



# Cisco Router Security Solutions



## Technical Overview

# Cisco Router Security Portfolio

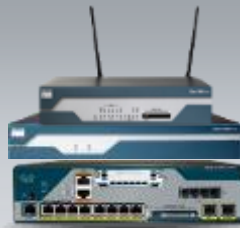
Performance and Services Density

**Service Integration  
Scaled to Fit Every Size Branch Office**

800 Series



1800 Series



2800 Series



3200 Series



Rugged and  
Mobile  
Applications

3800 Series



High  
Density and  
Performance for  
Concurrent  
Services

Embedded, Advanced Voice, Video,  
Data, and Security Services

Embedded Wireless, Security, and Data

Small Office and  
Teleworker

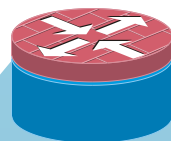
Small Branch

Medium  
Branch

Mobile/Rugged  
Branch

Medium to  
Large Branch

# Only Cisco Router Security Delivers All This



## Secure Network Solutions



Business  
Continuity



Secure  
Voice



Secure  
Mobility

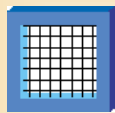


Compliance

## 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

# 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](https://cisco.com/go/securitycert)



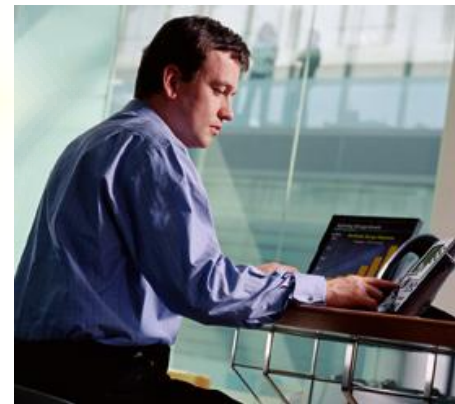
# Cisco Router Security

## Leadership in Innovation

Industry  
First

### Cisco Integrated Services Router Innovations in Security

- Industry-leading integration of VPN, routing, and QoS: DMVPN, GET VPN, SSL VPN, and Easy VPN
- Router-embedded security services: Application firewall, IPS, and URL filtering
- Cisco® Configuration Professional (CCP) with one-touch lockdown and security audit
- Router-integrated voice and security
- Router-integrated wireless with advanced security
- Router-integrated switching; Layer 2/3 security
- Secure WAN backup over DSL, cable, 3G, or satellite



# 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

# Cisco 800–3800 Security Router Bundles

## High Performance Voice and Security (HVSEC)

- Security
- Voice DSPs and Voice Gateway
- High Performance IPsec Acceleration and Compression
- Cisco CallManager Express / Survivable Remote Site Telephony License

## High Performance Security (HSEC)

- Security
- No Voice DSPs
- High Performance IPsec Acceleration and Compression

## Secure Voice (VSEC)<sup>† ‡</sup>

- Security
- Voice DSPs and Gateway
- Embedded IPsec Acceleration

## Basic Security (SEC)

- Security
- No Voice DSPs
- Embedded IPsec Acceleration

### All Security Bundles have:

- Site-to-Site VPN and Remote Access VPN
- Embedded IPsec acceleration
- SSL VPN\*
- ICSA & EAL4 certified Advanced Firewall
- IPS
- SDM, NetFlow
- WAN Backup, Router Availability and Service Protection

<sup>†</sup> Survivable Remote Site Telephony (SRST) version available

<sup>‡</sup> Cisco CallManager Express (CCME) version available

\* 10-25 user license included free on HSEC; additional licenses \$30 per user

# Integrated Threat Control

## Integrated Threat Control



Advanced Firewall



Content Filtering



Intrusion Prevention



Flexible Packet Matching



Network Admission Control



802.1x

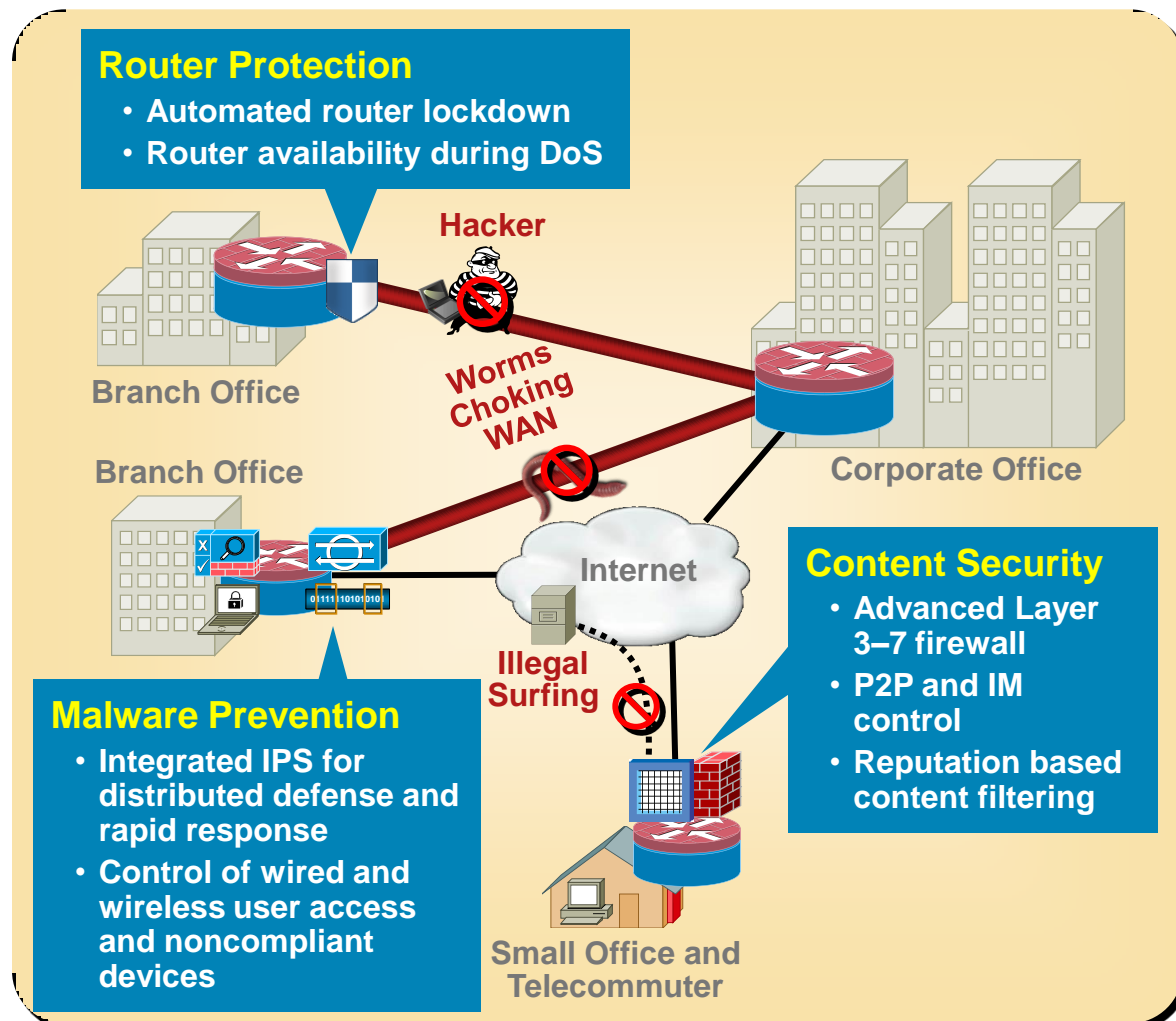


Network Foundation Protection

# 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 SDM and CSM

**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, CitrixImaClient
- Multimedia: Apple, RealAudio
- IPsec VPN: GDOI, ISAKMP
- Microsoft: MSSQL, NetBIOS
- Tunneling: L2TP, PPTP

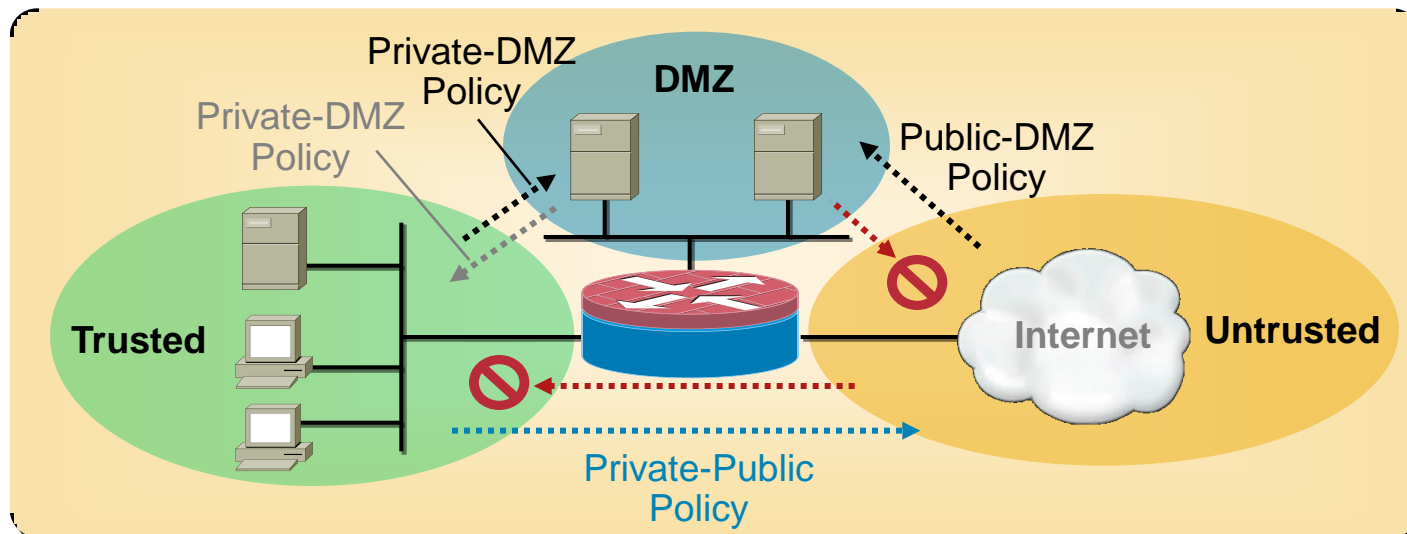


# Zone-Based Policy Firewall

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



# Application Inspection and Control

- Multichannel inspection
  - Recognizes application-specific protocols including control and data channels
  - Detects and prevents application-level attacks
- Protocol conformance

Checks varying levels depending on the specific protocol
- Protocol control

Granular enforcement for HTTP and P2P

For example, permit PUTs but deny GETs

## Cisco IOS Firewall-Recognized Application-Layer Protocols

- CU-SeeMe (cuseeme)
- FTP (ftp)
- Java (http)
- H.323 (h323)
- Microsoft NetShow (netshow)
- RealAudio (realaudio)
- Remote-procedure call (rpc)
- Session Initiation Protocol (sip)
- Skinny Client Control Protocol (skinny)
- Simple Mail Transfer Protocol (smtp/esmtp)
- StreamWorks (streamworks)
- Structured Query Language\*Net (sqlnet)
- TFTP (tftp)
- UNIX R commands (rcmd)
- VDOLive (vdolive)
- POP3 and IMAP (pop3 and imap)
- Application Firewall (appfw)
- UserDefined (user defined name)



# Cisco IOS Firewall Voice Features

Protocol	Supported	Comments
<b>H.323 V1 &amp; V2</b>	Yes	Tested using CME 4.0 Locally generated/terminated traffic supported
<b>H.323 V3 &amp; V4</b>	No	
<b>H.323 RAS</b>	Yes	In 12.4(11)T
<b>H.323 T.38 Fax</b>	No	
<b>SIP UDP</b>	Yes	CCM 4.2 supported RFC 2543, RFC 3261 not supported
<b>SIP TCP</b>	No	
<b>SCCP</b>	Yes	Tested with CCM 4.2/CME 4.0
<b>Locally generated traffic inspection for SIP/SCCP</b>	No	

