CISCO NETWORK FOUNDATION PROTECTION: PROTECTING THE CISCO CATALYST SERIES PLATFORM

SECURITY TECHNOLOGY GROUP

JANUARY 2005
Agenda

• Introduction
• Configuring Control Plane Protection
• Deployment Guide
• Summary and References
INTRODUCTION
Risk Landscape

- Denial of Service (DoS) attacks target the network infrastructure by generating IP traffic streams to the control plane at very high rates
- The control plane is forced to spend an inordinate amount of time, processing this malicious traffic
- Results in excessive CPU utilization and CPU resource hijacking by the hackers
- Examples of such attacks include:
  - TCP SYN floods
  - IP Fragments
  - Internet Control Message Protocol (ICMP) Echo Requests
  - Fraggle Attacks
Risk Landscape (Cont.)

- Attacks can devastate a network by causing:
  - High route processor CPU utilization (near 100%)
  - Loss of protocol keepalives and routing protocol updates
  - Route flaps and major network transitions
  - Slow or unresponsive interactive sessions via the CLI
  - Route Processor resource exhaustion
    - Resources such as memory and buffers are unavailable for legitimate IP data packets
    - Indiscriminate packet drops for all incoming packets
Keys to Prevent Attacks at the Routers

• To protect the router mechanisms have to:

  Identify DoS attack packets from valid packets (Classification)

  Once identified, mark, drop, or rate-limit (Service Policies)

  Separate data plane packets from control plane packets

  Provide DoS mechanisms independent from existing interface capabilities, but do not impact current performance

  Provide global CLI to minimize configuration changes to deployed networks
Securing the Router – Plane by Plane

Think “Divide and Conquer”: Methodical Approach to Protect Three Planes

1. Secure Control Plane
   - Ability to Route

2. Secure Management Plane
   - Ability to Manage

3. Secure Data Plane
   - Ability to Forward Data
Cisco NFP – Network Foundation Protection Alcazar Program

Secure Networks Must Be Built on a Secure Foundation

- **Control Plane Protection**: Lock down services and routing protocols
- **Management Protection**: Secure Access for Management and Instrumentation
- **Data Plane Protection**: Protect Data forwarding through the device

Secure Networks Must Be Built on a Secure Foundation.
Cisco NFP – Three Planes Definitions

Cisco Network Foundation Protection (NFP) is a Cisco IOS® Technology suite that protects network devices, routing and forwarding of control information, and management of traffic bounded to the network devices.

**Control Plane Protection** – protects the control plane traffic responsible for traffic forwarding
- Autosecure with rollback functionality
- Control Plane Protection
- CPU / Memory Threshold

**Management Plane Protection** – protects the management plane from unauthorized management access and polling
- Secure Shell (SSH) only access
- VTY Access Control List (ACL)
- Cisco IOS Software login enhancement
- Command Line Interface (CLI) views

**Data Plane Protection** – protects the data plane from malicious traffic
- Unicast RPF for anti-spoofing
- Control Plane Protection for Data traffic
- Committed Access Rate (CAR)
Introduction – Control Plane Protection Policing

CONTROL PLANE

<table>
<thead>
<tr>
<th>Management</th>
<th>ICMP</th>
<th>IPv6</th>
<th>Routing Updates</th>
<th>Management SSH, SSL</th>
<th>.....</th>
</tr>
</thead>
</table>

INPUT to the Control Plane

CONTROL PLANE POLICING (Alleviating DoS Attack)

OUTPUT from the Control Plane

SILENT MODE (Reconnaissance Prevention)

Processor Switched Packets

CEF/FIB LOOKUP

INCOMING PACKETS

PACKET BUFFER

OUTPUT PACKET BUFFER

Locally Switched Packets

Switched Packets

INPUT from the Control Plane

OUTPUT to the Control Plane

Management

SNMP, Telnet

ICMP

IPv6

Updates

SSH, SSL
Control Plane Protection – Policing for Cisco Catalyst Series Platform

Traffic to CPU

PFC3

hardware “control-plane”

Traffic to CPU

FABRIC

Traffic to CPU

Software “control-plane”

Traffic to CPU

CPU

Inband channel to RP CPU
Control Plane Protection – Policing for Cisco Catalyst Series Platform

Traffic to CPU

hardware “control-plane”

PFC3

FABRIC

DFC3

DFC3

Traffic to CPU

Software “control-plane”

Inband channel to RP CPU

CPU

Traffic to CPU

Traffic to CPU
# Introduction – What CPU Rate Limiters Are Available?

