Cisco IOS Security

The one product that has put Cisco on the face of the networking map is Cisco IOS software, which runs on a variety of platforms from routers and switches, as well as other devices. Cisco continually is enhancing the Cisco IOS to include new features and tools that enable you to deal with the networking problems you face every day.

When it comes to security, the Cisco IOS is packed with all kinds of security features that you can take advantage of in securing your network. Some security tools are part of the normal Cisco IOS packaging. Other tools require the purchase of the Cisco IOS Firewall feature set, which includes enhanced firewall tools to implement access control more securely. The following two sections discuss some of the security features you will find in the Cisco IOS software and compare two Cisco firewall products: the Cisco IOS router and the PIX.

Cisco IOS Uses

As I mentioned in the introduction to this section, the Cisco IOS is packed with many different kinds of security tools and features that enable you to implement a secure firewall system. Combined with the Cisco IOS Firewall feature set, you can set up your Cisco IOS router as a well-defended perimeter firewall or a scalable Internet firewall, providing a robust firewall solution. Here is just a small list of roles that your Cisco IOS router can play in a firewall system:

- A perimeter firewall
- An Internet firewall
- An internal firewall
- A VPN concentrator
- An IDS

Cisco IOS Security Features

The Cisco IOS Firewall feature set enhances the security of the normal Cisco IOS, adding much greater depth and flexibility to a security solution. Some of these features include address translation, authentication, encryption, stateful filtering, failover, URL content filtering, and many others. Here are some of the key benefits that the Cisco IOS Firewall software provides:

- Flexibility? As I already mentioned, the Cisco IOS firewall router can play many roles: VPN, filtering firewall, IDS, and others. This enables you to choose the features that you need to customize your security solution.
- Scalability? The Cisco IOS Firewall software is available on a wide range of router platforms and interface selection, enabling you to choose the appropriate product for your security solution.
- Easier provisioning and investment protection? The Cisco IOS Firewall software uses the same Cisco IOS interface that you are familiar with, reducing the learning curve in enabling Cisco IOS Firewall security features. This reduces your cost and also protects your investment by enabling you to upgrade a router product without having to completely redo the new router's configuration.
- VPN support? The Cisco IOS Firewall works with VPNs to enable you to use inexpensive public networks to provide secure connectivity between remote offices and users.

These are some of the many features you will find in the Cisco IOS, including the Cisco IOS Firewall feature set:

- Address translation? Supports many flavors of address translation, including NAT, PAT, and load distribution. With address translation, you have stricter control over traffic that enters and leaves your network, and you can keep your IP addressing design from prying external eyes.
- Audit trail? Supports detailed audit trails. With the Cisco IOS, you can record detailed information about transactions and denied connections, including the source and destination IP addresses and ports, and the number of bytes transmitted for the connection. This can be done on a per-application, per-feature basis.
- Authentication proxy? Supports per-user authentication and authorization for LAN and dialup connections. This enables you to authenticate users before they can access your resources, and then authorize which resources they can access. This can be done through Telnet, HTTP, or HTTPS. Authorization is implemented by downloading per-user access-control information.
- Basic filtering technologies? Supports basic Cisco IOS filtering technologies. Basic IOS filtering features, such as standard, extended, timed, lock-and-key, and reflexive ACLs, are available to you without having to purchase the Cisco IOS Firewall feature set.
- DoS? Supports DoS detection and prevention through features such as TCP Intercept and Context-Based Access Control (CBAC), enabling you to take actions such as logging, resetting connections, or even dropping connections.
- Dynamic port mapping? Supports mapping of ports to different numbers. Many applications run on ports that are different than the standard ones. For example, some web servers use ports 8080 and 8090. Dynamic port mapping allows the Cisco IOS to treat these ports as a port 80 connection and to perform special types of inspection on these connections.
- Intrusion detection? Supports real-time monitoring and detection of more than 100 different kinds of network threats and attacks. The Cisco IOS IDS can be used to supplement your IDS solution, as well as to provide a basic level of protection for SOHO environments.
- Java applet filtering? Supports filtering of Java applets. The Cisco IOS can filter Java applets that are embedded in HTTP connections, enabling you to prevent malicious applets from wreaking havoc on your users' desktops.
- Real-time alerts? Supports logging of real-time alerts to external devices, such as a syslog server or management platform. Real-time alerts enable you to rank security issues so that you can deal with them in an appropriate order, dealing with high-risk security issues first.
- Router authentication? Supports authentication of routing updates, preventing spoofing and routing attacks. With this feature, you can be assured that your routing information is protected from internal and external attacks.
- Stateful firewall filtering? Supports stateful filtering of traffic with CBAC, a component of the Cisco IOS Firewall feature set. CBAC implements the stateful firewall filtering feature in the Cisco IOS and can be used as a main firewall component in your network. Currently, stateful filtering is supported for TCP, UDP, and ICMP protocols.
- URL filtering? Supports URL filtering. With the help of an external WebSense or N2H2 web content filtering server, the Cisco IOS can filter URL content. These two servers contain your URL content-filtering policies, and the Cisco IOS acts as the filtering agent, using the policies on the servers to implement its filtering.
- Voice connections? Supports H.323v2, Skinny, and SIP voice connections. Certain applications, such as multimedia and voice, create problems with traditional firewalls. The Cisco IOS Firewall feature set

