Cisco Router Security Solutions – Seguridad en tu red WAN

Mauricio Martínez

CCIE #17838, CCSP

maumarti@cisco.com

Objectives

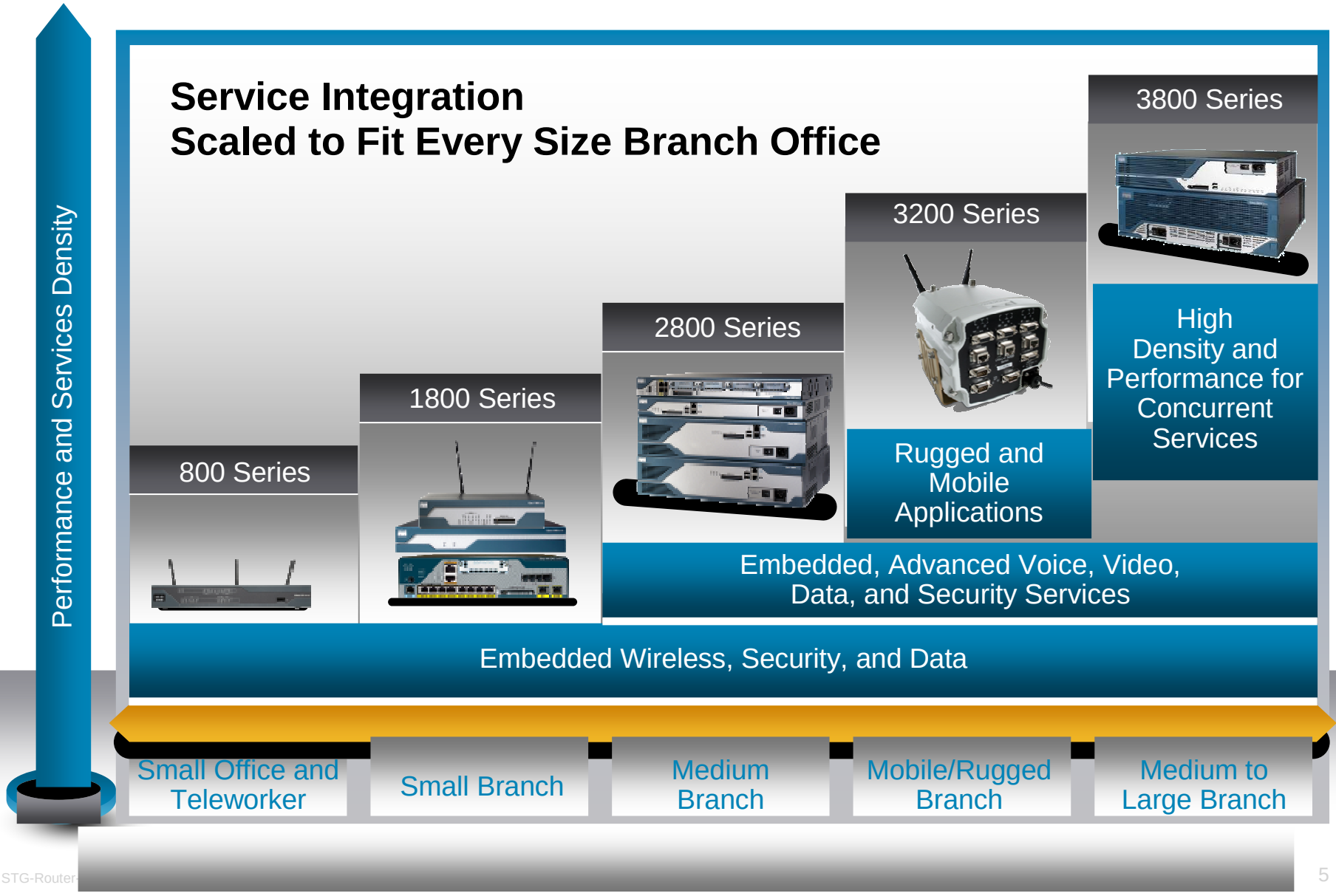
- Provide an overview of some key technologies and benefits
- Offer common usage scenarios
- Provide references to detailed material

The Branch Transformation

Today's Branch	Empowered Branch
 Aging, Disparate Data/ Voice Networks	Unified Voice/Data/Video Network Platform
 Saturated WAN, Poor Response Time	Optimized WAN, Accelerated Applications
 Blended Security Threats, Compliance	Self-Defending Networks
 Limited Mobility, Limited Disaster Recovery	High Availability, Unified Wireless—Wireline Business
 Inconsistent Branches and Branch-HQ solutions	Consistent Branches and Branch-HQ Services

Cisco Router Security
Technology Overview

Cisco Router Security Portfolio



Integrated Voice and Security

For Cisco 2800–3800 Integrated Services Routers

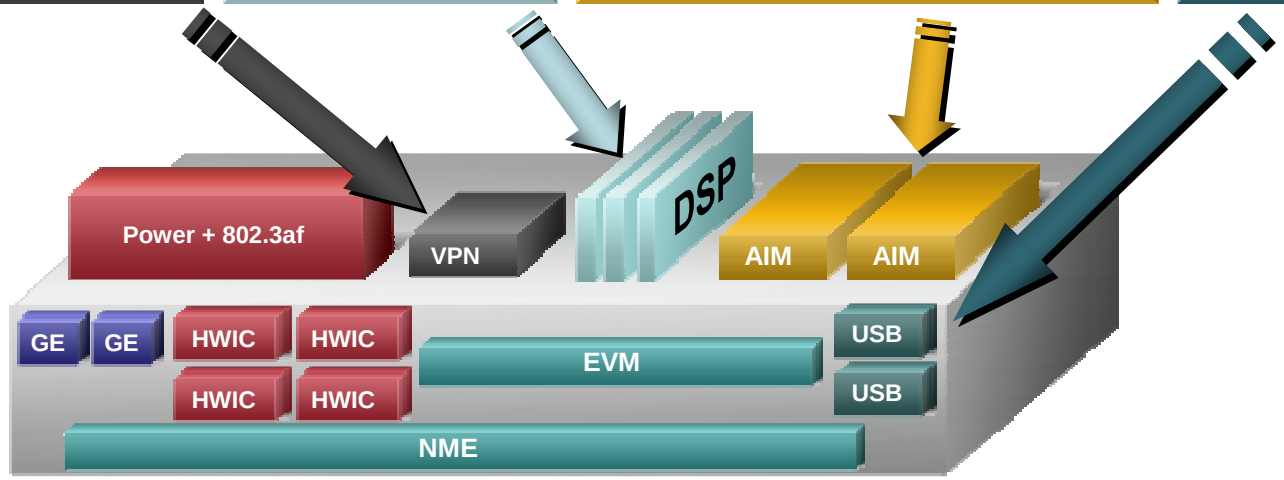
Secure Voice

Built-in VPN Acceleration
- High-performance crypto offload
- 3DES/AES encryption
- 4x faster than previous platforms

Secure Voice
- PVDM modules
- Support for SRTP

High-Performance AIM
- Optional AIM-VPN PLUS
- 3DES, AES, and compression
- 10x faster than previous platforms

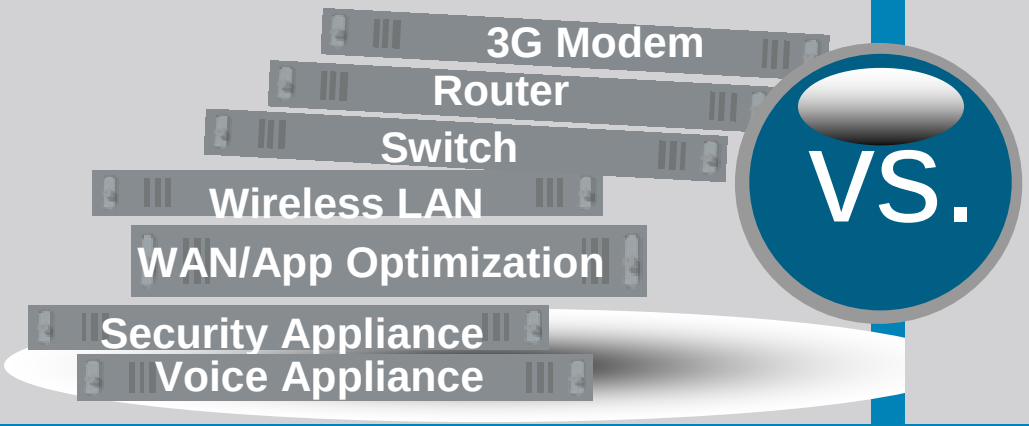
USB Port
- Removable
- Secure credentials



- ✓ Common hardware architecture
- ✓ Modular design
- ✓ Investment protection

Market Acceptance: Reaching 5 Million

Overlay Appliances

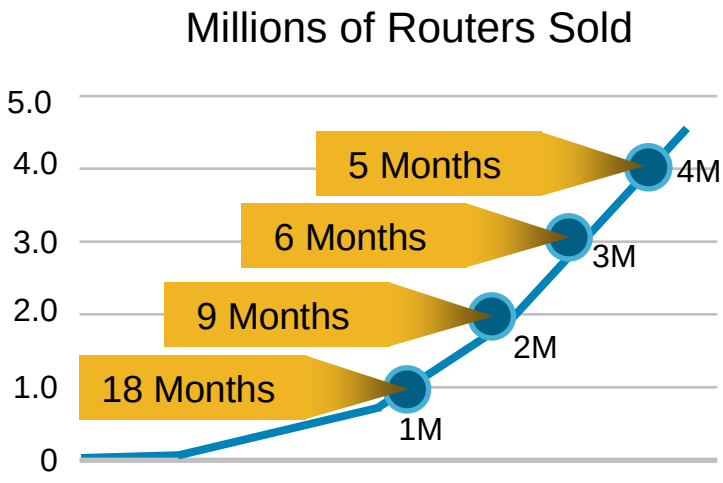


Integrated Services Router

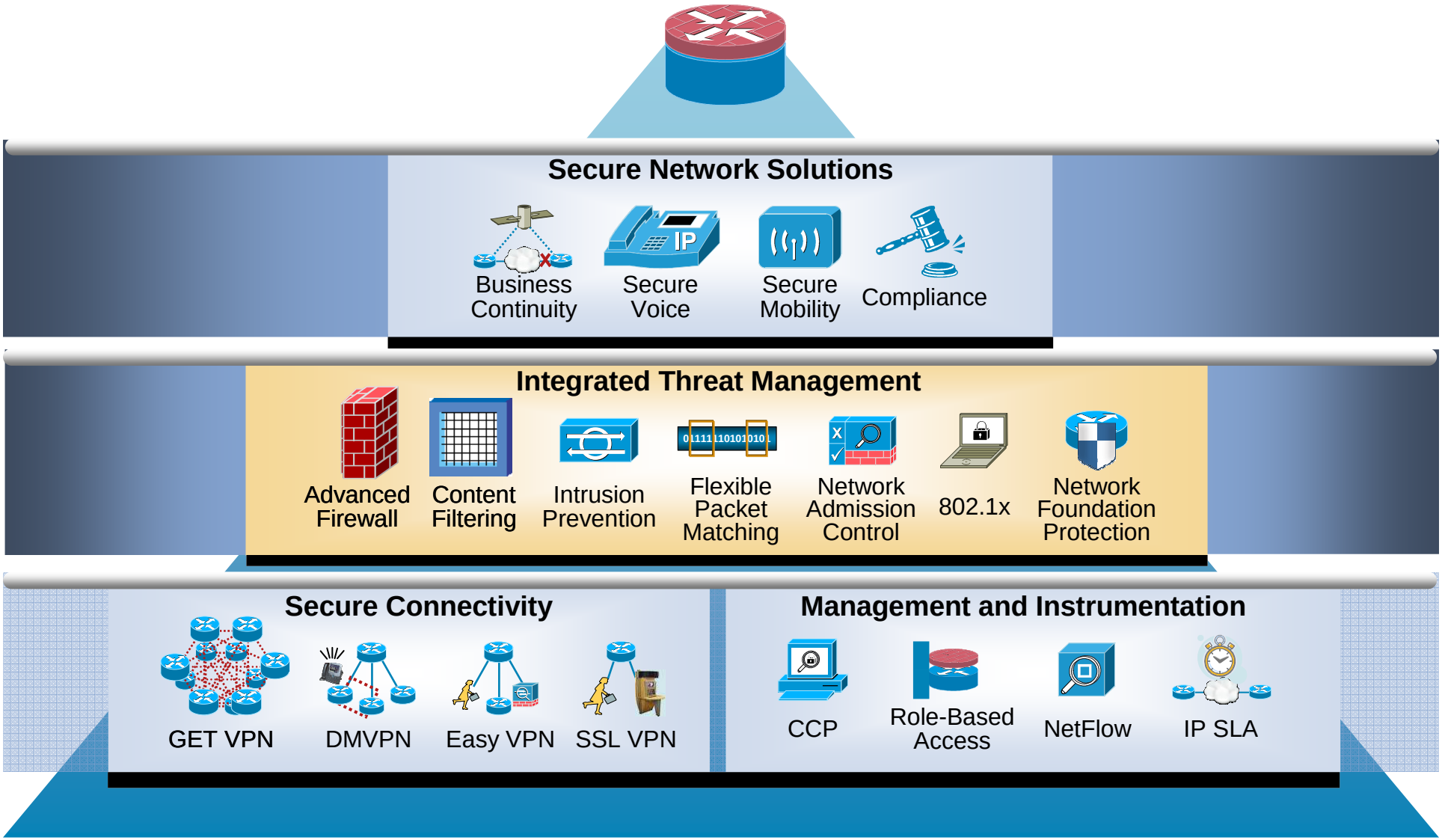
Cisco ISR 3845

With Voice, Wireless, Video, WAN Optimization, Switch

- 4 Millionth ISR at Coke-Cola Enterprises
- UC, data, video to 30,000 CCE employees
- Greater employee collaboration
- Business innovation