Note: Cisco® ASA supports H.323 V3 and V4, T.38 Fax and SIP TCP

# 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]
```

- If DoS counters are not adjusted, users may see slow network performance and high router CPU
- 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 ICASA certified
- Facilitates PCI compliance
- Now available with Cisco IOS 12.4(11)T2

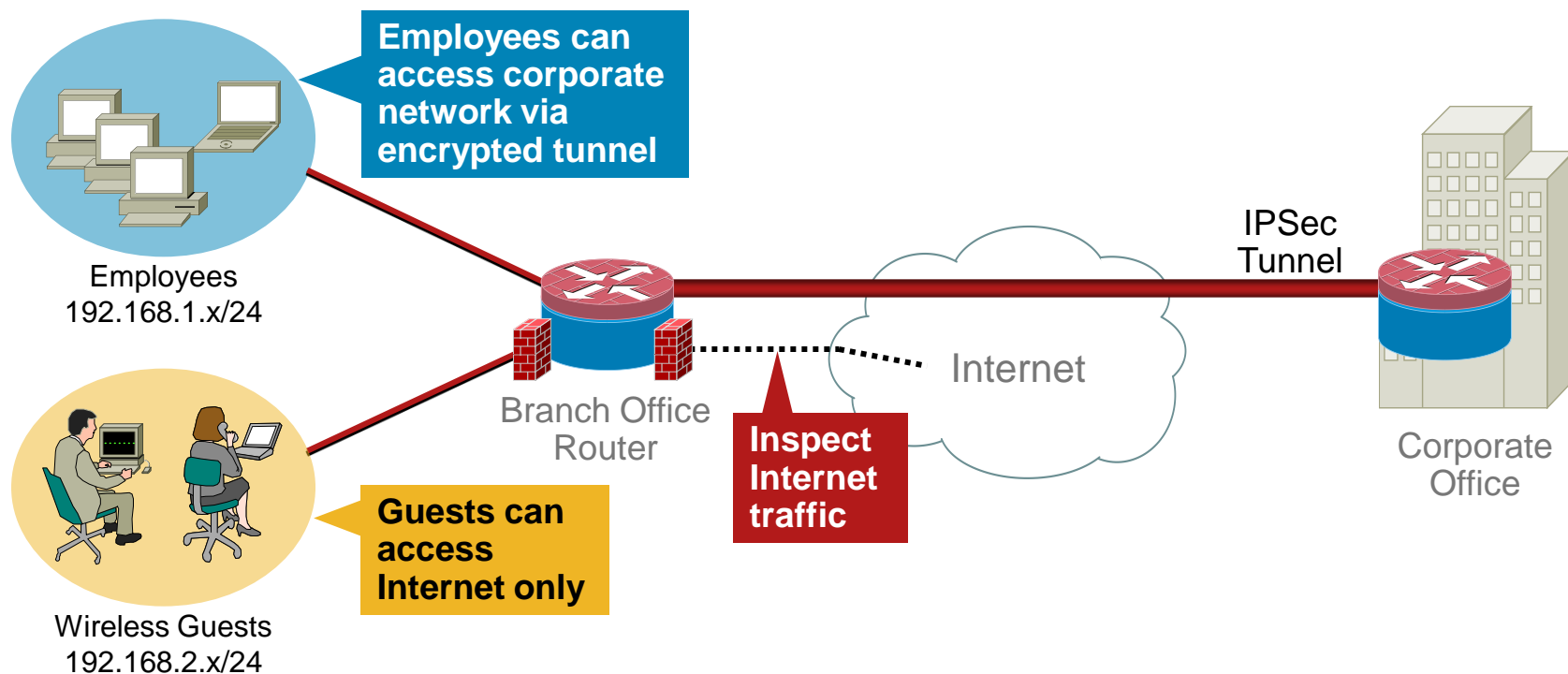
Firewall Features	Cisco ISR with WAAS	Most Competitors
Stateful Inspection	For all traffic	Tunnel traffic only
IP ACLs	✓	—
NAT	✓	—
Authentication Proxy	✓	—
No Static Open Ports	✓	—
Granular Per Session Policy	✓	—
QoS Policy	✓	—

# Cisco IOS Firewall Use Case 1

## Protect the LAN at Branch with Split Tunneling

Cisco® IOS® Firewall policies:

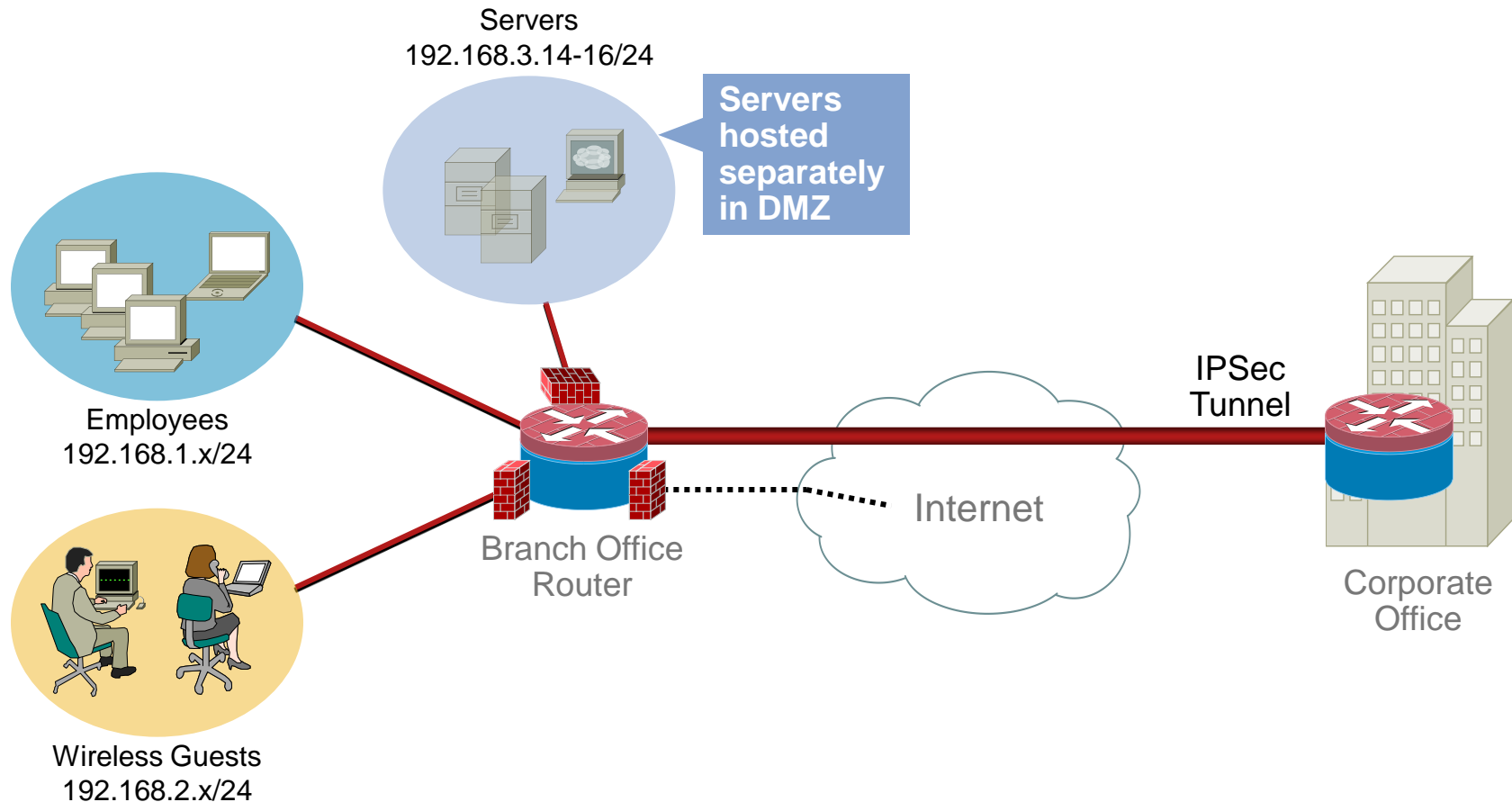
- Allow authenticated users to access corporate resources
- Restrict guest users to Internet access only
- Control peer-to-peer and instant messaging applications



# Cisco IOS Firewall Use Case 2

## Protect Servers at Remote Sites

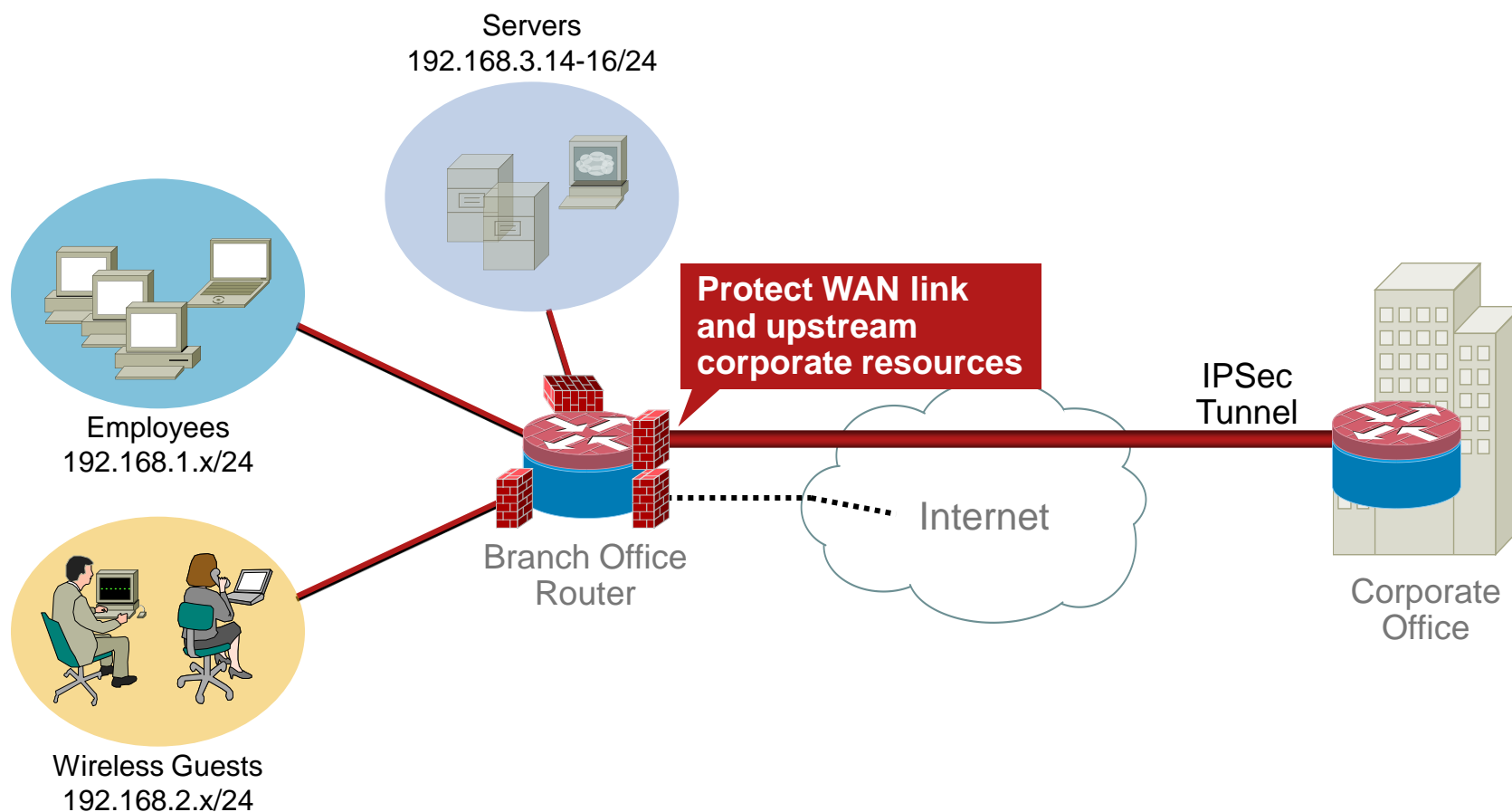
- Cisco® IOS® Firewall policies applied to DMZ protect distributed application servers and Web servers hosted at remote sites



# Cisco IOS Firewall Use Case 3

## Protect WAN Link and Corporate Office

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

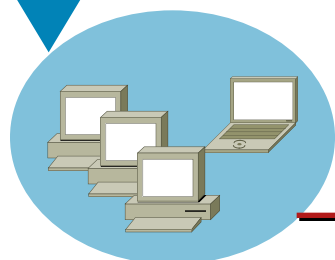


# Cisco IOS Firewall Use Case 4

## Transparent Firewall and IPS

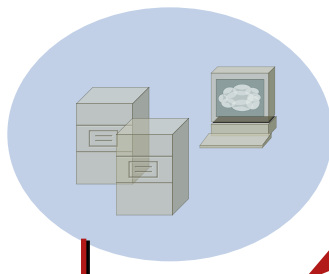
- Cisco® IOS® transparent firewall policies at bridge interfaces enforce inspection and control of LAN traffic
- Simplifies firewall and IPS deployment at small offices running key applications in a single address space

No change to statically addressed devices



Contractors  
192.168.1.13/24

Servers  
192.168.1.14-16/24

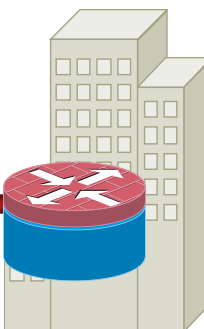


Supports DHCP pass through to assign DHCP addresses on opposite interfaces

Branch Office Router

IPSec Tunnel

Internet



Corporate Office

Restricts access to specified devices on a subnet

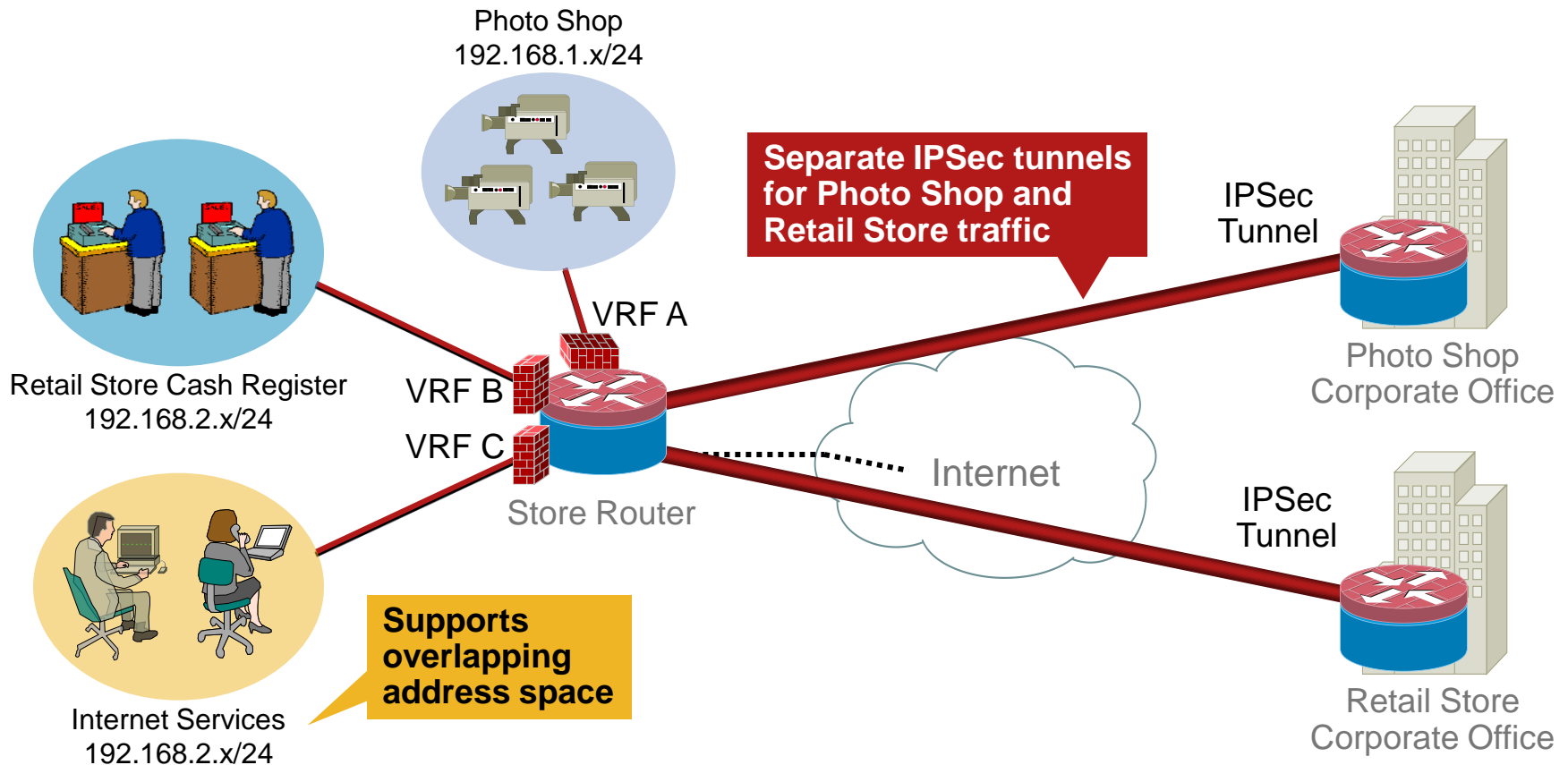


Wireless Guests  
192.168.1.12/24

# Cisco IOS Firewall Use Case 5

## 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



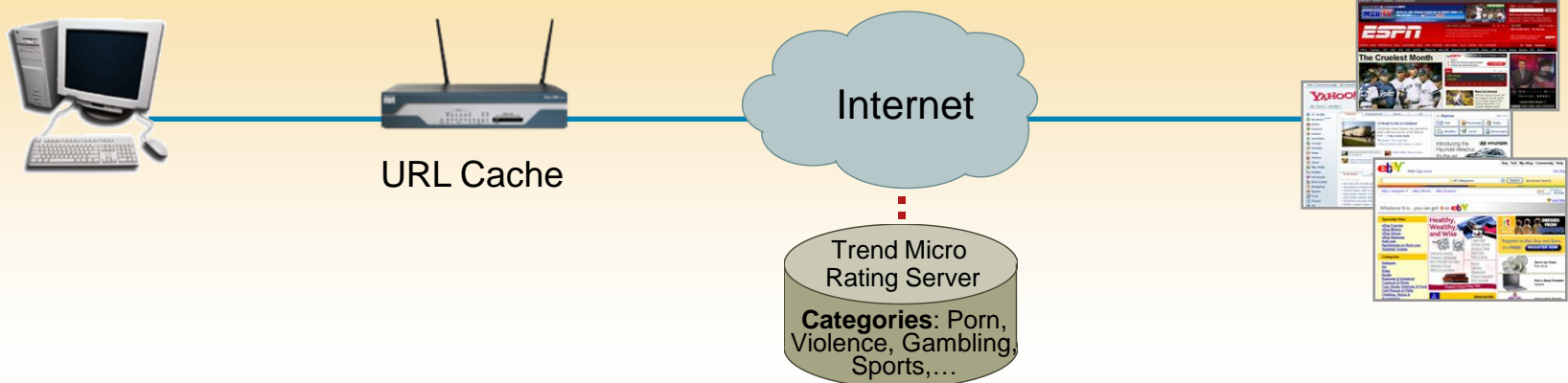


# Cisco IOS® Content Filtering with Trend Micro



## 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



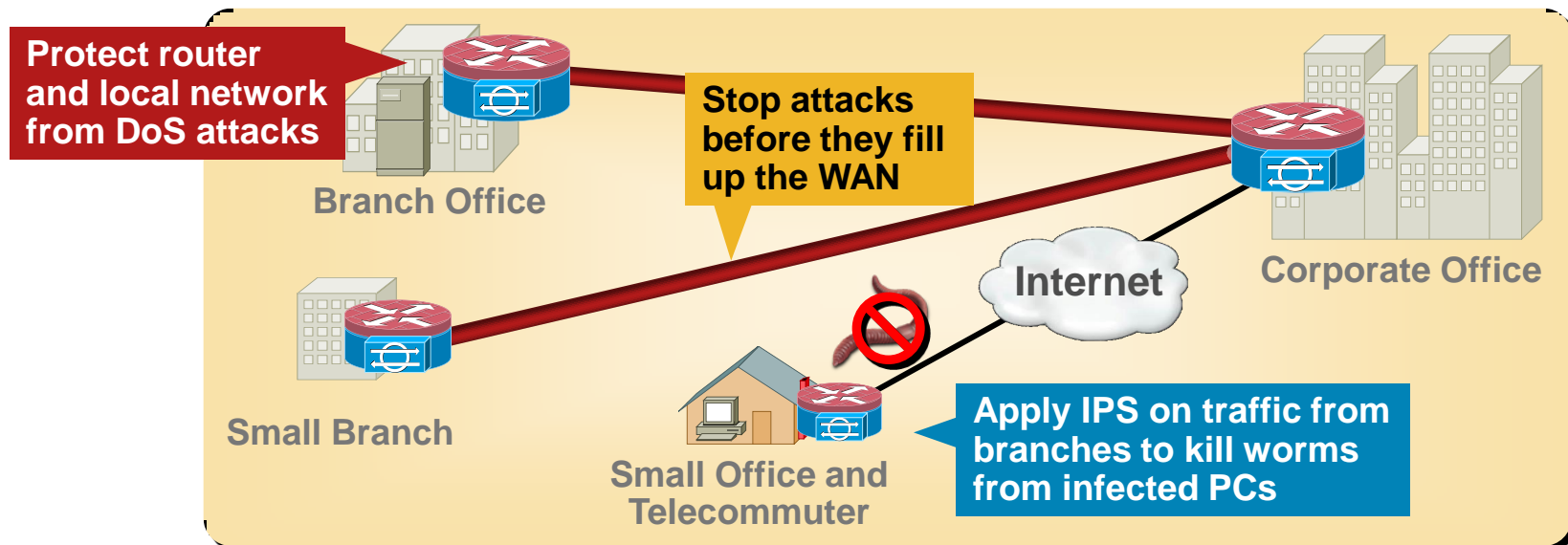


IPS

# Cisco IOS Intrusion Prevention (IPS)

## Distributed Defense Against Worms and Viruses

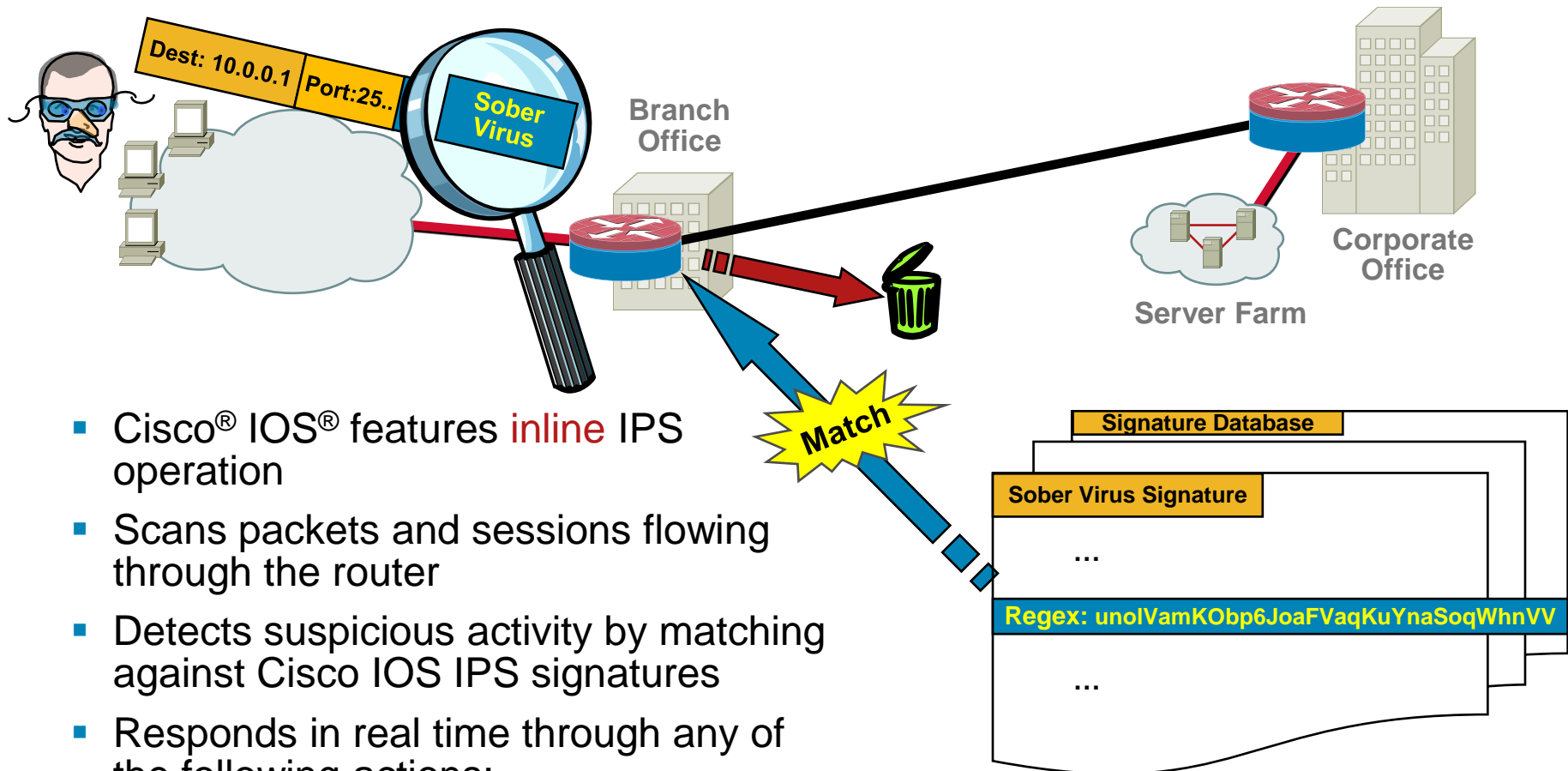
- Cisco® IOS® IPS stops attacks at the entry point, conserves WAN bandwidth, and protects the router and remote network from DoS attacks
- Integrated form factor makes it cost-effective and viable to deploy IPS in small and medium business and enterprise branch/telecommuter sites
- Supports a fully customizable 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





IPS

# Cisco IOS IPS Overview



- 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



IPS

NEW



## NME-IPS-K9

Cisco 2811, 2821,  
2851, 3800



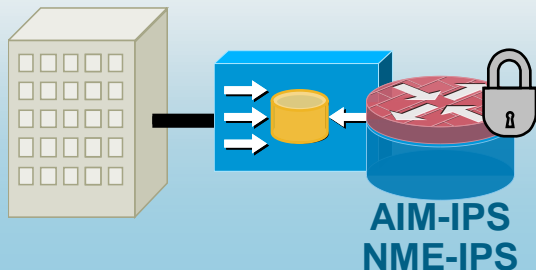
## AIM-IPS-K9

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



IPS

# 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



IPS

# 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.



IPS

# Latest Improvements in Cisco IOS IPS

Cisco IOS 12.4(11)T2 & later

Customer Pain Points	Features	Benefits
<b>Quick Response</b> <ul style="list-style-type: none"><li>Reduce timeline from vulnerability to signature deployment</li></ul>	<ul style="list-style-type: none"><li>NDA (encrypted) signature support and native support for MSRPC and Microsoft SMB signatures</li><li>Automated signature updates from a local TFTP or HTTP(S) server</li></ul>	<ul style="list-style-type: none"><li>Efficient protection against many new Microsoft and other vulnerabilities, some even before their public release</li><li>Protection from latest threats with minimal user intervention</li></ul>
<b>Improved Accuracy</b> <ul style="list-style-type: none"><li>Reduced false positives</li></ul>	<ul style="list-style-type: none"><li>Risk Rating value in IPS alarms based on signature severity, fidelity, and target value rating</li><li>Supports Signature Event Action Processor (SEAP)</li></ul>	<ul style="list-style-type: none"><li>Enables accurate and efficient IPS event correlation and monitoring</li><li>Quick and automated adjustment of signature event actions based on Risk Rating</li></ul>
<b>Manageability</b> <ul style="list-style-type: none"><li>Unauthorized wireless access</li></ul>	<ul style="list-style-type: none"><li>Individual and category-based signature provisioning through Cisco IOS CLI</li><li>IDCONF (XML) signature provisioning mechanism</li></ul>	<ul style="list-style-type: none"><li>Offers granular customization and tuning of signatures through custom scripts</li><li>Secure provisioning through CSM 3.1 and Cisco SDM 2.4 over HTTPS</li></ul>
<b>Common Operations</b> <ul style="list-style-type: none"><li>HQ to Branch</li></ul>	<ul style="list-style-type: none"><li>Same signature format as the latest Cisco® IPS appliances and modules</li></ul>	<ul style="list-style-type: none"><li>Common operations for Cisco IPS appliances and Cisco IOS® IPS</li></ul>

# 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







IPS

# Cisco IOS IPS Provisioning and Monitoring

## Up to 5 Routers

### Provisioning

- Cisco IPS Manager Express (IME)

### Monitoring

## More than 5 Routers

### Provisioning

- Cisco Security Manager (CSM) OR
- Cisco SDM and Cisco Configuration Engine for deployments sharing the same signature set

### Monitoring

- Cisco Security MARS (Recommended) OR
- Syslog Servers



# Cisco IOS IPS Deployment Steps

## Step 1

Latest Cisco IPS signature package:

<http://www.cisco.com/cgi-bin/tablebuild.pl/ios-v5sigup>

- Contains digitally signed file with signatures for entire Cisco IPS product line

## Step 2

Select one of the two recommended signature categories:  
IOS-Basic or IOS-Advanced

## Step 3

Use Cisco IOS CLI or SDM 2.4 or CSM 3.1 to customize signature list:

- Select additional signatures as desired
- Delete signatures not relevant to the applications you are running
- Tune actions of individual signatures (e.g. add “drop” action)
- Test your custom signature set in lab setting before deployment

For details, see IOS IPS configuration guide at

[http://www.cisco.com/univercd/cc/td/doc/product/software/ios124/124newft/124t/124t11/ips\\_v5.htm](http://www.cisco.com/univercd/cc/td/doc/product/software/ios124/124newft/124t/124t11/ips_v5.htm)



# Migrating to 12.4(11)T2 or Later

- Option 1: Existing customer using **noncustomized** prebuilt signature files (SDFs)
  - No signature migration needed
  - Signatures in 128MB.sdf are in **IOS-Basic** category
  - Signatures in 256MB.sdf are in **IOS-Advanced** category
- Option 2: Existing customer using **customized** prebuilt signature files (SDFs)
  - Signature migration (TCL) script available on Cisco.com to convert customized SDF to 5.x format
  - This migration script does **not** migrate user-defined (non Cisco) signatures
- Detailed migration procedure and CLI changes will be documented at [www.cisco.com/go/iosips](http://www.cisco.com/go/iosips)