## Unicast Rate Limiters

<table>
<thead>
<tr>
<th>Category</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CEF Receive</td>
<td>Traffic destined to the Router</td>
</tr>
<tr>
<td>CEF Glean</td>
<td>ARP packets</td>
</tr>
<tr>
<td>CEF No Route</td>
<td>Packets with not route in the FIB</td>
</tr>
<tr>
<td>IP Errors</td>
<td>Packets with IP checksum or length errors</td>
</tr>
<tr>
<td>ICMP Redirect</td>
<td>Packets that require ICMP redirects</td>
</tr>
<tr>
<td>ICMP No Route</td>
<td>ICMP unreachables for unrouteable packets</td>
</tr>
<tr>
<td>ICMP ACL Drop</td>
<td>ICMP unreachables for admin deny packets</td>
</tr>
<tr>
<td>RPF Failure</td>
<td>Packets that fail uRPF check</td>
</tr>
<tr>
<td>L3 Security</td>
<td>CBAC, Auth-Proxy, and IPSEC traffic</td>
</tr>
<tr>
<td>ACL Input</td>
<td>NAT, TCP Int, Reflexive ACLs, Log on ACLs</td>
</tr>
<tr>
<td>ACL Output</td>
<td>NAT, TCP Int, Reflexive ACLs, Log on ACLs</td>
</tr>
<tr>
<td>VAACL Logging</td>
<td>CLI notification of VAACL denied packets</td>
</tr>
<tr>
<td>IP Options</td>
<td>Unicast traffic with IP Options set</td>
</tr>
<tr>
<td>Capture</td>
<td>Used with Optimized ACL Logging</td>
</tr>
</tbody>
</table>

## Layer 2 Rate Limiters

<table>
<thead>
<tr>
<th>Category</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>L2PT</td>
<td>L2PT encapsulation/decapsulation</td>
</tr>
<tr>
<td>PDU</td>
<td>Layer 2 PDUs</td>
</tr>
</tbody>
</table>

## Multicast Rate Limiters

<table>
<thead>
<tr>
<th>Category</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Multicast FIB-Miss</td>
<td>Packets with no mroute in the FIB</td>
</tr>
<tr>
<td>IGMP</td>
<td>IGMP packets</td>
</tr>
<tr>
<td>Partial Shortcut</td>
<td>Partial shortcut entries</td>
</tr>
<tr>
<td>Directly Connected</td>
<td>Local multicast on connected interface</td>
</tr>
<tr>
<td>IP Options</td>
<td>Multicast traffic with IP Options set</td>
</tr>
<tr>
<td>V6 Directly Connect</td>
<td>Packets with no mroute in the FIB</td>
</tr>
<tr>
<td>V6*, G M Bridge</td>
<td>IGMP packets</td>
</tr>
<tr>
<td>V6*, G Bridge</td>
<td>Partial shortcut entries</td>
</tr>
<tr>
<td>V6 S, G Bridge</td>
<td>Partial shortcut entries</td>
</tr>
<tr>
<td>V6 Route Control</td>
<td>Partial shortcut entries</td>
</tr>
<tr>
<td>V6 Default Route</td>
<td>Multicast traffic with IP Options set</td>
</tr>
<tr>
<td>V6 Second Drop</td>
<td>Multicast traffic with IP Options set</td>
</tr>
</tbody>
</table>

## General Rate Limiters

<table>
<thead>
<tr>
<th>Category</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>MTU Failure</td>
<td>Packets requiring fragmentation</td>
</tr>
<tr>
<td>TTL Failure</td>
<td>Packets with TTL&lt;=1</td>
</tr>
</tbody>
</table>

Shared across the 10 hardware Revocation Lists.
Interaction Between Control Plane Protection, Policing, and CPU Rate Limiter

Special-case Rate Limiters **OVERRIDE**
Hardware Control Plane Policing!

Traffic to CPU → Special cases → hardware rate-limiters → Matches policy → hardware “control-plane” → CPU

PFC3/DFC3 → Special case traffic → software “control-plane”
Test Setup – Mitigation of Multiple Attacks

• CPP configuration
  policy-map CoPP
  class cpp-bgp
    police 32000 1500 1500 conform-action transmit exceed-action transmit
  class cpp-igp
    police 32000 1500 1500 conform-action transmit exceed-action transmit
  class cpp-management
    police 32000 1500 1500 conform-action transmit exceed-action transmit
  class cpp-monitoring
    police 600000 18750 18750 conform-action transmit exceed-action drop
  class cpp-critical
    police 32000 1500 1500 conform-action transmit exceed-action transmit
  class cpp-un-desirable
    police 320000 10000 10000 conform-action drop exceed-action drop
  class cpp-default
    police 620000 19375 19375 conform-action transmit exceed-action drop

• CPU Rate Limiter configuration
  mls rate-limit multicast ipv4 partial 1000 100
  mls rate-limit unicast ip options 1000 10
  mls rate-limit all ttl-failure 1000 10
CPU Rate Limiters Recommendations