Only Cisco Router Security Delivers All This



Cisco Router Security Certifications

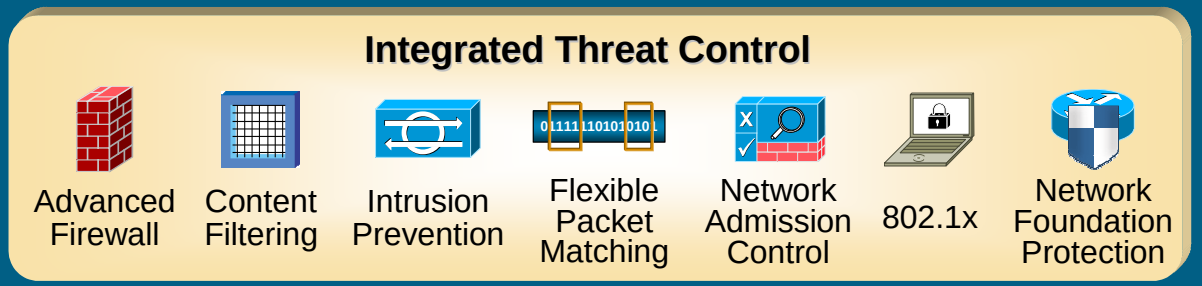
	FIPS	Common Criteria	
	140-2, Level 2	IPSec (EAL4)	Firewall (EAL4)
Cisco® 870 ISR	✓	✓	✓
Cisco 1800 ISR	✓	✓	✓
Cisco 2800 ISR	✓	✓	✓
Cisco 3800 ISR	✓	✓	✓
Cisco 7200 VAM2+	✓	✓	✓
Cisco 7200 VSA	✓	✓	---
Cisco 7301 VAM2+	✓	✓	✓
Cisco 7600 IPSec VPN SPA	✓	✓	---
Catalyst 6500 IPSec VPN SPA	✓	✓	---
Cisco 7600	✓	✓	✓

cisco.com/go/securitycert

Top Reasons to Buy Router Security

1. PROTECT THE ROUTER ITSELF – your first line of defense
2. A SINGLE BREACH could gravely impact the business
3. Advanced backup and teleworking for DISASTER RECOVERY
4. COMPLY with Government data and network privacy laws
5. Consolidate voice/video/data and wired/wireless SECURELY
6. Advanced ENCRYPTION for voice conversations and signaling
7. New ISRs deliver wire-rate PERFORMANCE WITH SERVICES
8. Easy to MANAGE a single-box Router/VPN/Firewall/IPS solution
9. REDUCE COST of service and subscription: single contract
10. 30-40% SAVINGS built into Security Router bundles

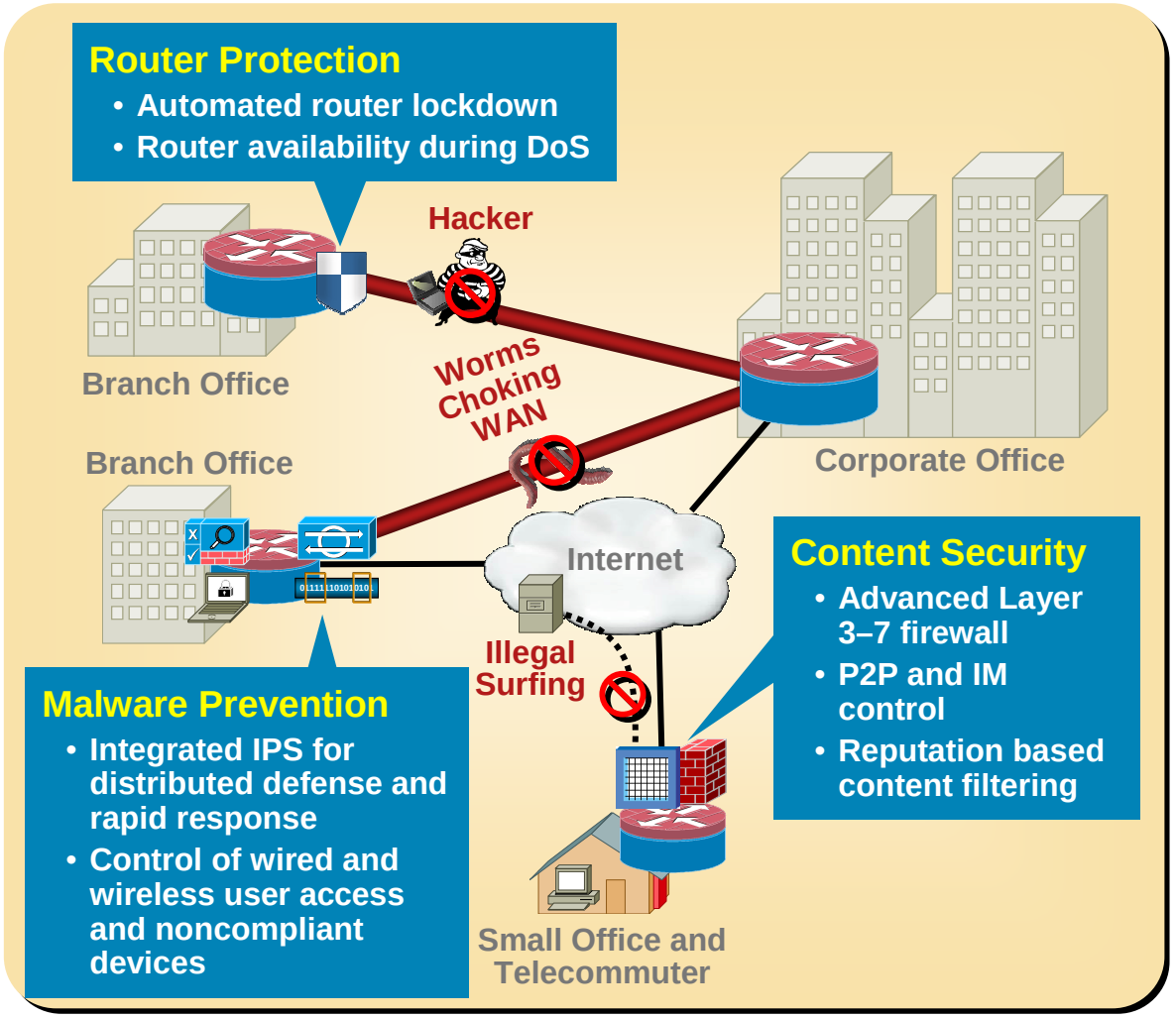
Integrated Threat Control



Integrated Threat Control Overview

Industry-Certified Security Embedded Within the Network

- Access branch office has secure Internet access and no need for additional devices
- Solution controls worms, viruses, and spyware right at the remote site; conserves WAN bandwidth
- Solution protects the router itself from hacking and DoS attacks



Cisco IOS Firewall

Stateful Firewall: Full Layer three through Layer seven deep packet inspection

Flexible Embedded ALG (Application Layer Gateway): Dynamic protocol and application engines for seamless granular control

Application Inspection and Control: Visibility into both control and data channels to ensure protocol and application conformance

Virtual Firewall: Separation between virtual contexts, addressing overlapping IP addresses

Intuitive GUI Management: Easy policy setup and refinement with GUI tools.

Resiliency: High availability for users and applications with stateful firewall failover

WAN Interfaces: Most WAN/LAN interfaces

Select List of Recognized Protocols

- HTTP, HTTPS, JAVA
- Email: POP, SMTP, IMAP, Lotus
- P2P and IM (AIM, MSN, Yahoo!)
- FTP, TFTP, Telnet
- Voice: H.323, SIP, SCCP
- Database: Oracle, SQL, MYSQL
- Citrix: ICA, CitrixIcaClient
- Multimedia: Apple, RealAudio
- IPsec VPN: GDOI, ISAKMP
- Microsoft: MSSQL, NetBIOS
- Tunneling: L2TP, PPTP

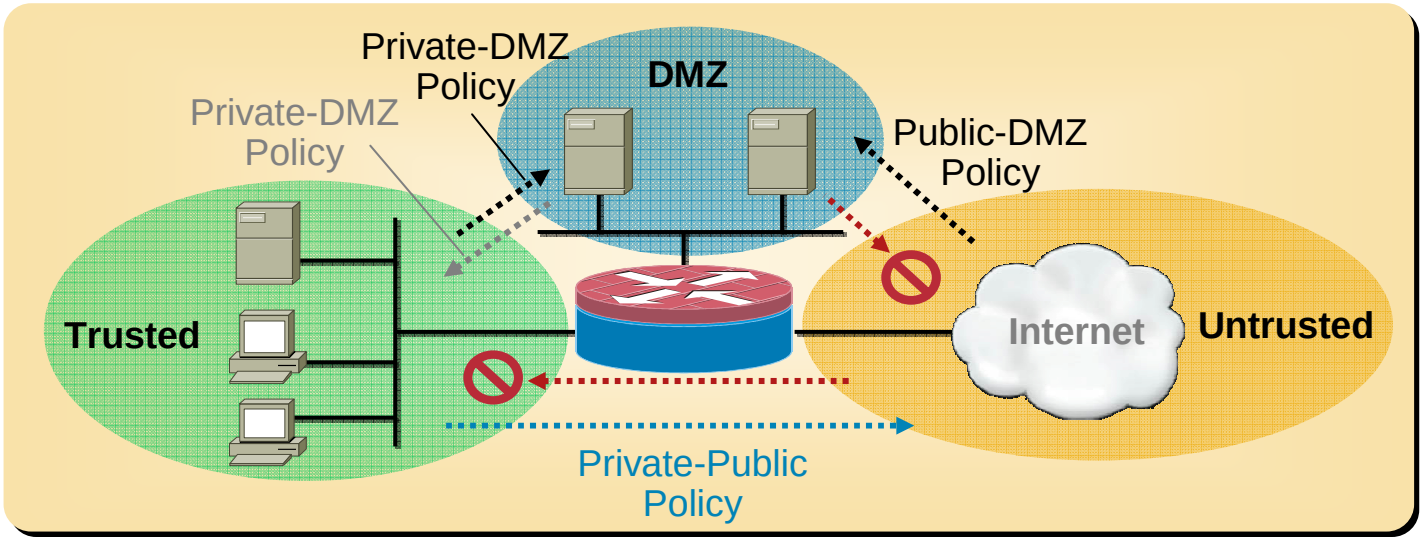
Zone-Based Policy Firewall

Advanced Firewall

- Allows grouping of physical and virtual interfaces into zones
- Firewall policies are configured on traffic moving between zones
- Simple to add or remove interface and integrate into firewall policy

Supported Features

- Stateful Inspection
- Application Inspection: IM, POP, IMAP, SMTP/ESMTP, HTTP
- URL filtering
- Per-policy parameter
- Transparent firewall
- VRF-aware firewall



Denial of Service (DoS) Protection

- DoS protection is enabled by default on Cisco® IOS® Firewall and IPS
- Activating Cisco IOS IPS or Firewall (independently or together) causes these default DoS settings to be used:

```
ip inspect max-incomplete high value (default 500)
ip inspect max-incomplete low value (default 400)
ip inspect one-minute high value (default 500)
ip inspect one-minute low value (default 400)
ip inspect tcp max-incomplete host value (default 50) [block-time minutes]
```

