SYSLOG Enhancements for Cisco IOS EasyVPN Server

In some situations the complexity or cost of the authentication, authorization, and accounting (AAA) server prohibits its use, but one of its key function—collection of useful logging information (accounting)—is still necessary. To facilitate this requirement for Cisco IOS® EasyVPN scenarios, Cisco Systems® has enhanced its syslog messages to provide needed information. The goal is to implement the most needed syslog messages on the Cisco® EasyVPN server in order to help troubleshoot and diagnose EasyVPN-related problems. This list was compiled with the help of Cisco Technical Assistance Center (TAC) engineers who provide daily support for these problems to Cisco customers. This white paper discusses the enhanced syslog messages.

The syslog messages discussed in this paper can easily be logged from a Cisco IOS EasyVPN server to an external syslog server. In comma separated variable (CSV) format, these records can easily be loaded and processed by an external software application such as a spreadsheet or a database. The syslog server software can run on a basic PC, and basic syslog server applications can be downloaded from the Internet. Cisco makes no recommendations on any particular type or version of syslog server software.

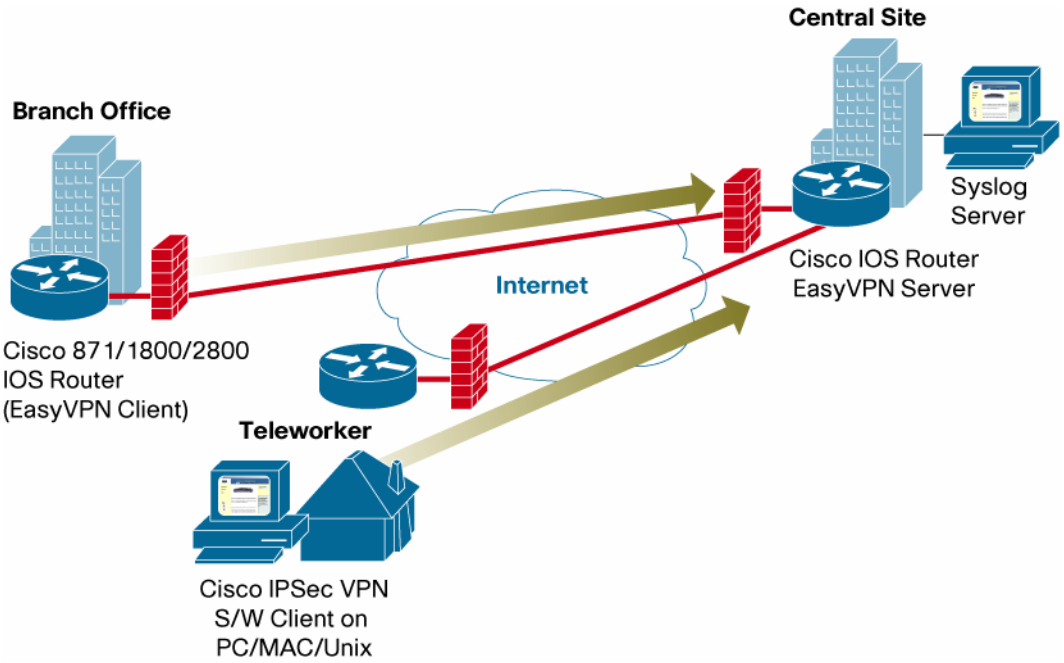
Syslog uses User Datagram Protocol (UDP) as the underlying transport mechanism, so the data packets are unsequenced and unacknowledged. On a heavily used network, some packets may be dropped and therefore logging information will be lost. Multiple syslog servers can be specified for redundancy.

For the timestamp on the syslog messages to be correct, the Cisco IOS Software router or gateway must be configured for time synchronization with a Network Time Protocol (NTP) time source. If the router has no NTP synchronization, the start and stop times of each syslog will be a zero (null) value. If an external NTP source is not available, the router needs to be set as an NTP master. This concept is explained in the “Configuration” section.

The greatest benefit of implementing these syslog enhancements is transparent customer experience when debugging problems with Cisco IOS EasyVPN servers, Cisco VPN 3000 Series concentrators or Cisco ASA 5500 Series adaptive security appliances. In other words, these enhancements help customers debug and understand EasyVPN across various platforms.

Topology

Figure 1. EasyVPN Server Logging to a Syslog Server



Prerequisites

Requirements

Syslog messages are implemented on the Cisco EasyVPN server side only.

Components Used

The support is available for all Cisco IOS routers (except Cisco 6500 and 7600) with Cisco IOS Software Release 12.4(4)T and higher.