supports a limited form of protocol fixup, which allows it to deal with dynamic connection and addressing allocations for H.323 and SIP.

This is just a small list of the security features that the Cisco IOS and Cisco IOS Firewall feature set support. Later chapters focus on all of these features, plus many more.

Cisco IOS Devices and Their Uses

One of the things you need to decide is which router platform or platforms you will use to implement your firewall system. With the Cisco IOS Firewall feature set, you have a wide range of choices of hardware platforms available for SOHO, branch office, extranet connections, and corporate office settings. Table 2-5 summarizes the Cisco recommendations for routers you should use for these environments.

Table 2-5. Router Recommendations

Routers	Recommendations
800, UBR 900, 1700	SOHO environments
2600, 3600, 3700	Branch offices and extranets
7100, 7200, 7400, 7500, Catalyst 6500 switches with the MSFC2	VPN and WAN aggregation points, as well as environments that need high-bandwidth throughput

NOTE

Table 2-5 contains basic recommendations. Note that every network and every situation is different. You need to carefully evaluate the needs of your network when choosing a Cisco product.

When to Use a Cisco IOS Firewall

The Cisco IOS Firewall typically is best suited when you need to integrate multiprotocol routing with security policies, providing secure firewall functions. However, there are many choices of firewall products, and many administrators and engineers have asked me which product they should choose. Answering this question is difficult:

- You must understand your company's issues and security policy.
- You must understand what products were meant to do.

I cannot help you that much with the first issue, but I can help you with the second issue, especially as it relates to choosing between a Cisco PIX or Cisco IOS firewall solution.

The PIX and the Cisco IOS router support many common security features and tools; however, I focus on just the differences so that you can develop a better understanding of what the two products cannot do or are not good at doing. Table 2-6 shows a list of these items.

Table 2-6. Cisco IOS Firewall and PIX comparison

Process or Feature	PIX	Cisco IOS Firewall

Process or Feature	PIX	Cisco IOS Firewall
Operating system	Has a dedicated operating system, which minimizes security risks.	Handles many processes, providing flexibility in implementing a multitude of features.
Scalability	Offers a wide variety of platforms and speed performance of more than 1 Gbps.	Offers a wide variety of platforms and interfaces? LAN, WAN, and MAN.
Authentication	Supports cut-through proxy with HTTP, HTTPS, FTP, and Telnet.	Supports authentication proxy with only Telnet, HTTP, and HTTPS.
Training and maintenance	Uses the FOS operating system, which is similar to but not the same as the Cisco IOS.	Runs the same Cisco IOS, requiring no additional training on its configuration.
One-box solution	Acts as a dedicated firewall appliance and is one of the best security products on the market, but requires other network devices for other services.	Provides a one-box solution, enabling you to use all of its services in a single chassis.
QoS	Does not have a rate-limiting function. It can limit only the number of connections.	Supports very sophisticated QoS features, enabling to limit the rate and level of service of a connection.
Application inspection	With the Protocol Fixup feature, can perform generic inspection of certain applications for a limited number of attacks.	Supports a form of protocol fixup similar to the PIX. However, the Cisco IOS also supports NBAR, which allows for a much better solution when dealing with filtering application content.

Typically, the PIX is used as a dedicated firewall appliance for wire-speed filtering of traffic and secure VPN connections. The Cisco IOS typically is used to enhance a router's security while it performs other services, such as QoS or multiprotocol routing. The Cisco IOS Firewall feature set typically is used to increase the protection of a perimeter router. However, I have seen PIXs used as both Internet and perimeter firewalls, and I also have seen Cisco IOS routers used for both solutions. Every network and every solution is different.