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

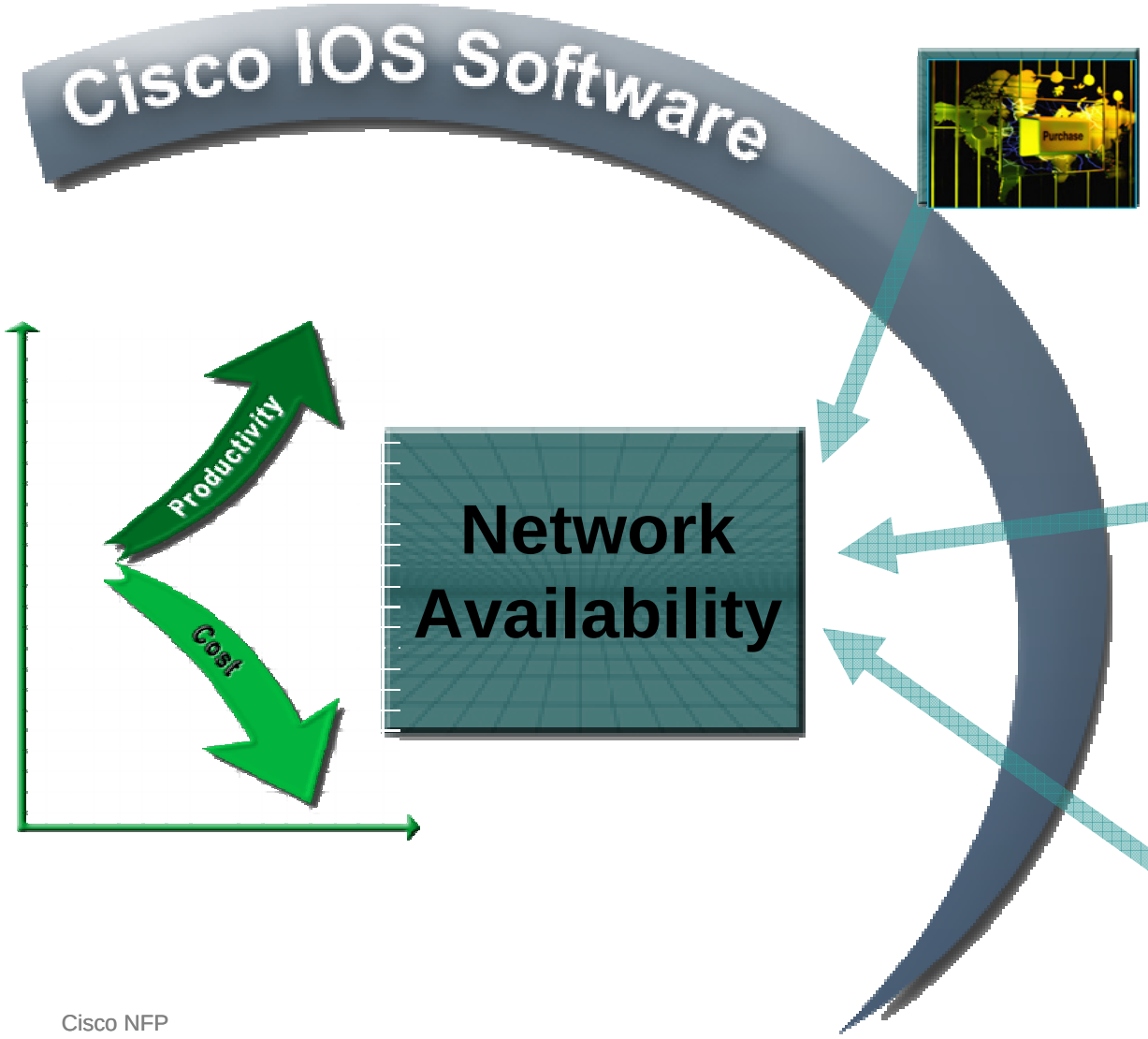
- **New unprecedented control of the network is required**

