setting or unsetting the peer statements shouldn't affect their order.

Please refer to the following link for more information on the basic Easy VPN configuration.

[http://www.cisco.com/en/US/products/sw/iosswrel/ps5012/products\\_feature\\_guide09186a00800a8565.html#1121329](http://www.cisco.com/en/US/products/sw/iosswrel/ps5012/products_feature_guide09186a00800a8565.html#1121329)

When the first peer is unavailable, the client should switch to the next Easy VPN peer without any problem.

### **Easy VPN Xauth User ID and Password Save Options**

This feature is in the base image and supports the Cisco 831 Ethernet Broadband Router, the Cisco 837 ADSL Broadband Router, and the Cisco 836 ADSL over ISDN Router. The feature is also known as Optimize Xauth by re-using the last successful username and password.

When the server allows user to use the saved password, the client configured username and password is used for Xauth. Hence, the client need not enter the information manually every time the VPN tunnel comes up.

Please refer to the following URL for more information on the basic Easy VPN configuration.

[http://www.cisco.com/en/US/products/sw/iosswrel/ps5012/products\\_feature\\_guide09186a00800a8565.html#1121329](http://www.cisco.com/en/US/products/sw/iosswrel/ps5012/products_feature_guide09186a00800a8565.html#1121329)

### **Next Hop Resolution Protocol for Dynamic Multipoint VPN**

This feature is in the plus image and supports the Cisco 831 Ethernet Broadband Router, the Cisco 837 ADSL Broadband Router, and the Cisco 836 ADSL over ISDN Router.

The Dynamic Multipoint VPN (DMVPN) feature allows users to better scale large and small IPSec VPNs by combining generic routing encapsulation (GRE) tunnels, IPSec encryption, and Next Hop Resolution Protocol (NHRP).

In the hub and spoke configuration, 83x will be spoke, therefore, support of NHRP is required.

For more details, please refer to the following URL:

[http://lbj.cisco.com/push\\_targets1/ucdit/cc/td/doc/product/software/ios122/122newft/122t/122t105/ftgreips.htm](http://lbj.cisco.com/push_targets1/ucdit/cc/td/doc/product/software/ios122/122newft/122t/122t105/ftgreips.htm)



Corporate Headquarters  
Cisco Systems, Inc.  
170 West Tasman Drive  
San Jose, CA 95134-1706  
USA  
www.cisco.com  
Tel: 408 526-4000  
800 553-NETS (6387)  
Fax: 408 526-4100

European Headquarters  
Cisco Systems International BV  
Haarlerbergpark  
Haarlerbergweg 13-19  
1101 CH Amsterdam  
The Netherlands  
www-europe.cisco.com  
Tel: 31 0 20 357 1000  
Fax: 31 0 20 357 1100

Americas Headquarters  
Cisco Systems, Inc.  
170 West Tasman Drive  
San Jose, CA 95134-1706  
USA  
www.cisco.com  
Tel: 408 526-7660  
Fax: 408 527-0883

Asia Pacific Headquarters  
Cisco Systems, Inc.  
Capital Tower  
168 Robinson Road  
#22-01 to #29-01  
Singapore 068912  
www.cisco.com  
Tel: +65 6317 7777  
Fax: +65 6317 7799

Cisco Systems has more than 200 offices in the following countries and regions. Addresses, phone numbers, and fax numbers are listed on the  
**Cisco Web site at [www.cisco.com/go/offices](http://www.cisco.com/go/offices)**

Argentina • Australia • Austria • Belgium • Brazil • Bulgaria • Canada • Chile • China PRC • Colombia • Costa Rica • Croatia  
Czech Republic • Denmark • Dubai, UAE • Finland • France • Germany • Greece • Hong Kong SAR • Hungary • India • Indonesia • Ireland  
Israel • Italy • Japan • Korea • Luxembourg • Malaysia • Mexico • The Netherlands • New Zealand • Norway • Peru • Philippines • Poland  
Portugal • Puerto Rico • Romania • Russia • Saudi Arabia • Scotland • Singapore • Slovakia • Slovenia • South Africa • Spain • Sweden  
Switzerland • Taiwan • Thailand • Turkey • Ukraine • United Kingdom • United States • Venezuela • Vietnam • Zimbabwe

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Cisco, Cisco Systems, Cisco IOS, and the Cisco Systems logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and certain other countries.

All other trademarks mentioned in this document or Web site 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.  
(0303R) N2/LW4380 0303