



Firewall Intrusion Detection System Signature Enhancements

Before this feature, the Cisco Firewall Intrusion Detection System (IDS) contained 59 signatures, which was only a small subset of the signatures supported by Cisco Secure IDS. The Firewall Intrusion Detection System Signature Enhancements feature introduces 42 additional IDS signatures to Cisco IOS IDS that are supported by other Cisco products, such as PIX; these newly added signatures are categorized as follows:

- Twenty-one of the 28 most commonly seen signatures in the Security Posture Assessment (SPA) findings
- Six of the 7 PIX signatures that were unavailable in IDS
- All 15 of the most dangerous HTTP signatures in the Cisco Secure IDS Network Security Database (NSDB)

Feature Specifications for Firewall Intrusion Detection System Signature Enhancements

Feature History

Release	Modification
12.2(11)YU	This feature was introduced.
12.2(15)T	This feature was integrated into Cisco IOS Release 12.2(15)T.

Supported Platforms

For platforms supported in Cisco IOS Release 12.2(11)YU and 12.2(15)T, consult Cisco Feature Navigator.

Finding Support Information for Platforms and Cisco IOS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS software image support. Access Cisco Feature Navigator at <http://www.cisco.com/go/fn>. You must have an account on Cisco.com. If you do not have an account or have forgotten your username or password, click **Cancel** at the login dialog box and follow the instructions that appear.

Contents

- [Restrictions for Firewall Intrusion Detection System Signature Enhancements, page 2](#)
- [Information About Firewall Intrusion Detection System Signature Enhancements, page 2](#)
- [How to Use the Firewall IDS Signature Enhancements, page 9](#)

- [Configuration Examples for Firewall IDS, page 13](#)
- [Additional References, page 13](#)
- [Command Reference, page 15](#)
- [Glossary, page 16](#)

Restrictions for Firewall Intrusion Detection System Signature Enhancements

Image Requirement

To use this feature, you must have a Cisco IOS image that contains Cisco IOS Firewall IDS.

Dynamic Signature Restriction

Dynamic signature updates are not supported in this feature.

Information About Firewall Intrusion Detection System Signature Enhancements

To use the Firewall Intrusion Detection System Signature Enhancements feature, you must understand the following concepts:

- [User Datagram Protocol Signatures, page 5](#)
- [HTTP Signatures, page 3](#)
- [User Datagram Protocol Signatures, page 5](#)
- [TCP Signatures, page 6](#)
- [IP Signatures, page 7](#)
- [IP Fragment Signatures, page 8](#)
- [Log Messages for IDS Signatures, page 8](#)

Domain Name System Signatures

In Cisco Secure IDS, Domain Name System (DNS) signatures are handled by the SERVICE.DNS.TCP and SERVICE.DNS.UDP signature microengines (SMEs), but because Cisco IOS IDS did not support DNS before this feature, a new application module has been implemented to handle DNS signatures for IDS. This new application module is similar to the SERVICE.DNS.SMEs except that signatures are stored in static data structures rather than in a dynamically downloadable Directory Administration Tool (DAT) file.

The newly added DNS signatures were chosen based on the following information:

- The Cisco Secure Encyclopedia, which generates vulnerability statistics using SPA data that has been collected by the Cisco Secure Consulting Services
- The Cisco PIX Firewall, Version 6.2

Table 1 identifies the DNS signatures that have been added to IDS.