  Technology Opportunity – enable customers to take control of their business

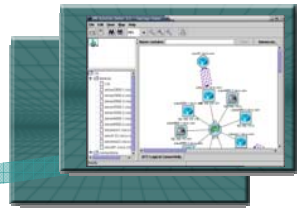
- **Driven by Business Deliverables:**

  Network Availability 99.999

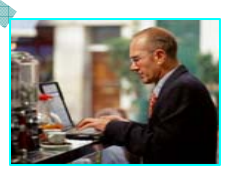
Secure Network = Available Network



Ability to Route

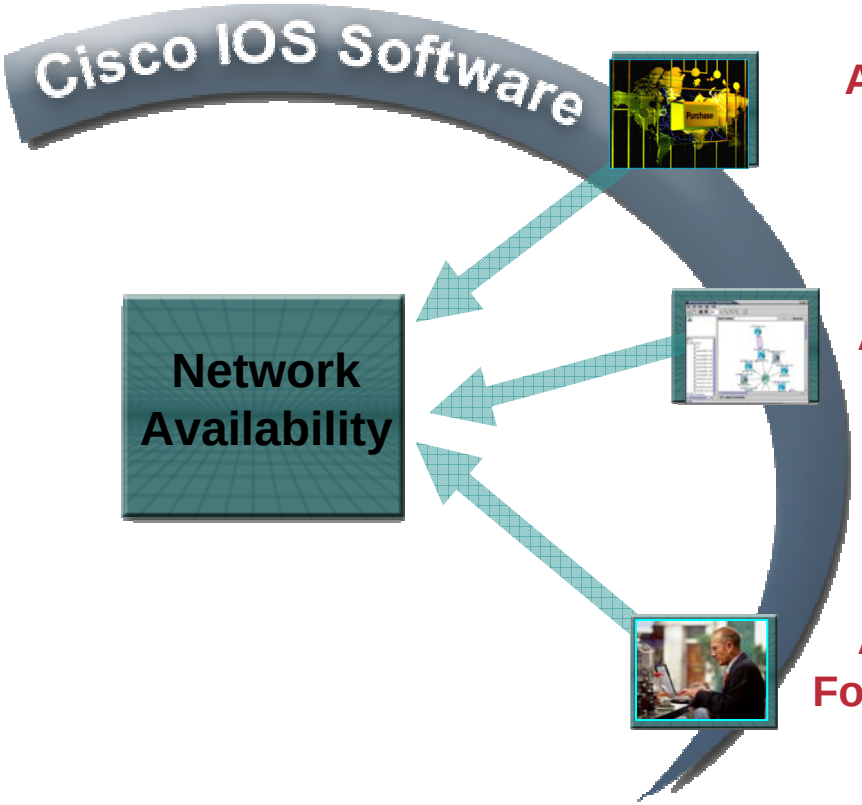


Ability to Manage



Ability to Forward Data

Securing the Router – Plane by Plane



Ability to Route → Secure **Control** Plane

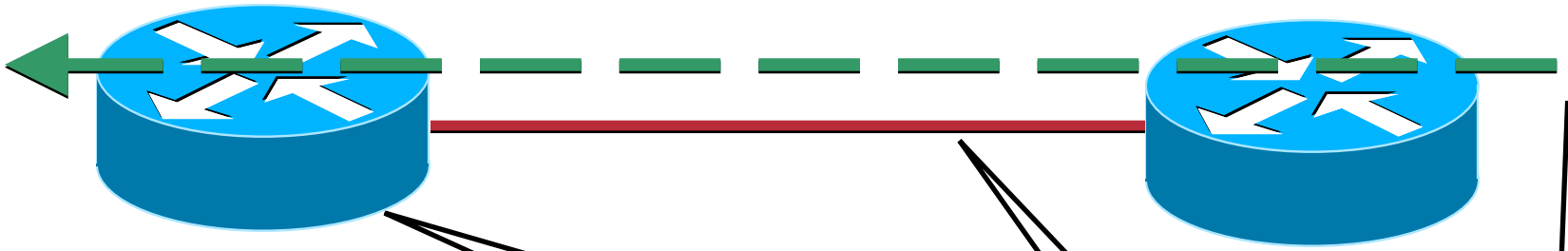
Ability to Manage → Secure **Management** Plane