- Firewall and IPS Design Guides include tuning procedure

  Design Guide : http://www.cisco.com/go/iosfw

  During lab performance tests, be sure to set DoS settings at maximum

Industry-First Firewall + WAN Acceleration Interoperability Solution

- Full stateful firewall transparently protects WAN accelerated traffic
- For integrated as well as independent deployments
- FIPS, Common Criteria EAL4 and ICSA certified
- Facilitates PCI compliance
- Now available with Cisco IOS 12.4(11)T2

Firewall Features	Cisco ISR with WAAS	Most Competitors
Stateful Inspection	For all traffic	Tunnel traffic only
IP ACLs	✓	–
NAT	✓	–
Authentication Proxy	✓	–
No Static Open Ports	✓	–
Granular Per Session Policy	✓	–
QoS Policy	✓	–

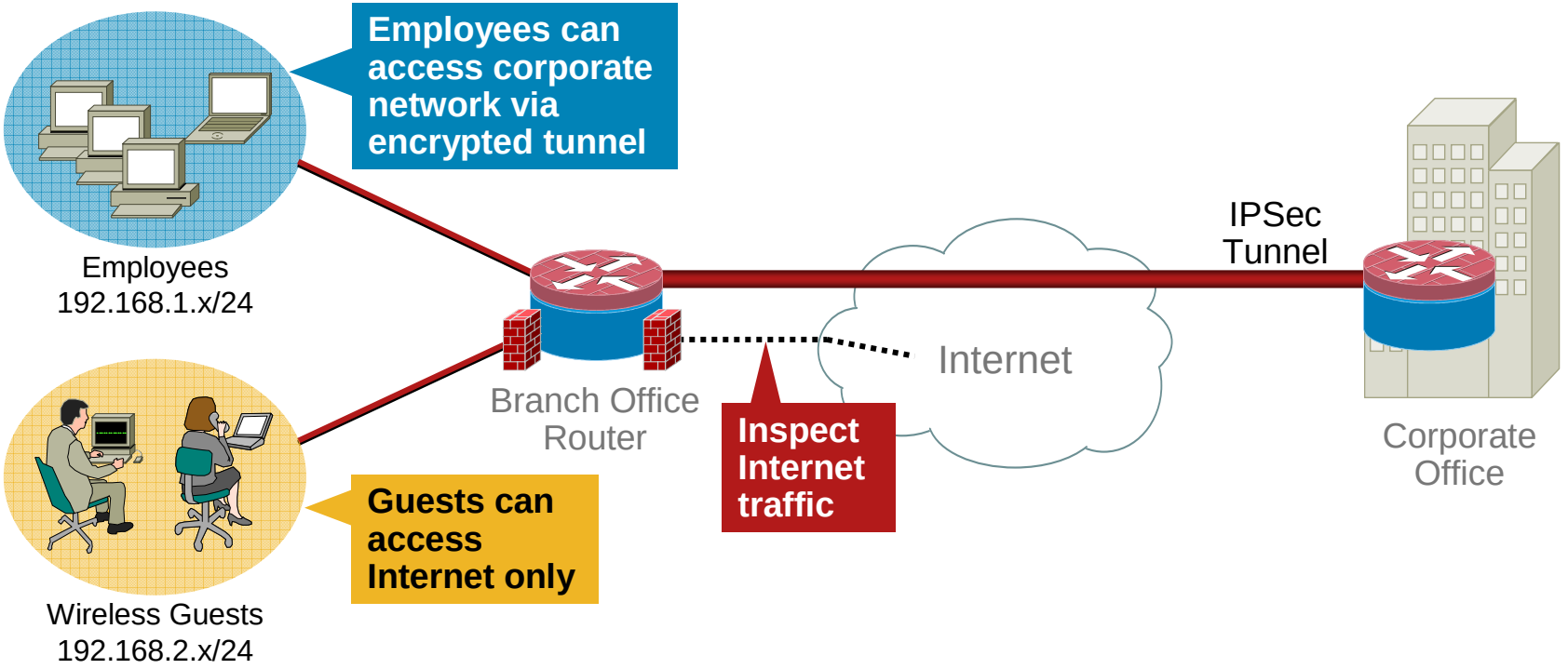
Cisco IOS Firewall Use Case 1

Advanced Firewall

Protect the LAN at Branch with Split Tunneling

Cisco® IOS® Firewall policies:

- Allow authenticated users to access corporate resources
- Restrict guest users to Internet access only
- Control peer-to-peer and instant messaging applications

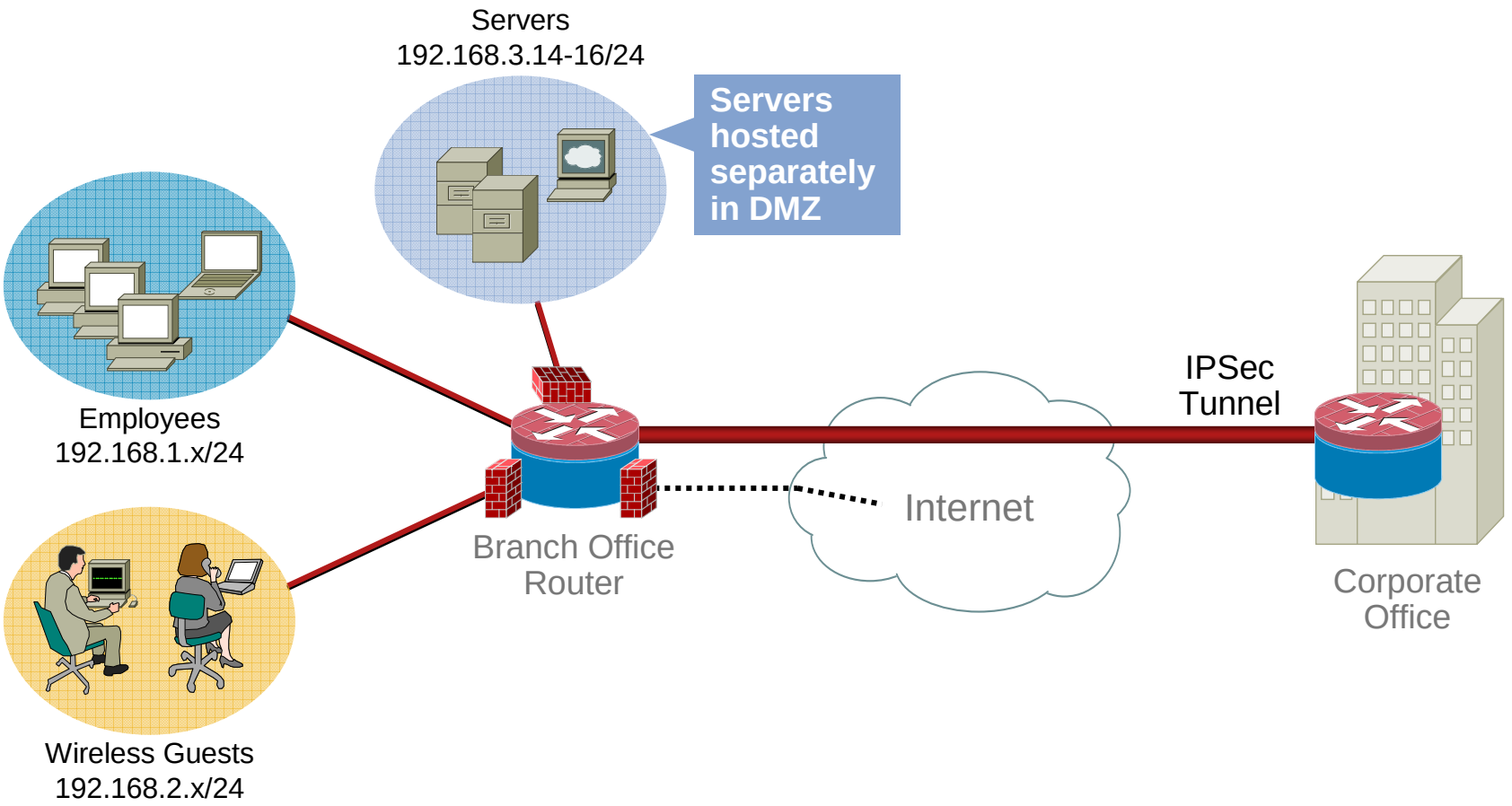


Cisco IOS Firewall Use Case 2

Advanced Firewall

Protect Servers at Remote Sites

- Cisco® IOS® Firewall policies applied to DMZ protect distributed application servers and Web servers hosted at remote sites

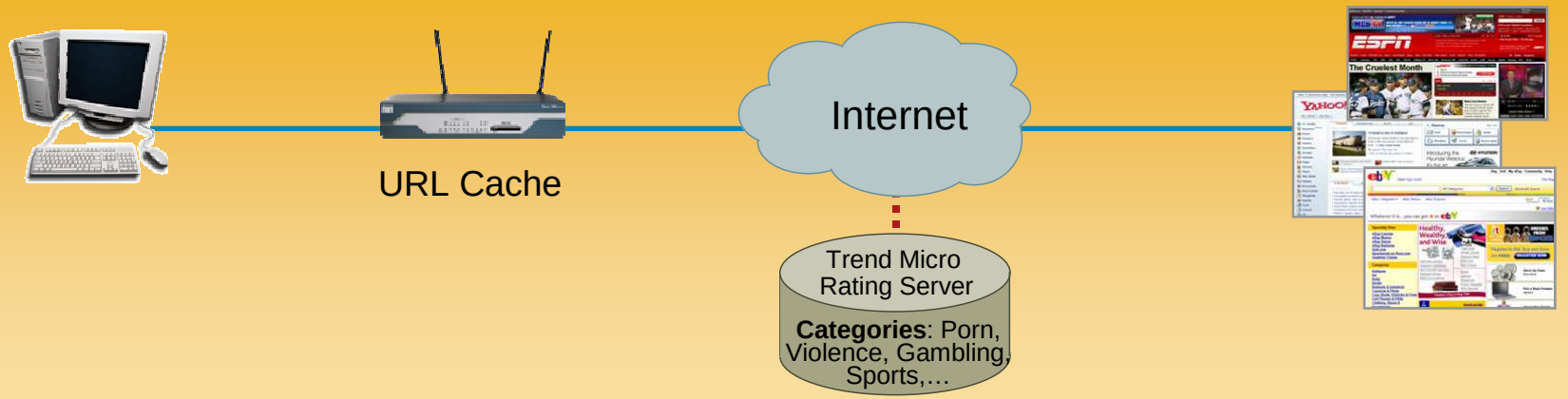


Cisco IOS® Content Filtering with Trend Micro

Content Filtering

A Web Security Solution That Protects Organizations from Known and New Internet Threats, While Improving Employee Productivity

- Ideal for Enterprise Branch and Small-Medium Businesses
- Block malicious sites and enforce corporate policies
- Offers category based security and productivity ratings
- Regulations such as HIPAA, FISMA, CIPA (Children's Internet Protection Act) mandate reliable content filtering.
- Policy is enforced and maintained on the router locally

