Cisco Router IDS Solution

The remainder of this chapter focuses on Cisco router IDS capabilities and the configuration of IDS using the Cisco IOS Firewall feature set. The Cisco IOS IDS implementation is suited best for midlevel to higher-level platforms because of the overhead associated with examining packets to detect threats and attacks on perimeter routers. It also can provide a level of protection for remote access and dialup connections. There are four basic reasons for deploying the Cisco IOS Firewall IDS:

- To extend security to your perimeter routers across an enterprise network, especially at branch and regional offices
- To provide a cost-effective IDS solution for small- to medium-size businesses
- To detect external attacks directed at the router itself where a network-based sensor, connected behind the router, cannot detect these attacks
- To implement a one-box perimeter solution

NOTE

The router IDS is not a full-blown IDS solution: Because it is an inline solution, it might affect the performance of the router. Therefore, you need to be careful about enabling it on a router. Also, the router supports a limited number of signatures and, therefore, should be coupled with a network-based IDS solution, such as the 4200 sensors, in medium- to large-size networks.

Signature Support

Whereas the Cisco network-based sensors, such as the 4200, support more than 1000 signatures, the Cisco IOS Firewall IDS feature supports only 100. Because of the limited number of signatures, the Cisco IOS IDS software typically is used at the perimeter of the network and in combination with other IDS solutions, such as dedicated hardware sensors.

For example, if you refer back to Figure 16-1, you can see that the hardware sensor sitting behind the perimeter router never sees the traffic that the perimeter router filters. With the Cisco IOS IDS software, the perimeter router at least can report a small number of attacks that are directed at the perimeter router or that the perimeter router filters; in either case, the hardware sensor behind the perimeter router would never see this traffic anyway. Even though the number of signatures is limited, the Cisco IOS IDS software looks for common attacks and threats. Table 16-2 lists the signatures supported by the Cisco IOS Firewall IDS feature set.

Table 16-2. Cisco IOS Supported Signatures

Signature Number	Type	Description
1000	Informational, atomic	Bad options exist in the IP header, or the IP header is incomplete or malformed.
1001	Informational, atomic	Option 7 in the IP header is marked (record the route of the packet).

1002	Informational, atomic	Option 4 in the IP header is marked (timestamp information requested).
1003	Informational, atomic	Option 2 (security) in the IP header is marked. This is obsolete.
1004	Informational, atomic	Option 3 in the IP header is marked (loose source-routing information).
1005	Informational, atomic	Option 8 (SATNET stream identifier) in the IP header is marked. This is obsolete.
1006	Informational, atomic	Strict source routing is requested for the packet.
1100	Attack, atomic	The "more fragments" flag is set to 1, or an offset is indicated in the Offset field.
1101	Attack, atomic	A packet has an IP protocol of 134 or higher. These protocols either are undefined or are reserved and should not be used. (The IP protocol number used to be 101.)
1102	Attack, atomic	This indicates a Land.c attack, in which the source and destination addresses are the same.
1104	Attack, compound	127.0.0.1 is detected in the source IP address field.
1105	Attack, compound	A broadcast address (255.255.255.255.) is detected in the source IP address field.
1106	Attack, compound	A multicast address is detected in the source IP address field.
1107	Informational, compound	RFC 1918 addresses are detected.
1202	Attack, compound	The reassembled packet is larger than the specified length or is greater than 65,535 bytes.
1206	Attack, compound	Any fragment (except the last) is less than 400 bytes.
2000	Informational, atomic	The ICMP type field is set to 0 (echo reply).
2001	Informational, atomic	The ICMP type field is set to 1 (host unreachable).
2002	Informational, atomic	The ICMP type field is set to 4 (source quench).
2003	Informational, atomic	The ICMP type field is set to 5 (redirect).
2004	Informational, atomic	The ICMP type field is set to 8 (echo request).
2005	Informational, atomic	The ICMP type field is set to 11 (time exceeded).
2006	Informational, atomic	The ICMP type field is set to 12 (parameter problem in the packet).