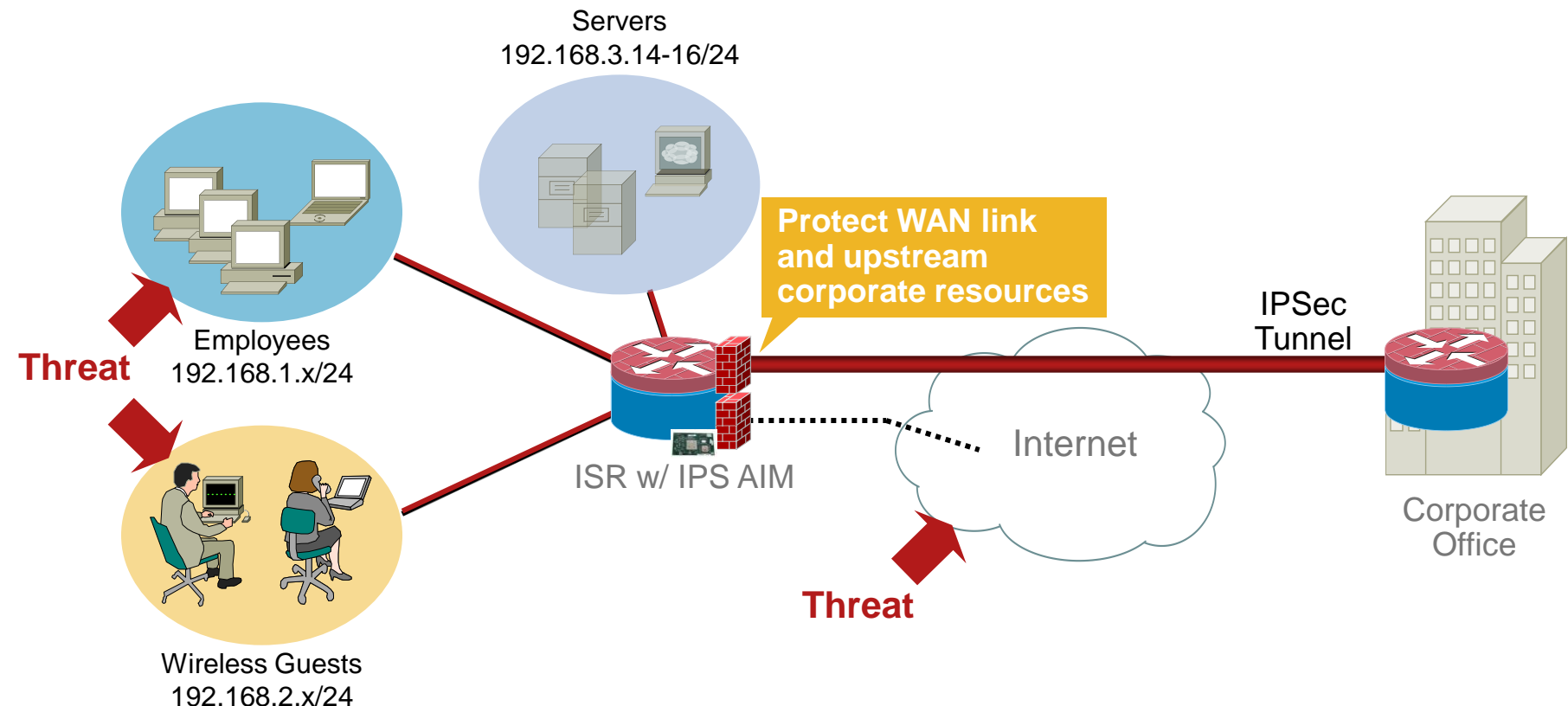


IPS

# Cisco IOS IPS Use Case 1

## 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



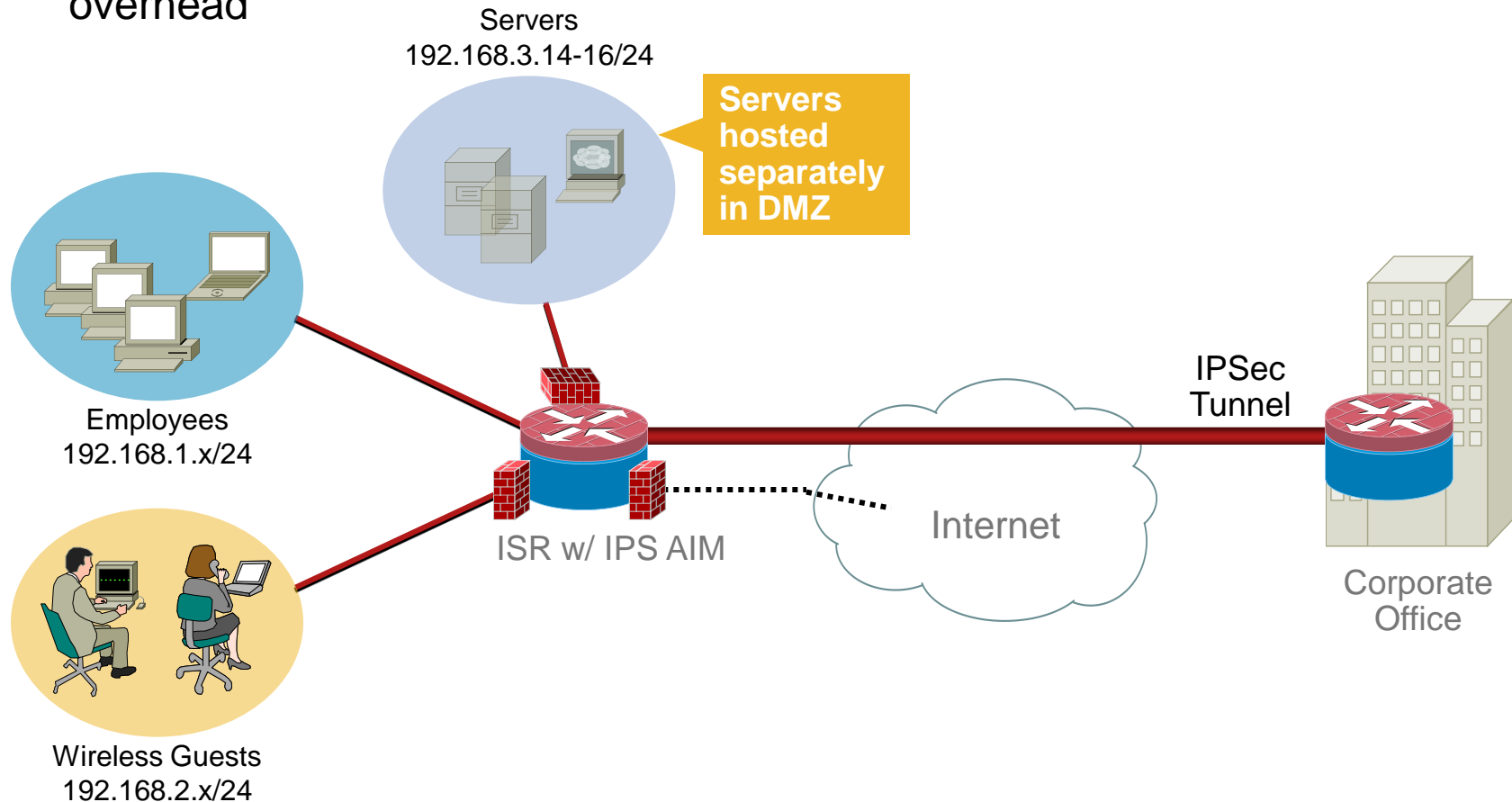


IPS

# 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

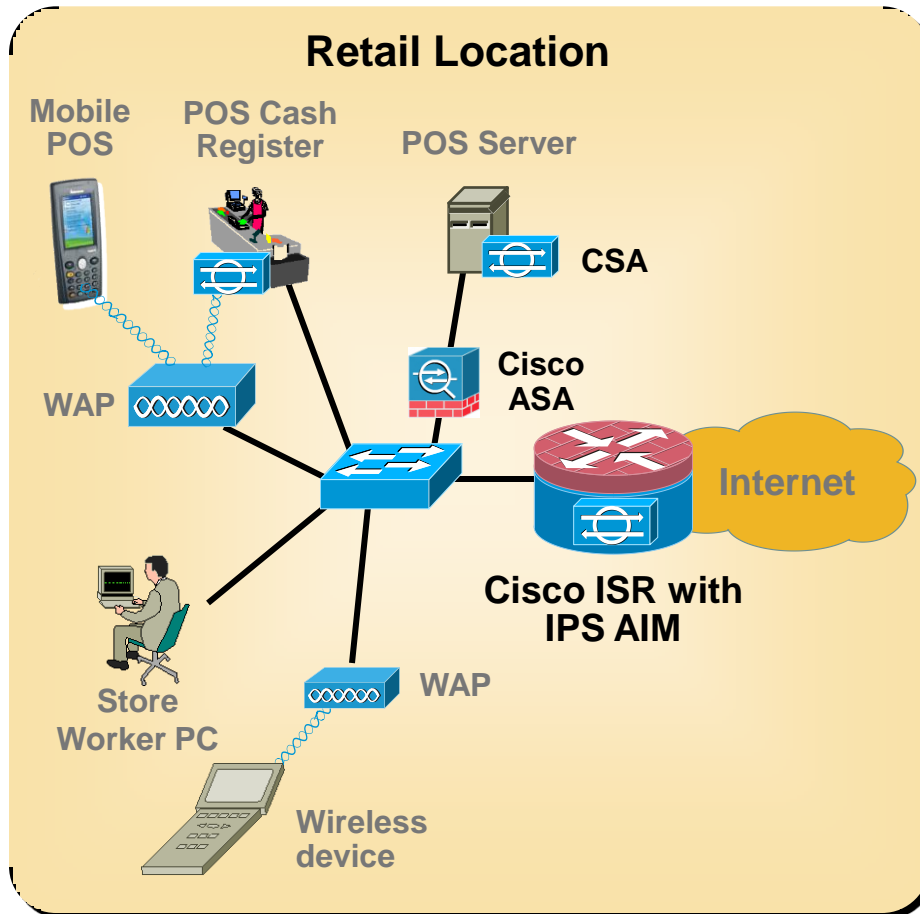




IPS

# 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



IPS

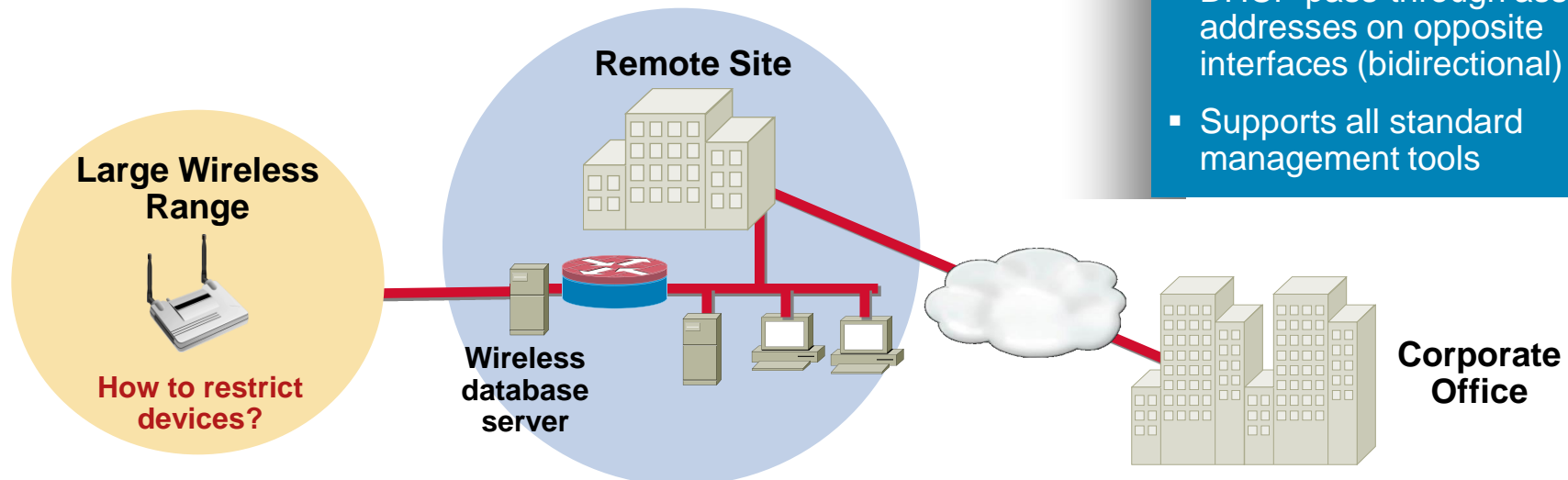
# Cisco IOS IPS Use Case 4

## Transparent IPS

- Provides Layer 2 connectivity with Layer 3 IPS support
- Easily add IPS to existing networks—  
**no IP subnet renumbering required**
- Operates on bridged packets; Layer 3 IPS continues to operate on routed packets

### Features Supported

- Sub-interfaces and VLAN trunks
- Spanning Tree protocol  
Handles PBDU packets correctly per 802.1d, not just “pass/drop”
- Mix Layer 2 and Layer 3 IPS on the same router
- No need for IP addresses on the interfaces
- DHCP pass-through assigns addresses on opposite interfaces (bidirectional)
- Supports all standard management tools

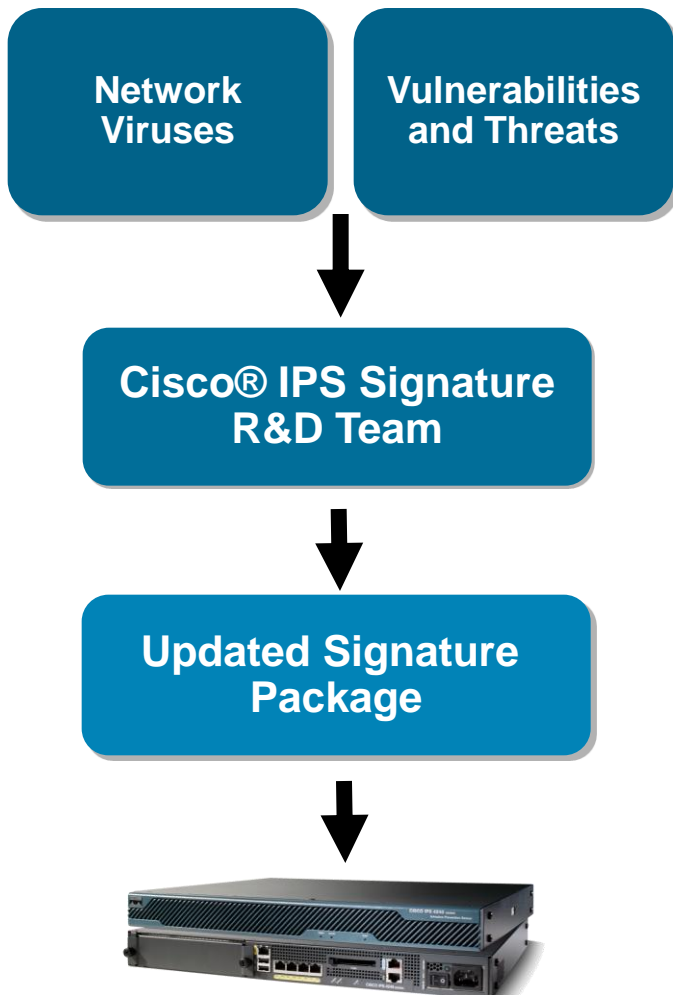




IPS

# Cisco Services for IPS

## Rapid Signature Updates for Emerging Threats



- Extensive 24-hour research capability gathers, identifies, and classifies vulnerabilities and threats
- Signatures are created to mitigate the vulnerabilities within hours of classification
- Signature updates are available to customers at [Cisco.com](http://Cisco.com)



# 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

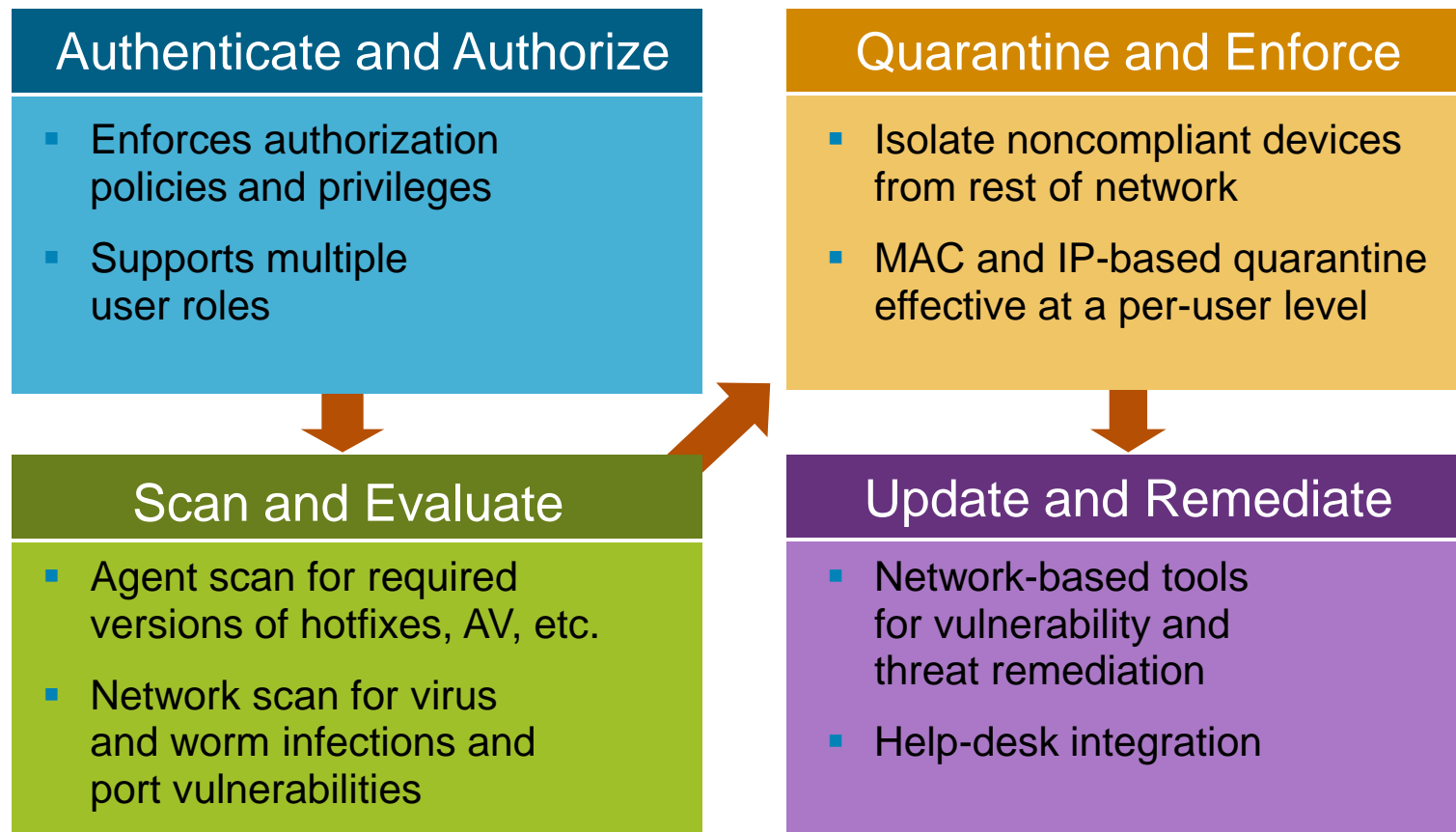
### Flexible Classification and Rapid Response

- 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 Network Admission Control

Using the *Network* to Enforce Policies Helps Ensure that Incoming Devices Are Compliant.



# Cisco NAC by the Numbers

**2000+**  
Customers

**47%**  
Market  
Share<sup>1</sup>

**No.1 NAC Vendor**  
Based on Network  
World Reader Survey<sup>3</sup>

**75%**  
of Infonetics Survey  
Respondents  
Ranked Cisco  
**No. 1** Among NAC  
Vendors<sup>1</sup>

**Gold Award:**  
Determined by  
Reader Survey<sup>2</sup>



 SearchNetworking.com

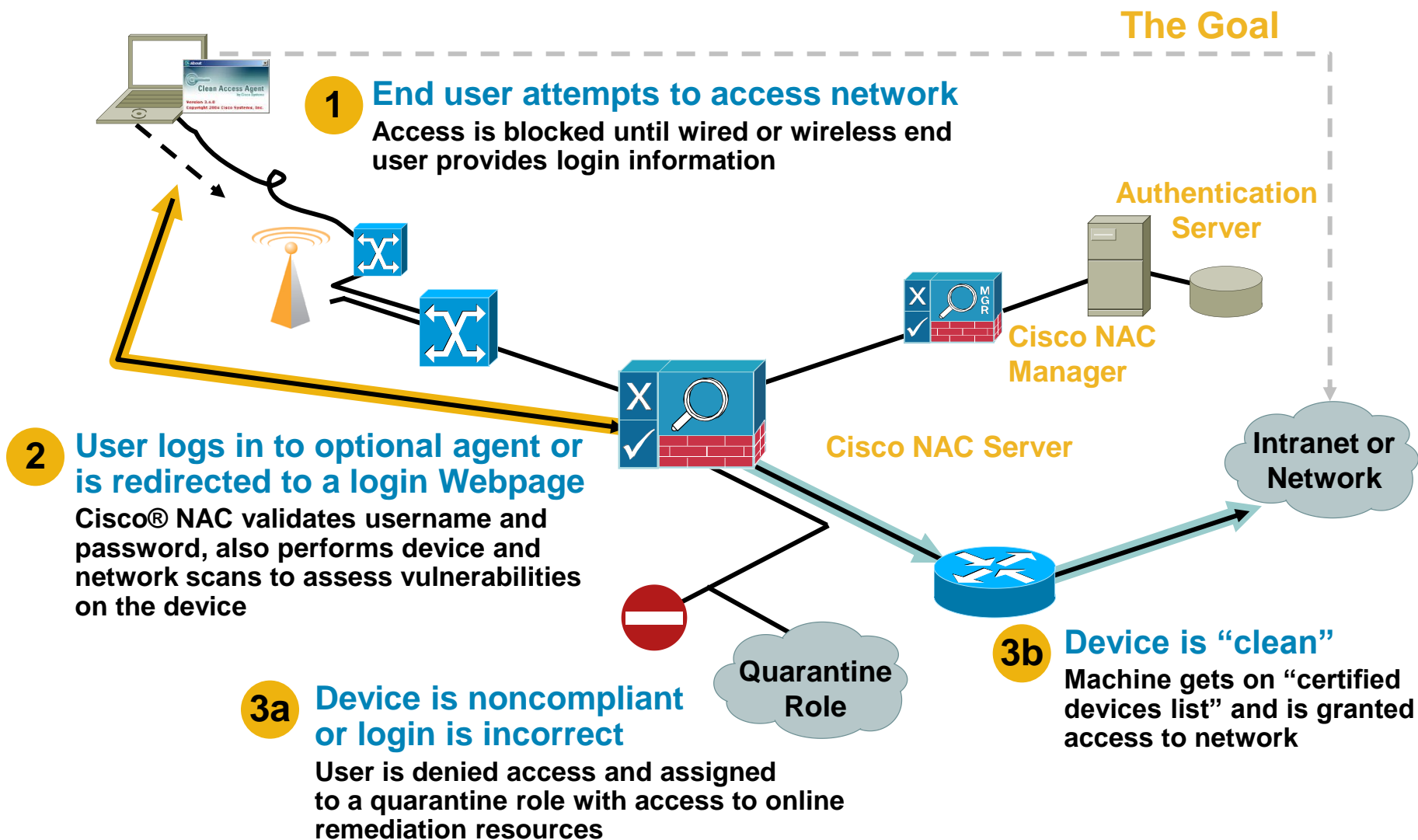


<sup>1</sup> Infonetics, May 2007

<sup>2</sup> March 2007 <http://searchnetworking.techtarget.com/productsOfTheYear/>

<sup>3</sup> May 2007 <http://www.networkcomputing.com/channels/security/showArticle.jhtml?articleID=199204304>

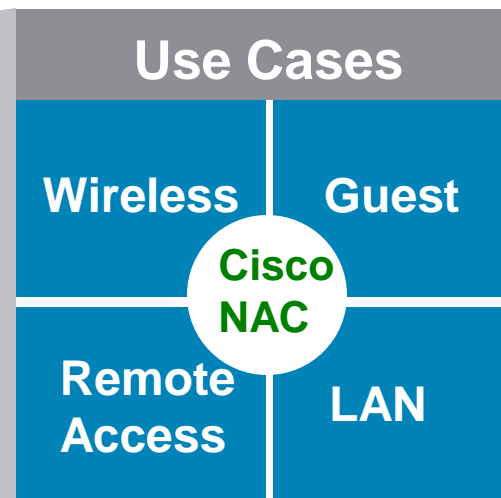
# Cisco NAC Appliance Flow



# Cisco NAC Network Module on Cisco Integrated Services Router



- Authentication and identity
- Security posture
- Enforcement
- Remediation



## Benefits:

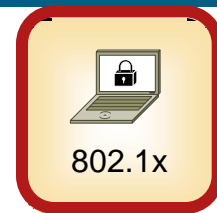
- **Pervasive security**  
One product for all use cases and locations
- **Consistent policy**  
One policy store for consistent application across entire organization
- **Transparent deployment**  
Integrated for easier deployment, troubleshooting, and management

# Cisco NAC: Any Combination Works

	Appliances (Overlay)	Cisco Integrated Services Router Network Module (Modular)
Primary use cases	Campus: Wired, wireless, remote, and guest access	Branch: Wired, wireless, remote, and guest access
Number of users	Increments of 100, 250, 500, 1500, and 2500 users per server	Increments of 50 or 100 per module
Policy store or management point	Cisco NAC Appliance Manager (manages both options)	
Deployment methods	Same deployment flexibility with Layer 2 or Layer 3, in-band or out-of-band, agent or agentless	
Form factor	Separate appliance	Fits into Cisco 2811, 2821, 2851, 3825, and 3845 Integrated Services Routers
High availability	Supported	Not supported

# Cisco IOS 802.1x

## Controlled Network Access



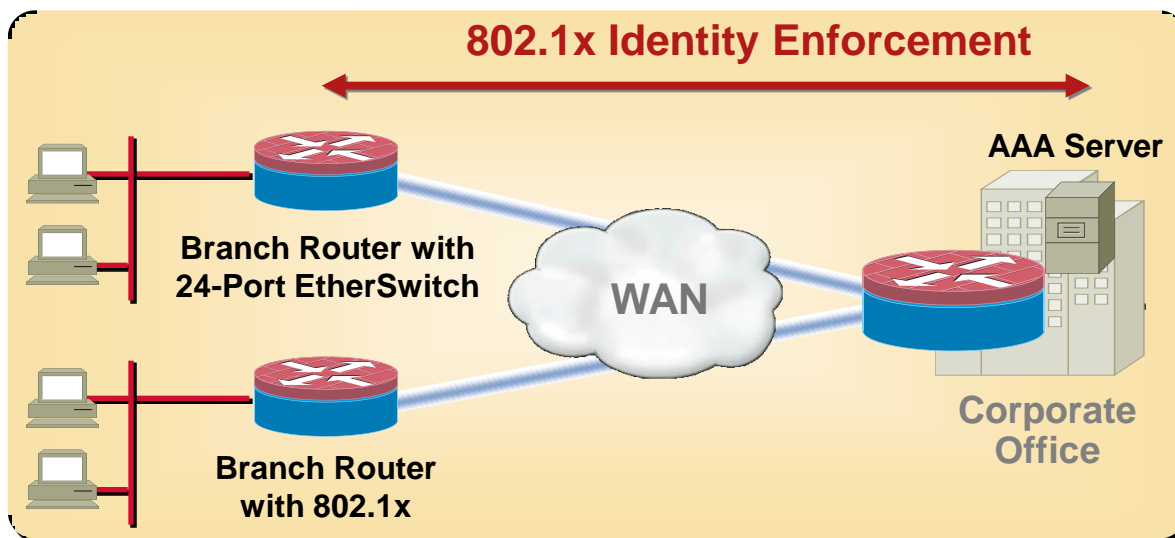
- New NME 16, 24, and 48-port EtherSwitch® modules support 802.1x authentication
  - Smaller port density HWIC4-9 supports only basic 802.1 authentication
- Controls who gets access to the network
  - 802.1x, ACL, port security, MAC address notify
- Secure management
  - RADIUS/TACAC+, SSH, SNMPv3
- Plus Power over Ethernet (POE) 802.3af

### Integrated Branch Switching



**NME-ESW**

**16-, 24-, and 48-Port  
10/100 EtherSwitch**





# Cisco IOS AutoSecure

## One-Touch Automated Router Lockdown

### Disables Nonessential Services

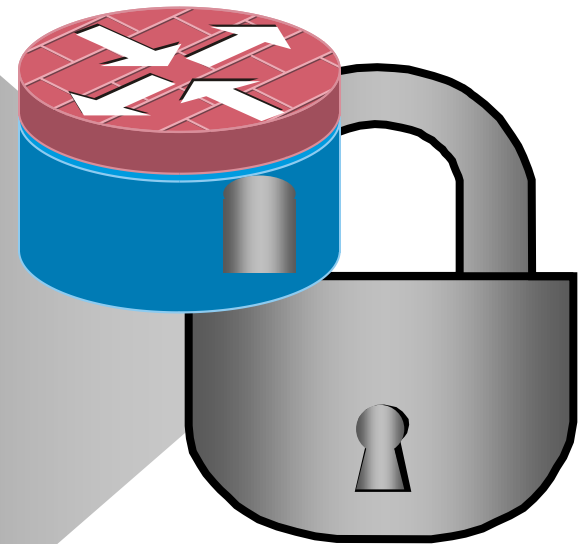
- Eliminates DoS attacks based on fake requests
- Disables mechanisms that could be used to exploit security holes

### 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

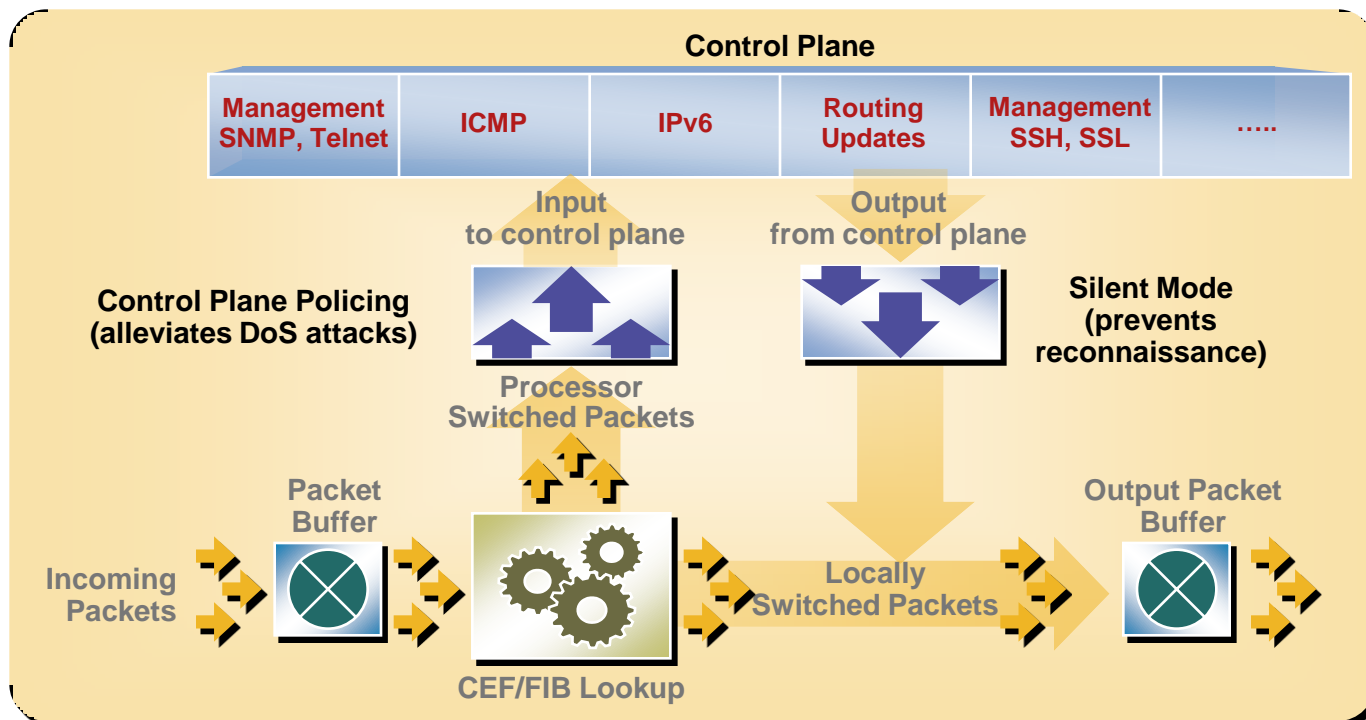




# Cisco IOS Control Plane Policing

## Continual Router Availability Under Duress

- Mitigates DoS attacks on control plane (route processor) such as ICMP floods
- Polices and throttles incoming traffic to control plane; maintains packet forwarding and protocol states during attacks or heavy traffic load

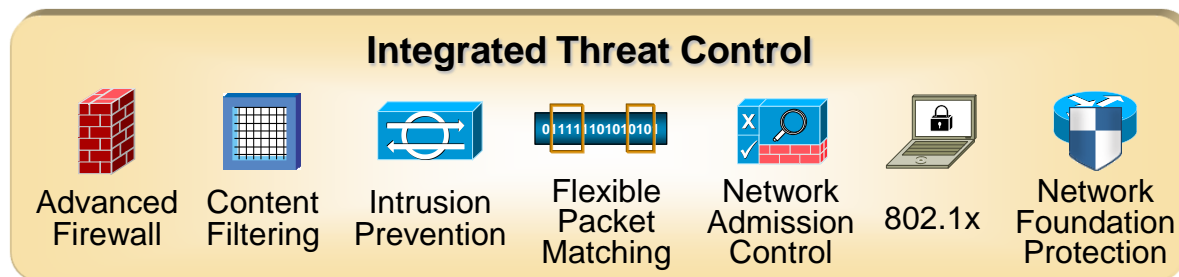


# Cisco Network Foundation Protection

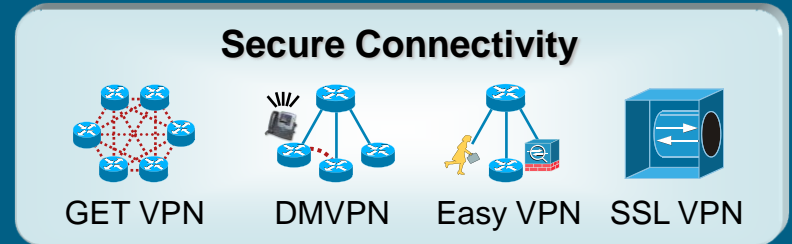
Data Plane Feature	Function and Benefit
<b>NetFlow</b>	<ul style="list-style-type: none"> <li>Macro-level, anomaly-based DDoS detection through counting the number of flows (instead of contents); provides rapid confirmation and isolation of attack</li> </ul>
<b>Access Control Lists (ACLs)</b>	<ul style="list-style-type: none"> <li>Protect edge routers from malicious traffic; explicitly permit the legitimate traffic that can be sent to the edge router's destination address</li> </ul>
<b>Flexible Packet Matching (FPM)</b>	<ul style="list-style-type: none"> <li>Next-generation "Super ACL"—pattern-matching capability for more granular and customized packet filters, minimizing inadvertent blocking of legitimate business traffic</li> </ul>
<b>Unicast Reverse Path Forwarding (uRPF)</b>	<ul style="list-style-type: none"> <li>Mitigates problems caused by the introduction of malformed or spoofed IP source addresses into either the service provider or customer network</li> </ul>
<b>Remotely Triggered Black Holing (RTBH)</b>	<ul style="list-style-type: none"> <li>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</li> </ul>
<b>QoS Tools</b>	<ul style="list-style-type: none"> <li>Protects against flooding attacks by defining QoS policies to limit bandwidth or drop offending traffic (identify, classify, and rate limit)</li> </ul>
Control Plane	Function and Benefit
<b>Receive ACLs</b>	<ul style="list-style-type: none"> <li>Control the type of traffic that can be forwarded to the processor</li> </ul>
<b>Control Plane Policing</b>	<ul style="list-style-type: none"> <li>Provides QoS control for packets destined to the control plane of the routers</li> <li>Ensures adequate bandwidth for high-priority traffic such as routing protocols</li> </ul>
<b>Routing Protection</b>	<ul style="list-style-type: none"> <li>MD5 neighbor authentication protects routing domain from spoofing attacks</li> <li>Redistribution protection safeguards network from excessive conditions</li> <li>Overload protection (e.g., prefix limits) enhances routing stability</li> </ul>
Management Plane	Function and Benefit
<b>CPU and Memory Thresholding</b>	<ul style="list-style-type: none"> <li>Protects CPU and memory of Cisco® IOS® Software device against DoS attacks</li> </ul>
