



Cisco IOS[®] Firewall Intrusion Detection System

Application Overview

As network security becomes increasingly critical to securing business transactions and computer resources, businesses must integrate security into the network design and infrastructure. Security policy enforcement is most effective when it is an inherent component of the network. Cisco Systems protects your business by providing easy-to-manage integrated security solutions for your network.

Cisco IOS[®] Firewall Intrusion Detection System (IDS) is a complementary solution to Cisco security appliances and can integrate easily with the appliances. The Cisco IOS IDS is a security-specific option for Cisco IOS Software, integrating robust firewall functions and intrusion detection for every network segment. Intrusion detection systems provide a level of protection beyond the firewall by protecting the network from internal and external security attacks and threats.

Cisco IOS IDS is ideal for any network perimeter, and is especially recommended in branch or regional office environments and for telecommuter use. It also can protect intranet and extranet connections where additional security is mandated, and branch office sites connecting to the corporate office or Internet.

The Cisco IOS IDS feature identifies more than a hundred of the most common security attacks using “signatures” to detect patterns of misuse in network traffic, including information and attack signatures. The intrusion-detection signatures included in the Cisco IOS Firewall were chosen from a cross section of intrusion-detection signatures. The

signatures represent severe breaches of security and the most common network attacks and information-gathering scans.

The Cisco IOS IDS is as an integrated intrusion detection sensor, watching packets and sessions as they flow through the router, scanning each to match the IDS signatures. Upon detection of suspicious activity, the Cisco IOS IDS responds before network security can be compromised and sends alarms to a management console. The network administrator can configure the Cisco IOS IDS to choose the appropriate response to security incidents. When packets in a session match a signature, the Cisco IOS IDS can be configured to take these actions:

- Send an alarm to a syslog server or a centralized management interface
- Drop the packet
- Reset the TCP connection

Cisco developed the Cisco IOS Software-based intrusion-detection capabilities in Cisco IOS Firewall with flexibility in mind, so that individual signatures could be disabled in case of false alarms. Also, while it is preferable to enable both the firewall and intrusion-detection



features of the Cisco IOS security engine to support a network security policy, each of these features may be enabled independently and on different router interfaces. Cisco IOS Software-based intrusion detection is part of the Cisco IOS Firewall.

The Cisco IOS IDS is the best choice for integrating multiprotocol routing with security policy enforcement. It scales to allow customers to choose a router platform based on bandwidth, LAN or WAN density, and multiservice requirements; simultaneously, it benefits from advanced security. Coupled with Cisco security appliances, Cisco IOS security solutions offer a layered approach to security. Cisco IOS security solutions can easily integrate with existing security appliances, thereby reducing total cost of ownership for the business.

Refer to these guidelines to choose the right Cisco router for varied security environments:

- *Telecommuters/Small/medium standalone offices:* Cisco 800, UBR900, SOHO 70, and 1700 Series Routers
- *Branch/Regional and extranet environments:* Cisco 2600XM, 3600XM and 3700 Series Routers
- *VPN and WAN aggregation points or other high-throughput environments:* Cisco 7100, 7200, 7400, 7500, RSM Series Routers; Cisco Catalyst® 5000 and Catalyst 6000 series switches.

For more detailed information about Cisco IOS IDS, refer to the Cisco IOS Firewall IDS Data Sheet, Cisco IOS Firewall IDS White Paper, and Cisco IOS Firewall IDS Design Guide.