Table 1 Newly Added DNS Signatures to the Firewall IDS

Signature ID	Signature Name	Signature Structure	Signature Description ¹
6050	DNS HINFO Request	Compound/Info	Triggers on an attempt to access host information (HINFO) records from a DNS server. This signature is indicative that your network may be under reconnaissance.
6051	DNS Zone Transfer	Compound/Info	Triggers on normal DNS zone transfers in which the source port is 53. This signature indicates that your network may be under reconnaissance.
6052	DNS Zone Transfer from High Port	Compound/Attack	Triggers on an illegitimate DNS zone transfer in which the source port is not equal to 53. Because of the access method, this signature indicates that your network is most likely under reconnaissance. If your network is under reconnaissance, it may be the prelude to more serious attacks.
6053	DNS Request for All Records	Compound/Info	Triggers on a DNS request for all records. This signature indicates that your network may be under reconnaissance.
6054	DNS Version Request	Compound/Info	Triggers when a request for the version of a DNS server is detected.
6055	DNS Inverse Query Buffer Overflow	Compound/Attack	Triggers when an IQUERY request arrives with a data section that is larger than 255 characters.
6056	DNS NXT Buffer Overflow	Compound/Attack	Triggers when a DNS server response arrives with a long NXT resource where the length of the resource data is > 2069 bytes or the length of the TCP stream containing the NXT resource is > 3000 bytes.
6057	DNS SIG Buffer Overflow	Compound/Attack	Triggers when a DNS server response arrives with a long SIG resource where the length of the resource data is > 2069 bytes or the length of the TCP stream that contains the SIG resource is > 3000 bytes.
6062	DNS Author's Request	Compound/Info	Triggers when a DNS query type TXT class CHAOS is detected with string the "Authors.Bind" (which is case insensitive).
6063	DNS Incremental Zone Transfer	Compound/Info	Triggers when a DNS query type of 251 is detected.

1. For the latest signature description, refer to Cisco MySDN, which can be found at the following URL: <http://tools.cisco.com/MySDN/Intelligence/home.x>

HTTP Signatures

In Cisco Secure IDS, HTTP signatures are handled by the SERVICE.HTTP and STATE.HTTP SMEs, but because Cisco IDS did not support HTTP before this feature, a new application module has been implemented to handle HTTP signatures for the Firewall IDS. The HTTP application module is similar to the SERVICE.HTTP and STATE.HTTP SMEs except that signatures are stored in data structures rather than in a dynamically downloadable DAT file.

Table 2 identifies the HTTP signatures that have been added to the Firewall IDS.

Table 2 Newly Added HTTP Signatures to the Firewall IDS

Signature ID	Signature Name	Signature Structure	Signature Description ¹
3215	IIS DOT DOT EXECUTE Attack	Compound/Attack	Triggers on any attempt to cause the Microsoft Internet Information Server to execute commands.
3229	Website Win-C-Sample Buffer Overflow	Compound/Attack	Triggers when an attempt is made to access the win-c-sample program distributed with WebSite servers.
3233	WWW count-cgi Overflow	Compound/Attack	Triggers when an attempt is made to overflow a buffer in the Common Gateway Interface (CGI) Count program.
5034	WWW IIS newdsn Attack	Compound/Attack	Triggers when an attempt is made to run the newdsn.exe command via the HTTP server. This signature can indicate a remote denial of service attack attempt because this command can be used to fill up the file system of the targeted host.
5035	HTTP cgi HylaFAX Faxsurvey	Compound/Attack	Triggers when an attempt is made to pass commands to the CGI program faxsurvey. This signature indicates abuse, and the source should be shunned.
5041	WWW anyform Attack	Compound/Attack	Triggers when an attacker attempts to execute arbitrary commands through the anyform cgi-bin script. The source address for this attack should be shunned.
5043	WWW Cold Fusion Attack	Compound/Attack	Triggers when an attempt is made to access example scripts shipped with Cold Fusion Servers. The source address for this signature should be shunned.
5044	WWW Webcom.se Guestbook Attack	Compound/Attack	Triggers when an attacker attempts to execute arbitrary commands through the rguest.exe or wguest.exe cgi-bin script of Webcom.se. The source address for this attack should be shunned.
5045	WWW xterm display Attack	Compound/Attack	Triggers when any cgi-bin script attempts to execute the command xterm -display. This signature may indicate an attempt to illegally log into your system. This attack can result in the attacker gaining access to your system. Serious system compromise is possible. No valid reason to execute xterm -display via this mechanism exists. Hosts that attempt to access execute xterm -display, especially from outside your network, should be shunned.
5050	WWW IIS .htr Overflow Attack	Compound/Attack	Triggers when an .htr buffer overrun attack is detected, indicating a possible attempt to execute remote commands or cause a denial of service against the targeted Windows NT IIS server. Hosts that attempt to cause this type of alarm, especially from outside your network, should be shunned.
5055	HTTP Basic Authentication Overflow	Compound/Attack	A buffer overflow can occur on vulnerable web servers if a large username and password combination is used with basic authentication.