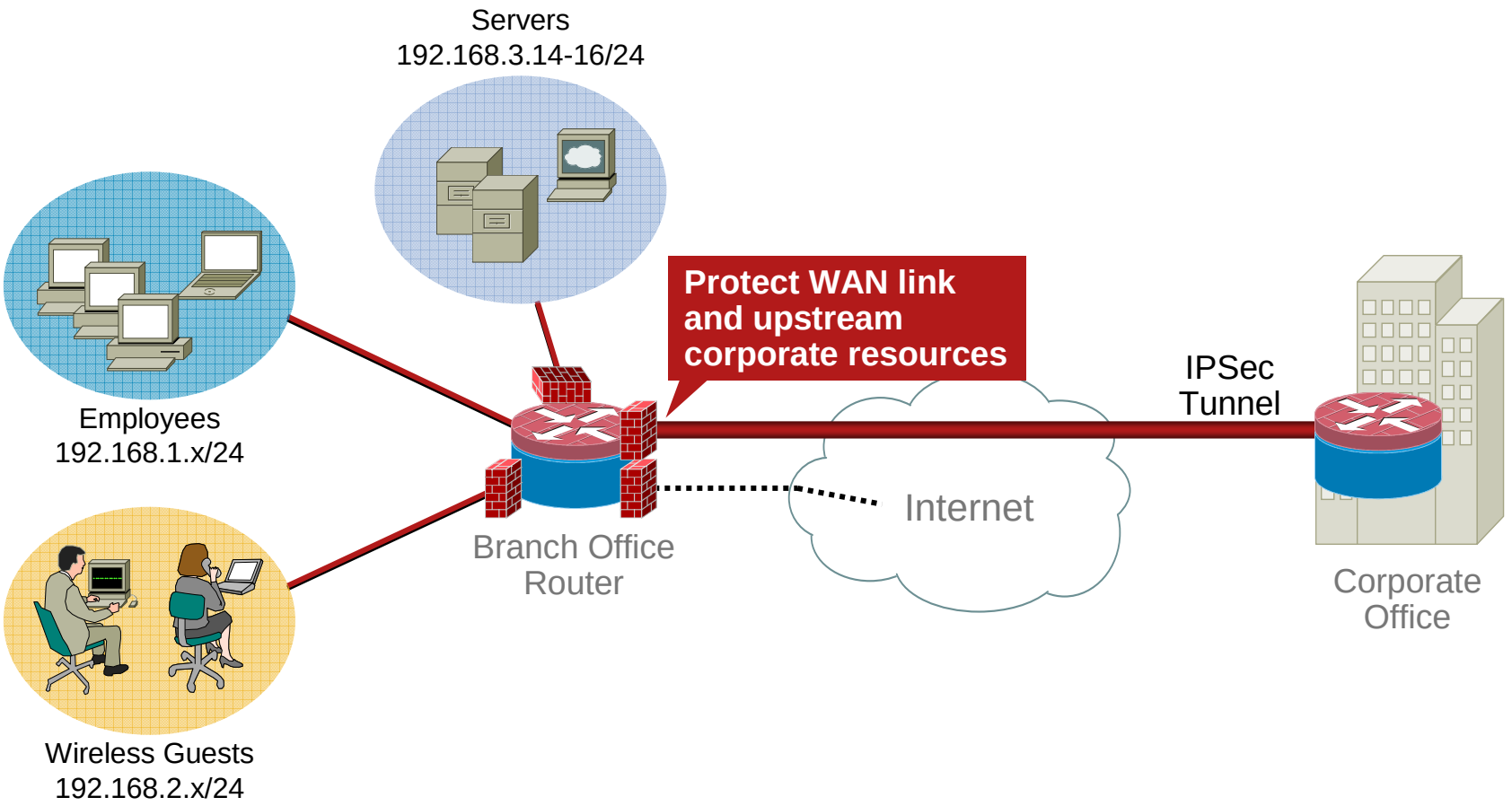


Cisco IOS Firewall Use Case 3

Advanced Firewall

Protect WAN Link and Corporate Office

- Cisco® IOS® Firewall policies applied to private interfaces protect WAN link from worms and protocol misuse attacks

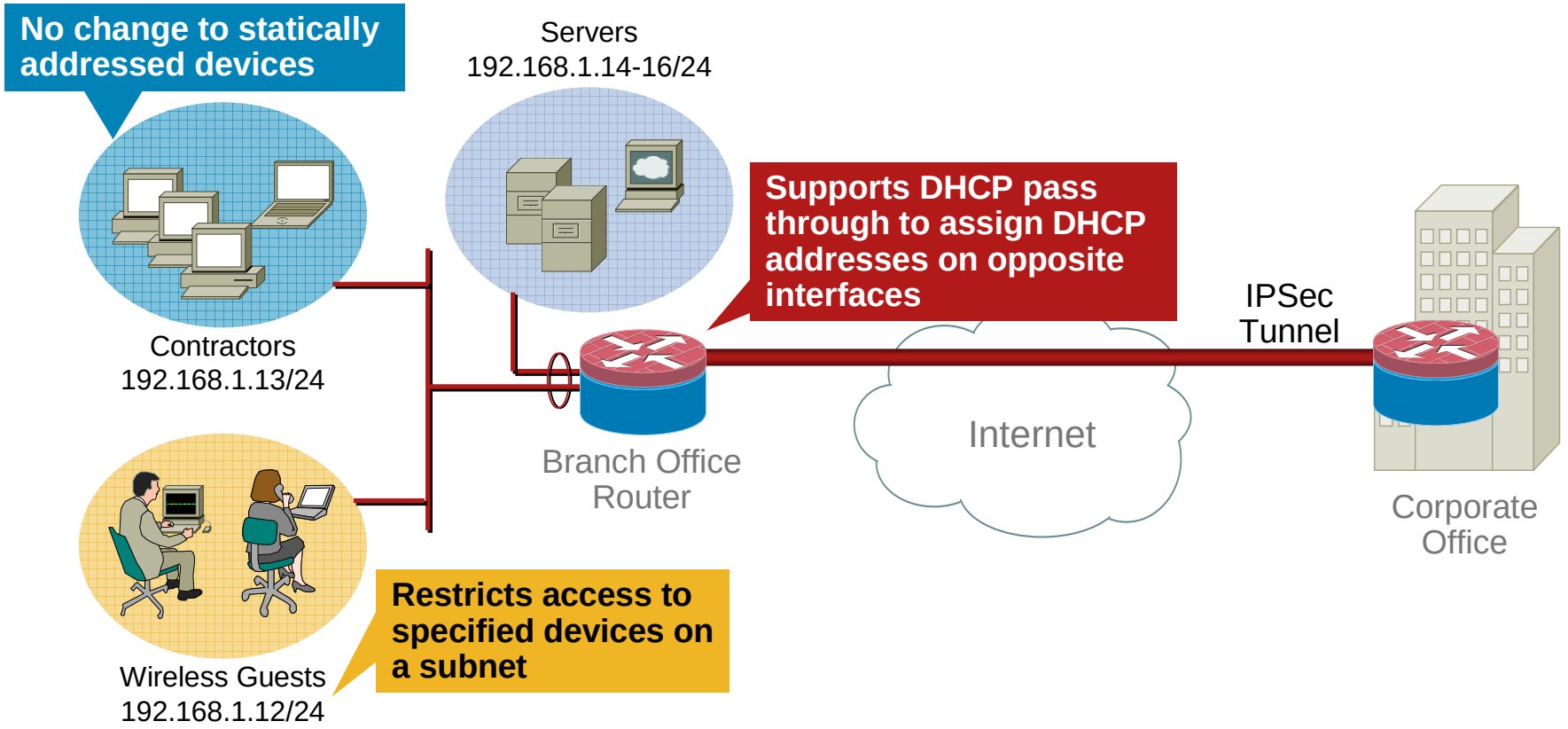


Cisco IOS Firewall Use Case 4

Advanced Firewall

Transparent Firewall and IPS

- Cisco® IOS® transparent firewall policies at bridge interfaces enforce inspection and control of LAN traffic
- Simplifies firewall and IPS deployment at small offices running key applications in a single address space

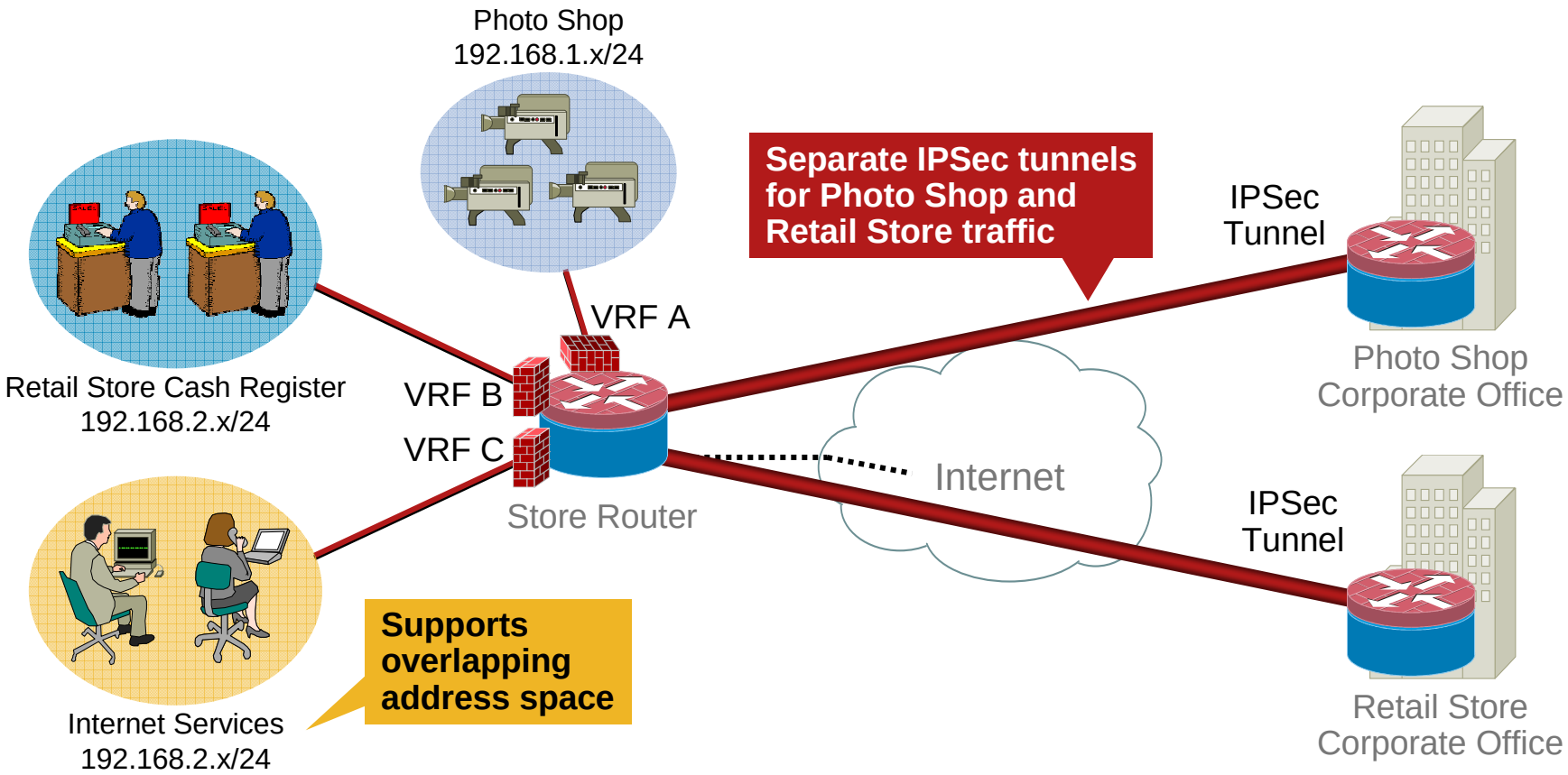


Cisco IOS Firewall Use Case 5

Advanced Firewall

Virtual Firewall

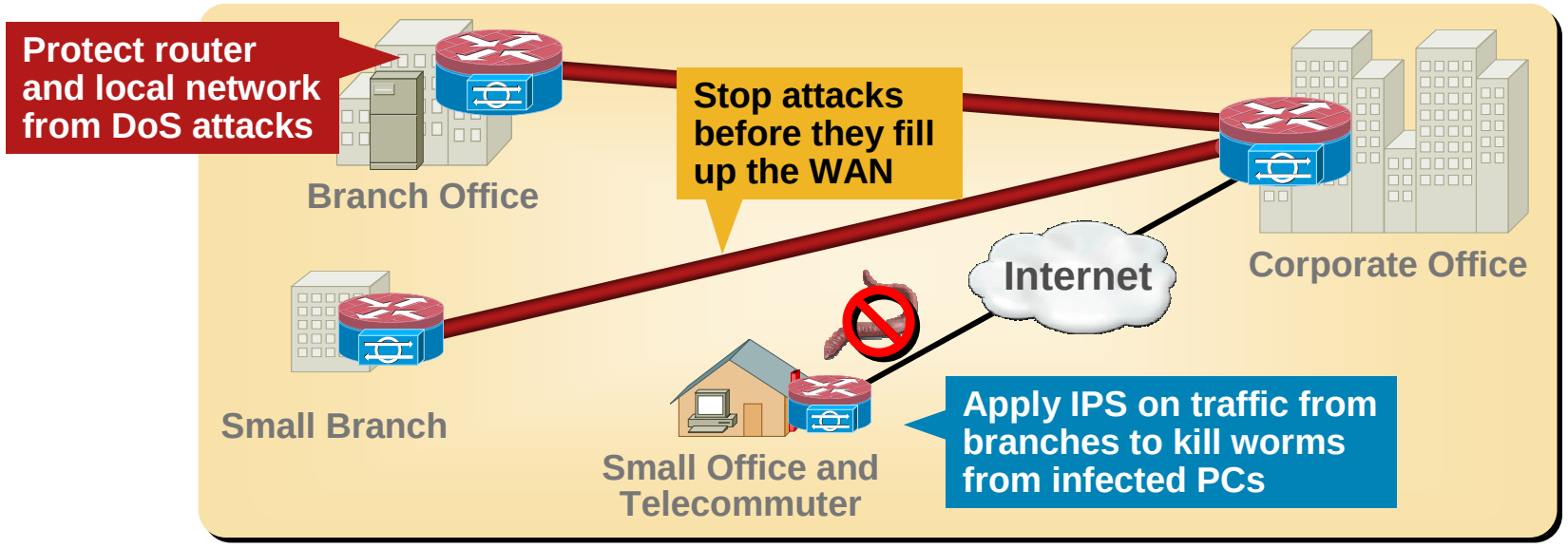
- Cisco® IOS® Firewall, NAT, and URL-filtering policies are virtual route forwarding (VRF) aware, providing support for overlapping address space, which simplifies troubleshooting and operations