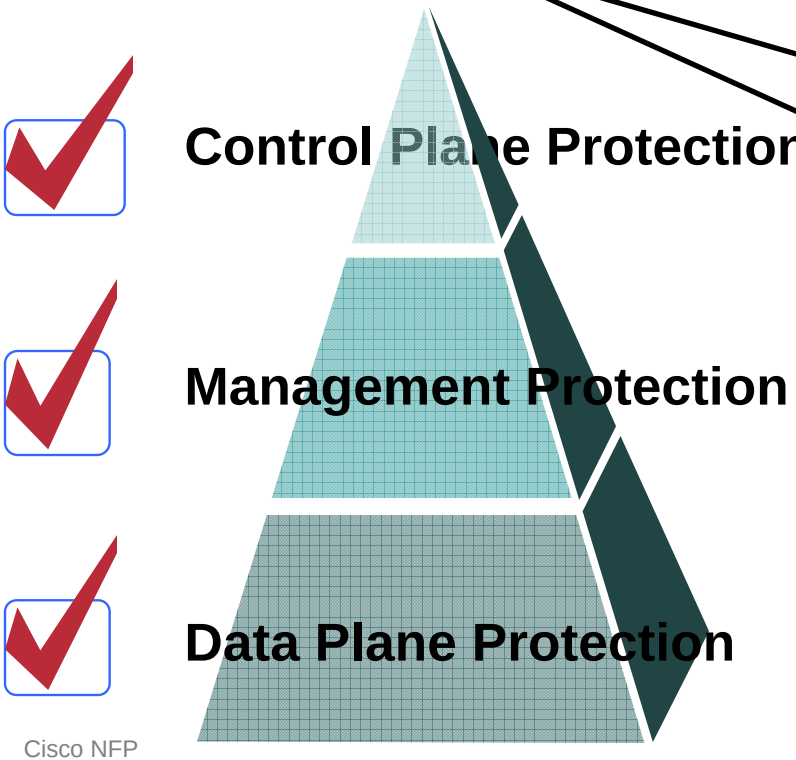
Ability to Forward Data → Secure **Data** Plane

