



Cisco Network Foundation Protection

Value-Added Security Services in Cisco IOS Software

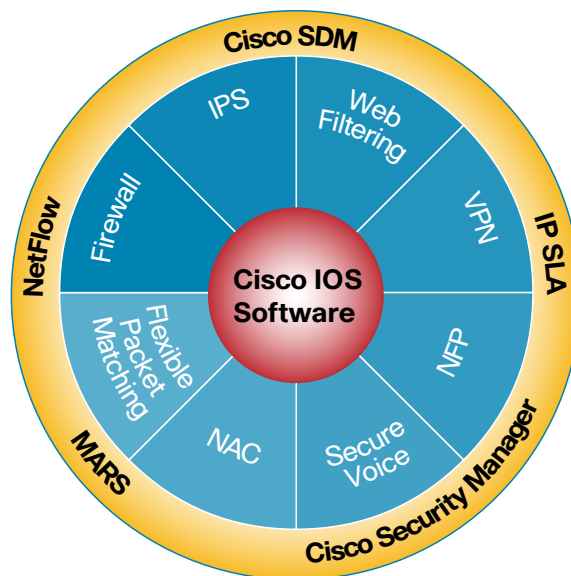
Integrated Router Security Solutions

Comprehensive network security features in Cisco routers help companies protect their infrastructures, devices, and important information, while reducing costs

In today's competitive business climate, connecting to the Internet is imperative; however, this exposes network elements and infrastructure to numerous threats. To address the increasing complexity of attacks in this heightened security environment, Cisco IOS® Software provides a rich set of security features and capabilities for network elements as well as the infrastructure, helping to ensure their availability under any circumstances.

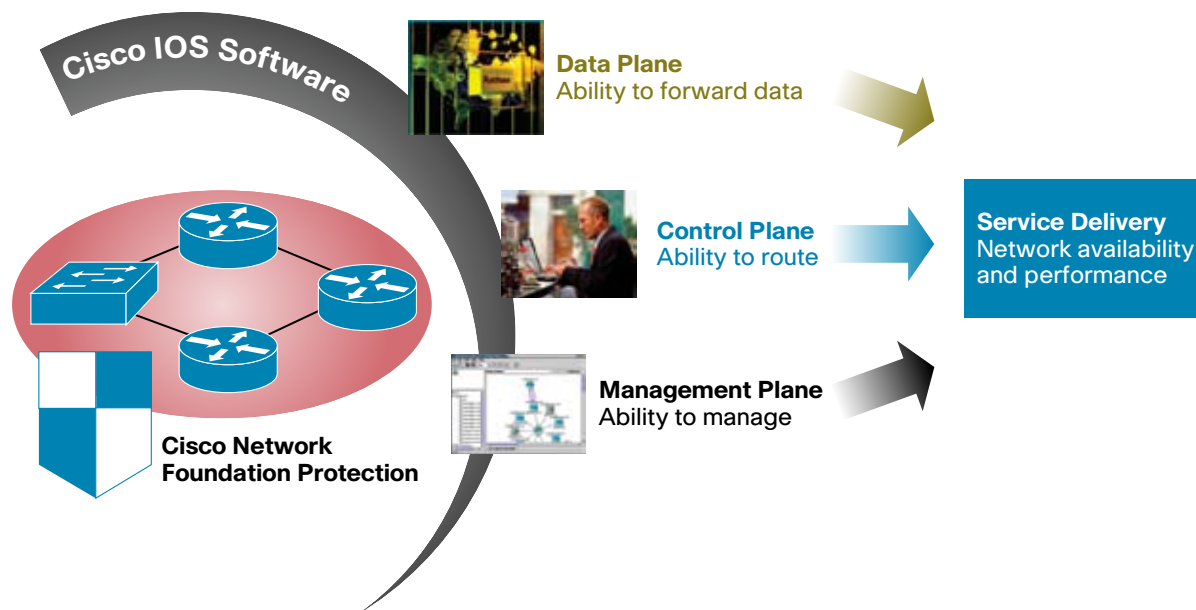
A secure infrastructure forms the foundation for service delivery. Continuous service delivery requires a methodical approach to protecting the router planes. The router is typically segmented into three planes, each with a clearly identified objective. The dataplane allows the ability to forward packets; the control plane allows the ability to route data correctly; and the management plane allows the ability to manage network elements.