2007	Informational, atomic	The ICMP type field is set to 13 (timestamp request).
2008	Informational, atomic	The ICMP type field is set to 14 (timestamp reply).
2009	Informational, atomic	The ICMP type field is set to 15 (information request).
2010	Informational, atomic	The ICMP type field is set to 16 (information reply).
2011	Informational, atomic	The ICMP type field is set to 17 (subnet mask request).
2012	Informational, atomic	The ICMP type field is set to 18 (subnet mask reply).
2150	Attack, atomic	An ICMP packet has the More Fragments flag set to 1, or an offset is indicated in the header.
2151	Attack, atomic	The length in the IP header is set to something larger than 1024 bytes.
2154	Attack, atomic	An ICMP packet has the last fragment bit set, and the following is true: ("IP offset" * 8) + "IP data length" > 65,535). This is called the Ping of Death.
3038	Attack, compound	A TCP segment does not have the SYN, FIN, ACK, or RST flags set (reconnaissance sweep).
3039	Attack, compound	A fragmented TCP FIN packet was sent to a port less than 1024, called an orphaned FIN.
3040	Attack, atomic	A TCP segment with no bits set is present in the flags field.
3041	Attack, atomic	A TCP segment has both the SYN and FIN bits set.
3042	Attack, atomic	A TCP segment has the FIN bit set but no ACK bit set.
3043	Attack, compound	A fragmented TCP segment has the SYN and FIN bits set.
3050	Attack, compound	Multiple TCP connections have been initiated but have not completed. This looks at only ports 21, 23, 25, and 80.
3100	Attack, compound	This looks for the mail attack against RFC-compliant SMTP servers, such as sendmail.
3101	Attack, compound	E-mail messages have the pipe symbol (|) in the To field.
3102	Attack, compound	E-mail messages have the pipe symbol (|) in the From field.
3103	Attack, compound	E-mail messages have the expn or vrfy commands.
3104	Attack, compound	E-mail messages have the wiz or debug commands.

3105	Attack, compound	E-mail messages have :decode@ in the e-mail header.
3106	Attack, compound	An e-mail message has more than 250 (default) Rcpt To lines.
3107	Attack, compound	A bug in Majordomo allows remote users to execute commands on the server.
3150	Attack, compound	The FTP site command was executed on an FTP connection.
3151	Informational, compound	The FTP syst command was executed on an FTP connection.
3152	Attack, compound	The FTP cwd ~root command was executed on an FTP connection.
3153	Attack, atomic	In an FTP connection, a port command was executed with a different address than the requesting source.
3154	Attack, atomic	A port number less than 1024 or greater than 65,535 was specified on an FTP connection.
3215	Attack, compound	Someone tried to execute a command, using a directory traversal bug, on an IIS web server (IIS DOT DOT EXECUTE attack).
3229	Attack, compound	Someone tried to access the win-c-sample program through a web server.
3233	Attack, compound	An overflow attempt against the CGI-bin count program was detected.
4050	Attack, atomic	The UDP segment length is less than the length in the IP header.
4051	Attack, compound	UDP packets have a source port of 7, 19, or 135 and a destination of 135 (Snork attack).
4052	Attack, compound	UDP traffic was sent to port 7 or 19 (Chargen attack).
4100	Attack, compound	Someone tried to access the /etc/passwd file through TFTP.
4600	Attack, compound	A malformed syslog message was sent to UDP port 514. This is called an Cisco IOS UDP bomb.
5034	Attack, compound	Someone tried to run the newdsn.exe program through an HTTP server.
5035	Attack, compound	An attacker tried to send commands through the CGI-bin program HylaFAX Faxsurvey.
5041	Attack, compound	An attacker tried to execute commands through a CGI-bin script.
5043	Attack, compound	An attacker tried to access scripts on a ColdFusion server.

5044	Attack, compound	An attacker tried to execute commands through the rguest.exe or wguest.exe CGI-bin scripts associated with the Webcom.se Guestbook.
5045	Attack, compound	A CGI-bin script attempted to execute the xterm-display command to circumvent a UNIX WWW server.
5050	Attack, compound	A .htr buffer overrun attack was detected against a Windows IIS server.
5055	Attack, compound	An HTTP buffer overflow attempt was made using a large username/password combination.
5071	Attack, compound	An attacker tried to access the msacds.dll WWW Windows file to execute commands or view secured files.
5081	Attack, compound	An attacker tried to access the cmd.exe program on a Windows WWW server.
5090	Attack, compound	An attacker tried to access a FrontPage CGI script with a filename ending in 0,0.
5114	Attack, compound	An attacker tried to exploit the Unicode ../ directory movement in WWW IIS.
5116	Attack, compound	An attacker sent shell metacharacters to be executed with the privilege level in the CGI script in Endymion MailMan.
5117	Attack, compound	An attacker attempted to execute code that exploits a vulnerability in phpGroupWare.
5118	Attack, compound	An attacker sent a special HTTP/GET request to upload files to the web server (called the eWave ServletEXEC 3.0C File Upload attack).
5123	Attack, compound	An abnormally large HTTP GET request was sent to a web server.
6050	Informational, compound	Someone attempted to access HINFO DNS records on a DNS server.
6051	Informational, compound	A DNS zone transfer with a source port of 53 (legitimate) was detected.
6052	Attack, compound	A DNS zone transfer with a different source port than 53 was detected.
6053	Informational, compound	Someone requested all the records for a DNS server.
6054	Informational, compound	Someone requested the version of a DNS server.
6055	Attack, compound	A DNS inverse query with more than 255 characters was detected, attempting a buffer overflow.
6056	Attack, compound	A DNS NXT buffer overflow against a DNS server was detected.
6057	Attack, compound	A DNS SIG buffer overflow against a DNS server was detected.