<b>Dual Export Syslog</b>	<ul style="list-style-type: none"> <li>Syslog exported to dual collectors for increased availability</li> </ul>

# 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 Connectivity










# Cisco IOS Secure Connectivity Overview

## Industry-Leading VPN Solutions

Solution	Key Technologies
Standard IPsec	<ul style="list-style-type: none"><li>▪ <b>Full standards compliance</b> for interoperability with other vendors</li></ul>
Advanced Site-to-Site VPN	<ul style="list-style-type: none"><li>▪ Hub-and-Spoke VPN:<ul style="list-style-type: none"><li>Enhanced Easy VPN – Dynamic Virtual Tunnel Interfaces, Reverse Route Injection, dynamic policy push and high scalability</li><li>Routed IPsec + GRE or DMVPN with dynamic routing</li></ul></li><li>▪ Spoke-to-Spoke VPN: <b>Dynamic Multipoint VPN (DMVPN)</b> – On-demand VPNs (partial mesh)</li><li>▪ Any-to-Any VPN: <b>Group-Encrypted Transport (GET) VPN</b> – No point-to-point tunnels</li></ul>
Advanced Remote Access VPN	<ul style="list-style-type: none"><li>▪ <b>Easy VPN (IPsec)</b>: Cisco dynamic policy push and FREE VPN Clients for Windows, Linux, Solaris and Mac platforms</li><li>▪ <b>SSL VPN</b>: No client pre-installation required and provides end-point security through Cisco Secure desktop</li></ul>

# Cisco IOS Secure Connectivity Portfolio

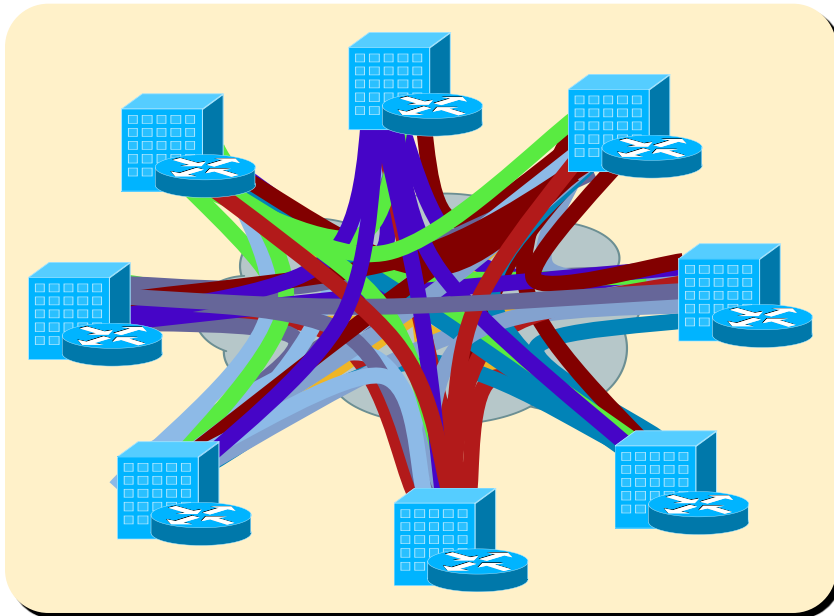
## Performance & Scalability

Cisco® Router Security Platforms	Cisco 800 ISR   Cisco 1800 ISR   Cisco 2800 ISR   Cisco 3800 ISR				Cisco 7301   Cisco 7200		Cisco 7600   Cisco Catalyst® 6500		Cisco XR12000
									
	30 Mbps   45 Mbps   66 Mbps   180 Mbps				5K tunnels   5K tunnels		16K tunnels		16K tunnels
	Up to 10 users   Up to 25 users				Up to 200 users   Up to 200 users				
VPN Modules									
	AIM-VPN/SSL-1   AIM-VPN/SSL-2   AIM-VPN/SSL-3				VAM II+   VSA		IPSec VPN SPA   IPSec VSPA <sup>1</sup> IPSec VPN SPA SPA-IPSEC-2G   WS-IPSEC-3   SPA-IPSEC-2G-2		
IPSec VPN		95 Mbps   145 Mbps   200 Mbps			280 Mbps   960 Mbps		2.4 Gbps   8.4 Gbps		2.5 Gbps
SSL VPN		Up to 75 users   Up to 150 users   Up to 200 users					<sup>1</sup> Only available on Catalyst 6500		

# Tunnelless VPNs

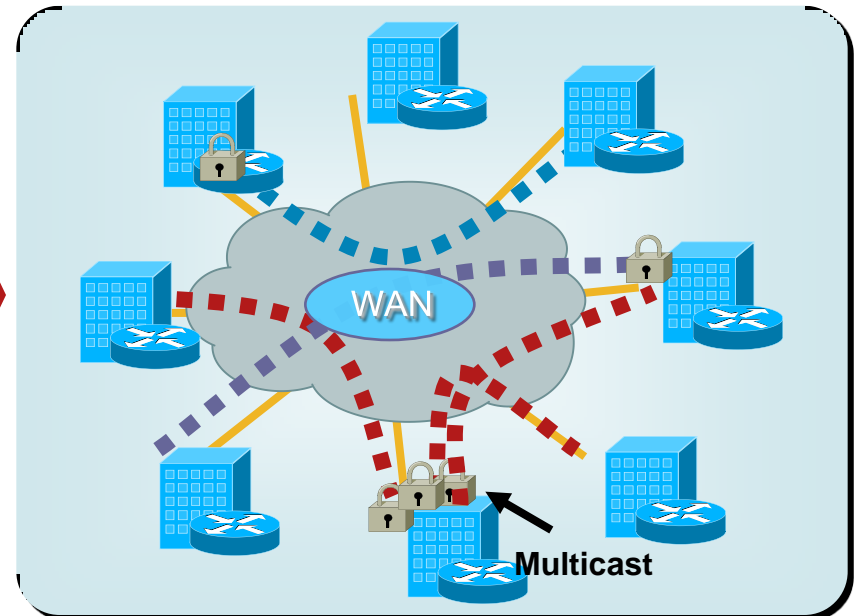
## A New Security Model

### IPSec Point-to-Point Tunnels



- Scalability—an issue ( $N^2$  problem)
- Overlay routing
- Any-to-any instant connectivity cannot be done to scale
- Limited advanced QoS
- Multicast replication inefficient

### Tunnelless VPN

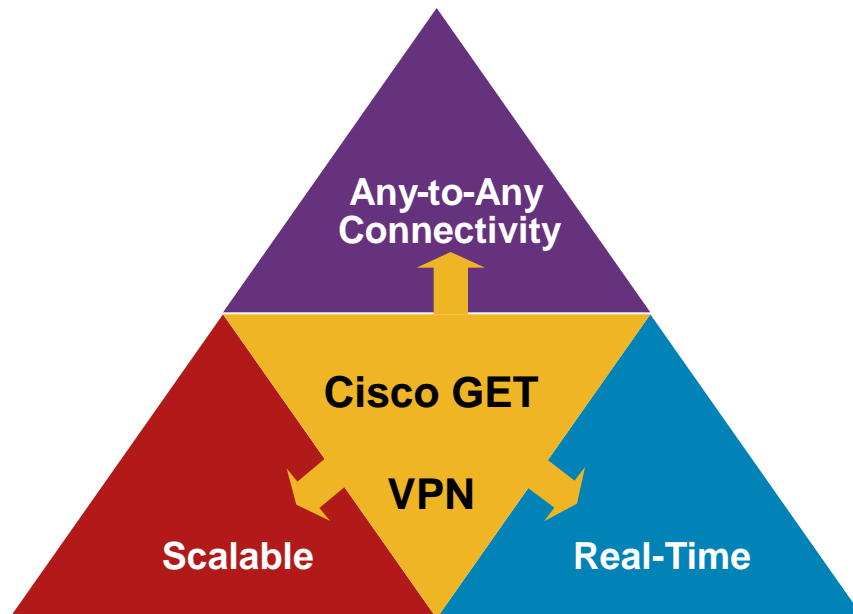


- Data is encrypted without need for tunnel overlay—scalable any-to-any
- Routing/multicast/QoS integration is optimal—native routing
- Encryption can be managed by either subscribers or service providers
- Customized, per-application encryption

# Cisco GET VPN



**Cisco® GET VPN delivers a revolutionary solution for tunnelless, any-to-any branch confidential communications**



## Key Benefits

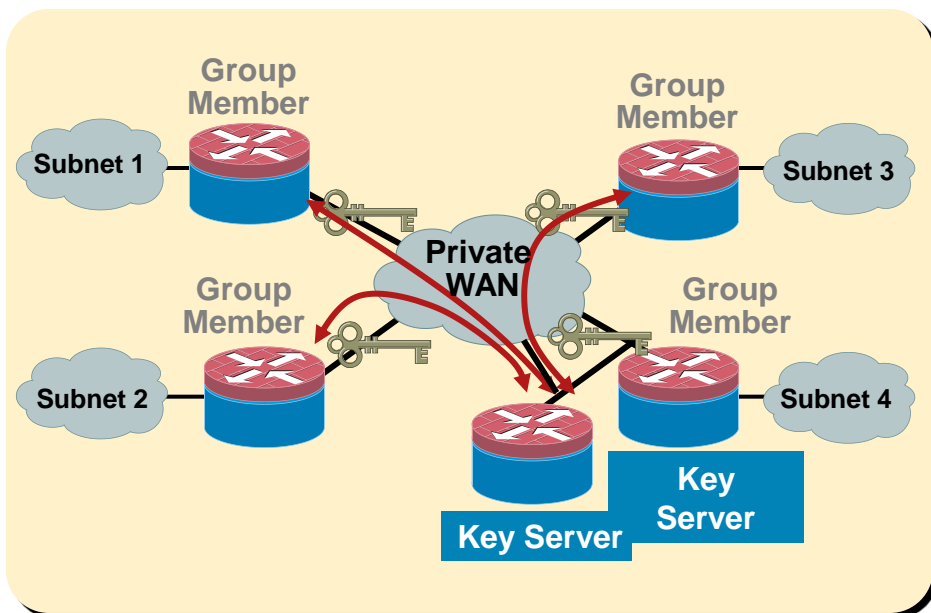
- Large-scale, any-to-any encrypted communications
- Native routing infrastructure without overlay
- Optimal for QoS and multicast—improves application performance
- Transport agnostic—private LAN/WAN, FR/AATM, IP, MPLS
- Offers flexible span of control among subscribers and providers
- Available on Cisco Integrated Services Routers, Cisco 7200, and Cisco 7301



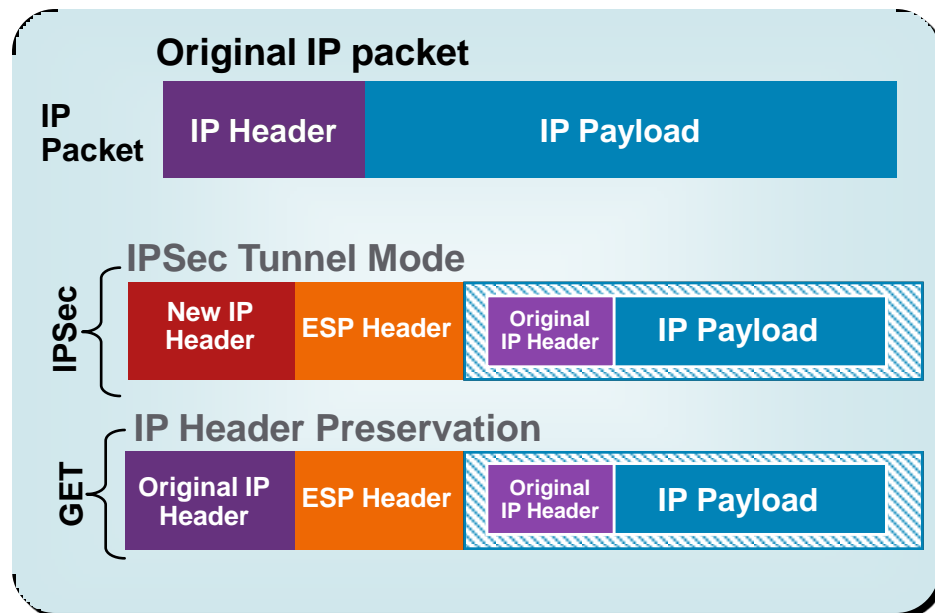
# Inside Cisco GET VPN



**GET VPN simplifies security policy and key distribution**



**GET VPN uses IP header preservation to mitigate routing overlay**



- GET uses Group Domain of Interpretation (GDOI): RFC 3547 standards-based key distribution
- GET adds cooperative key servers for high availability
- Key servers authenticate and distribute keys and policies; group member provisioning is minimized; application traffic is encrypted by group members

# Cisco GET VPN Features and Benefits



## VPN Technical Challenges

## GET VPN Solutions

- Multicast traffic encryption through IPSec tunnels:

Not scalable

Difficult to troubleshoot

- Encryption for native multicast and unicast traffic with GDOI
  - Allows higher scalability
  - Simplifies troubleshooting
  - Extensible standards-based framework

- Overlay VPN network

Overlay routing

Suboptimal multicast replication

Lack of advanced QoS

- IP header preservation

Multicast replication done by network core

Optimal routing introduced in VPN

Advanced QoS for encrypted traffic

- No full-mesh scalability

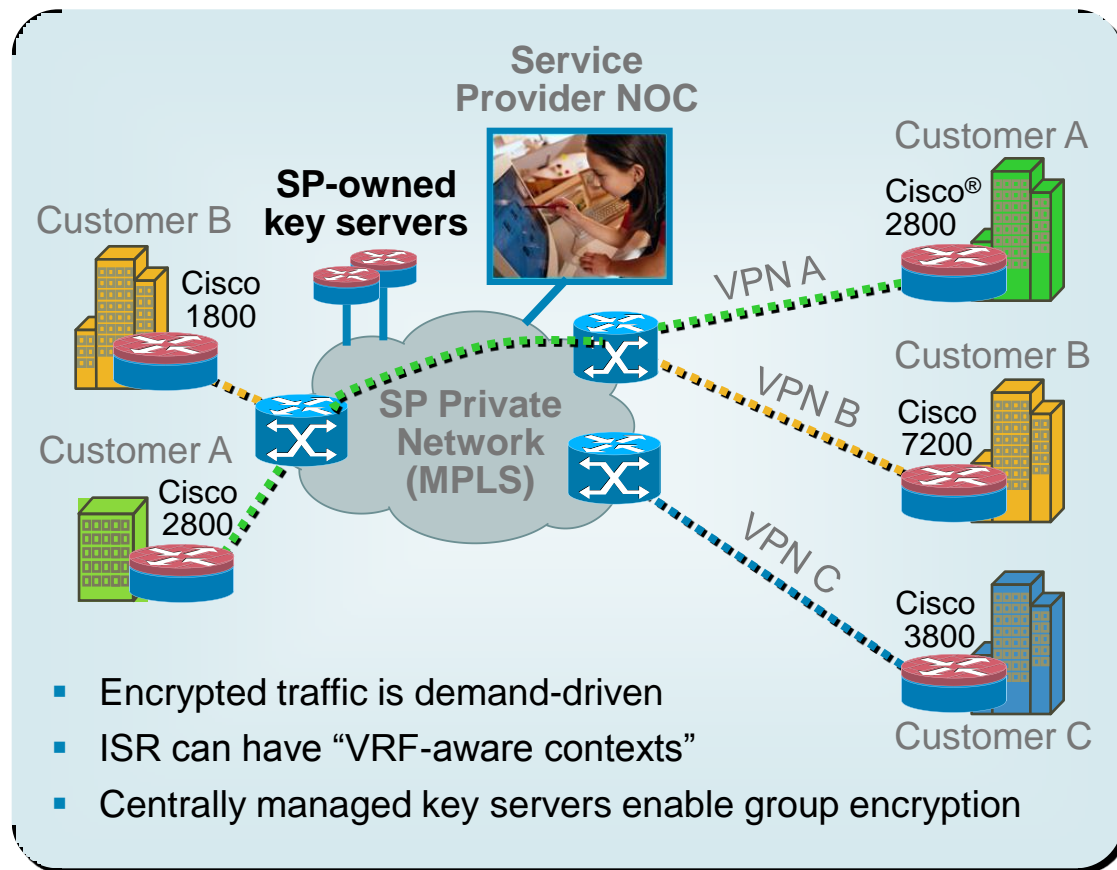
Primarily hub-and-spoke

Spoke-to-spoke not scalable

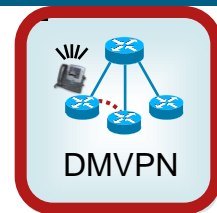
- Any-to-any instant enterprise connectivity
  - Leverages MPLS for instant communication
  - Optimal for voice-over-VPN deployments

# Managed Tunnelless VPN Services

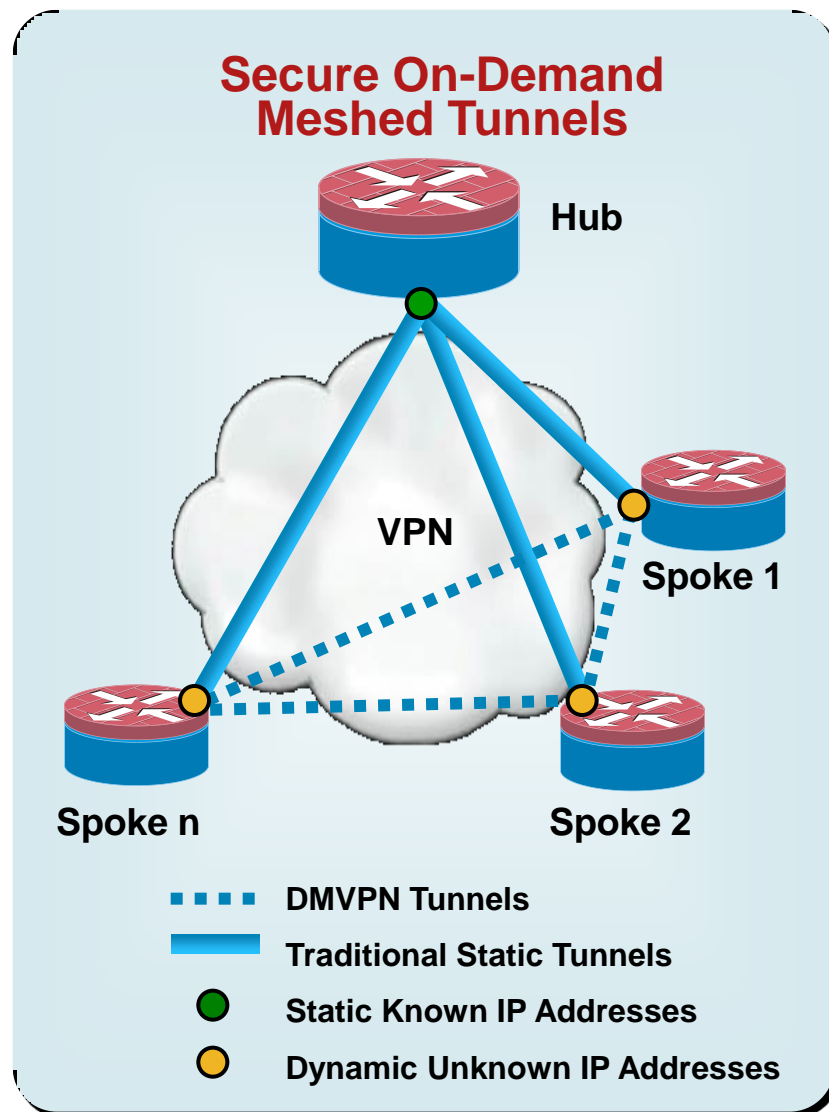
- Service integration delivers greater value, stronger branding
- Increased security
  - Helps businesses comply with regulations: HIPAA, PCI
- Operational simplicity
  - Centralized key server reduces complexity
  - Easy service rollout
- Optimized network utilization
- Service innovation, unique offering
- High-value services



# Cisco Dynamic Multipoint VPN



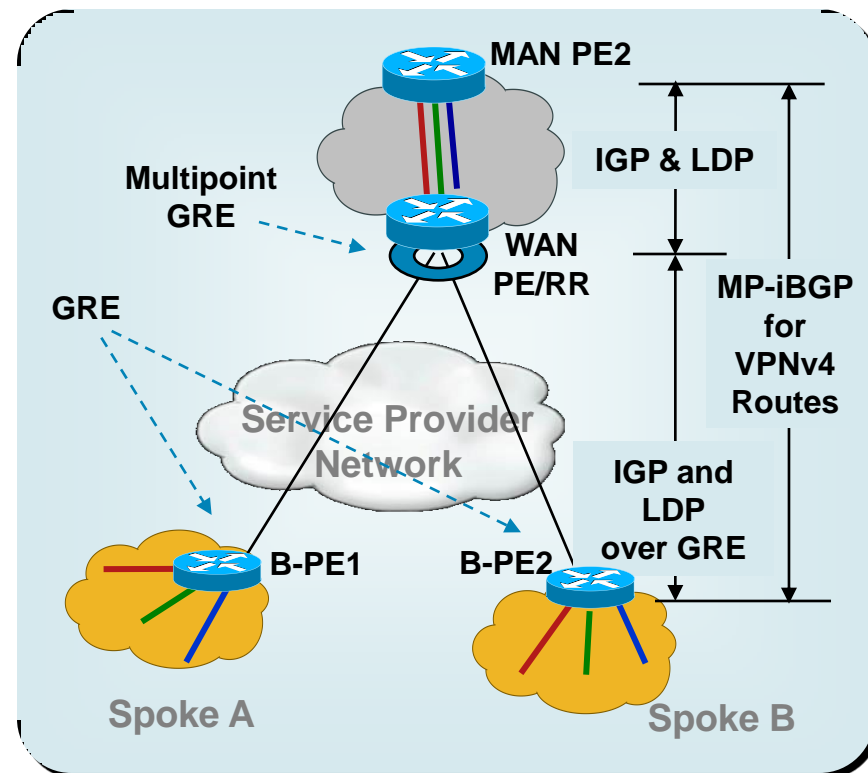
- **Full meshed** connectivity with simple configuration of hub and spokes
- Supports **dynamically** addressed spokes
- **Zero touch deployment and configuration** for new spokes
- What's new in 12.4(6)T – 9T
  - Improved Scaling – NHRP/CEF Rewrite and EIGRP Scaling enhancements
  - Manageability Enhancements

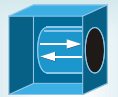




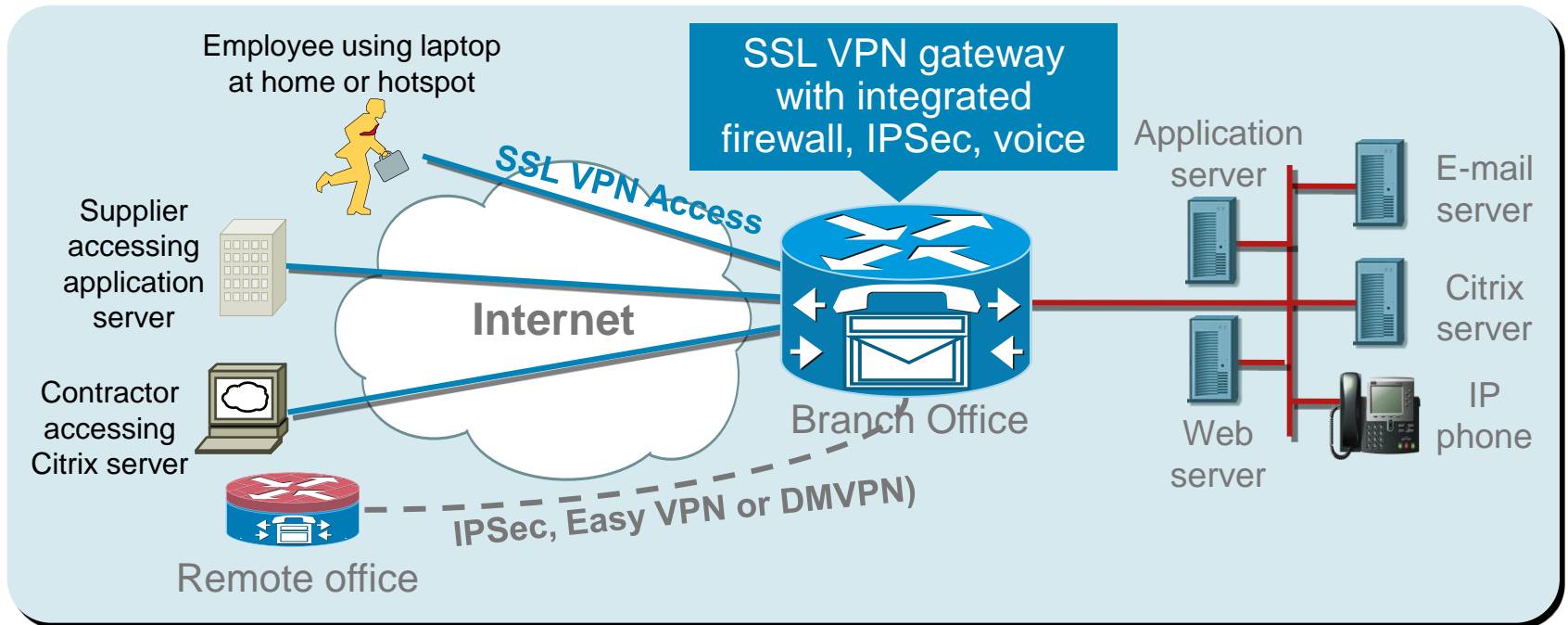
# RFC 2547 over Cisco DMVPN

- Allows large enterprise DMVPN customers to deploy MPLS segmentation
- Enables service providers to offer encrypted RFC 2547-based VPN services
- Shared control plane between RFC 2547 and DMVPN for advertising BGP/VPN prefixes
- Restrictions: Hub-and-spoke support only; not supported on Cisco® 870





# Cisco IOS SSL VPN Overview



- Provides secured access from unmanaged PCs – partners/employees can access corporate network using any PC from anywhere securely
- SSL VPN for mobile users connecting from partners, mobile devices, or public kiosks
- Use the same router to terminate IPsec from remote offices



# Cisco IOS SSL VPN Positioning

## For Enterprise Branch Office and SMB

### Small and Medium-Sized Businesses: Integrated Solution

- SSL VPN adds significant additional value to security router investment
- Cisco IOS® Software security routers offer the only one-box solution for IPsec, SSL VPN, Firewall, IPS, routing, ...
- Cisco IOS SSL VPN offers affordable, easy-to-use solution

### Enterprise: Distributed Branch-Office Access

- Branch-office router-based SSL VPN provides efficient remote access to local (branch) resources
  - Faster response time versus access to central gateway and back through the WAN
- Access policies are in line with users' configurations at work
  - Redirecting from central gateway requires setting up additional ACLs and tunnels
- Branch SSL VPN gateway backs up central gateway for redundancy and disaster recovery



# Cisco IOS SSL VPN Highlights

- **Advanced full-network access**

Cisco® AnyConnect VPN Client provides full-tunnel access for virtually any application; i.e.: Cisco Softphone; dynamically loaded client may be permanently installed or uninstalled after disconnect

