CISCO NETWORK FOUNDATION PROTECTION
SECURITY TECHNOLOGY GROUP
JANUARY 2005
Customers Must Take Control of Their Networks

• In Today’s Marketplace:
  Business = Network

• Internet has experienced paradigm shift from implicit trust to an Internet of pervasive distrust
  No packet can be trusted
  All packets must earn trust through a network device’s ability to inspect and enforce policy
  It is not enough to forward packets – they need to 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 99.999
Secure Network = Available Network

Cisco IOS Software

Ability to Route

Ability to Manage

Ability to Forward Data

Network Availability

Productivity vs. Cost
Securing the Router – Plane by Plane

Think “Divide and Conquer”: Methodical Approach to Protect Three Planes
Secure Networks Must Be Built on a Secure Foundation

- Control Plane Protection
- Management Protection
- Data Plane Protection

Lock down services and routing protocols

Secure Access for Management and Instrumentation

Protect Data forwarding through the device
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)
Cisco NFP in Signaling Point Core Network Security – Signaling Point Core Perspective

Deploy Security Features—
- Data Plane Configurations
  - Unicast RPF
  - rACLs, CoPP, CAR, etc.
  - Other (e.g. ICMP rate limits)
- Control Plane Configurations
  - rACLs, CoPP
  - Routing Plane protection (BGP peer authentication, route filtering via prefix filters, route maps, SPD)
  - Management Plane protection (SNMP v3, TACACS+, VTY ACLs, NTP authentication)
- Moving from “art” to “engineering” today
- Few products (startups) – highly niche oriented space
- SP Security Best Practices and Cisco SAFE Signaling Point Architecture

Protection for:
- Data Plane (router CPU, bandwidth)
- Control Plane (routing integrity, management, Back Office)
- No direct profit generation, but a lack of it will sure lead to losing money (redundancy, resilience, fat pipes, minimize impacts)

Maturity —
- Moving from “art” to “engineering” today
- Few products (startups) – highly niche oriented space
- SP Security Best Practices and Cisco SAFE Signaling Point Architecture
# Cisco Self-Defending Network Technologies – NFP

<table>
<thead>
<tr>
<th>Feature</th>
<th>Benefits</th>
</tr>
</thead>
<tbody>
<tr>
<td>Control Plane Protection</td>
<td>Reduces the success of a DDoS attack by policing the incoming rate of traffic to the control plane</td>
</tr>
<tr>
<td>Autosecure</td>
<td>Quickly locks down devices based on industry recognized best practices (NSA guidelines)</td>
</tr>
<tr>
<td>Routing protocol protection</td>
<td>Validates routing peers and source/destination of routing updates, filtering of prefixes</td>
</tr>
<tr>
<td>CPU/Memory Thresholding</td>
<td>Router remains operational under high loads caused by attacks through reserving CPU/memory</td>
</tr>
<tr>
<td>Management Plane Protection</td>
<td></td>
</tr>
<tr>
<td>Secure Access</td>
<td>SNMPv3, TACACS+, VTY ACLs, SSH</td>
</tr>
<tr>
<td>Image Verification</td>
<td>Verifies the Cisco IOS Software images that the router boots from</td>
</tr>
<tr>
<td>Role Based CLI Views</td>
<td>Allows for granular control of CLI with AAA user credential checking</td>
</tr>
<tr>
<td>Network Telemetry</td>
<td>Cisco IOS NetFlow for traffic and DDoS analysis</td>
</tr>
</tbody>
</table>
## Cisco Self-Defending Network Technologies – NFP (Cont.)

<table>
<thead>
<tr>
<th>Feature</th>
<th>Benefits</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data Plane Protection</td>
<td></td>
</tr>
<tr>
<td>Unicast RPF</td>
<td>Antispoofing for source IP address</td>
</tr>
<tr>
<td>Access Control Lists</td>
<td>ACLs - filter traffic through a device</td>
</tr>
<tr>
<td>Infrastructure ACL and CAR</td>
<td>Remove possibility for illegitimate users to send any traffic to link addresses</td>
</tr>
</tbody>
</table>
Cisco Network Foundation Worm Protection in Action

Protect and Police your business with a secure and available network

Protect the End Systems
- Cisco Security Agent

Police the Links
- Network Telemetry
- Traffic Rate Limiting
- Prefix filtering

Protect the Network Devices
- Auto Secure
- Control Plane Protection
- CPU/Memory Threshold
- Role based CLI Access
- Secure Management Access

Prevent the Attack
- Anti Spoofing
- Black Holing DDoS
- Routing Protocol Authentication

System Under Attack

Network Links Overloaded
- Loss of Availability
- High Packet Loss
- Latency
- Applications Impacted

Network Devices Overloaded
- Compromised: Ability to Route
- Ability to be managed
- Ability to Forward Data

End Systems Overloaded
- High CPU
- Applications Impacted
- System Crashes
Combining Everything

BGP security RTBH, uRPF RTRL / QPPB

Traffic diversion

Packet inspection And cleaning

Cisco Guard

uRPF ingress and egress filtering

Targeted Enterprise A

Targeted Enterprise B

RACL, iACL, CoPP Stack protection, Sink holes

Anomaly Detection
## Glossary

<table>
<thead>
<tr>
<th>Acronym</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CoPP</td>
<td>Control Plane Policing</td>
</tr>
<tr>
<td>RTBH</td>
<td>Remote Triggered Black Hole</td>
</tr>
<tr>
<td>RTRL</td>
<td>Remote Triggered Rate Limiting</td>
</tr>
<tr>
<td>rACL</td>
<td>Receive ACL</td>
</tr>
<tr>
<td>iACL</td>
<td>Infrastructure ACL</td>
</tr>
<tr>
<td>uRPF</td>
<td>Unicast Reverse Path Forwarding</td>
</tr>
</tbody>
</table>