Cisco IOS Intrusion Prevention (IPS)

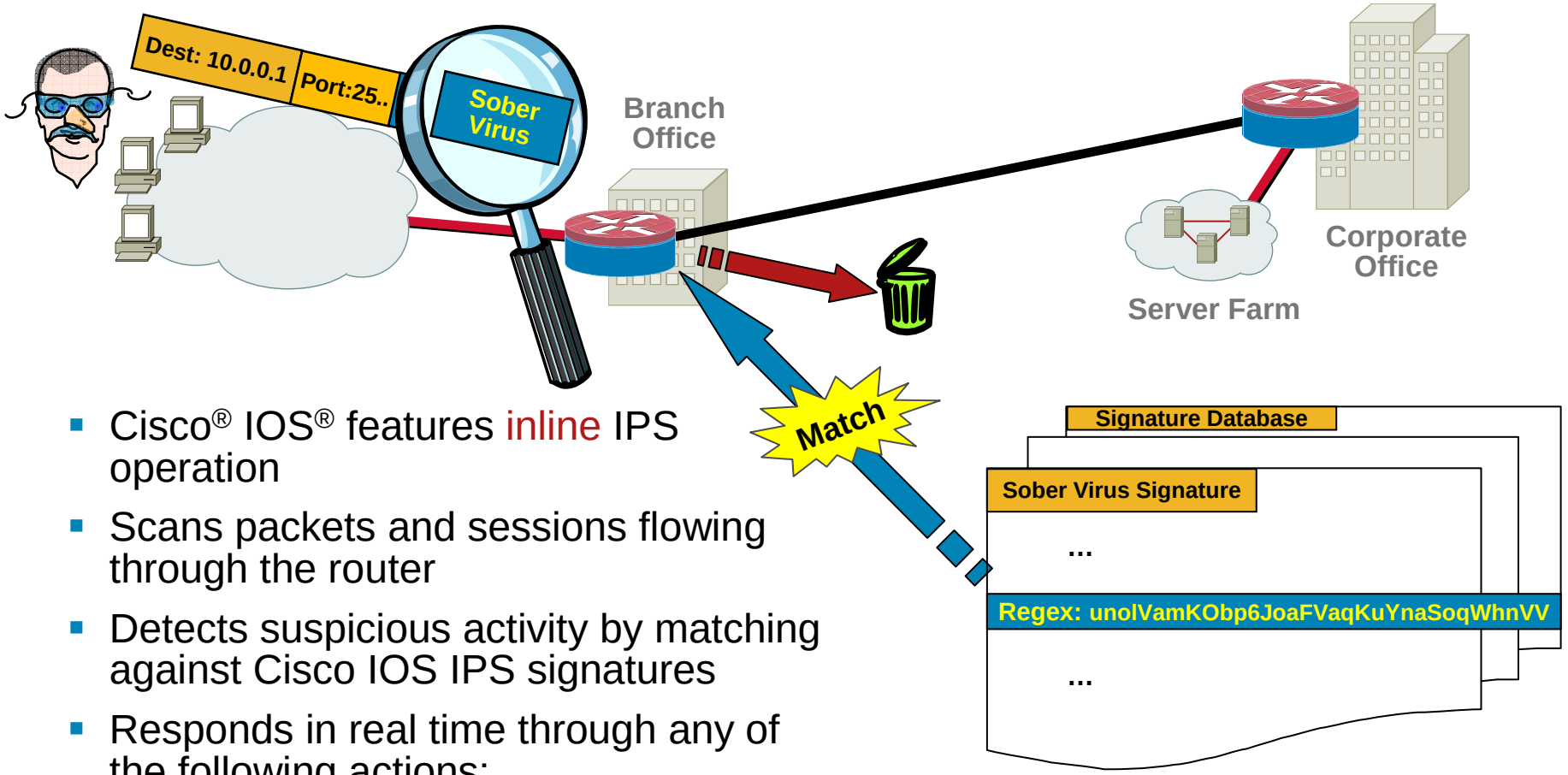
Distributed Defense Against Worms and Viruses

- Cisco® IOS® IPS stops attacks at the entry point, conserves WAN bandwidth, and protects the router and remote network from DoS attacks
- Integrated form factor makes it cost-effective and viable to deploy IPS in small and medium business and enterprise branch/telecommuter sites
- Supports a fully customizable subset of 2000+ signatures sharing the same signature database available with Cisco IPS sensors and modules
- Allows custom signature sets and actions to react quickly to new threats



Cisco IOS IPS Overview

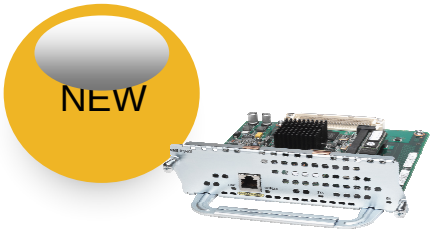
IPS



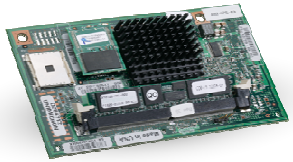
- Cisco® IOS® features inline IPS operation
- Scans packets and sessions flowing through the router
- Detects suspicious activity by matching against Cisco IOS IPS signatures
- Responds in real time through any of the following actions:

  ALARM, DROP, RESET, DENY-ATTACKER-INLINE, DENY-FLOW-INLINE

Intrusion Prevention System (IPS): AIM and NME

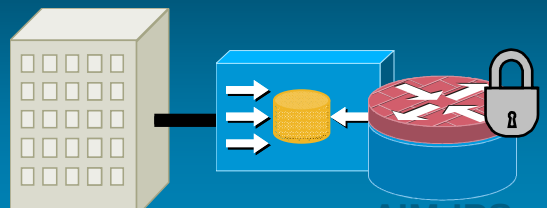


NME-IPS-K9
Cisco 2811, 2821, 2851, 3800



AIM-IPS-K9
Cisco 1841, 2800, 3800

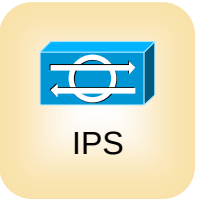
IOS Advanced Security or above
AIM – 12.4(15)XY, 12.4(20)T
NME – 12.4(20)YA



Accelerated Threat Control for Cisco ISR

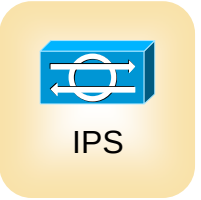
- Enables Inline and promiscuous Intrusion Prevention (IPS)
- Runs same software (CIPS 6.1) and enables same features as Cisco IPS 4200
- Performance Improvement by Hardware Acceleration. Dedicated CPU and DRAM to offload host CPU
  - AIM – Up to 45 Mbps
  - NME – Up to 75 Mbps
- Device management through Cisco IPS Device Manager (IDM), Cisco Configuration Professional (CCP); Network wide management through Cisco Security Manager (CSM)
- Supported by IPS Manager Express (IME) and CS-MARS on event monitoring and correlation

Integrating IPS AIM and NME



- Cisco IOS Firewall and IPS hardware are complementary technologies
  - Cisco IOS Firewall blocks unwanted traffic from entry into the network, ensures that applications traffic is legitimate
  - IPS AIM/NME inspects traffic the FW has allowed, as well as traffic from the trusted network, to prevent attacks
- Cisco IOS Firewall provides SYN Flood attack defense
- Cisco IOS Firewall and IPS AIM/NME maintain separate state tables for TCP traffic
  - Resets from one state table force session timeouts in the other

Cisco IOS IPS, IDS NME and IPS AIM



Capability	Cisco IOS IPS	Cisco IPS NME	Cisco IPS AIM
Dedicated CPU and DRAM for IPS	No	Yes	Yes
Inline and promiscuous detection and mitigation	Yes	Yes	Yes
Signatures supported	Subset of 2000+ signatures, subject to available memory	Full set of signatures (2200+)	Full set of signatures (2200+)
Automatic signature updates	Yes	Yes	Yes
Day-zero anomaly detection	No	Yes	Yes
Rate limiting	No	Yes	Yes
IPv6 detection	No	Yes	Yes
CSA – IPS collaboration	No	No	Yes
Meta event generator	No	Yes	Yes
Event notification	Syslog, SDEE	SNMP, SDEE	SNMP, SDEE
Device management	IOS CLI, SDM	IPS CLI, IME	IOS CLI, IME
System/network management	CSM	CSM	CSM
Event monitoring and correlation	IME, MARS	IME, MARS, on-box meta event generator	IME, MARS, on-box meta event generator

Note: Only one IPS service may be active in the router.
All others must be removed or disabled.

Cisco IPS Manager Express (IME)