- **Comprehensive endpoint protection**

Cisco Secure Desktop prevents digital leakage and protects user privacy; easy to implement and manage; works with desktop guest permissions

- **Ease of deployment and management**

Simple GUI-based provisioning and management with step-by-step wizards for easy deployment

- **SSL VPN gateway network integration**

Advanced authentication and access control with embedded certificate-authority server

Virtualization—allows segmentation as well as pooling of resources while masking the physical attributes and boundaries of the resources



# Advanced Full-Network Access Cisco AnyConnect VPN Client



- Extends the in-office experience
  - LAN-like full-network access; supports latency-sensitive applications such as voice
- Access across platforms
  - Windows 2000, XP (x86/x64), Vista (x86/x64)
  - Mac OS X 10.4 and 10.5, Linux Intel
- Always up-to-date
  - Remotely installable and configurable to minimize user demands
- No-hassle connections
  - No reboots required
  - Standalone, start work before login, Web launch, portal connection
  - MSI – Windows preinstallation package



# Comprehensive Endpoint Security

## Cisco Secure Desktop



### Complete Preconnect Assessment

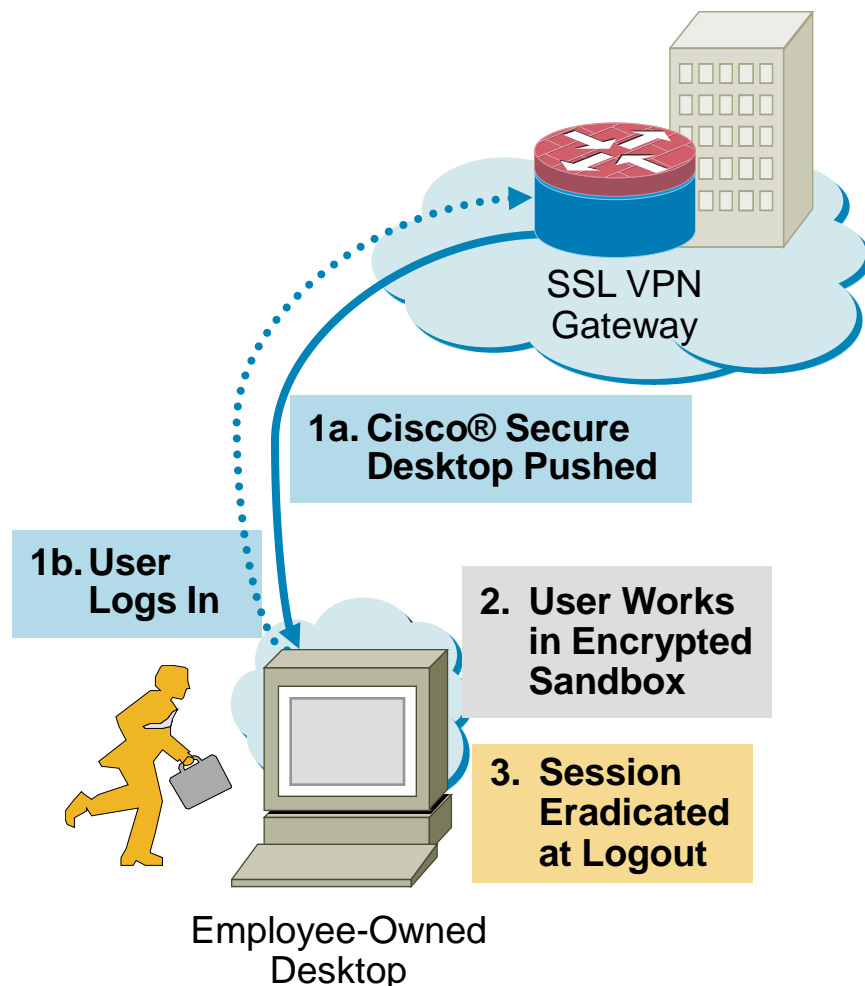
- Location assessment: Managed or unmanaged desktop?
- Security posture assessment: AV operational and up-to-date, personal firewall operational, malware present?

### Comprehensive Session Protection

- Data sandbox and encryption that protects every aspect of session
- Malware detection with hooks to Microsoft free antispyware software

### Postsession Clean-Up

- Encrypted partition overwrite (not just deletion) using DoD algorithm
- Cache, history, and cookie overwrite
- File download and e-mail attachment overwrite
- Autocomplete password overwrite



# Ease of Deployment and Management

## SSL VPN Wizard



- Set up portal IP address
- Multiple contexts
- Authentication through digital certificates

**SSL VPN Wizard**

**IP Address and Name**  
This is the IP address users will enter to access the SSL VPN portal page. If multiple SSL VPN services are configured in this router, the unique name is used to distinguish the service.

IP Address: 172.19.111.136 Name: tunnel

☐ Enable secure SDM access through 172.19.111.136

Domain: tunnel

**Digital Certificate**  
When users connect, this digital certificate will be sent to their web browser to authenticate the router.

Certificate: TP-self-signed-539420202

**Information**  
URL to login to this SSL VPN service: https://172.19.111.136/tunnel

< Back Next > Finish Cancel Help

# SSL VPN Gateway Network Integration

## Authentication and Access Control



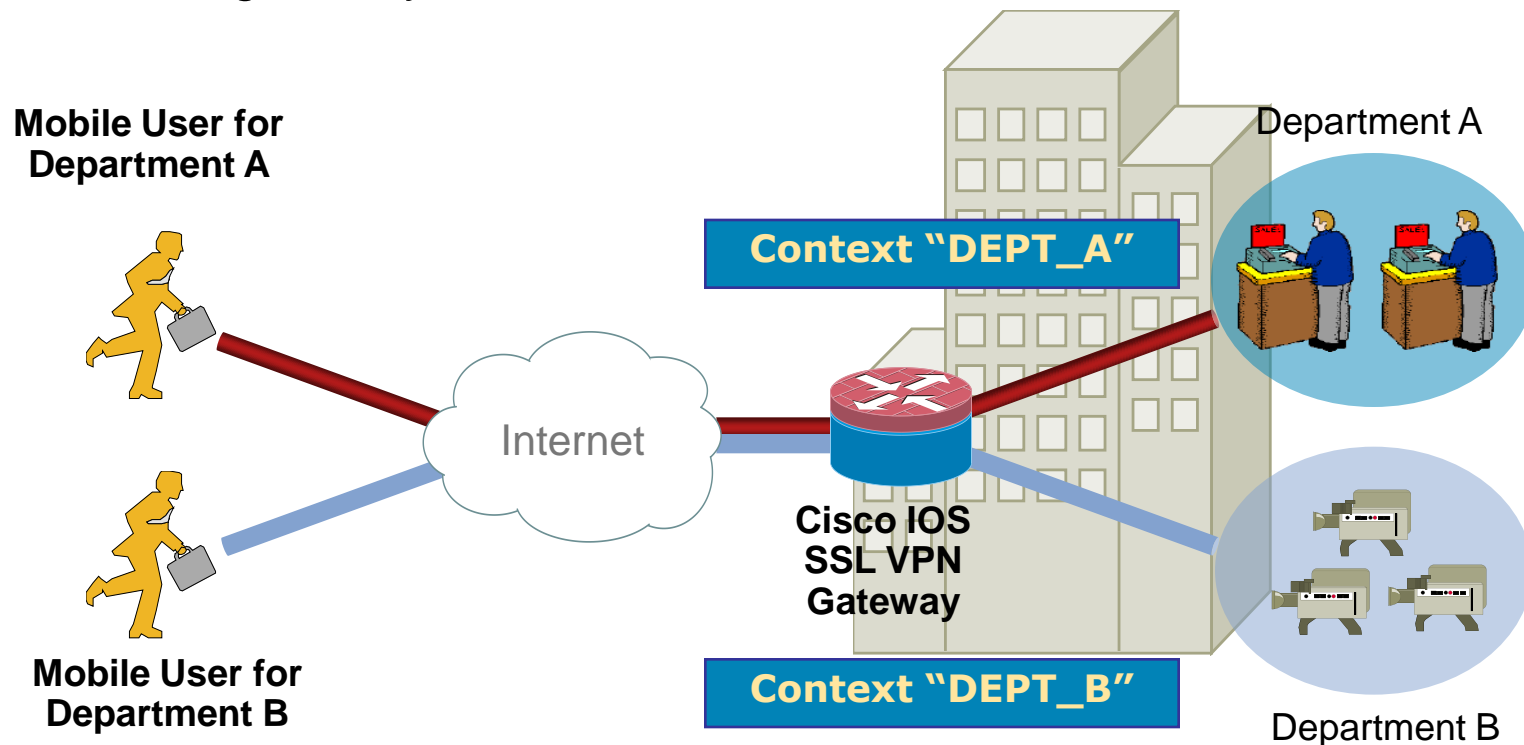
- Robust authentication
  - Digital certificates for SSL authentication
  - RADIUS or authentication, authorization, and accounting (AAA) to manage users
- Advanced network access control options
  - IP address, differentiated services code point/type of service (DSCP/ToS), TCP/User Datagram Protocol (UDP) port, per-user, and per-group

# SSL VPN Gateway Network Integration

## Multiple Contexts



- Cisco IOS® SSL VPN supports virtualization
- Cisco IOS® SSL VPN allows segregation of different extranet partners or different internal enterprise departments within a single SSL VPN gateway

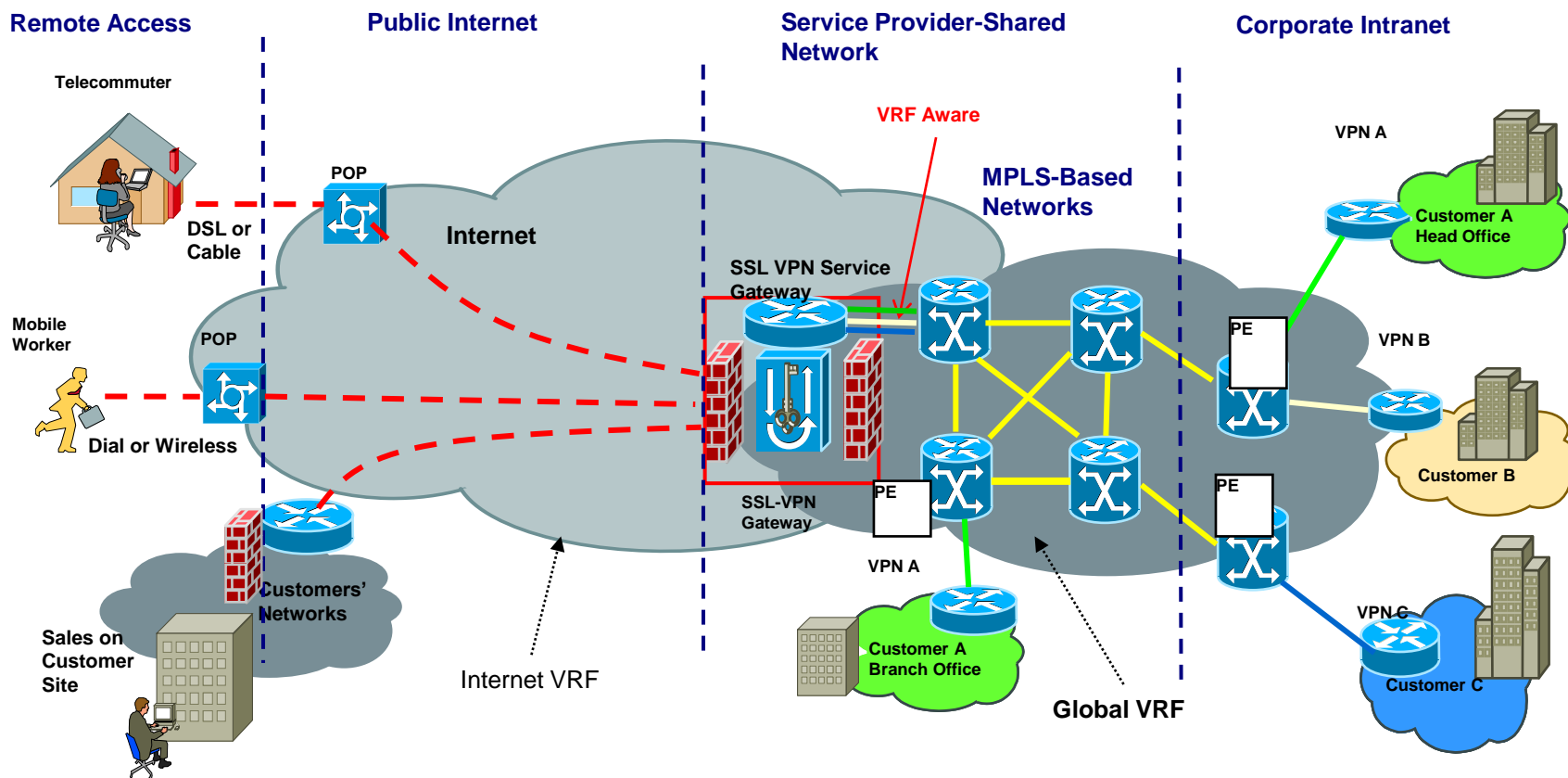


# SSL VPN Gateway Network Integration

## VRF Awareness



- Service providers can put specific Internet routes into a VRF configuration and transparently integrate the SSL VPN gateway into a shared MPLS network.
- Separating specific routes from the global routing table offers increased security.
- Overlapping IP address pools is supported.

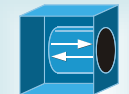


# Cisco IOS SSL VPN Licensing

Platform	Number of SSL VPN Users	
	Included	Maximum
<b>Fixed-Configuration Routers</b>		
Cisco® 871, 880 series	-	10
Cisco 1801, 1802, and 1803	-	25
Cisco 1811 and 1812	-	25
<b>Modular Routers (HSEC Bundles)</b>		
Cisco 1841 and 2801	10	75
Cisco 2811 and 2821	10	100
Cisco 2851	10	150
Cisco 3825 and 3845	25	200
<b>Head-end Routers</b>		
Cisco 7200 and 7301	-	200

- Flat pricing model, per simultaneous user
- Licenses available in 10-, 25-, and 100-user packs

} HSEC Bundle (with AIM)



# Cisco IOS SSL VPN—What's New

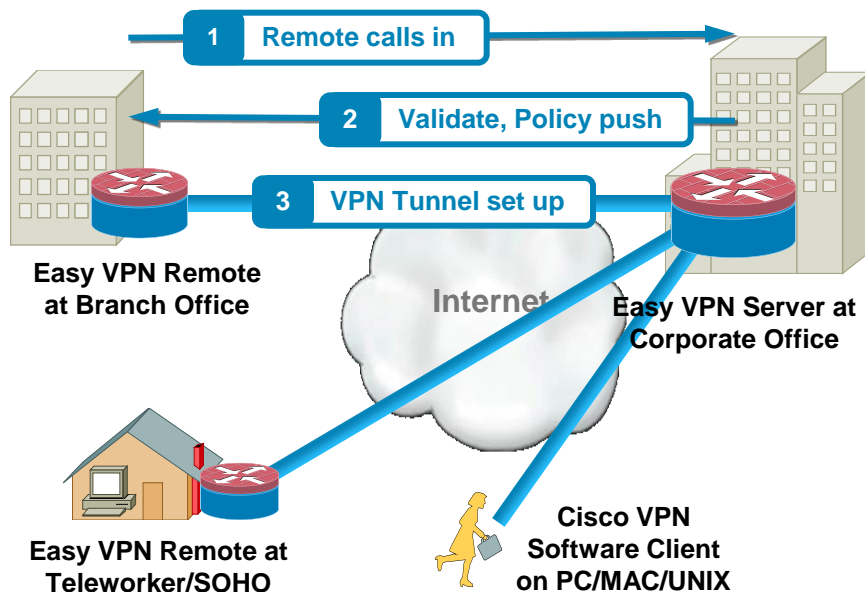
Feature	Benefit
<b>Multiple OS support for AnyConnect</b>	<ul style="list-style-type: none"><li>▪ Support for mixed OS environments</li><li>▪ Support for Windows Vista, XP, 2000, Mac OSX, and Linux</li></ul>
<b>AnyConnect Standalone Connect</b>	<ul style="list-style-type: none"><li>▪ Connect without having to always initiate from browser</li><li>▪ Reduce time required to connect from client</li></ul>
<b>Start Before Login</b>	<ul style="list-style-type: none"><li>▪ Allows client to establish a tunnel before the Windows login prompt</li><li>▪ Controlled by head-end device</li></ul>
<b>CEF Support</b>	<ul style="list-style-type: none"><li>▪ Improved tunnel client performance</li><li>▪ Improves integration with other features</li></ul>
<b>Access Control Enhancements</b>	<ul style="list-style-type: none"><li>▪ Eliminate prompt for login credentials for mobile operators</li></ul>



# Cisco Easy VPN

## Centralized Policy-Based Management

- Automated deployments—No user intervention  
Enforces consistent policy on remote devices  
Add new devices without changes at headend
- Supports dynamic connections with VPN
- Interoperable across Cisco® access and security devices
- Cisco VPN client—The only FIPS-certified client



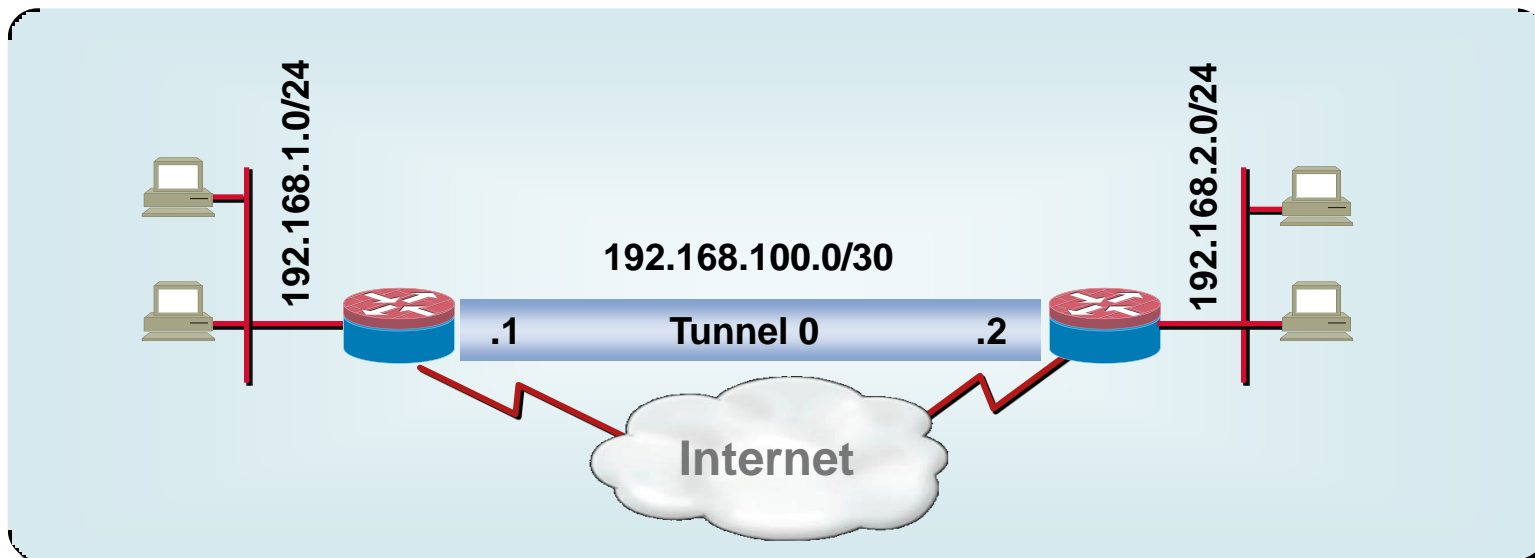
### What's New in Easy VPN?

- CTA/NAC policy enforcement
- Centralized policy push for integrated client firewall
- Password aging via AAA
- cTCP NAT transparency and firewall traversal
- DHCP client proxy and DDNS registration
- Split DNS
- Per-user policy from Radius
- Support for identically addressed spokes behind NAT with split tunnels
- VTI manageability—Display of VRF information, summary commands

# IPSec Virtual Tunnel Interface (VTI)

## Simplified VPN Deployment

- Eliminates crypto maps, ACLs, generic route encapsulation (GRE)
  - 1:1 relationship between tunnels and sites with dedicated logical interface
- Scales better than GRE
- Supports QoS, multicast, and other functions that previously required GRE
- Improves VPN interoperability with other vendors



# Hardware-Accelerated AES

## IPSec is moving to AES

- On July 26, 2004, NIST proposed withdrawing the FIPS for DES in a Federal Register notice  

“DES is now vulnerable to key exhaustion”  
<http://csrc.nist.gov/Federal-register/July26-2004-FR-DES-Notice.pdf>
- NIST is encouraging federal agencies to use the Advanced Encryption Standard (AES)  

Approved as an official government standard by Secretary of Commerce on May 26, 2002  
 U.S. Federal Government, enterprise, and service providers migrating from 3DES to AES
- IETF is promoting use of AES within ESP: this document is a **standards track**  
<http://www.ietf.org/internet-drafts/draft-ietf-ipsec-ciph-aes-cbc-05.txt>

	3DES	AES
Type of Algorithm	Symmetric, Feistel Cipher	Symmetric, Block Cipher
Key Size (in bits)	112 168	128 192 256
