Cisco Network Foundation Protection Overview

June 2005
Security is about the ability to control the risk incurred from an interconnected global network. Cisco NFP provides the tools, technologies, and services that enable users to secure their foundation.
What has Changed in the World of Security?

- Security represents the future of internetworking - a secure infrastructure forms the foundation for service delivery.
- Internet has changed from an environment of implicit trust to one of pervasive distrust:
  - No packet can be trusted.
  - All packets must earn trust through a network device’s ability to inspect and enforce policy.
  - Not enough to forward packets; packets must be classified properly and forwarded after applying the policy.
- New unprecedented control of the network is required:
  - Technology opportunity – enable customers to take control of their business.
- Driven by business deliverables:
  - Network availability, Quality of Service (QoS), and edge policy.
Securing the Router: Plane-by-Plane

Continuous service delivery requires methodical approach to protecting router planes

Data Plane
Ability to forward data

Control Plane
Ability to route

Management Plane
Ability to manage

Service Delivery
Network availability and performance
Security Toolkit: A Proactive Approach

Security Toolkit:
One or more techniques used to respond to a security related threat

Data Plane Protection
Control Plane Protection
Management Plane Protection

Select the right tool for the right job

Step 1: Identify:
- Threat type
- Type of security plane protection
- Role in the network

Step 2: Use the service segment perspective to determine toolkit placement
Cisco Network Foundation Protection: Enabling DDoS Protection (Clean Pipes)

Protects infrastructure, enables continuous service delivery

Data Plane
- Detects traffic anomalies & respond to attacks in real-time
- Technologies: NetFlow, IP source tracker, ACLs, uRPF, RTBH, QoS tools

Control Plane
- Defense-in-depth protection for routing control plane
- Technologies: Receive ACLs, control plane policing, routing protection

Management Plane
- Secure and continuous management of Cisco IOS network infrastructure
- Technologies: CPU & memory thresholding, dual export syslog
Cisco NFP: Key Messages

• Security – a proactive measure
  Reactive components help with tactical scenarios

• Toolkit approach for security
  “The right tool for the right job”

• Protect network elements on the Data, Control, and Management Planes

• Ensure service delivery
  Services such as VoIP and Clean Pipes require network availability and consistent performance
# Cisco NFP: Features and Benefits

<table>
<thead>
<tr>
<th>Plane</th>
<th>Cisco IOS Services</th>
<th>Benefits</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Data Plane</strong></td>
<td>NetFlow</td>
<td>• Macro-level anomaly-based DDoS detection through counting the number of flows (instead of contents); provides rapid confirmation and isolation of attack</td>
</tr>
<tr>
<td></td>
<td>IP source tracker</td>
<td>• Quickly and efficiently pinpoints the source interface an attack is coming from</td>
</tr>
<tr>
<td></td>
<td>Access control lists (ACLs)</td>
<td>• Protect edge routers from malicious traffic; explicitly permit the legitimate traffic that can be sent to the edge router's destination address</td>
</tr>
<tr>
<td></td>
<td>Unicast reverse path forwarding (uRPF)</td>
<td>• Mitigates problems caused by the introduction of malformed or spoofed IP source addresses into either the service provider or customer network</td>
</tr>
<tr>
<td></td>
<td>Remotely triggered black holing (RTBH)</td>
<td>• Drops packets based on source 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</td>
</tr>
<tr>
<td></td>
<td>QoS tools</td>
<td>• Protects against flooding attacks by defining QoS policies to limit bandwidth or drop offending traffic (identify, classify &amp; rate limit)</td>
</tr>
<tr>
<td><strong>Control Plane</strong></td>
<td>Receive ACLs</td>
<td>• Control the type of traffic that can be forwarded to the processor</td>
</tr>
<tr>
<td></td>
<td>Control plane policing</td>
<td>• Provides QoS control for packets destined to the control plane of the routers; ensures adequate bandwidth for high-priority traffic such as routing protocols</td>
</tr>
<tr>
<td></td>
<td>Routing protection</td>
<td>• MD5 neighbor authentication protects routing domain from spoofing attacks</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Redistribution protection safe-guards network from excessive conditions</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Overload protection (e.g. prefix limits) enhances routing stability</td>
</tr>
<tr>
<td><strong>Management Plane</strong></td>
<td>CPU &amp; memory thresholding</td>
<td>• Protects CPU &amp; memory resources of IOS device against DoS attacks</td>
</tr>
<tr>
<td></td>
<td>Dual export syslog</td>
<td>• Syslog exported to dual collectors for increased availability</td>
</tr>
</tbody>
</table>
Resources

• Cisco NFP
  www.cisco.com/go/nfp

• Cisco IOS Software Release 12.3T: New Security Features and Hardware, Product Bulletin No. 2358

• Control Plane Protection Documentation