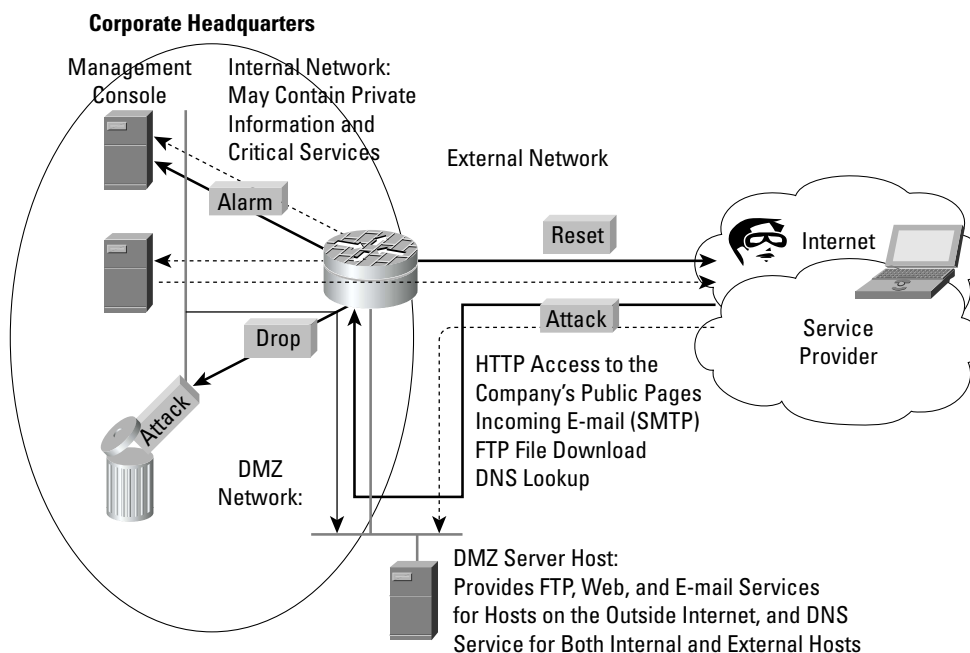
Corporate Internet Perimeter

Cisco IOS IDS combined with strong access control provides a fairly robust security service. The IDS router audits traffic from the untrusted Internet before it reaches the DMZ (Demilitarized Zone) or the corporate network. A DMZ network is used to provide services to the outside world. DMZ Servers are typically placed in a data center. The basic policy is to allow anyone on the Internet to connect to the WWW, FTP, and SMTP services on the DMZ network, and to make DNS queries to it. This allows external people to view the company's Web pages, pick up files the company has posted for outside consumption, and send mail into the company. The DMZ can also be configured such that Internet users connect to servers on the DMZ network to access public corporate information.

The DMZ network and the perimeter router are very vulnerable to security attacks from the untrusted Internet. Some of the common security attacks to the corporate perimeter include Denial of Service (DoS) attacks that can make the entire network unresponsive. Common DoS attacks include TCP syn floods, UDP floods, ICMP floods. Other attacks include IP spoofing or information gathering attacks such as a ping sweep or a port sweep. Intruders can also hack into CGI scripts to get access to the Web servers in the DMZ. Depending on the security policy, the router running Cisco IOS IDS monitors incoming traffic before the inbound access list is analyzed, and alerts the administrator of attacks or information-gathering activity. Typical security attacks exploit the trust relationship between the DMZ servers and the inside segment. In a typical scenario the attacker first compromises the server on the DMZ network, and then uses this server to access the inside. Once detected, the intrusion detection system can drop the packets, or in the case of a security attack, send TCP resets. Cisco security appliances may be more appropriate for corporations requiring more bandwidth or a dedicated IDS appliance to monitor traffic.



Figure 1



Inter-Departmental Resource Protection

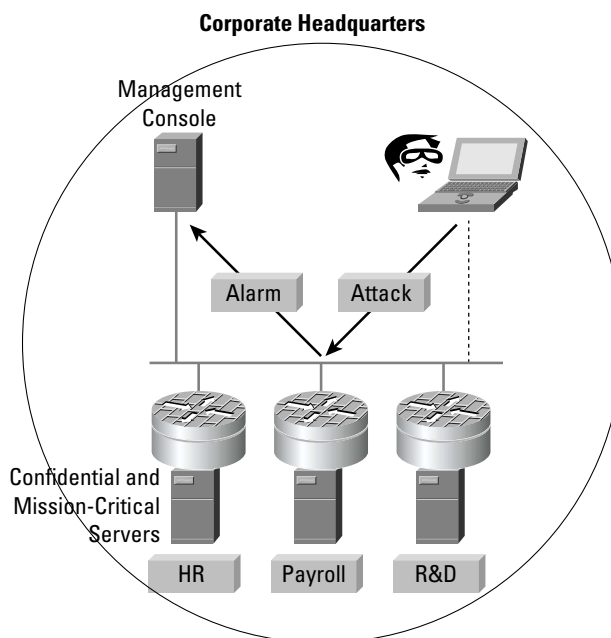
Internal attacks on the network can have a significant impact and can cause damage to the network. This deployment is for protection of mission-critical servers such as HR, ERP, CRM, or accounting systems. It is important to keep critical departments segregated from common traffic. Enabling Cisco IOS IDS on the router will help protect against security breaches from within the organization.

Departments with sensitive data are subject to many information-gathering attacks from within the organization. Employees might try to gain access to them by guessing or cracking passwords, and IP spoofing. No department is immune from disgruntled employees, corporate spies, visiting guests, and backdoor attacks creating holes in the network and putting information assets at risk.