Time to Crack*	4.6 billion years	149 trillion years

\* Assuming a machine could try 255 keys per second—NIST

# Cisco IOS Certificate Authority and PKI Services

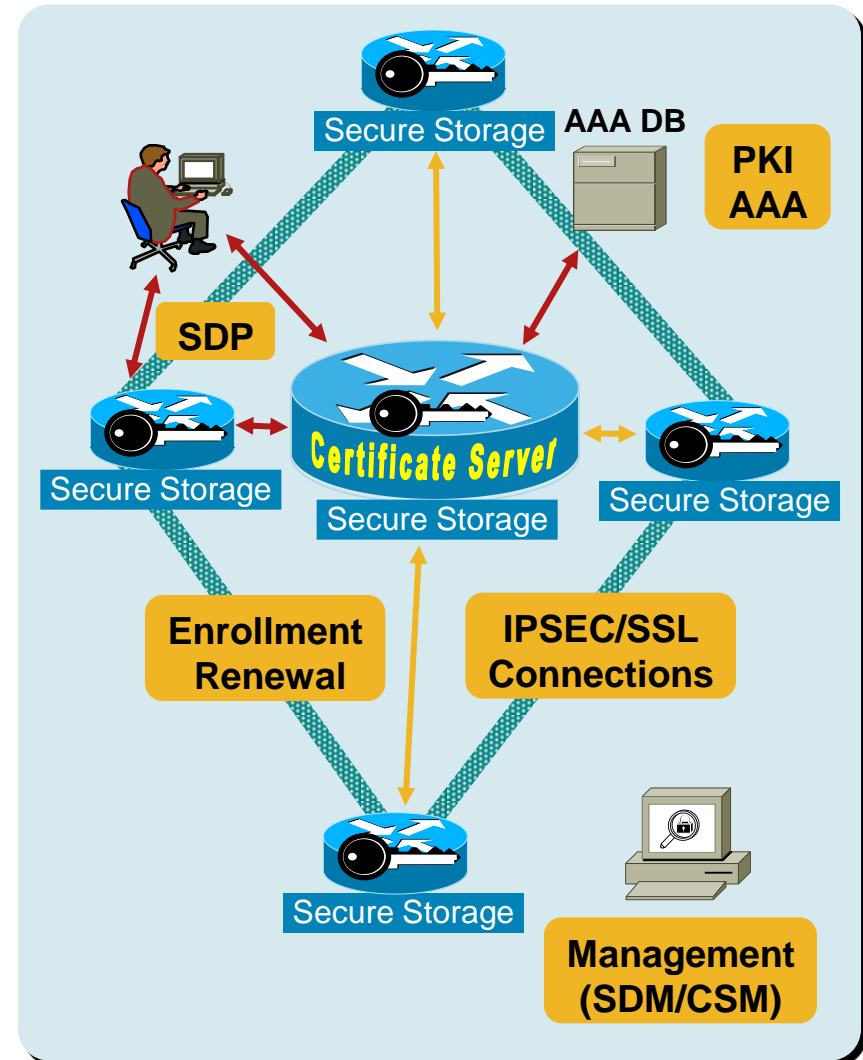


IPSec VPN

- Free IOS Certificate Server (router)
- Secure Device Provisioning (SDP) web-based GUI for enrolling client router into a PKI Network
- Fully functional PKI Client: Interoperability with third party CAs (Microsoft, Verisign, Netscape)
- PKI AAA integration for authentication & authorization
- Self Managing (Auto enroll/renew)
- IPSEC,SSL & TLS compliant

## What's New in IOS PKI?

- Extended Cert Chain Validation
- Alternate OCSP Server Validation
- CRL cache control



# Cisco IOS Secure Connectivity Summary

- **Industry-leading integration of VPN and networking**

Tunnelless IPSec, dynamic IPSec tunnels, QoS, multicast

- **Top-notch application support**

Voice, video, multicast and non-IP application support

- **Ease of deployment and management**

Easy VPN: Secure policy push for hardware and software clients

Low-touch, highly scalable deployment options, such as Secure Device Provisioning, Configuration Engine, Config Express

IP SLA—VPN performance and SLA conformance monitoring

# Secure Network Solutions

## Secure Network Solutions



Business  
Continuity



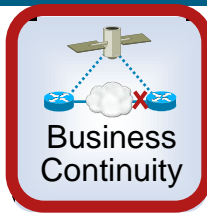
Secure  
Voice



Secure  
Mobility



Compliance



# Are You Prepared?

- What would you do if 50% of your employees couldn't come to work for a week?
- What would you do if 90% of your workforce couldn't come to work for a month?
- Can you maintain communications with your employees?
- Can you maintain business continuity with your employees working exclusively from home?

Are you prepared for what might happen tomorrow—  
pandemics, terrorism, natural disasters, transit strikes?

# Increased Workforce Resilience

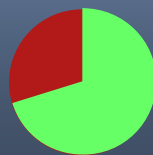
## The Key to Business Continuity

### Power Outage



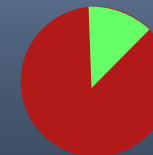
88% of  
Enterprises  
Prepared

### Failure of Server, Host, Application, Software



70% of  
Enterprises  
Prepared

### Workforce Disruption



13% of  
Enterprises  
Prepared

Only 13% of enterprises today are prepared for  
a major disruption in workforce operations



# Business Continuity Technology Overview

Solution	Key Technologies
<b>Cisco® Anywhere Office Solution</b>	<ul style="list-style-type: none"><li>▪ Laptop + VPN + IP communications software</li></ul>
<b>Cisco Virtual Office</b>	<ul style="list-style-type: none"><li>▪ SOHO ISR + IP phone for high-quality network access</li></ul>
<b>WAN backup over satellite and cable</b>	<ul style="list-style-type: none"><li>▪ Satellite network module</li><li>▪ Cable routers and HWICs</li></ul>
<b>Application-level resilience</b>	<ul style="list-style-type: none"><li>▪ Survivable Remote Site Telephony (SRST)</li><li>▪ Cisco IOS® IPSec stateful failover</li><li>▪ Cisco IOS Firewall stateful failover</li></ul>

# Cisco Anywhere Office Solution

## Remote Access VPN and PC-Based Telephony



Mobile Office with  
Complete Data and  
Voice Services

- Remote access to any application via SSL or IPSec VPN
- Mobile “any device” access via clientless SSL VPN
- PC-based office telephone via Cisco® IP Communicator
- On-demand conferencing and collaboration via Cisco MeetingPlace®
- Designed for employees who primarily communicate internally



# Cisco Virtual Office: Extending the Enterprise



## Solution Components:



### REMOTE SITE

- Cisco 800 series Integrated Services Router
- Cisco Unified IP Phone 7900 series



### HEAD-END SITE

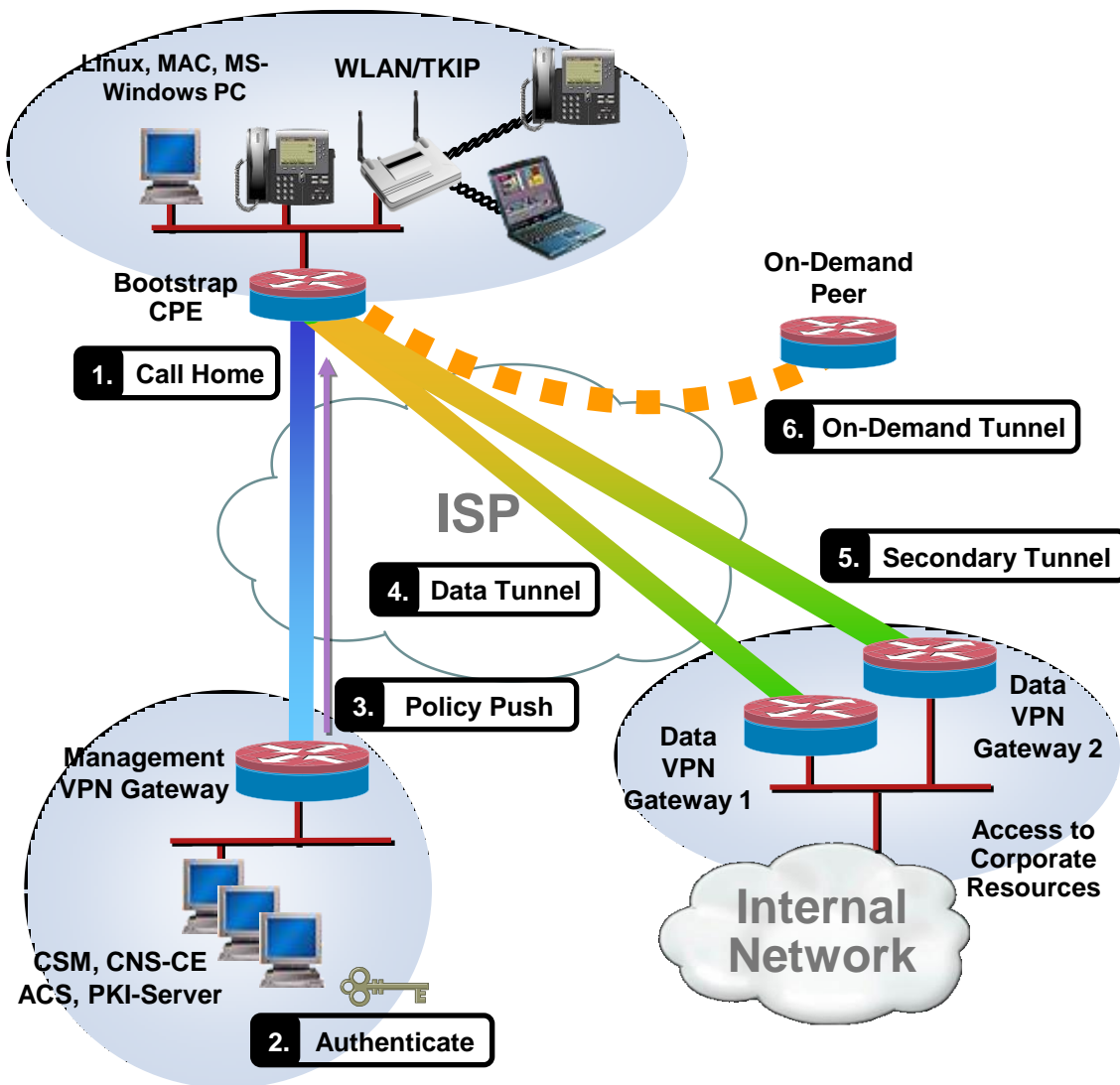
- Cisco 7200 series VPN aggregation router
- Cisco Security Manager
- Cisco Secure ACS
- Configuration Engine



### SERVICES

- Planning, design, and implementation
- Remote management
- Security optimization

# Cisco Virtual Office Deployment

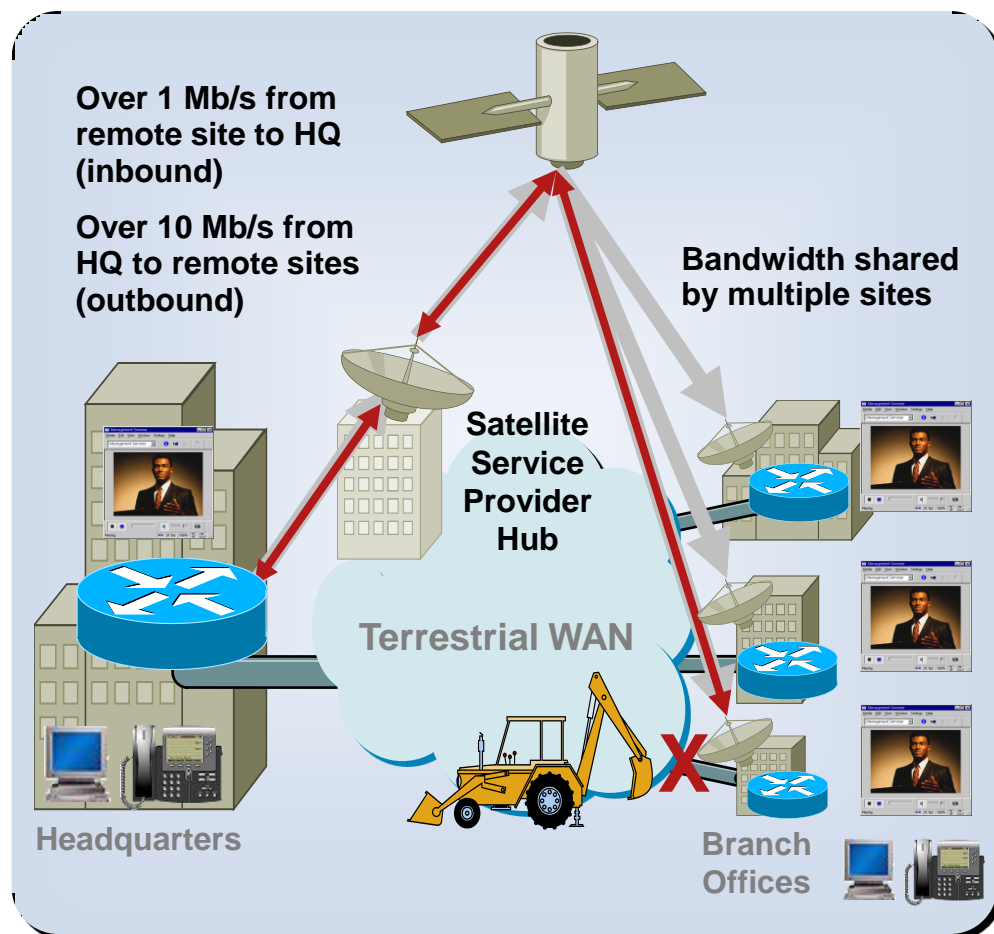


1. Remote routers "call home" and management tunnel is set up
2. Management server authenticates remote router using certificate authority and AAA servers
3. Management server pushes policy including new certificate
4. Remote router establishes primary DMVPN tunnel and access to corporate resources
5. Secondary DMVPN tunnel is established and stays active for instant failover
6. When required, remote router establishes direct spoke-to-spoke tunnel with other authorized remotes
7. Tunnel torn down after use

# VSAT Satellite WAN NM (NM-1VSAT)

## Disaster Recovery over Satellite Links

- Satellite WAN maintains business continuity if terrestrial link fails
  - Over 1 Mb/s per site (two-way)
  - Supplements or replaces ISDN backup
  - AES encryption if required
- Broadband connectivity for remote/temporary sites
  - Instant WAN connectivity for emergency response, portable applications, and remote locations without terrestrial broadband
  - For regional/continental coverage
- NM supported on 2800 and 3800 ISR and 2600XM and 3700 Routers
  - Ku-band and C-band support
  - Interoperable with Gilat-SkyEdge hubs and services



# Cisco Cable Access Router Portfolio

## Backup VPN Solutions over Cable

Cable HWIC can be used with 12 different modular ISR and access router models

Multiservice Capabilities



815 Fixed Configuration

SOHO



IAD243x with Cable HWIC



1841 with Cable HWIC

SMB/Small Branch



2691/2800 with Cable HWIC



3700/3800 with Cable HWIC

Enterprise Branch

Primary WAN

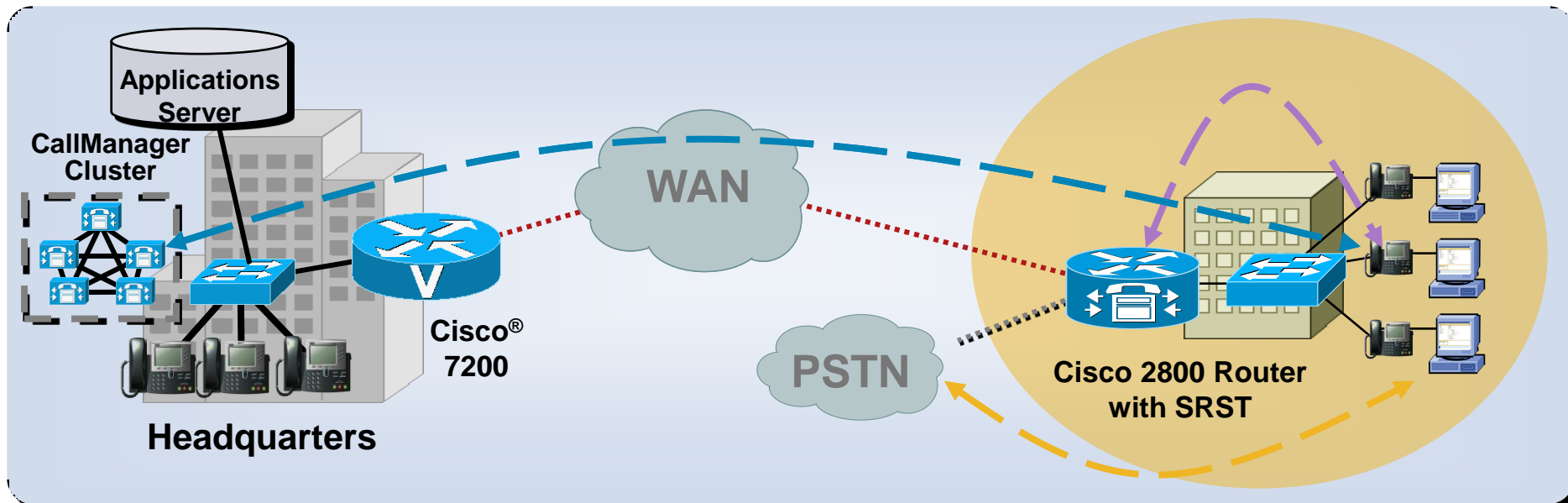
Primary WAN, WAN Backup, WAN Offload

# Survivable Remote Site Telephony

## Minimizing Business Impact of WAN Link Failure

- Cisco router autoconfigures, provides local call processing—no manual intervention required
- SRST IP phone calls remain secure
- When WAN is available, IP phones autorevert back to CallManager
- Calls in progress stay connected during WAN failure/restore

### Resiliency for Remote IP Telephony Users with Central CallManager





# Cisco IOS IPSec Stateful Fail Over

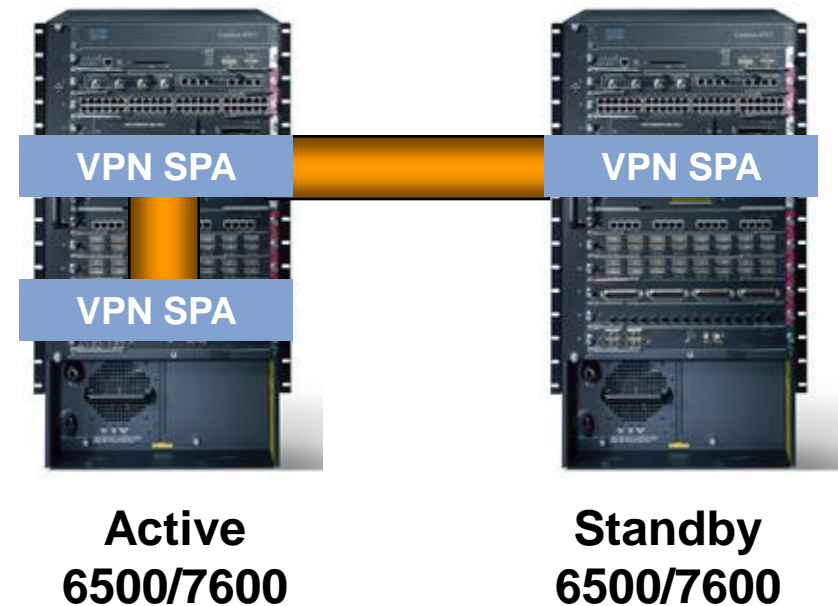
## Minimal Service Disruption

### Interchassis:

- IPSec tunnel between active/standby platforms for secure failover using State Synchronization Protocol (SSP) for site-site tunnels with preshared keys

### Intrachassis:

- Active/active stateful failover between VPNSMs; adds support for PKI and IPSec remote-access tunnels

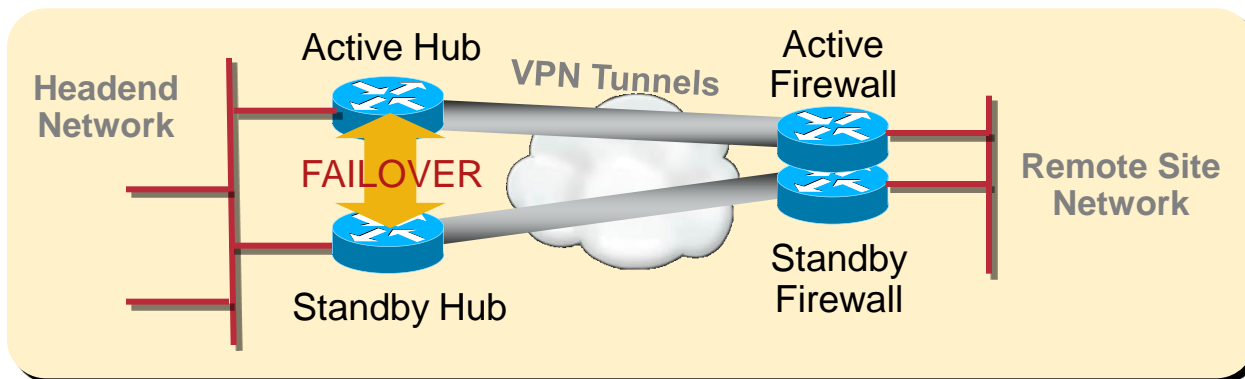
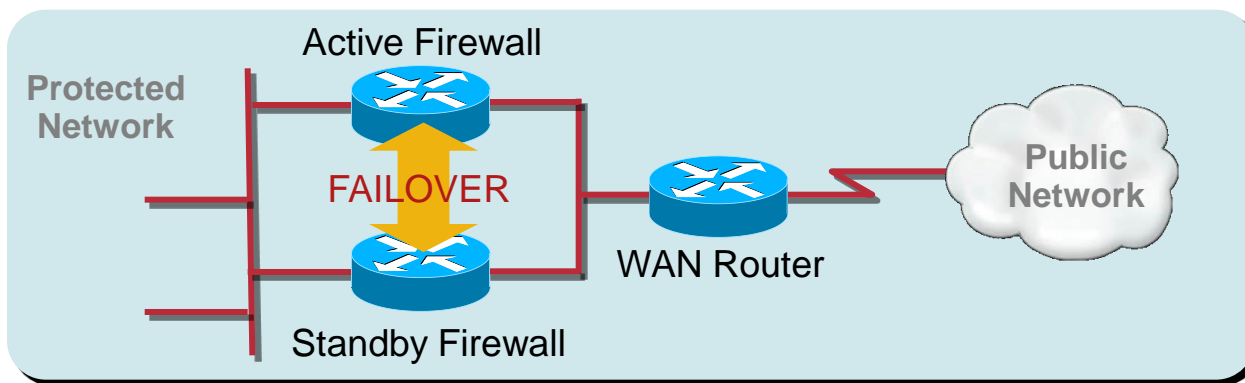




# Cisco IOS Stateful Firewall Failover

## For Cisco 3800 Integrated Services Routers

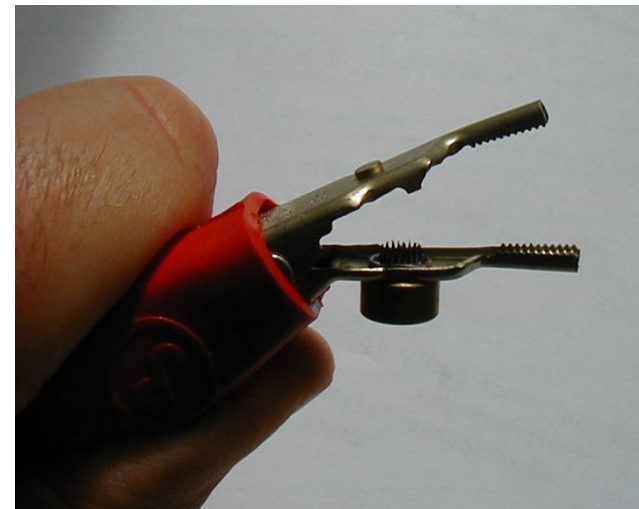
- Supports both LAN/VPN interfaces
- Active/Standby configuration
- Maximizes firewall uptime for mission-critical applications



# 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





# Integrated Voice and Security

For Cisco 2800–3800 Integrated Services Routers

## Built-in VPN Acceleration

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

## Secure Voice

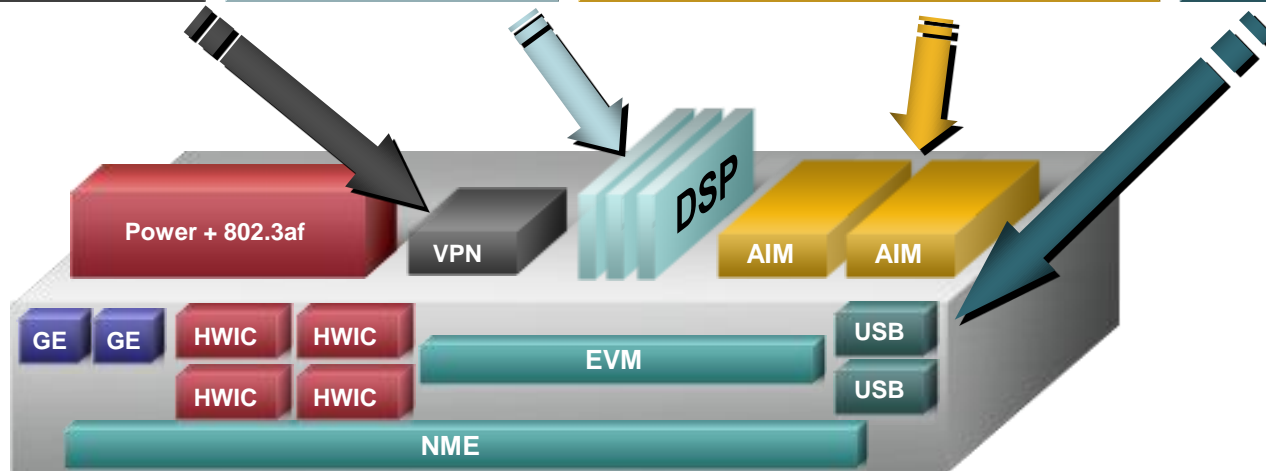
- PVDM modules
- Support for SRTP

## High-Performance AIM

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

## USB Port

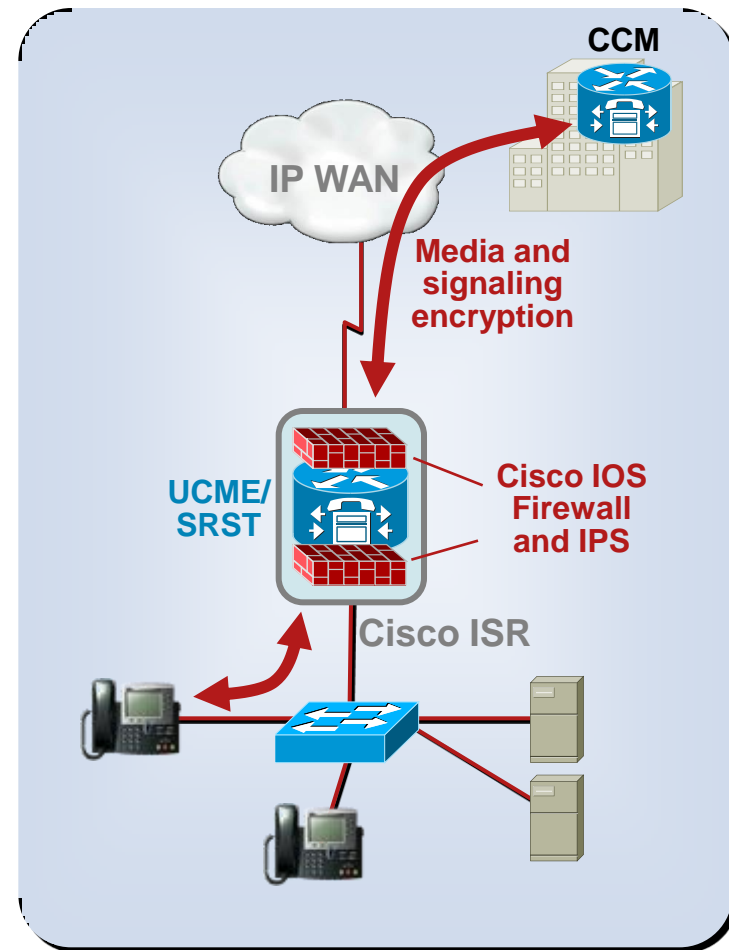
- Removable
- Secure credentials



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