Table 2 *Newly Added HTTP Signatures to the Firewall IDS (continued)*

Signature ID	Signature Name	Signature Structure	Signature Description ¹
5071	WWW msacds.dll Attack	Compound/Attack	Triggers when an attempt has been made to execute commands or view secured files with privileged access.
5081	WWW WinNT cmd.exe Access	Compound/Attack	Triggers when use of the Windows NT cmd.exe is detected in a URL.
5090	WWW Frontpage htimage.exe Access	Compound/Attack	Triggers when the FrontPage CGI program is accessed with a filename argument ending with "0,0."
5114	WWW IIS Unicode Attack	Compound/Attack	Triggers when an attempt to exploit the Unicode ../ directory traversal vulnerability is detected.
5116	Endymion MailMan Remote Command Execution	Compound/Attack	Endymion MailMan insecurely uses the perl function open(), which allows user-supplied input that contains shell metacharacters to be executed as shell commands with the privilege level of the CGI script.
5117	phpGroupWare Remote Command Exec	Compound/Attack	phpGroupWare is a multiuser groupware suite that is freely distributed. There is a problem in the software that could allow users to remotely execute malicious code by exploiting a vulnerable include() command.
5118	eWave ServletExec 3.0C File Upload	Compound/Attack	UploadServlet is a servlet that ServletExec contains in its server-side classes. UploadServlet, when invoked with a special formed HTTP or GET request, allows an attacker to upload any file to any directory on the server; the uploaded file may have code that can later be executed on the server, leading to remote command execution.
5123	WWW Host: field overflow	Compound/Attack	Triggers if web traffic is detected sending an abnormally large GET request with a large host field.

1. For the latest signature description, refer to Cisco MySDN, which can be found at the following URL: <http://tools.cisco.com/MySDN/Intelligence/home.x>

User Datagram Protocol Signatures

Cisco Secure IDS SME handles already supported atomic User Datagram Protocol (UDP) signatures by the UDP application module (ATOMIC.UDP); thus, the newly added UDP signatures will also be handled by the Cisco Secure IDS SME.

Table 3 identifies the UDP signatures that have been added to IDS.

Table 3 *Newly Added UDP Signatures to the Firewall IDS*

Signature ID	Signature Name	Signature Structure	Signature Description ¹
4051	Snork	Compound/Attack	Triggers when a UDP packet that has a source port of 135, 7, or 19 and a destination port of 135 is detected.

Table 3 Newly Added UDP Signatures to the Firewall IDS (continued)

Signature ID	Signature Name	Signature Structure	Signature Description ¹
4052	Chargen DoS	Compound/Attack	Triggers when a UDP packet is detected with a source port of 7 and a destination port of 19.
4600	IOS UDP Bomb	Compound/Attack	Triggers on receipt of improperly formed SYSLOG transmissions bound for UDP port 514. Note IDSIDS already supports the signature 4050 UDP Bomb, which is different from the Cisco IOS UDP Bomb.

1. For the latest signature description, refer to Cisco MySDN, which can be found at the following URL: <http://tools.cisco.com/MySDN/Intelligence/home.x>

TCP Signatures

Cisco Secure IDS SME handles already supported TCP signatures by the TCP application module (ATOMIC.TCP); thus, the newly added TCP signatures will also be handled by the Cisco Secure IDS SME.

Table 4 identifies the TCP signatures that have been added to IDS.