• Use all eight Layer 3 rate limiters!
  Easy task
• Consider most likely attack vectors for the network environment
  Enable the rate limiters most likely to be used
• Do not waste a rate-limiter on VACL logging, if it is not happening
  No mls rate-limit unicast acl vacl
• Disable redirects and save a rate limiter
  Hardware forwarding platform reduces need for redirect efficiency
• Maximum Transmission Unit (MTU) limiter is not required, if all interfaces have same MTU
CONFIGURING CONTROL PLANE PROTECTION
Configuring Control Plane Protection – Policing Four Step Process

1. Define a packet classification criteria
   router(config)# class-map <traffic_class_name>
   router(config-cmap)# match <access-group>

2. Define a service policy
   router(config-pmap)# policy-map<service_policy_name>
   router(config-pmap)# class <traffic_class_name>
   router(config-pmap)# police <rate> conform-action transmit
                  exceed-action drop

3. Enter control-plane configuration mode
   router(config)# control-plane
   router(config-cp)#

4. Apply QoS Policy
   router(config-cp)# service-policy input <service_policy_name>
Control Plane Policing Configuration

- Must enable QoS globally! (mls qos)
  Otherwise, CoPP is performed in software only
- Define ACLs to match traffic
  Permit means traffic will belong to class; deny means will fall through
- Define class-maps (class-map <name>)
  Use “match” statements to identify traffic associated with the class
  match {access-group | ip {precedence | dscp}}
- Define policy-map (policy-map <name>) and associate classes and actions to it
  Policing is the only supported action
  Usual Cisco Catalyst 6500 Series Switch policing syntax
- Tie the policy-map to the control-plane interface

```
mls qos

ip access-list extended CPP-MANAGEMENT
remark Remote management
permit tcp any any eq SSH
permit tcp any eq 23 any
permit tcp any any eq 23

class-map match-all CPP-MANAGEMENT
description Important traffic, eq management
```
Configuring CPU Rate Limiter

Apply a CPU Rate Limiter at a specific rate

Router(config)# mls rate-limit <all | unicast | multicast | layer 2> <special_case_rate_limiter> <packets_per_second>

Example: Rate Limit traffic with TTL=1 to 1000pps

Router(config)# mls rate-limit all ttl-failure 1000
Deployment Guide – Step I
Classify and Permit All Traffic

- Identify traffic of interest and classify it into multiple traffic classes
  - BGP
  - IGP
  - Management
  - Reporting
  - Monitoring
  - Critical Applications
  - Undesirable and Default
- Use ACLs to identify traffic in each class
  - Match criteria supported includes:
    - ip standard ACL 1-99
    - ip extended ACL 100-199
- Use protocol and port number for Modular Quality of Service (QoS) Command Line Interface (MQC) match
- Last ACL entry permits ip any any
  - Otherwise, implicit deny statement
- Apply ACLs to class-maps and permit traffic in each class
Deployment Guide – Step II
Review ACL Counters and Initial Policy

• show policy-map control-plane and show mls qos ip command
  Displays dynamic information for monitoring control plane policy
  Statistics include rate information and number of packets/bytes confirmed or exceeding each traffic classes

• show access-lists command
  Provides packet count statistics per ACL entry (ACE), when traffic matches a particular entry
  This data is used to develop a policy that ensures that identified traffic is matching as expected
  Absence of any hits on an entry indicate lack of traffic matching the ACE criteria –the rule might be re-written
Deployment Guide – Step III
Define Control Plane Policy

• Explicitly allow needed and known critical protocols such as BGP and EIGRP
  Conform and exceed action $\rightarrow$ transmit

• Define other required, but not critical traffic, such as ICMP, SNMP, SSH, Telnet, and default
  Conform action $\rightarrow$ transmit, exceed action $\rightarrow$ drop

• Drop all other undesirable traffic

• Depending on class defined, apply appropriate policy
  Routing Protocol traffic (BGP, IGP) - no rate limit
  Management traffic (SNMP, SSH, NTP, and etc) – conservative rate limit
  Reporting traffic (SAA combined with DSCP) – conservative rate limit
  Monitoring traffic (ICMP, traceroute) – conservative rate limit
  Critical traffic (HSRP, SIP/VoIP, DLSw) – conservative rate limit
  Default traffic – low rate limit
  Undesirable traffic (DoS Attacks) – drop
Deployment Guide – Step IV
Define CPU Rate Limiters

- Use all eight Layer 3 rate limiters!
  Easy task
- Consider most likely attack vectors for the network environment
  Enable the rate limiters, which are most likely to be used
- Do not waste a rate-limiter on VACL logging, if it is not happening
  No mls rate-limit unicast acl vacl
- Disable redirects and save a rate limiter
  Hardware forwarding platform reduces need for redirect efficiency
- MTU limiter is not required, if all interfaces have same MTU
- Configure PDU Layer 2 rate limiter with care
  Calculate expected/possible number of valid PDUs (ballpark), double or triple them and include BPDUs, DTP, VTP, PAgP/LACP, UDLD, and etc.
  Remember that Revocation Lists do not discriminate between “good” frames and “bad” frames
Deployment Guide – Step IV
Which CPU Rate Limiters are Needed?