6062	Informational, compound	A DNS query of type TXT was made with the string Authors.Bind.
6063	Informational, compound	A DNS query type 251 was detected for a zone transfer.
6100	Informational, atomic	Someone tried to register new RPC services on a host.
6101	Informational, atomic	Someone tried to unregister RPC services on a host.
6102	Informational, atomic	An RPC dump request was made to a host.
6103	Attack, atomic	A proxied RPC request was sent to the portmapper process on a host.
6150	Informational, atomic	A request was sent to the portmapper process for the YP server daemon.
6151	Informational, atomic	A request was sent to the portmapper process for the YP bind daemon.
6152	Informational, atomic	A request was sent to the portmapper process for the YP password daemon.
6153	Informational, atomic	A request was sent to the portmapper process for the YP update daemon.
6154	Informational, atomic	A request was sent to the portmapper process for the YP transfer daemon.
6155	Informational, atomic	A request was sent to the portmapper process for the mount daemon.
6175	Informational, atomic	A request was sent to the portmapper process for the rexd daemon.
6180	Informational, atomic	A call was sent to the portmapper process for the rexd daemon. This typically indicates an access attack.
6190	Attack, atomic	A large statd request was sent, probably indicating a buffer overflow attack method.
8000:2101	Attack, atomic	Someone entered the string passwd during an FTP session, probably indicating that someone was trying to download the system's password file.

NOTE

More than 40 signatures were added in 12.2(15)T; therefore, if you have an older Cisco IOS version, the number of signatures that the Cisco IOS Firewall feature set supports is actually less than 60. Read the Cisco IOS release notes to determine what signatures are enabled for the Cisco IOS version that you currently are running on your router.

Router IDS Process

By default, IDS is not enabled on a router that has the Cisco IOS Firewall feature set installed. Instead, you must create audit rules, which specify the signatures that the Cisco IOS should use when looking for suspicious traffic, threats, or attacks. Cisco divides the signatures into two basic categories on the Cisco IOS, based on their severity: informational and attack. You can enable one or both groups. Also, you can selectively enable or disable specific signatures, or specify that a signature be enabled or disabled for a specific host or hosts.

After you have created your audit rule, you need to activate it on the router's interface(s) in an in or out direction. After you do this, IDS is enabled. If you applied the audit rule inbound, all packets are audited entering the interface. Unlike most other features, IDS is performed before any inbound ACL is processed; this enables you to detect external threats coming into your network. If you apply an audit policy outbound on an interface, as long as traffic is permitted into the router and routed to the outbound interface, the audit policy is used. In this case, IDS examines packets before the outbound ACL, if any, is processed on the interface.

When comparing a packet or packets against the router's signatures, the Cisco IOS does it in this order:

1. IP signatures
2. ICMP signatures
3. TCP or UDP signatures (depending on the connection type)
4. Application layer signatures

NOTE

One important thing to point out about the matching process is that, as soon as the Cisco IOS finds a match on one signature, it immediately stops looking for any other matches within the same type. However, it continues to look for matches in other modules. For example, if the Cisco IOS finds an IP signature match, it does not look for any other IP signature matches, but it continues on to ICMP. This is different from the Cisco 4200 hardware sensors, which look for all possible signature matches in all categories.

When a router with the firewall IDS enabled detects an attack, it can take one of three actions:

- Generate an alarm, which, by default, is displayed on the console. This alarm also can be sent to a syslog server or to Cisco Secure IDS Director, a centralized management platform.
- For TCP connections, reset them.
- Drop the packet.

TIP

Cisco highly recommends that you use the reset and drop actions together.

Even though all 100 signatures are enabled by default, you selectively can disable them if the router is triggering a high number of false positives. You can even disable a signature selectively based on the device that triggered the alarm.

Memory and Performance Issues

I previously discussed some general issues with IDS solutions. This section discusses some issues that are specific to the Cisco IOS and the IDS and its configuration. Obviously, the performance of IDS on a Cisco router depends on many things, including these:

- The processor on the router.
- The amount of memory on the router. For compound signatures, the CBAC allocates memory to maintain not only the state information for the connection, but also internal caching of packets.

- The amount of traffic traveling through the router.
- Whether the router is performing encryption.

NOTE

Enabling or disabling specific signatures does not impact the performance of IDS on the router. Likewise, interface ACLs do not impact IDS performance. However, if you are using an ACL to determine what packets trigger signatures, there will be a significant impact in the performance of the router.