Firewalls and access lists are typically enabled on these network segments to block unauthorized access. IDS provides an additional layer of security on these segments and protects sensitive data from internal as well as external attacks. IDS can monitor this traffic and notify the administrator of attacks or information-gathering activity via the management console. Furthermore, it is important to refine the IDS configuration to avoid false alarms, leading to management nightmares for network administrators. For example, IDS might be configured to only notify the administrator rather than drop the packet, in case of false alarms.



Figure 2



Branch Office and Partner Extranet Deployment

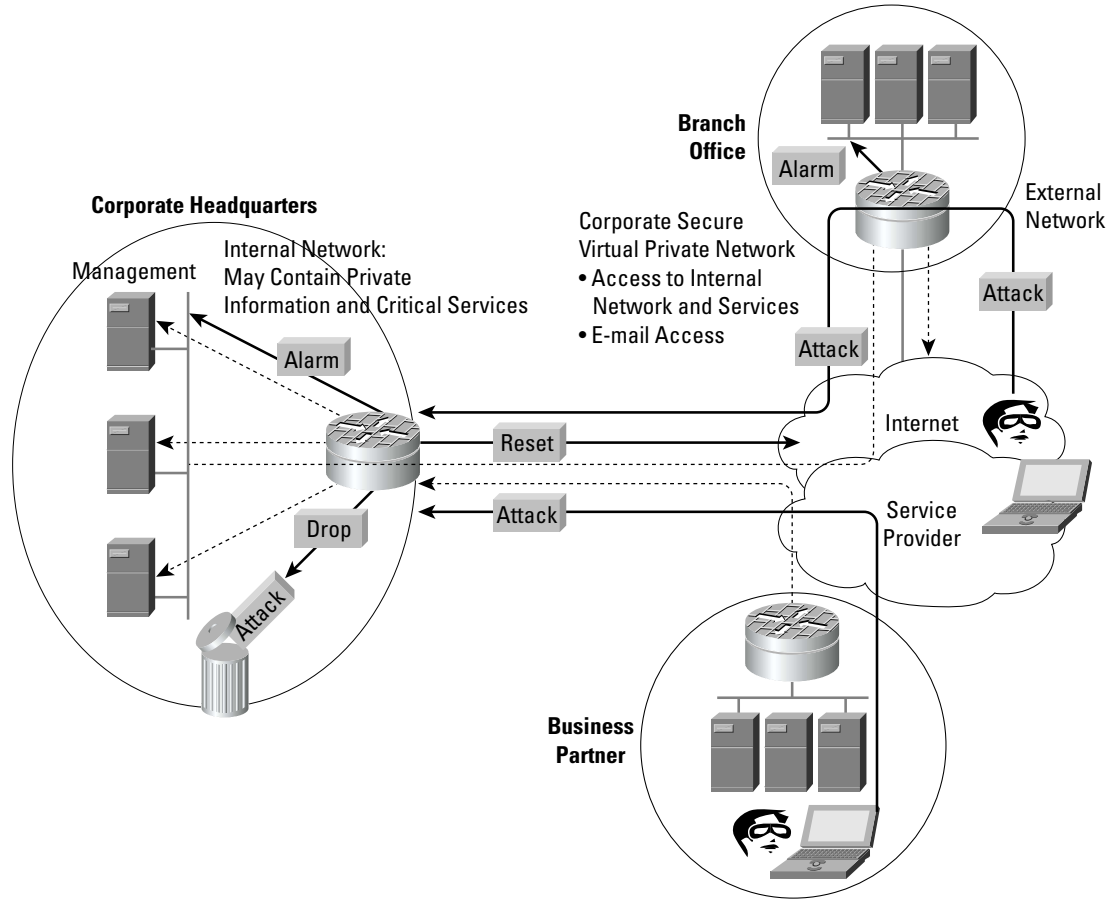
Most enterprises are virtual organizations, spread across many branch offices, all needing to be connected to headquarters with access to a central organization. In some cases, they may be dependent on sharing proprietary information directly with partners via Internet or WAN connectivity.

Both types of connectivity are vulnerable to security attacks from the untrusted Internet. The branch offices are subject to attacks such as ping sweep, port sweep, IP spoofing, or other attacks to get into the internal network via the branch office. Because of the distance from headquarters, branch offices can be more prone to user efforts to gain access to departments in the corporate network. The partners are part of the company's extranet segment, which is vulnerable to attacks both from within the partner site and the untrusted Internet. The partners can be connected to specific servers on the corporate network, therefore, should be protected.