Table 4 Newly Added TCP Signatures to the Firewall IDS

Signature ID	Signature Name	Signature Structure	Signature Description ¹
3038	Fragmented NULL TCP Packet	Compound/Attack	Triggers when a single, fragmented TCP packet that has none of the SYN, FIN, ACK, or RST flags set has been sent to a specific host. This signature indicates that a reconnaissance sweep of your network may be in progress. The use of this type of packet indicates an attempt to conceal the sweep and may be a prelude to a more serious attack. This type of packet should never occur in legitimate traffic. The source of this packet should be shunned.

Table 4 Newly Added TCP Signatures to the Firewall IDS (continued)

Signature ID	Signature Name	Signature Structure	Signature Description ¹
3039	Fragmented Orphaned FIN Packet	Compound/Attack	Triggers when a single, fragmented orphaned TCP FIN packet is sent to a privileged port (having a port number less than 1024) on a specific host. This signature indicates that a reconnaissance sweep of your network may be in progress. The use of a single, fragmented FIN packet, when no other alarms fire, indicates an attempt to conceal the sweep by slowly scanning the network in an effort to beat port or host scan detectors. This attempt may be the prelude to a more serious attack.
3043	Fragmented SYN/FIN Packet	Compound/Attack	Triggers when a single, fragmented TCP packet with the SYN and FIN flags is set and sent to a specific host. This signature indicates that a reconnaissance sweep of your network may be in progress. The use of this type of packet indicates an attempt to conceal the sweep, and this attempt may be a prelude to a more serious attack. This type of packet should never occur in legitimate traffic. The source of this packet should be shunned.

1. For the latest signature description, refer to Cisco MySDN, which can be found at the following URL: <http://tools.cisco.com/MySDN/Intelligence/home.x>

IP Signatures

Cisco Secure IDS SME handles already supported atomic IP signatures by the IP application module (ATOMIC.L3.IP); thus, the newly added IP signatures will also be handled by the Cisco Secure IDS SME.

Table 5 identifies the IP signatures that have been added to IDS.

Table 5 Newly Added IP Signatures to the Firewall IDS

Signature ID	Signature Name	Signature Structure	Signature Description ¹
1101	Unknown IP Protocol	Compound/Info	Triggers when an IP datagram is received with the protocol field set to 134 or greater. This signature does not preclude the possibility that exploits do exist outside of the realm of the Cisco Systems knowledge domain. Note Signature 1101 is already supported; the recognized protocols have been modified.
1104	IP Localhost Source Spoof	Compound/Attack	Triggers when an IP packet with a source address of 127.x.x.x is detected. This signature may be indicative of someone trying to take advantage of local host trust relationships to either gain access to or in some other way subvert a target machine.

Table 5 Newly Added IP Signatures to the Firewall IDS (continued)

Signature ID	Signature Name	Signature Structure	Signature Description ¹
1105	Broadcast Source Address	Compound/Attack	Triggers when an IP packet with a source address of 255.255.255.255 is detected. This signature may be an indicator of an IP spoof attack or an attempt to subvert a firewall, proxy, or gateway.
1106	Multicast IP Source Address	Compound/Attack	Triggers when an IP packet with a source address of 224.x.x.x is detected. This signature may be an indicator of an IP spoof attack or an attempt to subvert a firewall, proxy, or gateway.
1107	RFC 1918 Addresses Seen	Compound/Info	Triggers when RFC 1918 addresses are detected.

1. For the latest signature description, refer to Cisco MySDN, which can be found at the following URL: <http://tools.cisco.com/MySDN/Intelligence/home.x>

IP Fragment Signatures

Cisco Secure IDS SME handles already supported IP Fragment signatures by the IP Fragment application module (ATOMIC.L3.IP); thus, the newly added IP Fragment signatures will also be handled by the Cisco Secure IDS SME.

Table 6 identifies the IP Fragment signatures that have been added to IDS.