Think "Divide and Conquer": Methodical Approach to Protect Three Planes

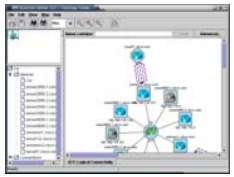
Cisco Network Foundation Protection

Secure Networks Must Be Built on a Secure Foundation





Lock down services and routing protocols

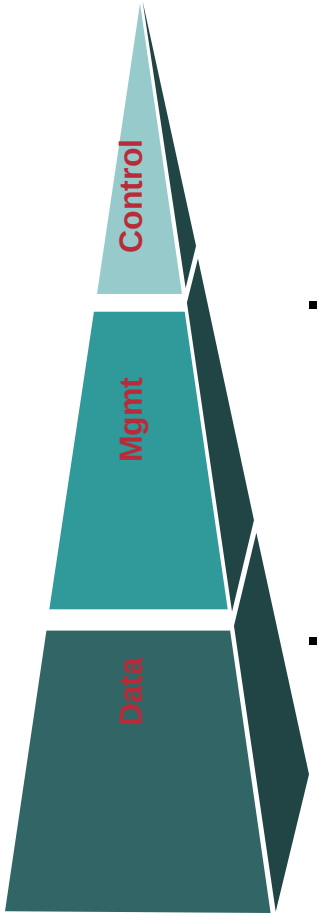


Secure Access for Management and Instrumentation

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

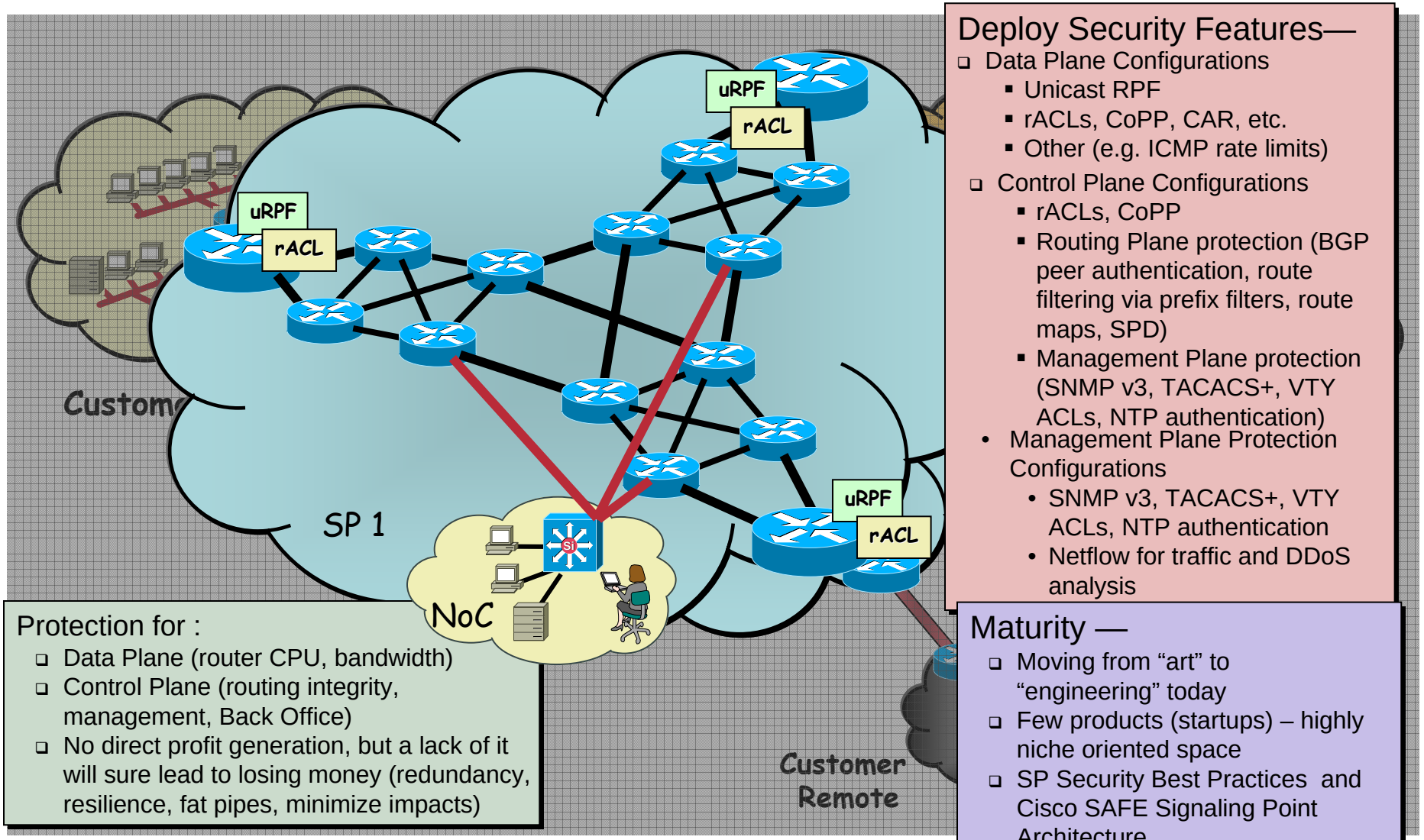
Management Plane Protection – protects the management plane from unauthorized management access and polling