All-In-One IPS Management Application for up to 5 IPS Sensors

New

Startup Wizard: Gets you up and running in just minutes

Dashboard: Puts needed information at your finger tips

Configuration: Save time with intuitive interface

Reporting: Create and share security and compliance reports

Monitoring: See what's happening with real-time and historical security events

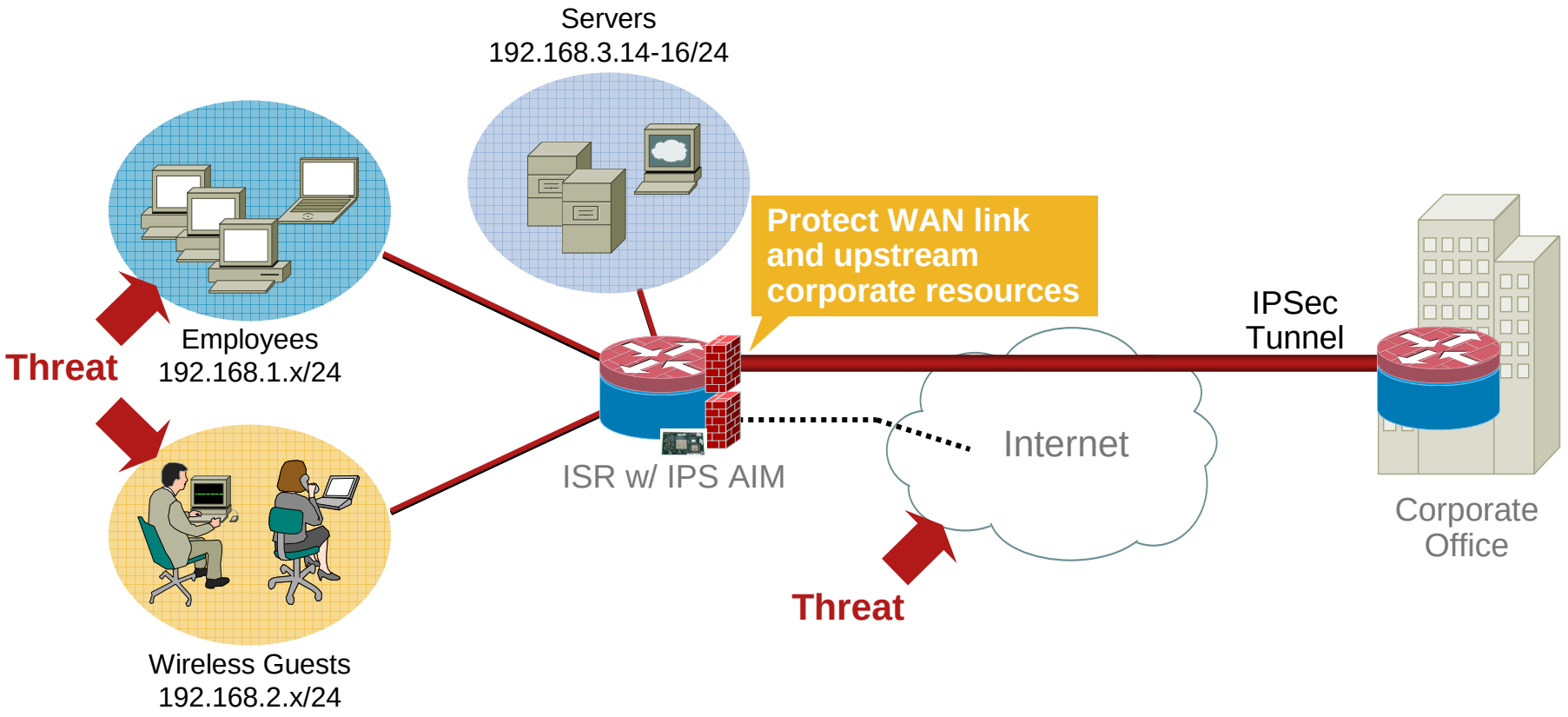
At-A-Glance Dashboard

Cisco IOS IPS Use Case 1

IPS

Protect WAN Link and Head Office

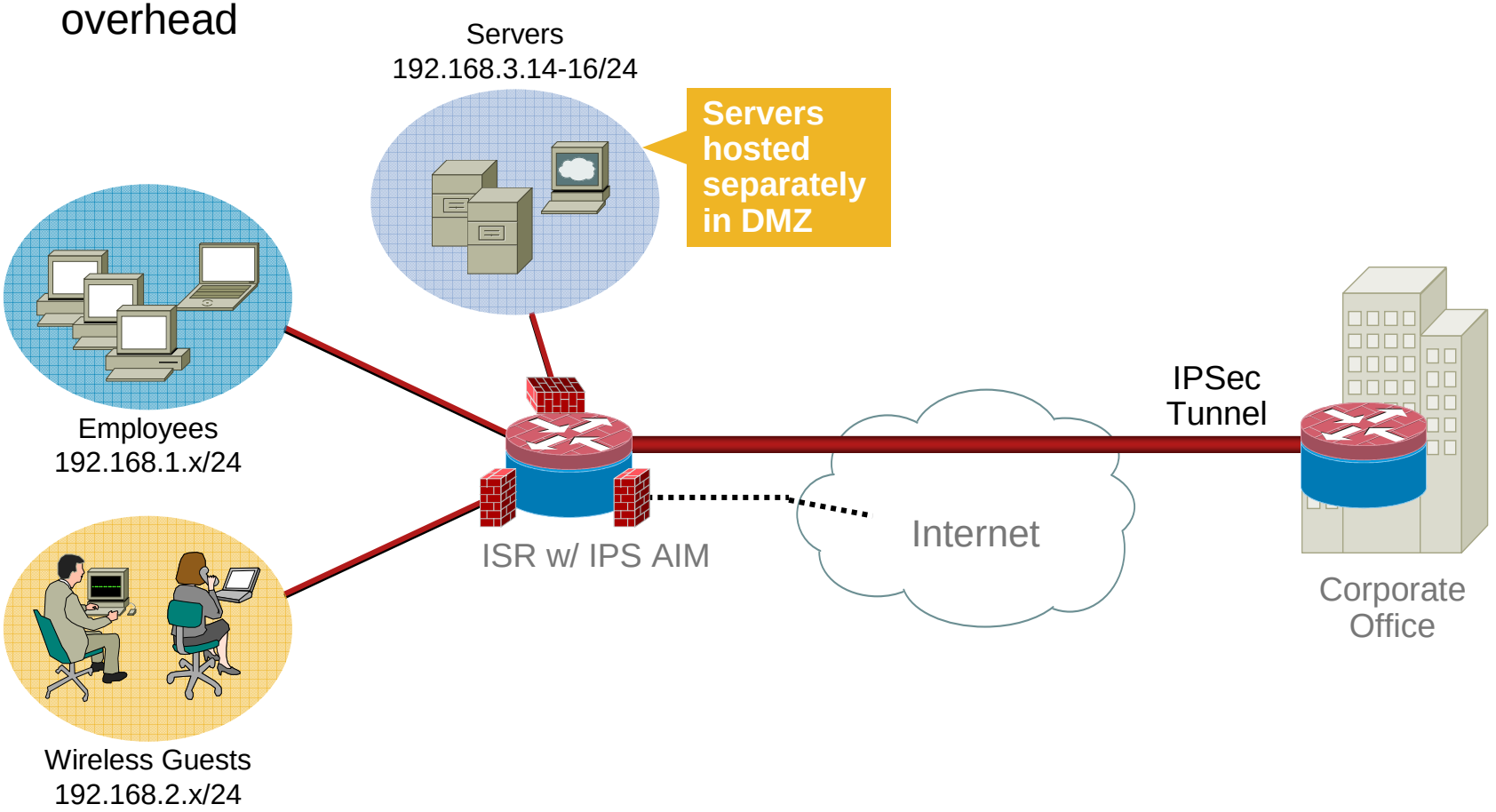
- Branch office LAN are prone to attacks from Internet from split tunnels, contaminated laptops and rogue wireless access points
- Stops worms and trojan horses *before* they enter corporate or SP network
- Moves attack protection to the network edge



Cisco IOS IPS Use Case 2

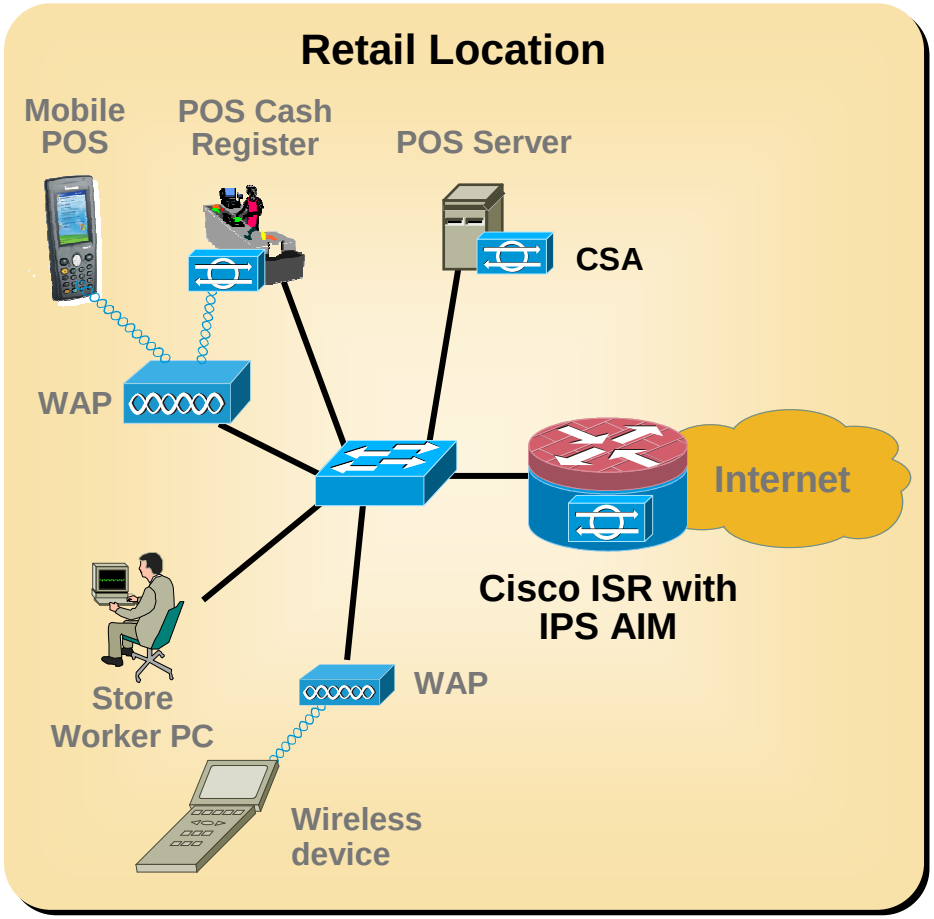
Protect Servers at Remote Sites

- Protect distributed application servers and web servers hosted at remote sites
- Endpoint attack relevance identifies server OS with minimal administration overhead



Cisco IOS IPS Use Case 3

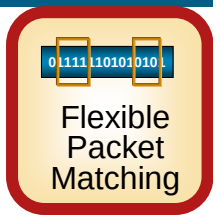
Enhanced PCI Compliance, Requirement 11



- Provides Intrusion Prevention in depth, as part of PCI Compliant Self Defending Network
- Event correlation provides audit trail for tests and validation exercises
- Integrates with IOS FW, IPSEC, SSL VPN and other IOS security technologies for complete solution
- Offloads all IPS inspection from router CPU
- Filters inspected traffic via ACLs

Flexible Packet Matching (FPM)

Rapid Response to New and Emerging Attacks



- Network managers require tools to filter day-zero attacks, such as before IPS signatures are available
- Traditional ACLs take a shotgun approach—legitimate traffic could be blocked

  Example: Stopping Slammer with ACLs meant blocking port 1434—denying business transactions involving Microsoft SQL
- FPM delivers flexible, granular Layer 2–7 matching

  Example: port 1434 + packet length 404B + specific pattern within payload → Slammer
- Useful for CERT-like teams within service providers and enterprise customers

Flexible Classification and Rapid Response

- Goes beyond static attributes—specify arbitrary bits/bytes at any offset within the payload or header
- Classify on multiple attributes within a packet
- Set up custom filters rapidly using XML-based policy language

Cisco IOS AutoSecure

One-Touch Automated Router Lockdown

Network Foundation Protection

Disables Nonessential Services

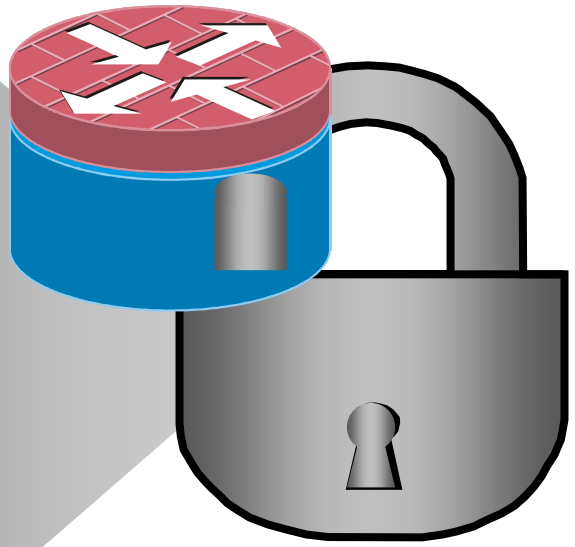
- Eliminates DoS attacks based on fake requests
- Disables mechanisms that could be used to exploit security holes

Enforces Secure Access

- Enforces enhanced security in accessing device
- Enhanced security logs
- Prevents attackers from knowing packets have been dropped

Secures Forwarding Plane

- Protects against SYN attacks
- Antispoofing
- Enforces stateful firewall configuration on external interfaces, where available

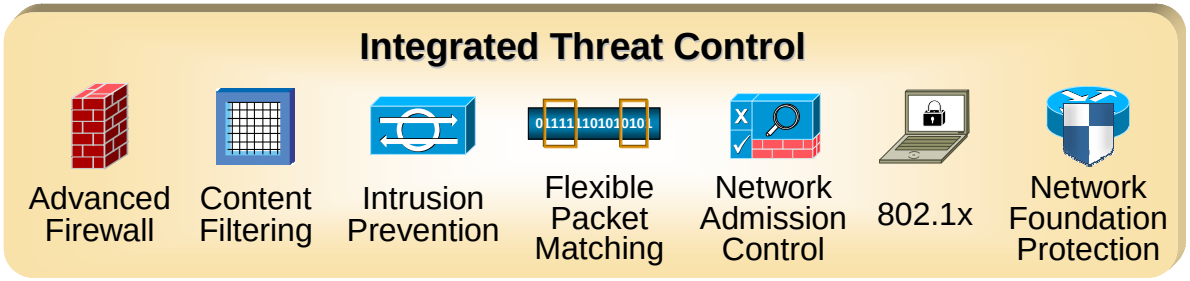


Cisco Network Foundation Protection

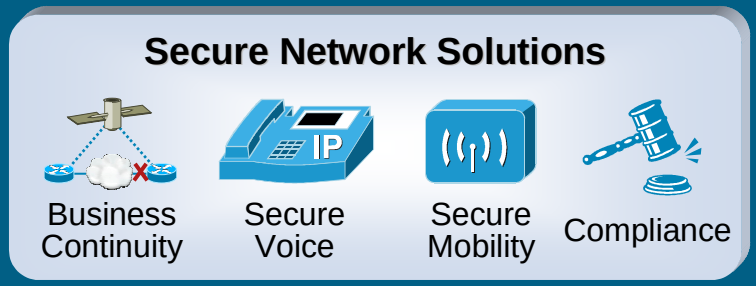
Data Plane Feature	Function and Benefit
NetFlow	▪ Macro-level, anomaly-based DDoS detection through counting the number of flows (instead of contents); provides rapid confirmation and isolation of attack
Access Control Lists (ACLs)	▪ Protect edge routers from malicious traffic; explicitly permit the legitimate traffic that can be sent to the edge router's destination address
Flexible Packet Matching (FPM)	▪ Next-generation “Super ACL”—pattern-matching capability for more granular and customized packet filters, minimizing inadvertent blocking of legitimate business traffic
Unicast Reverse Path Forwarding (uRPF)	▪ Mitigates problems caused by the introduction of malformed or spoofed IP source addresses into either the service provider or customer network
Remotely Triggered Black Holing (RTBH)	▪ 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
QoS Tools	▪ Protects against flooding attacks by defining QoS policies to limit bandwidth or drop offending traffic (identify, classify, and rate limit)
Control Plane	**Function and Benefit**
Receive ACLs	▪ Control the type of traffic that can be forwarded to the processor
Control Plane Policing	▪ Provides QoS control for packets destined to the control plane of the routers ▪ Ensures adequate bandwidth for high-priority traffic such as routing protocols
Routing Protection	▪ MD5 neighbor authentication protects routing domain from spoofing attacks ▪ Redistribution protection safeguards network from excessive conditions ▪ Overload protection (e.g., prefix limits) enhances routing stability
Management Plane	**Function and Benefit**
CPU and Memory Thresholding	▪ Protects CPU and memory of Cisco® IOS® Software device against DoS attacks
Dual Export Syslog	▪ Syslog exported to dual collectors for increased availability