# Secure Voice Overview

- Cisco® IOS® Firewall and IPS—to inspect router-generated traffic and secure call processing at the branch
- SRTP voice call encryption (SRST)
- TLS encrypts signaling, protects called number, pins, encryption keys (SRST, CME\*)
- Security and performance: VPN between sites
  - High-quality voice through QoS, DMVPN and GET VPN integration
- Integrated switch security
  - Cisco EtherSwitch® services modules for ISRs provide integrated security features and 802.3af Line power for IP phones
- VoIP endpoint protection



# Cisco IOS Firewall—Protection for Voice Signaling and Network Infrastructure



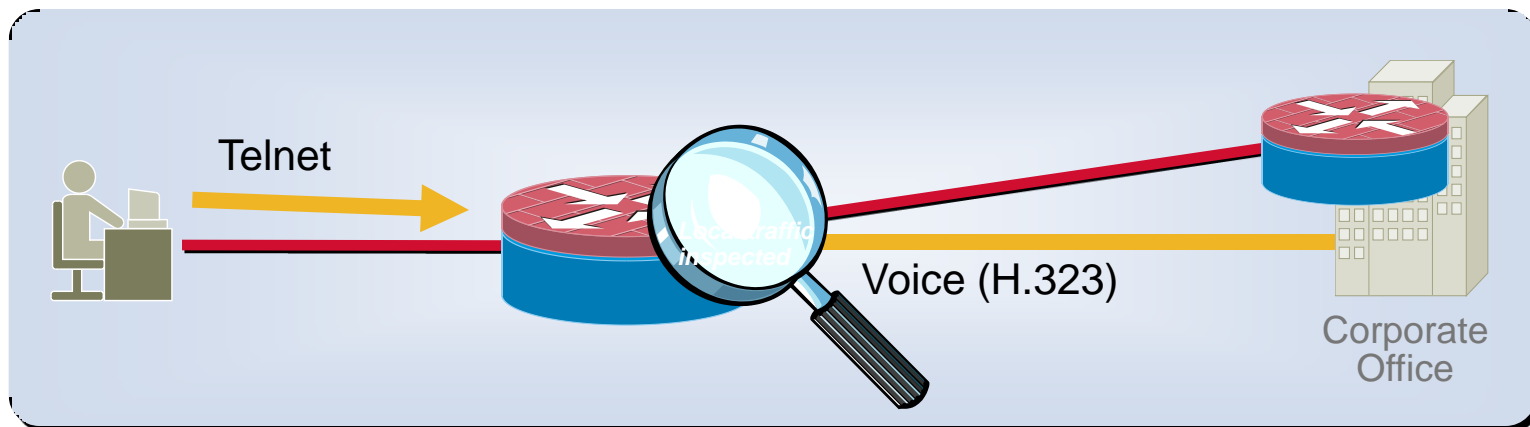
## Protection against Hijacking and Denial of Service

- 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





# SRTP and TLS Encryption

## Secure Voice Design Considerations

Design Criteria	Benefits
Voice media and signaling encryption for Cisco® SIP phones	<ul style="list-style-type: none"><li>▪ Extends the benefits of SRTP/TLS to Cisco SIP Phones 7911, 7941, 7961, 7970, 7971</li><li>▪ Full interoperability between Secure SCCP and Secure SIP endpoints</li></ul>
Extend voice and signaling encryption to voice gateways and between Cisco Unified CallManager clusters	<ul style="list-style-type: none"><li>▪ Media and signaling encryption of H.323 intercluster trunks between CCM clusters</li><li>▪ Signaling encryption of SIP gateways</li><li>▪ SRTP interoperability between H.323 and MGCP gateways and SIP/SCCP IP phones</li></ul>
Enable voice and signaling encryption on Cisco Unified CallManager CTI interface	<ul style="list-style-type: none"><li>▪ Extends the benefits of SRTP/TLS to CTI applications</li></ul>
HTTP Digest Authentication on Cisco Unified CallManager	<ul style="list-style-type: none"><li>▪ Interoperates with SIP gateways and SIP phones to authenticate user agent to SIP proxy or registrar</li></ul>
Encryption of configuration file on Cisco IP Phones	<ul style="list-style-type: none"><li>▪ Protects privileged information such as passwords, credentials, and server addresses</li></ul>

**All these require Cisco Voice Security Router Bundles**

# Voice, Video and Data over VPN

## High-Quality Voice and Video over Shared Networks

### Business Problem

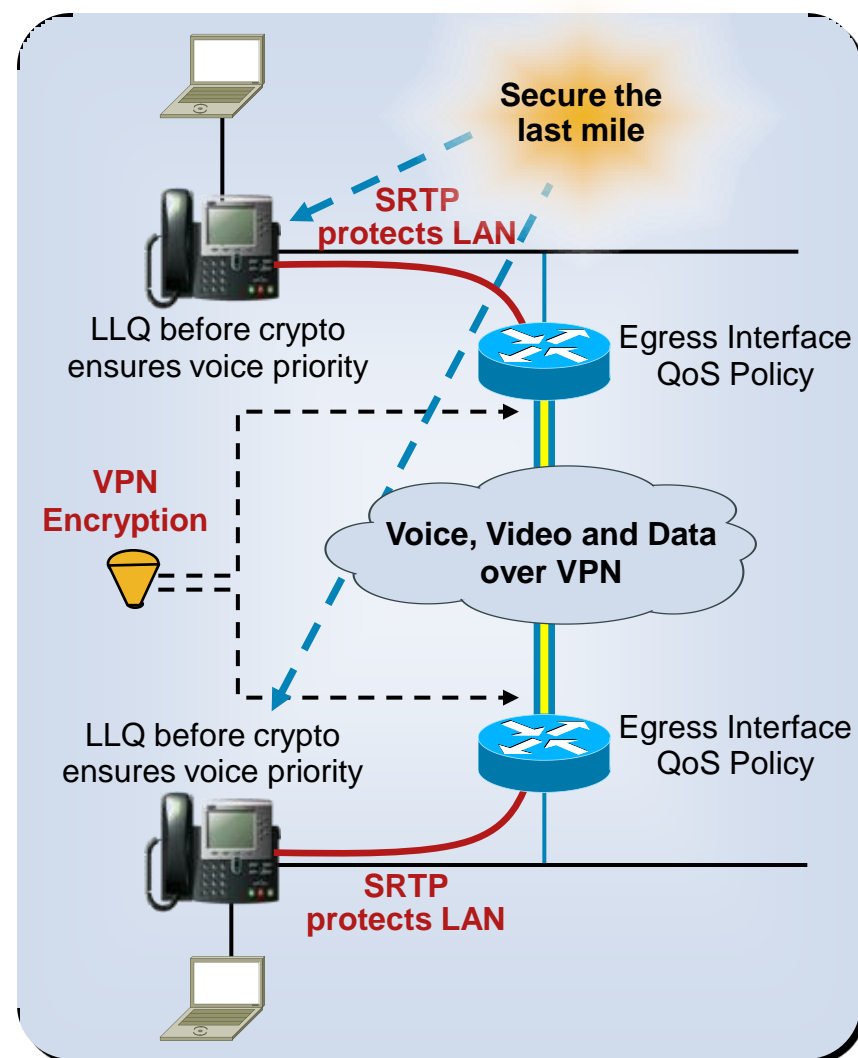
- Managing separate voice and data networks is inefficient and costly

### Voice, Video, and Data over VPN

- DMVPN or GET VPN for site-to-site access
- Data, voice, and video traffic delivered with QoS policies for latency-sensitive traffic

### Benefits

- Wire-speed encryption for Layer 2 and Layer 3
  - Cisco® PVDM supports AES encryption for SRTP (VoIP)
  - SRTP/TLS allows IP phone and gateway AES encryption to protect voice calls
- Toll-quality, jitter-free secure voice and video
  - QoS, SLA, and secure multicast support
- Reduced telco charges





# Cisco EtherSwitch Services Modules

## Integrated Switch Security for Voice and Data

- Four form factors: 16, 24, 48, and 24 + StackWise (HULC) interfaces
- Cisco® Catalyst® Integrated Security Features (CISF) to mitigate many known IP voice attacks and tools (e.g., VoMiT, Ettercap, Dsniff)

VLAN ACLs, DHCP snooping, dynamic ARP inspection, IP source guard, port security, Scavenger-class QoS

MAC address notify, RADIUS/TACAC+, 802.1x, ACL, SSH, SNMPv3, IPv6

- Full software feature parity with Cisco Catalyst 3560 and 3750
- 802.3af PoE and Cisco inline power on all ports—simplifies IP phone and wireless AP deployment



24 and 48-port  
EtherSwitch modules



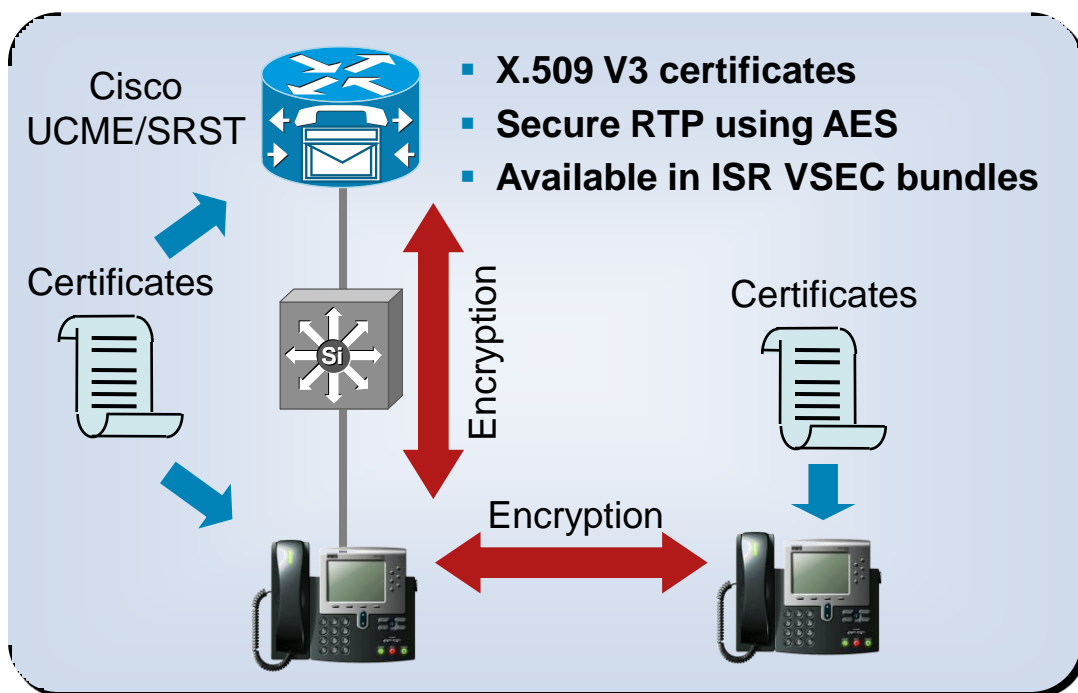
16-port switch and 24-port with  
two StackWise® interfaces



# VoIP Endpoint Protection

## 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

# Cisco 2800–3800 Voice and Security Bundles



Cisco 3800	VSEC	VSEC-CCME	VSEC-SRST	V3PN
<b>Part Numbers</b>	<ul style="list-style-type: none"> <li>C3825-VSEC/K9</li> <li>C3845-VSEC/K9</li> </ul>	<ul style="list-style-type: none"> <li>C3825-VSEC-CCME/K9</li> <li>C3845-VSEC-CCME/K9</li> </ul>	<ul style="list-style-type: none"> <li>C3825-VSEC-SRST/K9</li> <li>C3845-VSEC-SRST/K9</li> </ul>	<ul style="list-style-type: none"> <li>C3825-V3PN/K9</li> <li>C3845-V3PN/K9</li> </ul>
<b>Included</b>	Cisco® IOS® Advanced IP Services, <b>128 MB Flash/512 MB DRAM</b> <b>New</b> →			64 MB Flash/256 MB DRAM
<b>VPN Accelerator</b>	None	None	None	<ul style="list-style-type: none"> <li>C3825: AIM-VPN/EPII-PLUS</li> <li>C3845: AIM-VPN/HPII-PLUS</li> </ul>
<b>Voice DSP</b>	C3825: PVDM 2-64, C3845: PVDM 2-64 →			
<b>Call Processing License</b>		<ul style="list-style-type: none"> <li>C3825: 168-user CCME</li> <li>C3845: 240-user CCME</li> </ul>	<ul style="list-style-type: none"> <li>C3825: 168-user SRST</li> <li>C3845: 240-user SRST</li> </ul>	<ul style="list-style-type: none"> <li>C3825: 168-user CCME*</li> <li>C3845: 240-user CCME*</li> </ul>

\* Convertible to SRST

Cisco 2800	VSEC	VSEC-CCME	VSEC-SRST	V3PN
<b>Part Numbers</b>	<ul style="list-style-type: none"> <li>C2801-VSEC/K9</li> <li>C2811-VSEC/K9</li> <li>C2821-VSEC/K9</li> <li>C2851-VSEC/K9</li> </ul>	<ul style="list-style-type: none"> <li>C2801-VSEC-CCME/K9</li> <li>C2811-VSEC-CCME/K9</li> <li>C2821-VSEC-CCME/K9</li> <li>C2851-VSEC-CCME/K9</li> </ul>	<ul style="list-style-type: none"> <li>C2801-VSEC-SRST/K9</li> <li>C2811-VSEC-SRST/K9</li> <li>C2821-VSEC-SRST/K9</li> <li>C2851-VSEC-SRST/K9</li> </ul>	<ul style="list-style-type: none"> <li>C2801-V3PN/K9</li> <li>C2811-V3PN/K9</li> <li>C2821-V3PN/K9</li> <li>C2851-V3PN/K9</li> </ul>
<b>Included</b>	Cisco IOS Advanced IP Services, 64 MB Flash/256 MB DRAM →			
<b>VPN Accelerator</b>	None	None	None	AIM-VPN/EPII-PLUS
<b>Voice DSP</b>	C2801: PVDM2-8, C2811: PVDM2-16, C2821: PVDM 2-32, C2851: PVDM2-48 →			
<b>Call Processing License</b>	None	<ul style="list-style-type: none"> <li>C2801: 24-user CCME</li> <li>C2811: 36-user CCME</li> <li>C2821: 48-user CCME</li> <li>C2851: 96-user CCME</li> </ul>	<ul style="list-style-type: none"> <li>C2801: 24-user SRST</li> <li>C2811: 36-user SRST</li> <li>C2821: 48-user SRST</li> <li>C2851: 96-user SRST</li> </ul>	<ul style="list-style-type: none"> <li>C2801: 24-user CCME*</li> <li>C2811: 36-user CCME*</li> <li>C2821: 48-user CCME*</li> <li>C2851: 96-user CCME*</li> </ul>

\* Convertible to SRST



Secure  
Mobility

# Optimized for Secure Mobility



**Wireless Interface Card  
for Cisco® 1841, 2800, 3800 Series**

## Cisco 850 Series



- Stateful firewall and VPN
- 4-port 10/100 switch
- 802.11b/g option, single fixed antenna

## Cisco 870, 880 Series



- Higher performance
- Stateful firewall, VPN, IPS, antivirus, NAC
- 802.11b/g and 802.11n options, multiple antennas
- Advanced QoS features
- 4-port 10/100 managed switch
- Up to 3 VLANs

## Cisco 1800 Series



- Wire-speed performance
- Stateful firewall, VPN, IPS, antivirus, NAC
- Integrated backup port for redundant WAN links and load balancing
- 802.11a and 802.11b/g option, multiple antennas
- 8-port 10/100 managed switch, internal power supply, optional internal POE
- Up to 8 VLANs

# Integrated Wired/Wireless Access

## Business Problem

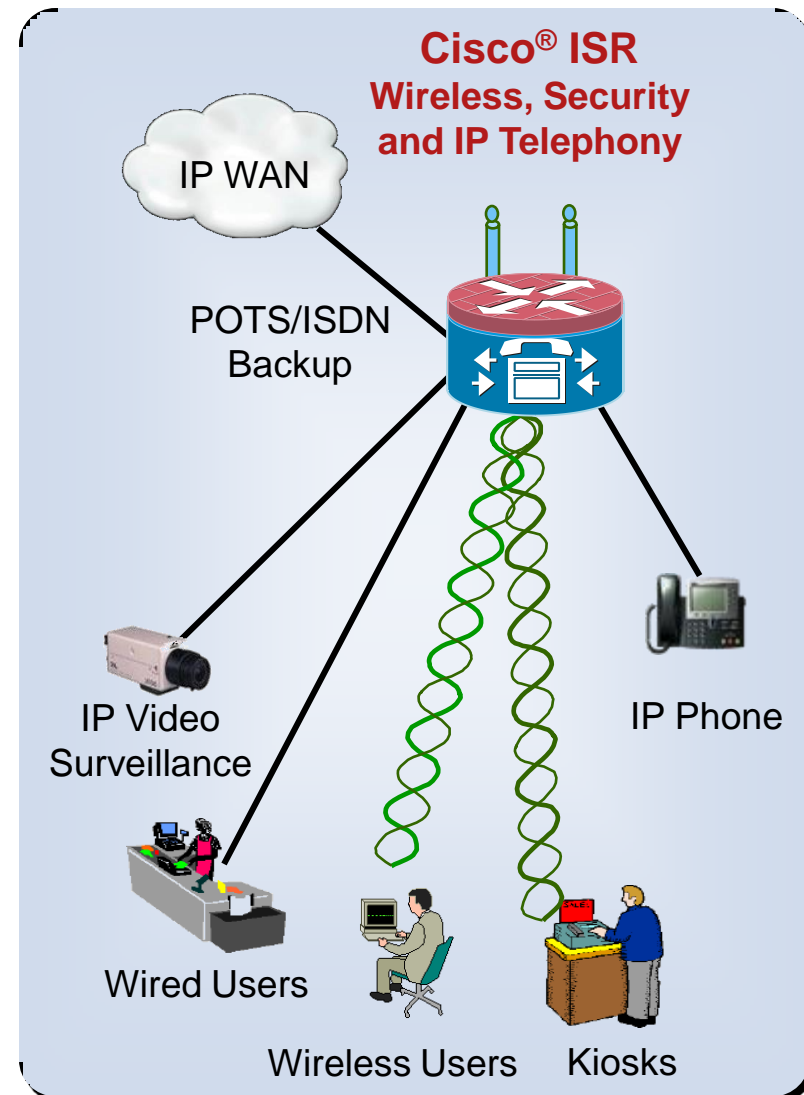
- Mobile access to critical applications and data throughout the site, while maintaining security