1. Cisco Express Forwarding glean
   - Limits traffic requiring ARP for a next hop
   - Does NOT limit ARP traffic!

2. Multicast default adjacency
   - Limits traffic punted to establish multicast control plane state (e.g.: new S,G traffic)

3. ACL bridged input
   - ACL bridged output
     - Limit packets with ACL bridge result (e.g, “log” ACEs)

4. TTL failure
   - Limits unicast traffic with expiring TTL

5. Unicast IP options
   - Limits unicast packets with IP options

6. Multicast IP options
   - Limits multicast packets with IP options
Deployment Guide – Step IV
Which CPU Rate Limiters are Needed?

7. ICMP unreachable no-route
   ICMP unreachable ACL-drop
   Limit unroutable or ACL-denied traffic

8. IP errors
   Limits error packets (e.g.: bad L3 checksum, L2/L3 length mismatch)

9. IP RPF traffic
   Limits uRPF failed traffic
   Freebie along with above limiters

10. ICMP redirect
    Limits traffic punted to trigger a redirect

11. Multicast IGMP (Layer 2)
    Limits IGMP packets to the SP CPU

12. Layer 2 PDU (Layer 2)
    Limits Layer 2 protocol data units (BPDUs, VTP, DTP, PAgP, etc)
Deployment Guide – Step V
Fine Tune the Policy

- Ensure that unexpected results are investigated
- Increasingly restrict source and destination addresses
  Only certain hosts send SNMP polls, ICMP requests, or SSH/telnet into a router
- BGP peers are using loopback
- Use class-default to identify unclassified packets
- Remove permit ip any any any when confident with results
- Additional information:
Control Plane Policy Template

- class-map match-all cpp-bgp
  - BGP
- class-map match-all cpp-igp
  - EIGRP, OSPF, etc...
- class-map match-all cpp-management
  - SNMP, NTP, SSH, TACACS, TFTP, etc...
- class-map match-all cpp-reporting
  - Echo, echo-reply with DSCP marking per class
- class-map match-all cpp-monitoring
  - ICMP, traceroute, etc...
- class-map match-all cpp-critical-applications
  - HSRP, DLSw, SIP/VoIP, etc...
- class-map match-all cpp-layer-2-protocols
  - ARP
- class-map match-all cpp-default
  - Non-specifically marked traffic
- class-map match-any cpp-deny
  - Classified attack traffic
SUMMARY AND REFERENCES
Summary – Control Plane Protection Policing

- **Unicast Traffic**
  Hardware mechanism for defining and implementing sophisticated router protection schemes

- **Multicast Traffic**
  Hardware independent mechanism for defining and implementing sophisticated router protection scheme after first pass through CPU rate limiters

- Protection against DoS attacks targeted towards the network infrastructure
- Easy deployment by leveraging existing MQC infrastructure
- Consistent implementation strategy across all Cisco hardware
- Increased reliability, security, and availability of the network
References

- Cisco IOS Security Infrastructure
  www.cisco.com/go/autosecure/

- Cisco IOS Software Release 12.2(18)SXD
  www.cisco.com/go/release122s/

- Deploying Control Plane Protection - Policing

- Control Plane Protection – Policing Feature Guide

- QoS Command Reference Guide
## Hardware Support

<table>
<thead>
<tr>
<th>Hardware</th>
<th>Availability</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Cisco 7600 Series Router</td>
<td>• Cisco IOS Software Release 12.2(18)SXD1</td>
</tr>
<tr>
<td>• Cisco Catalyst® 6500 Series</td>
<td></td>
</tr>
<tr>
<td>Switch</td>
<td></td>
</tr>
<tr>
<td>• Cisco 7200 Series Router</td>
<td>• Cisco IOS Software Release 12.2(18)S</td>
</tr>
<tr>
<td>• Cisco 7500 Series Router</td>
<td></td>
</tr>
<tr>
<td>• Cisco 12000 Series Internet</td>
<td>• Cisco IOS Software Release 12.0(29)S</td>
</tr>
<tr>
<td>Router</td>
<td></td>
</tr>
<tr>
<td>• Cisco 1751 Series Router</td>
<td>• Cisco IOS Software Release 12.3(4)T</td>
</tr>
<tr>
<td>• Cisco 2600-XM Series</td>
<td></td>
</tr>
<tr>
<td>• Cisco 3700 Series Router</td>
<td></td>
</tr>
<tr>
<td>• Cisco 7200 Series Router</td>
<td></td>
</tr>
</tbody>
</table>