Configuration

Following is a sample configuration that enables the router to generate the indicated EasyVPN syslog messages and send them to an external syslog server. These syslog messages can be enabled using a command-line interface (CLI) as follows:

```
router#(config)crypto logging ezvpn <group> (New enhancement in
12.4(4)T)


!--- Providing the Group name is optional and would enable syslogs
only for that particular group. If no group name is provided, syslogs
will get enabled for all ezvpn connections to the server. These are
informational messages (Sev 6 messages)


router#(config)crypto logging session (Available since 12.3T)


!--- Enables basic crypto logging. These are notification messages
(Sev 5 messages)
```

Note: Enabling logging for informational messages (severity 6) shows both notification and informational messages (use command: "**logging trap informational**" to see all messages up to severity 6).

To allow the records to be timestamped:

```
router#(config)service timestamps log datetime msec localtime

!--- Ensure that the records are timestamped with an accurate value.
```

To allow the records to be sent to a syslog server:

```
router#(config)logging <IP_address or hostname of the Syslog server>

!--- Identifies a syslog server host to receive logging messages.
```

Enhanced EasyVPN SYSLOG Messages

Enabling EasyVPN session monitoring (enabling **crypto logging session** and **crypto logging ezvpn**) sends these messages to a syslog server (enable **logging** <ip_addr>). The **crypto session** messages are severity 5 (notification), whereas the **crypto ezvpn** messages are severity 6 (informational). Enabling logging for informational messages (severity 6) shows all these messages (enable **logging trap informational** to see all messages up to severity 6).

The following syslog messages (available with the **crypto logging ezvpn** command) are supported on EasyVPN servers starting Cisco IOS Software Release 12.4(4)T and higher.

Table 1. An internet key exchange (IKE) packet was sent to the peer but the peer has not responded within the timeout window

Feature	Description
Event Text	Message not received, retransmitting, peer address: %s
Explanation:	This event indicates that an IKE packet was sent to the peer but the peer has not responded within the timeout window (8 seconds). For remote access, this event can happen when the user takes a long time to log in.
Recommended Action:	If the condition persists, check the following: 1) the wrong IP address may be configured for the remote peer; 2) the remote peer may be down or may have crashed during negotiation; or 3) a preshared key or digital certificate authentication failure has occurred.

Table 2. The Software or EasyVPN Client Cannot Obtain an IP address because the pool is not configured or the allocated address space is already in use

Feature	Description
Event Text	Cannot obtain an IP address for remote peer.
Explanation	This message indicates that a request for an IP address for a remote-access client from the internal utility that provides these addresses could not be satisfied.
Recommended Action	Check the configuration of IP address assignment method(s).

Table 3. An access control list (ACL) is not defined but it has been associated within an isakmp profile

Feature	Description
Event Text	Split tunneling policy requires network list but none is configured.
Explanation	When the split tunneling policy is set to either split tunneling or to allow local LAN access, a network list must be defined to represent the information required by the VPN client.
Recommended Action	Check the configuration of network list(s).

Table 4. When client machine is missing the firewall policy, they cannot connect

Feature	Description
Event Text	Client did not report firewall in use, but there is a configured firewall: %s tunnel. Expected—Vendor: %s(%d), Product %s(0x%08x), Caps: %04x.
Explanation	The client did not report a firewall in use through [IS THAT OK?] ModeCfg, but one is required. The event lists the expected values, and whether the tunnel is terminated or allowed. Note that the number following the product string is a bitmask of all the allowed products.
Recommended Action	This message is informational only; no action is required.

Table 5. The VPN client user has successfully negotiated Network Address Translation Traversal (NAT-T) for the IP Security (IPSec) session

Feature	Description
Event Text	NAT-Traversal successfully negotiated!\nIPSec traffic will be encapsulated to pass through NAT devices.
Explanation	NAT-T was negotiated and all further IPSec data will be encapsulated.
Recommended Action	This message is informational only; no action is required.

Table 6. The router reaches a point where it cannot initiate any additional IKE tunnels

Feature	Description
Event Text	%s memory resources are critial,\nIKE data on interface %d, from Peer %s dropped
Explanation	This event indicates that the concentrator has received an IKE packet from a remote entity trying to initiate a tunnel. Because memory resources are at a critical state, it is not allowing establishment of any more tunnels. The IKE packet has been ignored and dropped.
Recommended Action	If the condition persists, verify that the concentrator is efficiently configured. This event could indicate that a concentrator with increased memory is required for this application.

Table 7. The hardware client is initializing to a backup server

Feature	Description
Event Text	Initializing Backup Server [%s]
Explanation	The hardware client is failing over to a backup server or a failed Domain Name System (DNS) lookup for the primary server that caused the system to initialize a backup server. A tunnel initiated after this point will be aimed at the specified backup server.
Recommended Action	This message is informational only; no action is required.