Table 6 Newly Added IP Fragment Signatures to the Firewall IDS

Signature ID	Signature Name	Signature Structure	Signature Description ¹
1202	IP Fragment Overrun - Datagram Too Long	Compound/Attack	Triggers when a reassembled fragmented datagram exceeds the declared IP data length or the maximum datagram length. By definition, no IP datagram should be larger than 65,535 bytes; systems that try to process these large datagrams may crash. This type of fragmented traffic may be indicative of a denial of service attempt.
1206	IP Fragment Too Small	Compound/Attack	Triggers when any fragment other than the final fragment is less than 400 bytes, indicating that the fragment is likely to be intentionally crafted. Small fragments may be used in DOS attacks or in an attempt to bypass security measures or detection.

1. For the latest signature description, refer to Cisco MySDN, which can be found at the following URL: <http://tools.cisco.com/MySDN/Intelligence/home.x>

Log Messages for IDS Signatures

Each signature has an appropriately defined log message that can include information such as message limit, recommended action, DDTS component, and Technical Assistance Center (TAC) details.

IDS newly added signature alters (as well as the already supported 59 signatures) are displayed in the following format:

```
%IDS-n-SIG_NAME: Sig:XXXX: Description - from &i to %i
```

An “n” refers to the severity of the logging. In IDS, all signatures have “n” set to level 4, meaning LOG_WARNING, which does not follow the recommended alarm level posed by the NSDB for various signatures.

**Note**

All messages sent to Cisco Secure IDS via the Post Office protocol have a different format from other messages; these messages contain the severity level recommended from the NSDB.

To enable log messages for IDS signatures, refer to the chapter “[Configuring Cisco IOS Firewall Intrusion Detection System](#)” in the *Cisco IOS Security Configuration Guide*, Release 12.2.

How to Use the Firewall IDS Signature Enhancements

Although this feature does not introduce any new or modified commands, you must still configure and apply audit rules to your router to support the Cisco Firewall IDS. This section contains the following procedure:

- [Configuring and Applying Audit Rules, page 9](#)

Configuring and Applying Audit Rules

To configure your router to support the Firewall IDS and support the newly added signatures, use the following commands.

Prerequisites

Before applying audit rules to your router, you should initialize the Firewall IDS on your router. For information on completing this task, refer to the section “[Initializing Cisco IOS Firewall IDS](#)” in the chapter “[Configuring Cisco IOS Firewall Intrusion Detection System](#)” of the *Cisco IOS Security Configuration Guide*, Release 12.2.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip audit info {action [alarm] [drop] [reset]}**
or
ip audit attack {action [alarm] [drop] [reset]}
4. **ip audit name *audit-name* {info | attack} [list *standard-acl*] [action [alarm] [drop] [reset]]**
5. **ip audit signature *signature-id* {disable | list *acl-list*}**
6. **interface *interface-number***
7. **ip audit *audit-name* {in | out}**
8. **exit**
9. **ip audit po protected *ip-addr* [to *ip-addr*]**

DETAILED STEPS

	Command or Action	Purpose
Step 1	<p>enable</p> <p>Example: Router> enable</p>	<p>Enables privileged EXEC mode.</p> <ul style="list-style-type: none"> Enter your password if prompted.
Step 2	<p>configure terminal</p> <p>Example: Router# configure terminal</p>	<p>Enters global configuration mode.</p>
Step 3	<p>ip audit info {action [alarm] [drop] [reset]}</p> <p>Example: Router(config)# ip audit info action alarm</p> <p>or</p> <p>ip audit attack {action [alarm] [drop] [reset]}</p> <p>Example: Router(config)# ip audit attack action alarm</p>	<p>Sets the default actions for information and attack signatures.</p> <ul style="list-style-type: none"> Both types of signature can take any or all of the following actions: alarm, drop, and reset. The default action is alarm.