Integrated Threat Control Summary

- Safeguard the remote LAN and servers from attacks
  - Advanced firewall, IPS, flexible packet matching (FPM)
- Defend against worms and keep the WAN clean
  - IPS, FPM, NAC, 802.1x
- Protect the router itself from hacking and DoS attacks
  - One-touch router lockdown, control plane protection, advanced firewall, IPS, FPM
- Integrated solution
  - Simplifies deployment and management (SDM, CSM, CS-MARS)
  - Minimizes cost of support and software subscription
- Cisco® Router Security can satisfy a majority of PCI compliance requirements
  - Now viable to deploy firewall and IPS at remote sites

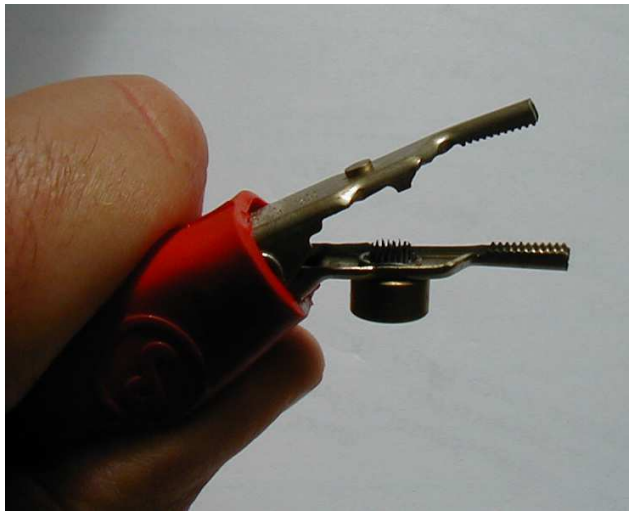


Secure Network Solutions



The Challenges of Securing IP Communications

- Traditional telephony threats remain in the converged world of IP Communications
  - Eavesdropping
  - Toll fraud
  - Denial of service
- Threats are now common to data and voice services
  - Loss of data confidentiality (finance data or voice call)
  - Denial of service (e-commerce site or telephony call signaling)
- Integrated security systems offer a cost-effective means of delivering secure IP Communications



Cisco IOS Firewall—Protection for Voice Signaling and Network Infrastructure

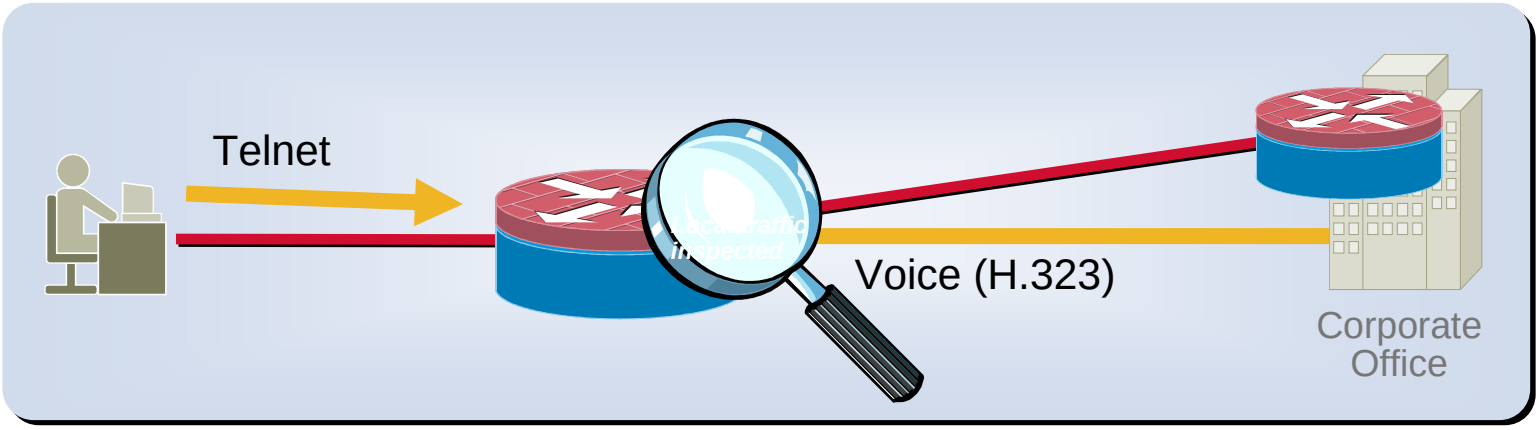
Protection against Hijacking and Denial of Service

- Cisco® IOS® Firewall inspects and controls traffic to and from the voice gateway services on the router

  Inspects single-channel management/control plane traffic and multichannel H.323 protocol connections to and from the router

  Provides security against voice connection hijacking while also performing protocol anomaly detection

  Inspects TCP and UDP channels to and from the router, dynamically opening pinholes on the interface ACL to allow return traffic

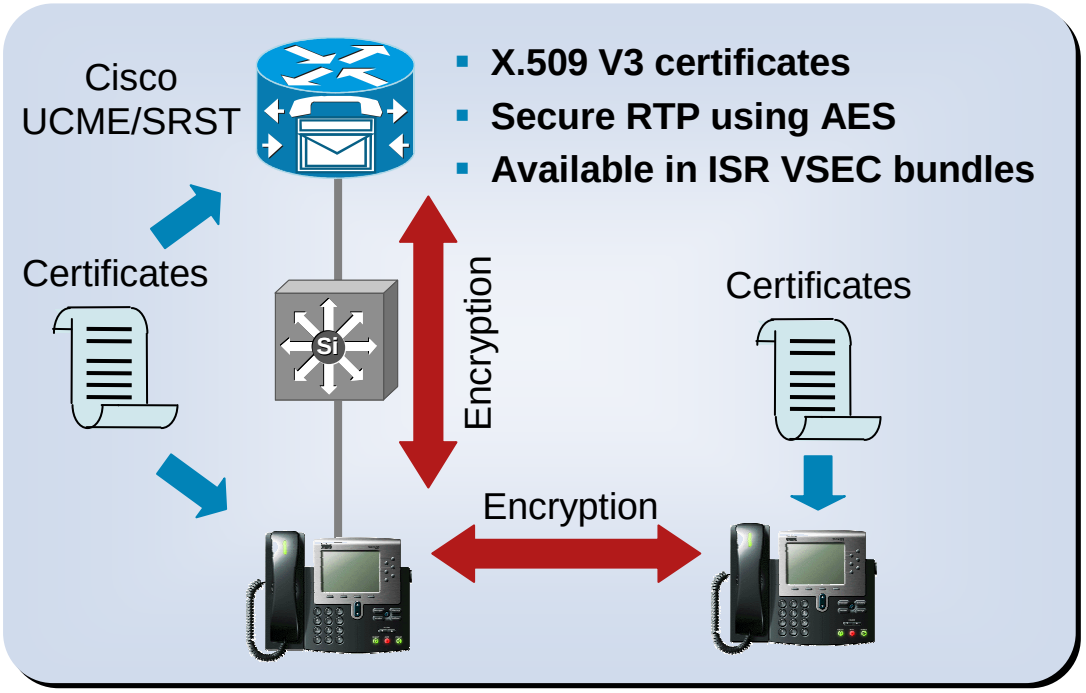


VoIP Endpoint Protection

Secure Voice

Business Problem

- "Defense in depth" for VoIP networks
- Protect the firmware and configuration files of phones
- Encrypt voice conversations on IP phones (SIP and SCCP), and analog phones



Encrypted VoIP Endpoints

- Conversations between Cisco IP phones or analog phones are protected using secure RTP (SIP and SCCP phones)

Authenticated VoIP Endpoints

- X.509 v.3 certificates in phones, Cisco® CallManager, CallManager Express, and SRST
- Certificates ensure reliable device authentication
- Encrypted voice calls using secure RTP

Signed Firmware Images

- Unique signature for each phone model

Signed and Encrypted Config Files

- Phone configuration protected from unauthorized changes

PCI Applies to Nearly Every Industry

Compliance

Utilities

Two Main Themes of Compliance

- The entity must protect the confidentiality, integrity and availability of information
- This protection must occur while the information is residing on devices and in transit

Steps for Compromised Entities

- Shut down access to data
- Contain and limit exposure
- Alert law enforcement, FBI, Card companies, etc.
- Provide account numbers to card brands within 24 hours
- Complete an incident report to card brands
- Complete an independent forensics review, vulnerability scan, and compliance questionnaire

Leverage the Existing Network

Reduce Capital and Operational Expenses Dramatically

- Use ISR as a WAN router plus firewall, IPS, VPN, VoIP call manager, wireless...
- Use CSA for virus, worm, day-zero protection

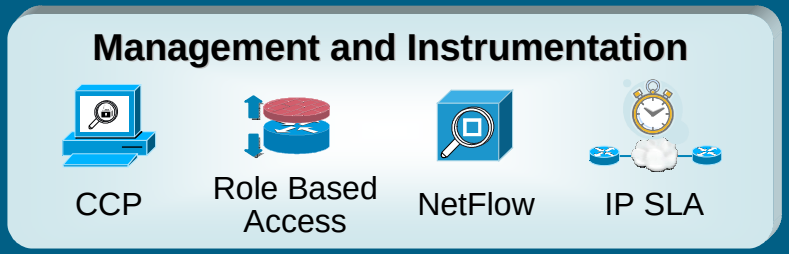
  Data-theft prevention, planned patch-management process, protection against unauthorized access and use
- Use CS-MARS for monitoring, analysis, and response

  Efficient reporting for compliance and management improvement

Cisco® Self-Defending Network—Comprehensive, End-to-End Solution

- Cost-effective
- Enables new business initiatives
- Increases employee productivity
- Improves customer satisfaction
- Addresses PCI compliance

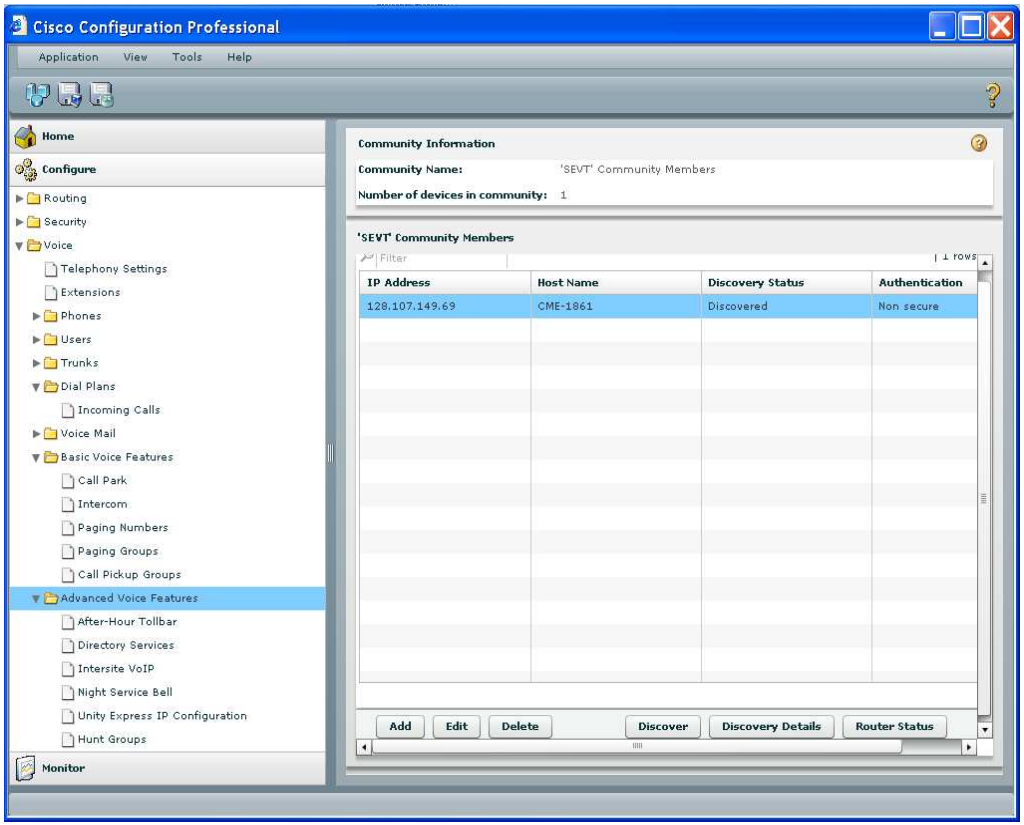
Management and Instrumentation



Cisco Configuration Professional

- Unified GUI
  - Routing
  - Security
  - Unified Communications
- Wizard led configuration
  - LAN, WLAN, and WAN
  - Firewall, IPS, and VPN
  - QoS, ACLs
- Voice Gateway, SRST or CME Configuration