Table 8. The Save Password feature is turned on or off

Feature	Description
Event Text	Save Password option is SET (ON) or not SET (OFF).
Explanation	The Save Password option is either ON or OFF. Save Password control allows you to save your Xauth password locally on your PC so that after you have initially entered the password, the Save Password attribute is pushed from the server to the client.
Recommended Action	This message is informational only; no action is required.

Table 9. Show details about why authentication has been successful

Feature	Description
Event Text	CRYPTO-6-EZVPN_STATUS: (Server) Authentication PASSED User=<username>lab Group=<Group-name> Client_public_addr=<ip addr> Server_public_addr=<ip addr>
Explanation	This event simply indicates that there was a successful authentication request.
Recommended Action	No action is required.

Table 10. Show details about why authentication has failed

Feature	Description
Event Text	Authentication failed: Reason = %s\nhandle = %d, server = %s, user = %s
Explanation	This message is seen when the authentication server is unavailable because it is down or because there is no route available to get to it; in other words, this message appears when the user does not see a response from the authentication server.
Recommended Action	If the server is reported as offline, the concentrator has not received an Address Resolution Protocol (ARP) response or a reply to an authentication request. Verify the server is functioning and reachable through the concentrator.

Table 11. Show why authentication was rejected.

Feature	Description
Event Text	CRYPTO-6-EZVPN_STATUS: (Server) Authentication REJECTED User=<username>lab Group=<Group-name> Client_public_addr=<ip addr> Server_public_addr=<ip addr>
Explanation	This event indicates that an authentication request has been rejected. The event text points to the server and user ID. Reasons and handles are not always available but usually are.
Recommended Action	Check user names and passwords; also verify that connection policies are met.

For example, 05/12/2004 09:53:38.300 SEV=3 AUTH/5 RPT=45090

Authentication rejected: Reason = Simultaneous logins exceeded for user

Table 12. When a user chooses the Group Lock option but does not comply, the user sees this message.

Feature	Description
Event Text	User (%s) not member of group (%s), authentication failed.
Explanation	The user is configured for a different group than what was sent in the IPSec negotiation.
Recommended Action	If using the Cisco VPN client and preshared keys, make sure that the group configured on the client is the same as the group associated with the user on the concentrator. If using digital certificates, the group is dictated either by the OU field of the certificate or the user defaults to the base group.

Table 13. A user tries to use the same string as group name and user name

Feature	Description
Event Text	User (%s) matched with group name, authentication failed.
Explanation	The user tried to authenticate by using the same string as both the group name and user name.
Recommended Action	Group name and user name must be different (and correct) for the user to be authenticated.

Table 14. The EasyVPN client is not sending the right user credentials

Feature	Description
Event Text	Headend security gateway has failed our user authentication attempt -\ncheck configured user name and password.
Explanation	The EasyVPN client (for example, the Cisco VPN 3002) has failed extended authentication. This problem is most likely a problem with the user name, password, or authentication server.
Recommended Action	Verify that the configured user name and password values on each side match. Also verify that the authentication server at the headend is operational.

Table 15. An individual user authentication is not successful

Feature	Description
Event Text	RADIUS Proxy encountered an error processing authentication request.
Explanation	This is a generic message that may indicate a failure anywhere from the RADIUS server not being available to an internal software error. This message is specific to “individual user auth” for client machines located behind a remote hardware client.
Recommended Action	Verify that the concentrator and the RADIUS server are communicating correctly—check versions of code, supported protocols, and interoperability.

Table 16. The client sent authentication method differs from the group configured authentication mode

Feature	Description
Event Text	Client IKE Auth mode differs from the group’s configured Auth mode.
Explanation	The client tries to negotiate with preshared keys while its group is configured to use digital certificates.
Recommended Action	Check the client configuration.

Related Information

For further information about logging commands, go to http://www.cisco.com/en/US/products/sw/iosswrel/ps1831/products_command_reference_chapter09186a00800ee834.html#1017129.

For further information about the Cisco IOS EasyVPN solution, go to http://www.cisco.com/en/US/products/ps6659/products_ios_protocol_option_home.html.

Americas 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: 408 527-0883

Asia Pacific Headquarters
Cisco Systems, Inc.
168 Robinson Road
#28-01 Capital Tower
Singapore 068912
www.cisco.com
Tel: +65 6317 7777
Fax: +65 6317 7799

Europe Headquarters
Cisco Systems International BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands
www-europe.cisco.com
Tel: +31 0 800 020 0791
Fax: +31 0 20 357 1100

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.

Printed in USA C11-328553-01 7/07