Command or Action	Purpose
<p>Step 4</p> <pre>ip audit name audit-name {info attack} [list standard-acl] [action [alarm] [drop] [reset]]</pre> <p>Example:</p> <pre>Router(config)# ip audit name ids-policy info action alarm</pre>	<p>Creates audit rules, where <i>audit-name</i> is a user-defined name for an audit rule.</p> <ul style="list-style-type: none"> For example: <pre>ip audit name audit-name info ip audit name audit-name attack</pre> <p>The default action is alarm.</p> <p>Note Use the same name when you assign attack and information type signatures.</p> <ul style="list-style-type: none"> You can also use the ip audit name command to attach access control lists (ACLs) to an audit rule for filtering out sources of false alarms. In this case, <i>standard-acl</i> is an integer representing an ACL. If you attach an ACL to an audit rule, the ACL must also be defined: <pre>ip audit name audit-name {info attack} list acl-list</pre> <p>In the following example, ACL 99 is attached to the audit rule INFO, and ACL 99 is defined:</p> <pre>ip audit name INFO info list 99 access-list 99 deny 10.1.1.0 0.0.0.255 access-list 99 permit any</pre> <p>Note The ACL in the preceding example is <i>not</i> denying traffic from the 10.1.1.0 network (as expected if it were applied to an interface). Instead, the hosts on that network are not filtered through the audit process because they are trusted hosts. On the other hand, all other hosts, as defined by permit any, are processed by the audit rule.</p>

	Command or Action	Purpose
Step 5	<p><code>ip audit signature signature-id {disable list acl-list}</code></p> <p>Example: Router(config)# ip audit signature 2345 list 91</p>	<p>Disables individual signatures.</p> <ul style="list-style-type: none"> Disabled signatures are not included in audit rules, as this is a global configuration change. <p><code>ip audit signature signature-number disable</code></p> <p>To reenable a disabled signature, use the no ip audit signature command, where <i>signature-number</i> is the number of the disabled signature.</p> <ul style="list-style-type: none"> You can also use the ip audit signature command to apply ACLs to individual signatures for filtering out sources of false alarms. In the following, case <i>signature-number</i> is the number of a signature, and <i>acl-list</i> is an integer representing an ACL: <p><code>ip audit signature signature-number list acl-list</code></p> <p>For example, in the following, ACL 35 is attached to the 1234 signature and then defined:</p> <pre>ip audit signature 1234 list 35 access-list 35 deny 10.1.1.0 0.0.0.255 access-list 35 permit any</pre> <p>Note The ACL in the preceding example is <i>not</i> denying traffic from the 10.1.1.0 network (as expected if it were applied to an interface). Instead, the hosts on that network are not filtered through the signature because they are trusted hosts or are otherwise causing false positives to occur. On the other hand, all other hosts, as defined by permit any, are processed by the signature.</p>
Step 6	<p><code>interface interface-number</code></p> <p>Example: Router(config-if)# interface Ethernet 0/0</p>	Enters interface configuration mode.
Step 7	<p><code>ip audit audit-name {in out}</code></p> <p>Example: Router(config-if)# ip audit ids-policy in</p>	<p>Applies an audit rule at an interface.</p> <ul style="list-style-type: none"> With this command, <i>audit-name</i> is the name of an existing audit rule, and <i>direction</i> is either in or out.
Step 8	<p><code>exit</code></p> <p>Example: Router(config-if)# exit</p>	Exits interface configuration mode.
Step 9	<p><code>ip audit po protected ip-addr [to ip-addr]</code></p> <p>Router(config)# ip audit po protected 10.1.1.0</p>	<p>Configures which network should be protected by the router.</p> <ul style="list-style-type: none"> Here, <i>ip_addr</i> is the IP address to protect.

Configuration Examples for Firewall IDS

This section provides the following configuration example:

- [IDS on a Router Configuration Example, page 13](#)

IDS on a Router Configuration Example

The following example shows how to enable a Cisco IOS router for the Firewall IDS:

```
ip audit name EXAMPLE attack action alarm drop reset
ip audit name EXAMPLE info action alarm
ip cef
interface Serial0
  ip address 191.1.1.1 255.255.255.0
  ip audit EXAMPLE in
  ip route-cache cef
  no shutdown
```

Additional References

For additional information related to Firewall Intrusion Detection System (IDS) Signature Enhancements, refer to the following references:

- [Related Documents, page 13](#)
- [Standards, page 13](#)
- [MIBs, page 14](#)
- [RFCs, page 14](#)
- [Technical Assistance, page 14](#)

Related Documents

Related Topic	Document Title
IDS information and configuration tasks	The chapter “ Configuring Cisco IOS Firewall Intrusion Detection System ” in the <i>Cisco IOS Security Configuration Guide</i> , Release 12.2
IDS commands	The chapter “ Cisco IOS Firewall Intrusion Detection System Commands ” in the <i>Cisco IOS Security Command Reference</i> , Release 12.2
Vulnerability statistics using SPA data that has been collected by the Cisco Secure Consulting Services	Cisco Secure Encyclopedia

Standards

Standards	Title
None	—

MIBs

MIBs ¹	MIBs Link
None	To obtain lists of supported MIBs by platform and Cisco IOS release, and to download MIB modules, go to the Cisco MIB website on Cisco.com at the following URL: http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml

1. Not all supported MIBs are listed.

To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL:

<http://tools.cisco.com/ITDIT/MIBS/servlet/index>

If Cisco MIB Locator does not support the MIB information that you need, you can also obtain a list of supported MIBs and download MIBs from the Cisco MIBs page at the following URL:

<http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml>

To access Cisco MIB Locator, you must have an account on Cisco.com. If you have forgotten or lost your account information, send a blank e-mail to cco-locksmith@cisco.com. An automatic check will verify that your e-mail address is registered with Cisco.com. If the check is successful, account details with a new random password will be e-mailed to you. Qualified users can establish an account on Cisco.com by following the directions found at this URL:

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

RFCs

RFCs ¹	Title
RFC 0768	<i>User Datagram Protocol</i>
RFC 0791	<i>Internet Protocol</i>
RFC 0793	<i>Transmission Control Protocol</i>
RFC 1035	<i>Domain Names—Implementation and Specification</i>
RFC 1945	<i>Hypertext Transfer Protocol -- HTTP/1.0</i>
RFC 2616	<i>Hypertext Transfer Protocol -- HTTP/1.1</i>

1. Not all supported RFCs are listed.

Technical Assistance

Description	Link
Technical Assistance Center (TAC) home page, containing 30,000 pages of searchable technical content, including links to products, technologies, solutions, technical tips, and tools. Registered Cisco.com users can log in from this page to access even more content.	http://www.cisco.com/public/support/tac/home.shtml

Command Reference

This feature uses no new or modified commands. All other commands used with this feature are documented in the Cisco IOS Release 12.2 T command reference publications.

Glossary

ACL—access control list. ACL is a list kept by routers to control access to or from the router for a number of services (for example, to prevent packets with a certain IP address from leaving a particular interface on the router).

CBAC—Context-Based Access Control. CBAC is the protocol that provides internal users with secure access control for each application and for all traffic across network perimeters. CBAC enhances security by scrutinizing both source and destination addresses and by tracking the connection status of each application.

Compound—Type of attack signature that occurs across multiple packets on the context of a session (referred to as composite in the Network Security Database [NSDB].)

Cisco IOS Firewall IDS—The limited subset of Cisco Secure IDS features provided in Cisco IOS.

The Cisco IOS Firewall IDS feature supports intrusion detection technology for low-range to high-end router platforms with firewall support. It is ideal for any network perimeter, and especially for locations in which a router is being deployed and additional security between network segments is required. It also can protect intranet and extranet connections where additional security is mandated, and branch-office sites connecting to the corporate office or Internet.

Cisco Secure IDS—Enterprise-scale, real-time intrusion detection system designed to detect, report, and terminate unauthorized activity throughout a network.

NSDB—Network Security Database. A NSDB is a database that contains the collection of signatures defined and supported by Cisco Secure IDS.

SME—signature micro engine. SME is the code in Cisco Secure IDS that implements the state machine to process a given set of similar signatures.

SPA—Security Posture Assessment. Determines the most commonly found vulnerabilities.

**Note**

Refer to the [Internetworking Terms and Acronyms](#) for terms not included in this glossary.