- 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)
- Management Plane Protection Configurations
  - SNMP v3, TACACS+, VTY ACLs, NTP authentication
  - Netflow for traffic and DDoS analysis

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

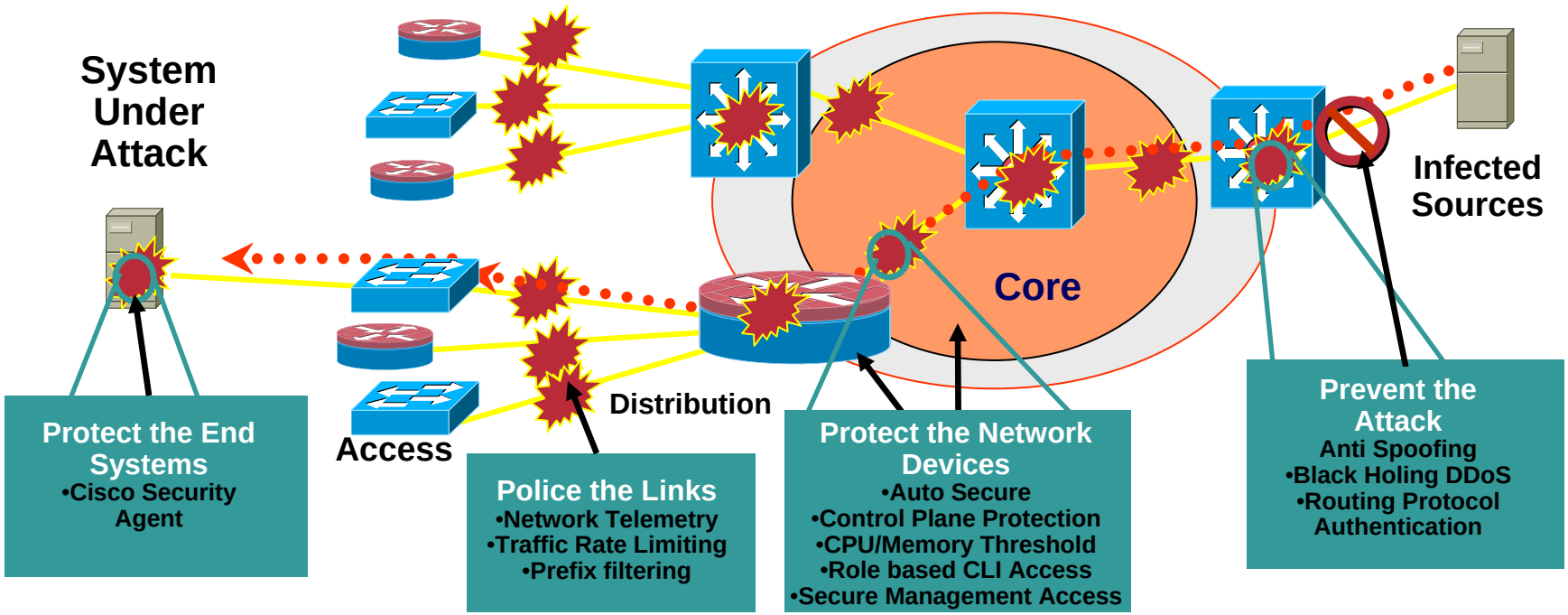
Cisco Self-Defending Network Technologies – NFP

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

Cisco Self-Defending Network Technologies – NFP (Cont.)