Free Download:
http://www.cisco.com/go/ciscocp



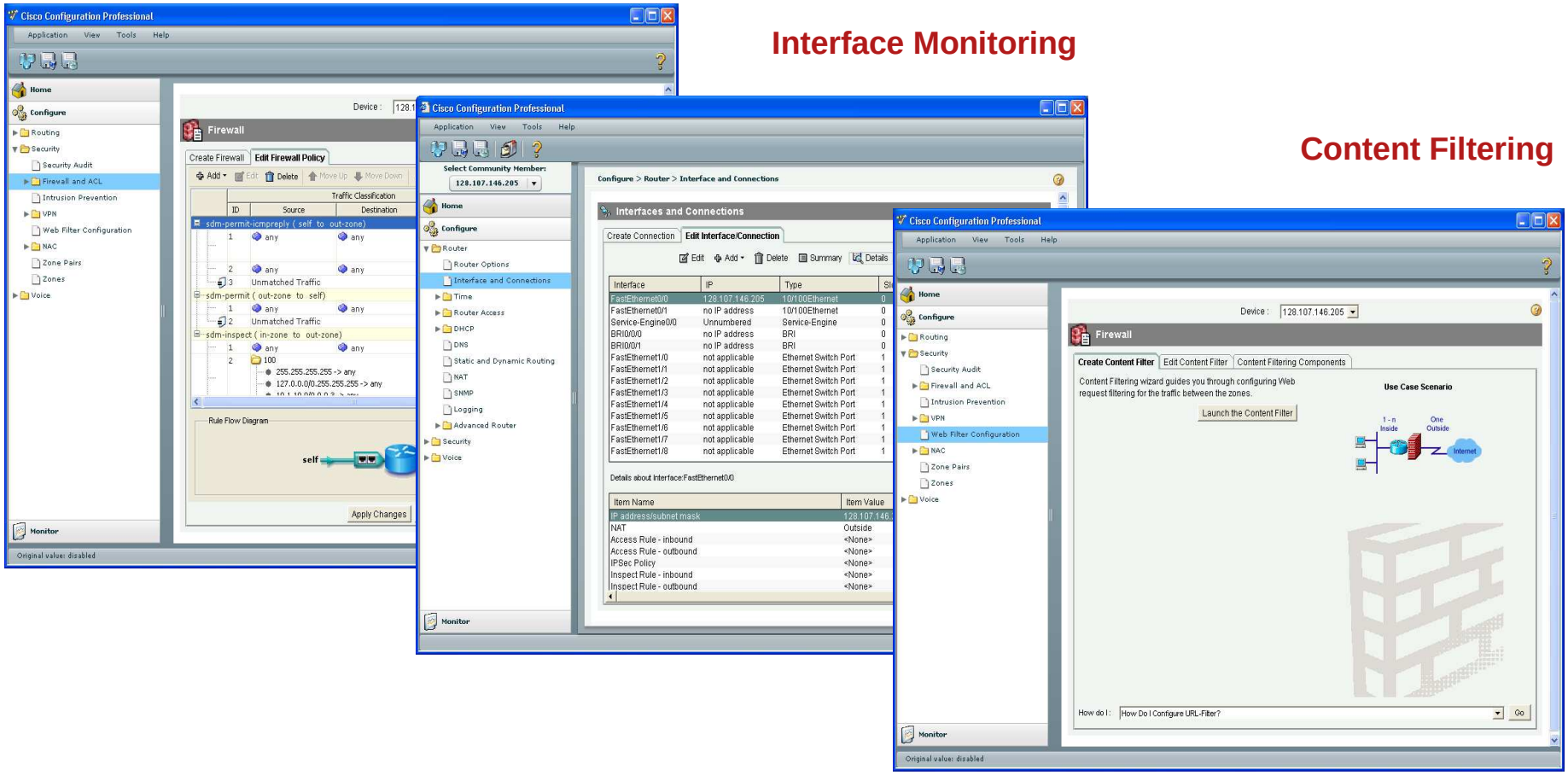
Cisco CCP:
Extensive Application Intelligence

CCP

Zone Based Firewall

Interface Monitoring

Content Filtering



Cisco IOS – Industry Leadership in Instrumentation

- Your network management system is only as good as the data you can get from the devices in the network
- For example, NetFlow and IPS feed into CS-MARS, delivering superior monitoring

Cisco® IOS® Instrumentation Feature	Value to Network Manager
NBAR	Network performance data (latency and jitter)
NetFlow	Detailed statistics for all data flows in the network
Role-based CLI access	Provides partitioned, nonhierarchical access (e.g., network and security operations)
SNMP V3 and SNMP informs	Reliable traps using SNMP informs
Syslog manager and XML-formatted syslog	Total flexibility to parse and control syslog messages on the router itself
TCL scripting and Kron (Cron) jobs	Flexible, programmatic control of the router

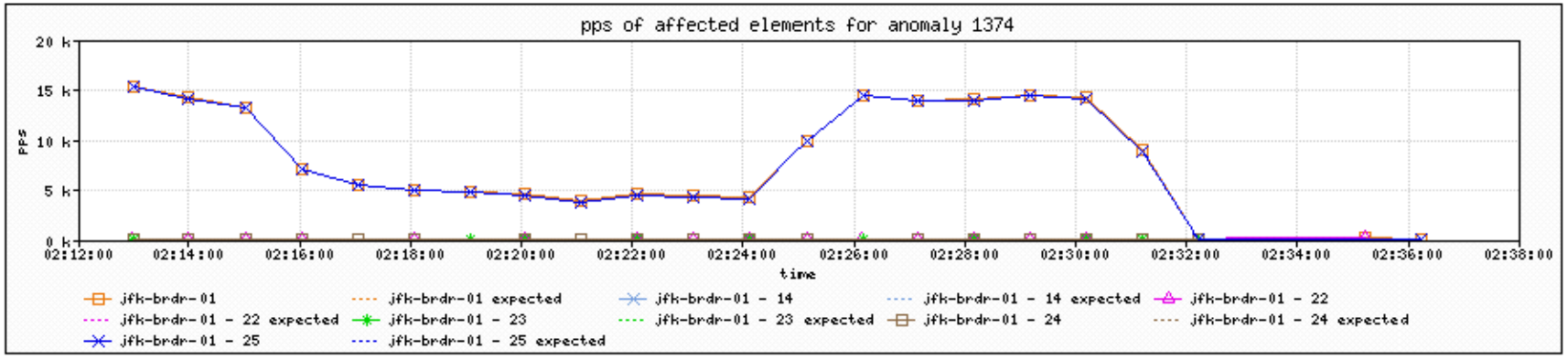
NetFlow Day-Zero Attack Detection

NetFlow

- Monitor traffic for anomalies
- Identify and classify the attack
- Trace attack to its source

Cisco® IT prevented SQL slammer at Cisco, watching flows per port

ID	Importance	Severity	Duration	Direction	Resource	Start Time	End Time	Class	Subclass	Acti
1374	High	1,540.0% of 1.00 Kpps	0h 25m 15s	Incoming	QWEST_BACKBONE 205.171.0.0/16 QWEST_BACKBONE	02:11:00 GMT 15 Dec 2002	02:36:15 GMT 15 Dec 2002	Profiled	UDP Protocol Anomaly	Repo



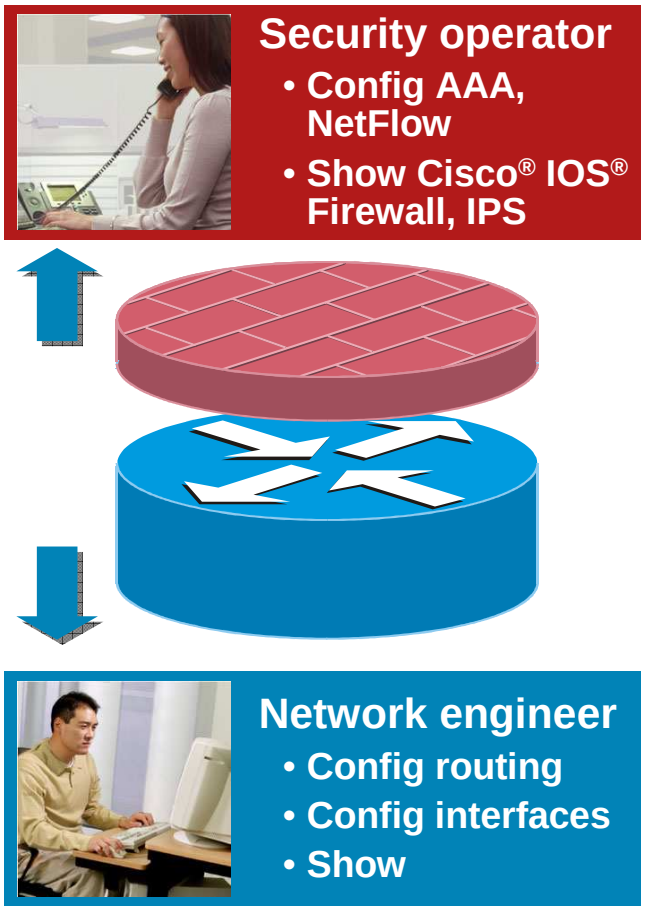
Role-Based CLI Access

- Provide a view-based access to CLI commands

  View: Set of operational commands and configuration capabilities

- User authentication is done via an external or internal AAA server (or TACACS+)
- Customer can define up to 15 views, plus one reserved for the root user

Customized Access to Match Operational Needs

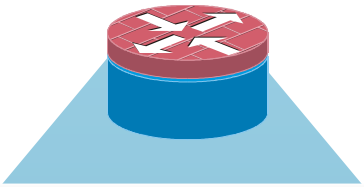


Cisco IOS Secure Device Operation

Cisco® IOS® Security Feature	Function and Benefit
Encrypted web access	▪ Web-based device management (SDM) access encrypted with HTTPS
Encrypted CLI access	▪ Telnet CLI and HTTPS secured with SSHv2 and SSL encryption
Secure management access	▪ SNMPv3 allows secure management using off-the-shelf and custom applications ▪ Cisco IOS supports DES and AES encryption ▪ SANS Institute recently rated the highest network security concern after basic concerns like password
Public key infrastructure (PKI)	▪ Provides advanced security when compared with traditional preshared keys ▪ Removes the danger of preshared keys falling into the wrong hands
Secure RSA private key	▪ Protects against routers being taken over: if the hacker attempts to change the configuration, the private key is erased, rendering the router useless
Certificate server	▪ Lightweight certificate server provided within Cisco IOS to ease deployment
AAA integration	▪ Allows user or group-specific permissions to be stored conveniently in a AAA server
Security audit	▪ Provides audit trail of configuration changes
Role-based CLI access	▪ Allows separate sets of commands and levels of access ▪ Policy making separated from ongoing operations, providing accountability
Configuration and event logging	▪ Logs configuration changes on per-user and per-session basis, ensuring reliable logging ▪ More visibility and accountability, greater confidence in reporting mechanism

Summary

Only Cisco Router Security Delivers All This



Secure Network Solutions

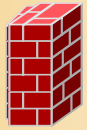
Business Continuity

Secure Voice

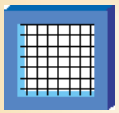
Secure Mobility

Compliance

Integrated Threat Management



Advanced Firewall



Content Filtering

Intrusion Prevention

Flexible Packet Matching

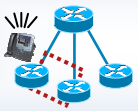
Network Admission Control

802.1x

Network Foundation Protection

Secure Connectivity

GET VPN



DMVPN

Easy VPN

SSL VPN

Management and Instrumentation

CCP

Role-Based Access

NetFlow

IP SLA

Summary

- Cisco® Router Security deliver defense-in-depth network protection
- Solutions for enterprise network security requirements

www.cisco.com/go/routersecurity