Cisco IOS IDS-enabled routers can be deployed at the perimeter of the branch office network and the extranet partner site. IDS is activated on both the outgoing and the incoming interface to monitor traffic and watch for suspicious activity generating from the partner's network or the branch office. The IDS configuration should be in a restrictive stance because signatures matched here have successfully passed through the firewall already. The administrator can be notified of any form of security attack or information-gathering activity via the management console at headquarters. In case of regional offices, management is typically located at the regional office location.



Figure 3



Telecommuter Deployment

Corporate telecommuters have a LAN network in the house with several different computers connected to it. They are subscribed to an Internet service provider (ISP) service that provides them connectivity to the Internet. They connect to the corporate network via a virtual private network (VPN). Business resources for the telecommuter such as e-mail, confidential information, and server access reside on the corporate network. Telecommuters need the same amount or more protection as the corporate employees due to the nature of their virtual setup. Their offices don't have physical security such as badge entry, like corporate headquarters, thus exposing them to more risk.

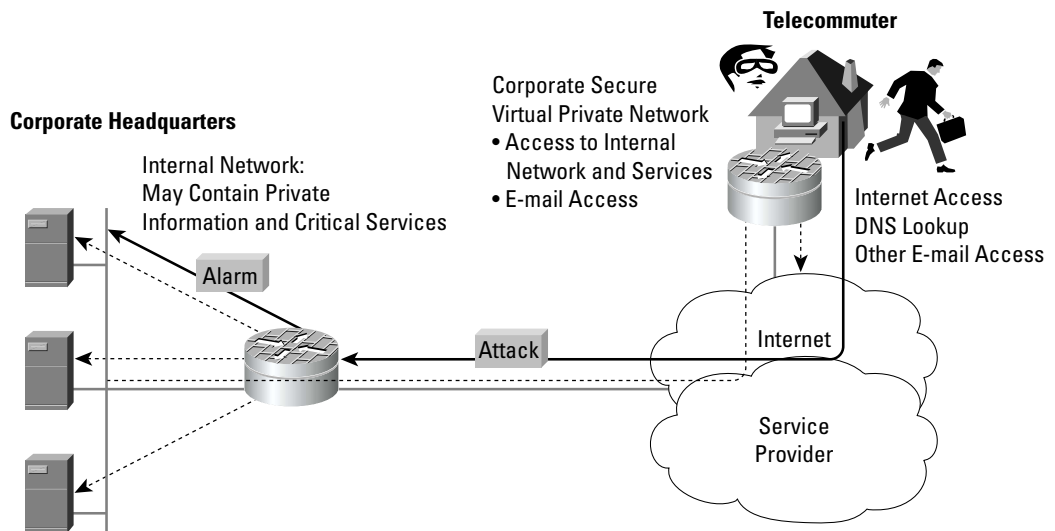
Typically a firewall is enabled at the perimeter router of a telecommuter setup and permits only outgoing connections. The computers on the home LAN can connect to the Internet via the ISP network, but no outside initiated sessions to the private LAN are allowed. The telecommuter can view Web pages, send e-mail messages, pick up incoming e-mail messages from the corporate network or ISP, retrieve software via FTP, connect remotely using Telnet, and join in multimedia conferences, all without exposing services on the LAN.



Even though firewall is enabled to restrict access from the untrusted Internet, intruders can still potentially invade the perimeter router on the telecommuter side and gain access to the corporate network. Some of the common security attacks include IP spoofing, man-in-the-middle attacks, and unauthorized access that may have slipped through the firewall. Outgoing traffic from the telecommuter's end can also pose a threat to the internal network, in case the telecommuter attempts to compromise the corporate network or the Internet.

IDS can be applied at the ingoing and outgoing interfaces of the perimeter router to monitor and discard malicious activity. The administrator on the corporate side can be notified of the activities via the IDS management console. Cisco IOS IDS gives customers the flexibility of implementing instances of intrusion detection in the appropriate traffic segment based on corporate telecommuter policy.

Figure 4



Summary

The Cisco IOS IDS provides *Integrated Network Security* through Cisco IOS Software. A robust security policy entails more than perimeter control or IDS setup and management—security policy enforcement must be an inherent component of the network. Cisco IOS Software is an ideal vehicle for implementing a global security policy. Building an end-to-end Cisco solution allows security practitioners to enforce security policies throughout the network as it evolves.



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: +65 317 7777
Fax: +65 317 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**

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 © 1992-2002, Cisco Systems, Inc. All rights reserved. Catalyst, Cisco, Cisco IOS, Cisco Systems, 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.
(0208R) TS/LW3851 11/02