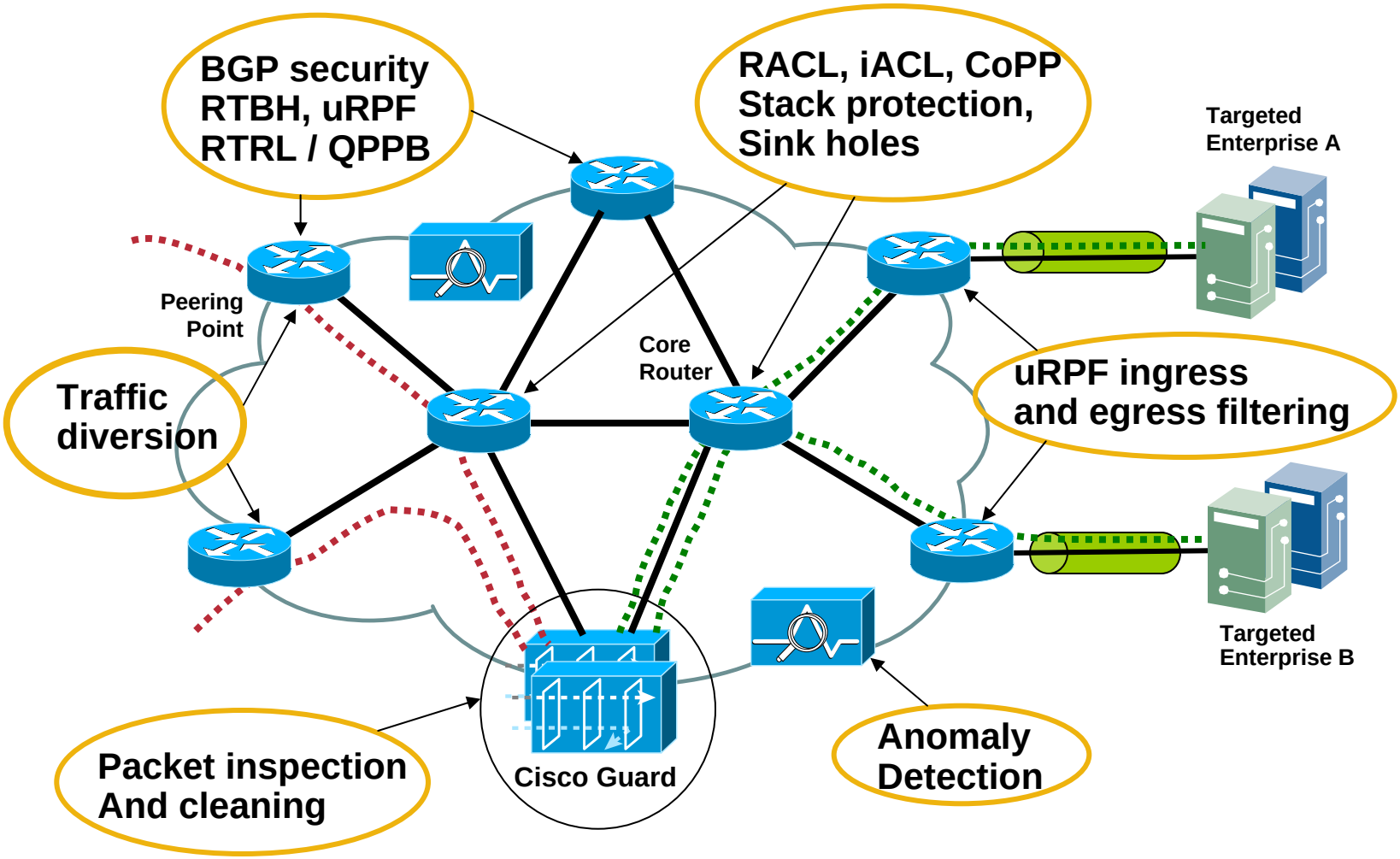
Feature	Benefits
Data Plane Protection	
Unicast RPF	Antispoofing for source IP address
Access Control Lists	ACLs - filter traffic through a device
Infrastructure ACL and CAR	Remove possibility for illegitimate users to send any traffic to link addresses

Cisco Network Foundation Worm Protection in Action



Protect and Police your business with a secure and available network

Combining Everything



Glossary

Acronym	Description
CoPP	Control Plane Policing
RTBH	Remote Triggered Black Hole
RTRL	Remote Triggered Rate Limiting
rACL	Receive ACL
iACL	Infrastructure ACL
uRPF	Unicast Reverse Path Forwarding