Cisco® Network Foundation Protection (NFP) provides an umbrella strategy for infrastructure protection by encompassing the tools, technologies, and services that enable organizations to secure their foundation. This, in turn, enables controlling packet flows and protecting a network against security threats such as DDoS.



Secure networks must be built on a secure foundation. Cisco Network Foundation Protection uses the following methods to secure a router:

- **Control plane protection:** Protects the control plane traffic responsible for traffic forwarding by "locking down" services and routing protocols
- **Management plane protection:** Protects the management plane from unauthorized management access and polling and provides secure access for management and instrumentation
- **Data plane protection:** Protects the data plane from malicious traffic and protects data forwarded through the device





How do I secure each router plane?

A router can be logically divided into three functional planes:

- 1. Data plane:** The vast majority of packets handled by a router travel through the router by way of the data plane
- 2. Management plane:** Traffic from management protocols and other interactive access

protocols, such as Telnet, Secure Shell (SSH) Protocol, and SNMP, pass through the management plane

- 3. Control plane:** Routing control protocols, keepalives, ICMP with IP options, and packets destined to the local IP addresses of the router pass through the control plane

In securing each plane, network security administrators should take the “security toolkit” approach—selecting the security tool and technology based on assessing and identifying risks and threats to the network infrastructure. The following table shows the available technologies within NFP to secure each plane and its associated benefit.

Planes	Technologies	Benefits
Data Plane	NetFlow	Macro-level anomaly-based DDoS detection through counting the number of flows (instead of contents); provides rapid confirmation and isolation of attacks
	Access Control List	Protects edge routers from malicious traffic; explicitly permit the legitimate traffic that can be sent to the edge router’s destination address
	Unicast Reverse Path Forwarding (uRPF)	Mitigates problems caused by the introduction of malformed or spoofed IP source addresses into either the service provider or customer network
	Remote Triggered Black Hole (RTBH)	Drops packets based on source or destination IP address; filtering is at line rate on most capable platforms. Hundreds of lines of filters can be deployed to multiple routers even while the attack is in progress
	QoS Tools	Protects against flooding attacks by defining QoS policies to limit bandwidth or drop offending traffic (identify, classify and rate limit)
Management Plane	CPU/Memory Threshold Notification	Provides alerts for high CPU rates or low memory availability; provides early indication of an attack
	Management Plane Protection (MPP)	Delivers better control over device’s management by defining a management interface to restrict which physical/logical interfaces can accept network management traffic
	Role Based Access Control (RBACL)	Enhances the security of a device by defining the set of CLI commands accessible to a user; prohibits users from viewing CLI commands that are inaccessible to them
	Secure Access	Provides secure access to the device using SSH, SNMPv3, TACACS+, VTY ACLs, and Cisco IOS Login enhancements
	Image Verification	Verifies the Cisco IOS Software images that the router boots from by embedding the MD5 hash coding in the image and providing automatic MD5 hash checksum
	Configuration Logger	Tracks configuration changes entered on a per-session and per-user basis by providing a configuration log
Control Plane	Control Plane Protection (CPPr)	Reduces the success of a DDoS attack by providing early rate-limiting of traffic destined to the control plane, early dropping of packets destined to closed Cisco IOS TCP/UDP ports and limiting protocol queue usage
	Routing Protection	Validates routing peers, enhances routing stability, and provides overload protection by using MD5 peer authentication and redistribution protection
	Receive ACLs	Controls the type of traffic that can be forwarded to the route processor by explicitly permitting or denying traffic
	BGP TTL Security Check	Protects eBGP sessions from DoS and hijack attacks by enabling a lightweight security mechanism to validate TTL values