Control Plane Security Overview in Cisco IOS Software

In today's competitive business climate, connecting to the Internet is imperative; however, this also exposes network elements and infrastructure to myriad threats. Cisco IOS® Software provides a rich set of security features that address this complexity of attacks and help ensure the availability of network elements under any circumstances.

Cisco Network Foundation Protection (NFP) is an umbrella strategy encompassing Cisco IOS Security features that provides the tools, technologies, and services that enable organizations to secure their network foundations. NFP helps to establish a methodical approach to protecting router planes, forming the foundation for continuous service delivery.

The router is typically segmented into three planes of operation, each with a clearly identified objective. The data plane allows the ability to forward data packets; the control plane allows the ability to route data correctly; and the management plane allows the ability to manage network elements.

The vast majority of packets handled by a router travel through the router by way of the forwarding plane, or data plane. However, the system's route processor must handle certain packets, such as routing protocols, keepalives, packets destined to the local IP addresses of the router, and packets from management protocols and other interactive access protocols, such as Telnet and Secure Shell (SSH) Protocol. In addition, packets from protocols such as Internet Control Message Protocol (ICMP), with IP options, and others, might require handling by the route processor as well. This type of traffic is often referred to as control plane traffic.

Packet overloads on a router's control plane can slow down routing processes and, as a result, degrade network service levels and user productivity. Packets that traverse the control plane are those destined for that router's CPU, as opposed to network endpoints. All packets entering the control plane are redirected by the forwarding plane.

One cause for an overburdened router control plane is a router making inefficient use of shared CPU and memory resources. The same result can occur if reconnaissance or denial-of-service (DoS) attacks appear on the control plane, or if a routing protocol otherwise misbehaves. For example, if a high volume of rogue packets generated by a virus or worm is presented to the control plane, the router will spend an excessive amount of time processing and discarding unnecessary traffic. This can eventually overwhelm the route processor, which is responsible for handling router control plane functions, and possibly bring router processes to a halt.

Following is an overview of several Cisco IOS Software security features that protect the control plane of networking devices.

Receive Access Control Lists

Receive Access Controls Lists (rACLs) are designed to protect the route processor on high-end routers from unnecessary traffic that could potentially affect system performance.

The rACL feature uses standard or extended ACLs that control the traffic sent by the various line cards to the route processor on distributed architectures such as Cisco 12000 Series Routers. An rACL does not apply to transit traffic.

The rACL feature helps mitigate attacks directed at the route processor that are intended to overwhelm its capacity. On distributed architectures such as the Cisco 12000 Series Router, the route processor has a limited capacity to process traffic delivered from the line cards destined to the route processor itself. If a high volume of data requires “punting” traffic to the route processor, this can overwhelm the route processor, resulting in a DoS condition. An rACL typically consists of permit statements allowing the protocols and sources that are expected by the route processor, and may also include deny statements explicitly blocking unwanted traffic.

The rACL feature provides the following benefits:

- Protects high-priority routing protocol traffic from an attack, because filtering occurs after an input ACL is applied on the ingress interface.
- Protects against remote intrusions and access restriction to Cisco IOS services if unwanted services are inadvertently left enabled. Access to the router can be restricted to known, trusted sources and expected traffic profiles.
- Prevents DoS floods from degrading the performance of the route processor by filtering traffic on distributed line cards before packets are received by the router processor.

Originally introduced for Cisco 12000 Series Routers, rACLs are now available on other high-end routing platforms, including Cisco 7500 and 10000 Series Routers.

For additional information on the rACL feature, please visit:

- IP Receive ACL Feature Guide: http://www.cisco.com/en/US/partner/products/sw/iosswrel/ps1829/products_feature_guide09186a00805e9255.html
- GSR: Receive Access Control Lists White Paper: http://www.cisco.com/en/US/tech/tk648/tk361/technologies_white_paper09186a00801a0a5e.shtml
- Infrastructure Protection on Cisco IOS Software-Based Platforms: http://www.cisco.com/en/US/prod/collateral/iosswrel/ps8802/ps6970/ps1838/prod_white_paper0900aecd804ac831.pdf

Control Plane Policing

The control plane policing (CPP) feature significantly improves upon the rACL feature. Whereas rACLs allow the configuration of basic “permit” and “deny” filters for traffic destined to the router CPU, the CPP feature extends this by allowing users to configure a quality of service (QoS) filter that can also “rate-limit” this traffic. The CPP feature protects the control plane of Cisco IOS Software-based routers and switches against many attacks, including reconnaissance and denial-of-service (DoS) attacks. In this manner, the control plane can maintain packet forwarding and protocol state despite an attack or heavy load on the router or switch.

The CPP feature uses the modular QoS command-line interface (MQC) for configuring QoS policy for traffic destined to the control plane. The MQC allows classification of control plane traffic into classes, and lets you define and apply distinct QoS policies to separately rate limit the traffic in each class, such as:

- Permit all packets
- Drop all packets
- Drop packets that exceed the specified rate limit

The CPP feature provides the following benefits:

- Protection against DoS attacks targeted toward the network infrastructure by traffic flows and protocols that must be permitted, but where rate limiting offers substantial protection
- Eases deployment; CPP uses the existing MQC infrastructure, which allows customers to preserve the existing interface configurations and add global control-plane-specific commands to address security goals
- A consistent implementation strategy across all Cisco hardware
- Increased reliability, security, and availability of the network

For additional information on the CPP feature, please visit:

- Deploying Control Plane Policing White Paper: http://www.cisco.com/en/US/prod/collateral/iosswrel/ps6537/ps6586/ps6642/prod_white_paper0900aecd804fa16a.shtml
- Control Plane Policing Feature Guide: http://www.cisco.com/en/US/partner/products/sw/iosswrel/ps1838/products_feature_guide09186a008052446b.html
- Infrastructure Protection on Cisco IOS Software-Based Platforms: http://www.cisco.com/en/US/prod/collateral/iosswrel/ps8802/ps6970/ps1838/prod_white_paper0900aecd804ac831.pdf

Control Plane Protection

Cisco Control Plane Protection (CPPr) extends the CPP feature by enabling classification of the control plane traffic based on packet destination and information provided by the forwarding plane, allowing appropriate throttling for each category of packet. The feature creates three virtual control plane subinterfaces under the aggregate control plane interface for this purpose:

- **Control plane host subinterface:** Traffic directly destined for one of the router interfaces that must be processed by the router CPU, including tunnel termination, management, and routing protocol packets.
- **Control plane transit subinterface:** Data plane traffic traversing the router for forwarding that must be processed by the router CPU before it can be forwarded out of the router.
- **Control plane cef-exception subinterface:** Traffic that is redirected to the route processor because:
  - A configured router feature requires additional processing
  - Traffic related to router or network operations (such as keepalive packets) has been queued directly from a router network interface card driver for forwarding to the route processor
  - Packets have certain attributes that require further processing by the route processor, such as IP options or TTL = 0 or 1 (this is the least frequent exception)

Each subinterface is mutually exclusive; a packet emerging from the classifier will only enter one subinterface. Traffic traversing each control plane subinterface can be independently classified and controlled using unique CPP configurations.

In addition to providing the ability to limit traffic on each control plane subinterface, the CPPr feature supports Per-Protocol Queue Thresholding and port filtering capabilities.

The Per-Protocol Queue Thresholding feature provides a mechanism for limiting the number of packets for a given higher-level protocol allowed in the control plane IP input queue by the control plane host subinterface. This prevents the IP input queue from being overwhelmed by any single protocol.

The port filtering feature uses the host subinterface to provide early policing of packets destined for closed TCP/UDP ports, or ports to which the router is not configured to listen. This prevents unnecessary processing of packets that are ultimately to be discarded, and reduces process overhead that could be potentially exploited as an attack vector.

The port filter maintains a dynamic global database of all open TCP and UDP ports, including ports used by translators such as Network Address Translation (NAT) and Network Address Port Translation (NAPT). The registry provides network managers with a single place to look for open ports to assist them in security hardening of their network infrastructures.

Configuring the CPPr feature on your Cisco IOS Software-based router provides the following benefits:

- Extends protection against DoS attacks on infrastructure routers by providing a mechanism for finer policing of control plane traffic that allows you to rate-limit each type individually.
- Provides a mechanism for early dropping of packets that are directed to closed or nonlistened Cisco IOS TCP/UDP ports.

- Provides ability to limit protocol queue usage such that no single protocol flood can overwhelm the input interface.
- Provides QoS control for packets that are destined to the control plane of Cisco routers.
- Provides better platform reliability, security, and availability.
- Provides a dedicated control plane subinterface for aggregate, host, transit and cef-exception control plane traffic processing.
- Provides CPU protection so it can be used for important jobs, such as routing.

For additional information on the CPPr feature, please visit:

Control Plane Protection Feature Guide
http://www.cisco.com/en/US/products/ps6441/products_feature_guide09186a0080556710.html.

Scheduler Allocate

The Scheduler Allocate feature allows you to configure the amount of time the router CPU spends on interrupt-level (e.g. data plane) and process-level (e.g. control plane) operations. It allows you to limit the amount of time spent on switching within any one network interrupt context and guarantees the minimum amount of time to spend at the process level.

When used in conjunction with other control plane security features, the Scheduler Allocate feature helps to mitigate the effects of DoS attacks by ensuring that processes are run often enough so that system queues do not overflow.

For additional information on the scheduler allocate feature, please visit:

Performing Basic System Management Configuration Guide
http://www.cisco.com/en/US/partner/products/ps6441/products_configuration_guide_chapter09186a008030c799.html.

Summary

Even the most robust software implementations and hardware architectures are vulnerable to DoS attacks, which cause failures in a network infrastructure by flooding it with worthless traffic camouflaged as specific types of control packets directed at the control plane processor. Distributed DoS attacks multiply the amount of worthless IP traffic, sometimes by as much as many gigabytes per second, by involving hundreds of sources. These IP streams contain packets that are destined for processing by the control plane of Cisco route processors. Based on the high rate of rogue packets presented to the route processor, the control plane is forced to spend an inordinate amount of time processing and discarding the DoS traffic.

To counter these and similar threats directed toward the heart of the system—the processor—Cisco IOS Software provides several security services to protect the control plane of network devices. Cisco control plane security features help routers efficiently share CPU and memory resources.

For More Information

To learn more about these features and other features designed to protect your Cisco infrastructure, please visit http://www.cisco.com/go/nfp.

Americas 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: 408 527-0883

Asia Pacific Headquarters
Cisco Systems, Inc.
168 Robinson Road
#28-01 Capital Tower
Singapore 068912
www.cisco.com
Tel: +65 6317 7777
Fax: +65 6317 7799

Europe Headquarters
Cisco Systems International BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands
www-europe.cisco.com
Tel: +31 0 800 020 0791
Fax: +31 0 20 357 1100

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.

Printed in USA C11-398082-00 3/07