## Solution

- Integrated Wireless Access Points and Structured Wireless Aware Networks

## Benefits





- Convenient, easy-to-deploy integrated access points
- Rogue access point detection** to protect against unauthorized access
- Authentication:** 802.1x Cisco LEAP, PEAP-MSCHAPv2, PEAP-GTC, EAP-TLS, and EAP-FAST  
Local LEAP authentication takes over if RADIUS server is down
- Encryption:** TKIP encryption and support for static and dynamic 802.11 WEP keys
- State-of-the-art network management via CiscoWorks Wireless LAN Solution Engine





Secure  
Mobility

# Cisco IOS Secure Mobility Features

Feature	 Cisco® 870	 Cisco 880	 Cisco 1800 Fixed	 Modular with HWIC-AP (1800/2800/3800)
802.11 modes supported	802.11b/g	802.11b/g/n	802.11a/b/g	802.11a/b/g
Antennas	Diversity	MIMO	Diversity	Diversity
Dual-mode antennas	No	No	Yes (802.11a/b/g)	Yes (802.11a/b/g)
Replaceable antennas	Yes	Yes	Yes	Yes
AZR support	No	Yes	Yes	Yes
Number of SSIDs and wireless VLANs	10	16	16	16
LEAP, PEAP, EAP-TLS, 802.1x, static and dynamic WEP, PSK, WPA, TKIP/SSN, MAC auth, survivable local auth, RADIUS	Yes	Yes	Yes	Yes
WAN options	ADSL/G.SHDSL/ FE	ADSL/FE/ G.SHDSL/3G	ADSL/FE/ G.SHDSL	ADSL/FE/ G.SHDSL/Serial
Management	CCP, SDM, CLI	CCP, SDM, CLI	CCP, SDM, CLI	CCP, SDM, CLI

# Compliance Regulations Overview

Regulation	Information Protected	Date of Enforcement
HIPAA	Health information of patients	1996
GLBA	Consumer financial information	1999
SOX	Business financial and accounting information	2002
CA SB 1386*	Consumer personal information	2003
PCI	Credit card information	2008**

\*As of July, 2008, 44 states had passed security breach notification laws

\*\* PCI DSS version 1.2 (October)

# PCI Applies to Nearly Every Industry



# The Payment Card Industry (PCI) Data Security Standard



- Published January 2005
- Impacts ALL who **process, transmit, or store** cardholder data
- Also applies to 3<sup>rd</sup>-party hosting companies, information storage companies, etc.
- Monthly fines ranging from \$5,000 to \$50,000 for missed deadlines
- Has global reach**

Theater	Level 1	Level 2	Level 3
US	SEP 2007	DEC 2007	DEC 2008
Western Europe	Negotiated individually	MAR-DEC 2008	MAR-DEC 2008
Asia	DEC 2009	DEC 2009	DEC 2009
Canada	2008 TBD	2008 TBD	2008 TBD
Latin American CEMEA	Not Published yet		
CEMEA American Latin	Not Published yet		
Canada	2008 TBD	2008 TBD	2008 TBD

Source: pcisecuritystandards.org



# 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

## Management and Instrumentation



CCP



Role Based  
Access



NetFlow



IP SLA

# Total Security System Management

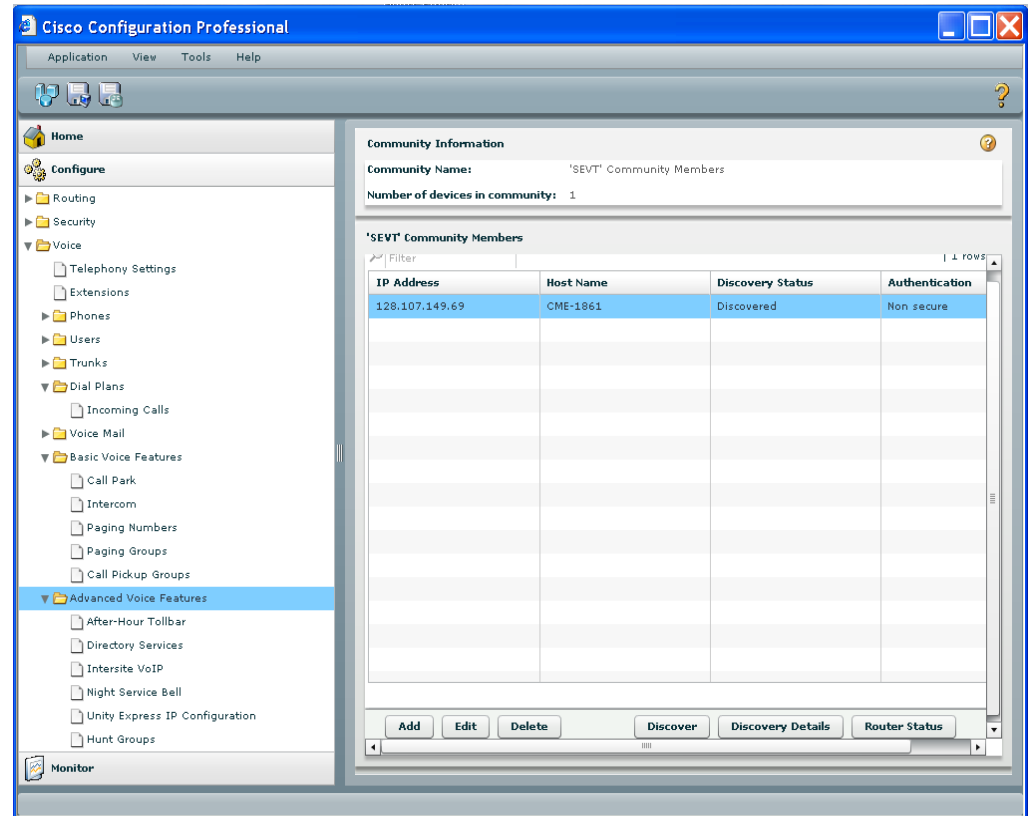


Reduced complexity for more effective risk analysis and operational control

# 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

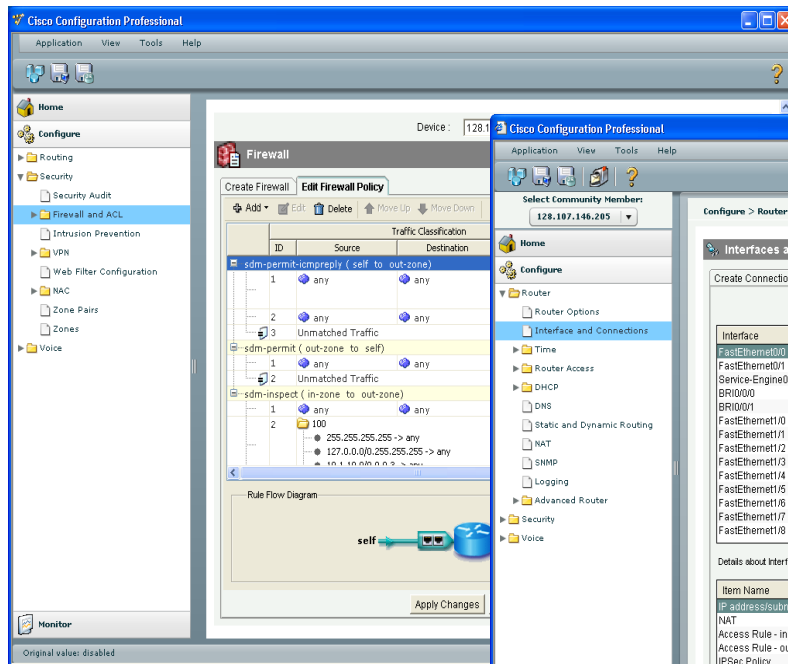
Free Download:  
<http://www.cisco.com/go/ciscocp>



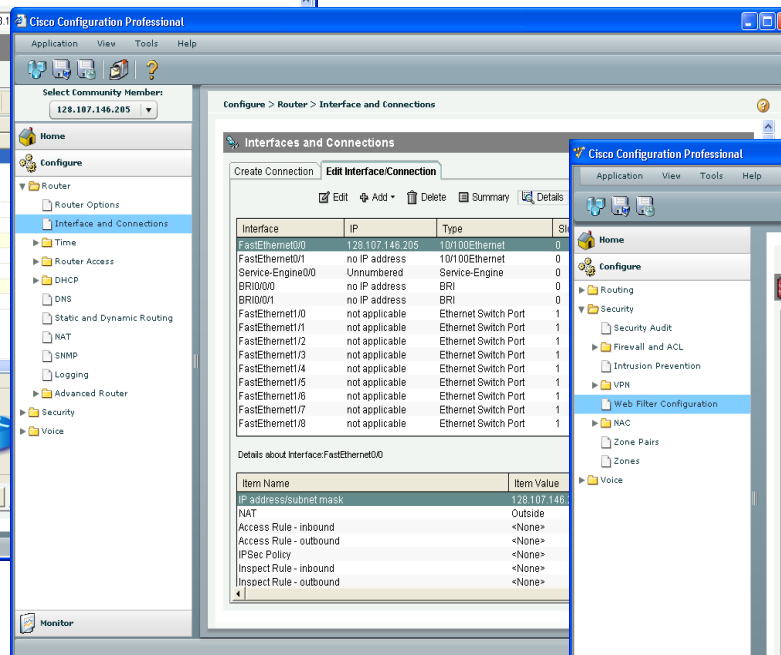
# Cisco CCP: Extensive Application Intelligence



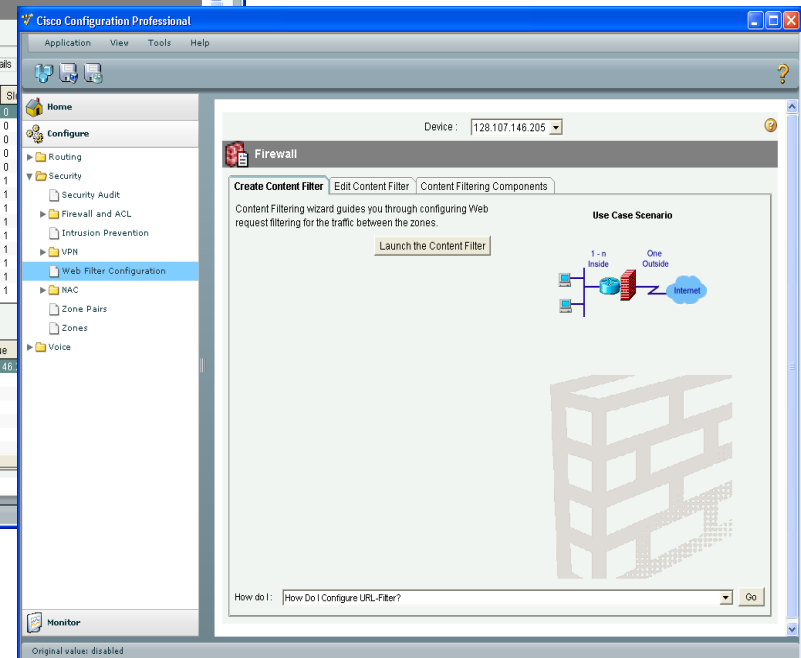
## Zone Based Firewall



## Interface Monitoring



## Content Filtering





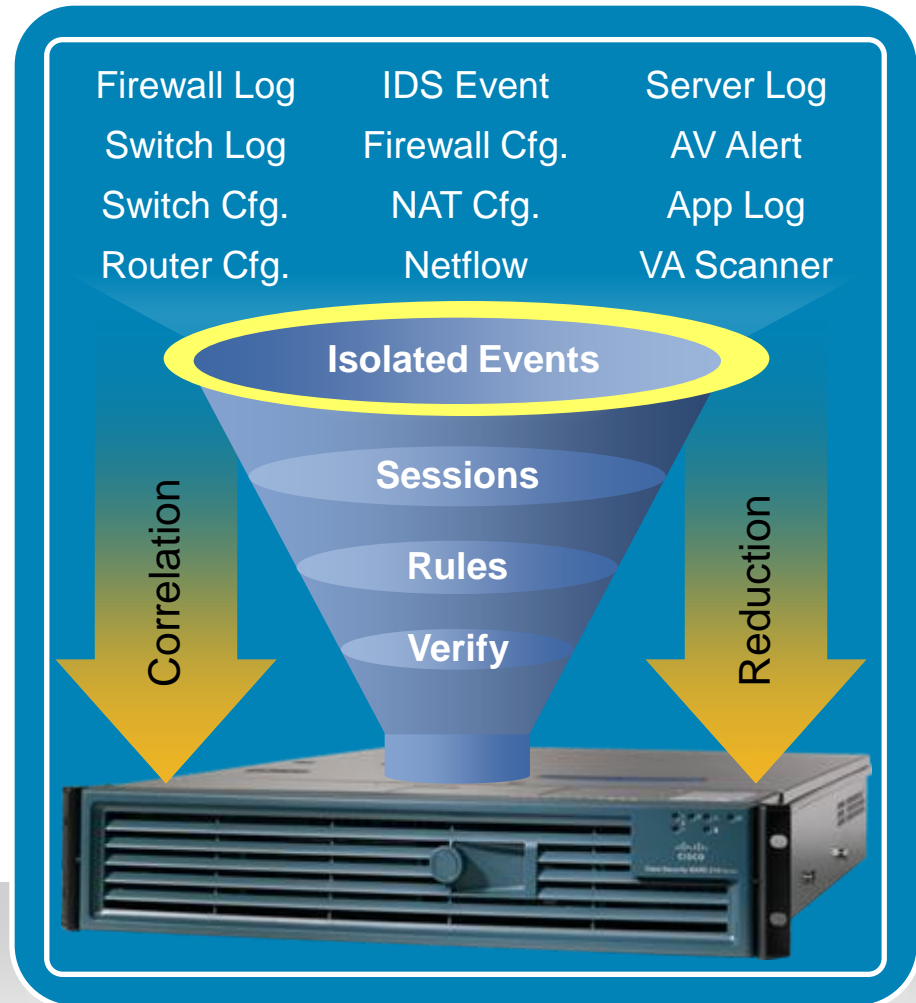
# Cisco Security Manager



- Unified services management for security including firewall, VPN, and IPS
- Intuitive, feature-rich user interface
- Different views for different administrative preferences
  - Device View
  - Topology View
  - Policy View
- Efficient management architecture for large-scale security deployments

# Cisco Security MARS

- MARS is an acronym = Monitoring, Analysis, and Response System
- Security threat mitigation appliance
- Rapid threat detection, isolation and mitigation, topologically aware
- Command and control for your existing network security
- Correlates data from across disparate multi-vendor security devices and applications





# Cisco IOS – Industry Leadership in Instrumentation

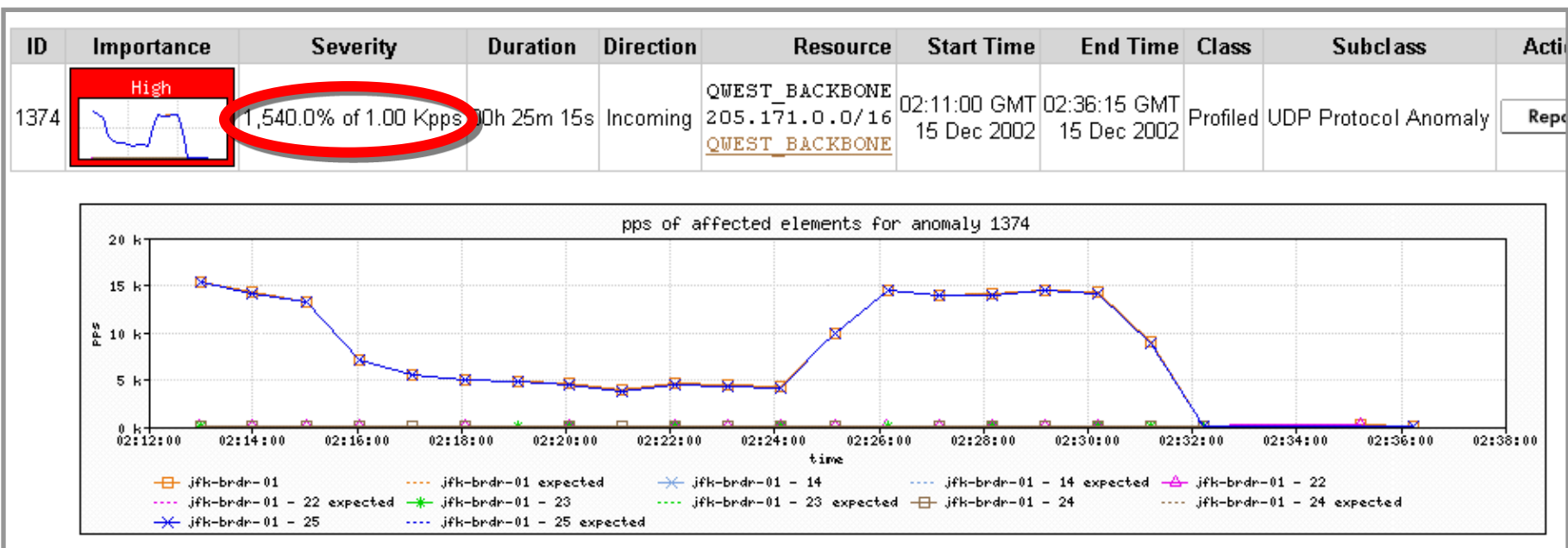
- Your network management system is only as good as the data you can get from the devices in the network
- For example, NetFlow and IPS feed into CS-MARS, delivering superior monitoring

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

- 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**



# Role-Based CLI Access

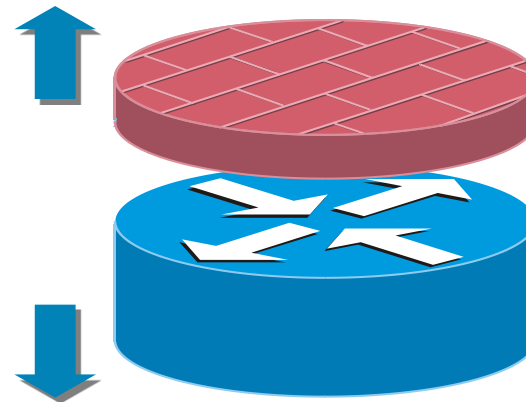
- Provide a view-based access to CLI commands
  - View: Set of operational commands and configuration capabilities
- User authentication is done via an external or internal AAA server (or TACACS+)
- Customer can define up to 15 views, plus one reserved for the root user

Customized Access to Match Operational Needs



**Security operator**

- Config AAA, NetFlow
- Show Cisco® IOS® Firewall, IPS



**Network engineer**

- Config routing
- Config interfaces
- Show

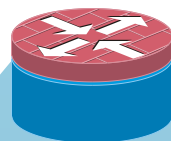
# Cisco IOS Secure Device Operation

Cisco® IOS® Security Feature	Function and Benefit
Encrypted web access	<ul style="list-style-type: none"> <li>Web-based device management (SDM) access encrypted with HTTPS</li> </ul>
Encrypted CLI access	<ul style="list-style-type: none"> <li>Telnet CLI and HTTPS secured with SSHv2 and SSL encryption</li> </ul>
Secure management access	<ul style="list-style-type: none"> <li>SNMPv3 allows secure management using off-the-shelf and custom applications</li> <li>Cisco IOS supports DES and AES encryption</li> <li>SANS Institute recently rated the highest network security concern after basic concerns like password</li> </ul>
Public key infrastructure (PKI)	<ul style="list-style-type: none"> <li>Provides advanced security when compared with traditional preshared keys</li> <li>Removes the danger of preshared keys falling into the wrong hands</li> </ul>
Secure RSA private key	<ul style="list-style-type: none"> <li>Protects against routers being taken over: if the hacker attempts to change the configuration, the private key is erased, rendering the router useless</li> </ul>
Certificate server	<ul style="list-style-type: none"> <li>Lightweight certificate server provided within Cisco IOS to ease deployment</li> </ul>
AAA integration	<ul style="list-style-type: none"> <li>Allows user or group-specific permissions to be stored conveniently in a AAA server</li> </ul>
Security audit	<ul style="list-style-type: none"> <li>Provides audit trail of configuration changes</li> </ul>
Role-based CLI access	<ul style="list-style-type: none"> <li>Allows separate sets of commands and levels of access</li> <li>Policy making separated from ongoing operations, providing accountability</li> </ul>
Configuration and event logging	<ul style="list-style-type: none"> <li>Logs configuration changes on per-user and per-session basis, ensuring reliable logging</li> <li>More visibility and accountability, greater confidence in reporting mechanism</li> </ul>

# Summary



# Only Cisco Router Security Delivers All This



## Secure Network Solutions



Business  
Continuity



Secure  
Voice



Secure  
Mobility

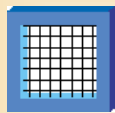


Compliance

## Integrated Threat Management



Advanced  
Firewall



Content  
Filtering



Intrusion  
Prevention



Flexible  
Packet  
Matching



Network  
Admission  
Control

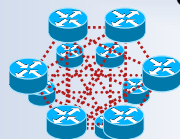


802.1x



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](http://www.cisco.com/go/routersecurity)



