



Cisco IOS Firewall offers Stateful Inspection and Application Control

Businesses today rely on their networks to enable business functions and meet organizational goals. This often means making the network more accessible to partners, suppliers, or customers, and there are some associated risks. A more open network may expose proprietary business information and confidential data, and may lead to the inappropriate use of company resources and productivity loss. Worms, viruses, and malware can affect productivity and result in high costs associated with downtime and corporate reputation. These risks need to be mitigated with effective, reliable traffic control.

Cisco IOS® Firewall manages these risks by providing stateful traffic inspection to restrict unwanted traffic and maintain integrity of business-critical traffic. It includes application inspection features that control unauthorized application use on the network and protect software vulnerabilities in client and server applications. Cisco IOS Firewall is a secure, cost-effective, integrated solution, offering the scalability and stability that businesses demand.

One of the biggest advantages of an integrated security approach is that it allows users to build upon their existing IT infrastructure, which simplifies the process of deploying end-to-end security. The following Cisco IOS Firewall facts highlight several of the benefits.

- **A fully featured firewall**

Cisco IOS Firewall is a complete perimeter security solution—sometimes more comprehensive than standalone, appliance-based firewalls. Cisco IOS Firewall features include zone-based firewalling, HTTP application inspection, instant messaging and peer-to-peer application inspection, and flexible packet matching. It can help protect applications for unified communications, wireless, and wide area application services.

- **A certified firewall**

Cisco IOS Firewall is FIPS- and Common Criteria EAL4-certified. The Federal Information Processing Standard (FIPS) is a U.S. and Canadian government standard that specifies security requirements for cryptographic modules. Common Criteria is an international standard for evaluating IT product security and reliability. It is recognized by more than 15 countries around the world. Table 1 provides certification details.

Table 1. Cisco IOS Firewall Certifications for FIPS and Common Criteria

	FIPS	Common Criteria		
	140-2, Level 2	IPsec (EAL2)	IPsec (EAL4)	Firewall (EAL4)
Cisco® 800, 1800, 2800, and 3800 Series Integrated Services Routers	✓	✓	✓	✓
Cisco 1900,2900, 3900 Next Generation Integrated Services Routers	In Process	In Process	In Process	In Process
Cisco 7200 Series Routers with VAM2+ or VSA	✓	✓	✓	✓
Cisco 7301 Router with VAM2+	✓	✓	✓	✓
Cisco 7600 Series IPsec VPN SPA	✓	✓	✓	—
Cisco Catalyst® 6500 Series IPsec VPN SPA	✓	✓	✓	—

- **Performs at the branch**

Cisco integrated services routers are designed for fast, scalable delivery of business-critical applications. Cisco IOS Firewall is an integral component of this service, providing performance that is ideal for small to medium-sized branch office deployments, particularly in commercial and retail environments. This integrated solution is ideal for organizations with today's bandwidth intensive web 2.0 applications.

- **An extensive user base**

Cisco integrated services router deployments now exceed six million worldwide. Forty-one percent of these routers have shipped with Cisco IOS Firewall, making it one of the most widely deployed firewalls in the world. With this broad footprint and flexibility, this solution is the most cost-effective way to deploy firewall services, particularly across small, medium-sized, and branch offices.



• **Helps organizations meet PCI compliance requirements**

Cisco IOS Firewall helps companies address their PCI Data Security Standard (DSS) requirements. Requirement #1 states that organizations must install and maintain a firewall configuration to protect data. Cisco IOS Firewall also helps with Requirement #10, which deals with alerts and monitoring. Cisco integrated services router security features help address nine of the 12 requirements for PCI compliance, making this an ideal solution to meet compliance requirements (Table 2).

Table 2. Cisco Solutions for Meeting PCI DSS Requirements

PCI Requirement	Next Gen ISR	ISR	ASA	Security Agent	NAC	MARS	Wireless	Switch	Mgmt
Firewall	X	X	X	X	X	X		X	X
Password	X	X	X	X			X	X	X
Stored Data	X	X		X					
Encryption	X	X	X				X	X	X
Antivirus	X	X	X	X	X	X			
Systems and Apps	X	X	X	X	X	X	X	X	X
Restrict Access				X		X	X	X	X
Unique User ID						X	X	X	X
Physical Access									
Track and Monitor	X	X		X		X			X
Test Systems	X	X	X	X	X	X	X	X	X
Policy	X	X	X	X	X	X	X	X	X

For additional information on Cisco security solutions for PCI, please visit <http://www.cisco.com/go/pci>

• **An ideal solution for branch office deployments**

Cisco IOS Firewall is deployed extensively for customers with many small branch locations, remote offices, or employees that work from a home office. It provides deployment flexibility, broad security coverage, and the cost benefits that are included in an integrated security approach—in a simple-to-use, reliable, and cost-effective firewall solution.

Cisco IOS Firewall is ideal for organizations that fall under these categories:

- Enterprise organizations with small branch or remote offices and a distributed network architecture
- Commercial, retail, healthcare, and professional services industries
- Organizations where network operations and security operations are either tightly linked or on the same team
- Organizations looking to reduce network complexity and devices
- Organizations looking to reduce costs and lower total cost of ownership (TCO)
- Organizations looking to meet regulatory compliance requirements

Integrated Router Security Solutions

In today's challenging economic environment, Cisco IOS Firewall is an obvious choice for businesses that are looking to stay agile and competitive while delivering more robust and scalable services. The rich feature set, simplicity of deployment, and relative low cost make the Cisco IOS Firewall—and the corresponding security features on the Cisco integrated services routers—an ideal solution for an end-to-end security deployment.

For more information about Cisco IOS Firewall and other integrated router security features, please visit: <http://www.cisco.com/go/routersecurity>.