Securing Places in the Network

Nadhem J. Al-Fardan
Consulting System Engineer
Cisco Systems - Saudi Arabia

AGENDA

The Agenda for the next **45** Minutes !

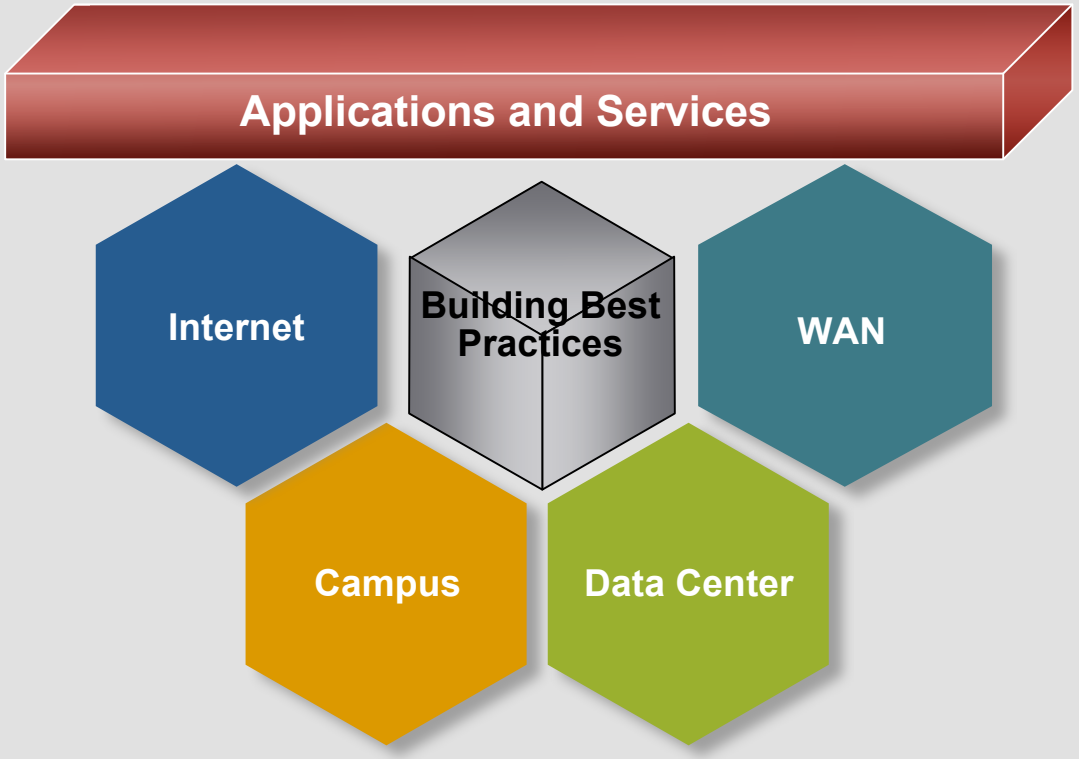
- What are the “Places in the Network” ?
- Place I - The Campus
- Place II - The Data Center
- Securing Services - Unified Communications (UC)


Lost City of Geraptiku
Island Mystic
Cooking Pot
Rock Pool
Gadgads Game
Techo Mtn
Trading Post
Training School
The Beach
Island Arena
Tiki Tours
Haiku Generator
Kitchen Quest
Island Market
Harbour
Tiki Tack
Beach Volleyball
Tombola
HARBOUR
Tropical Foods

Places in the Network

The Objective is to build best practices in architecting your network.

Today's session will look on how to secure some of these locations



Place I
The Campus

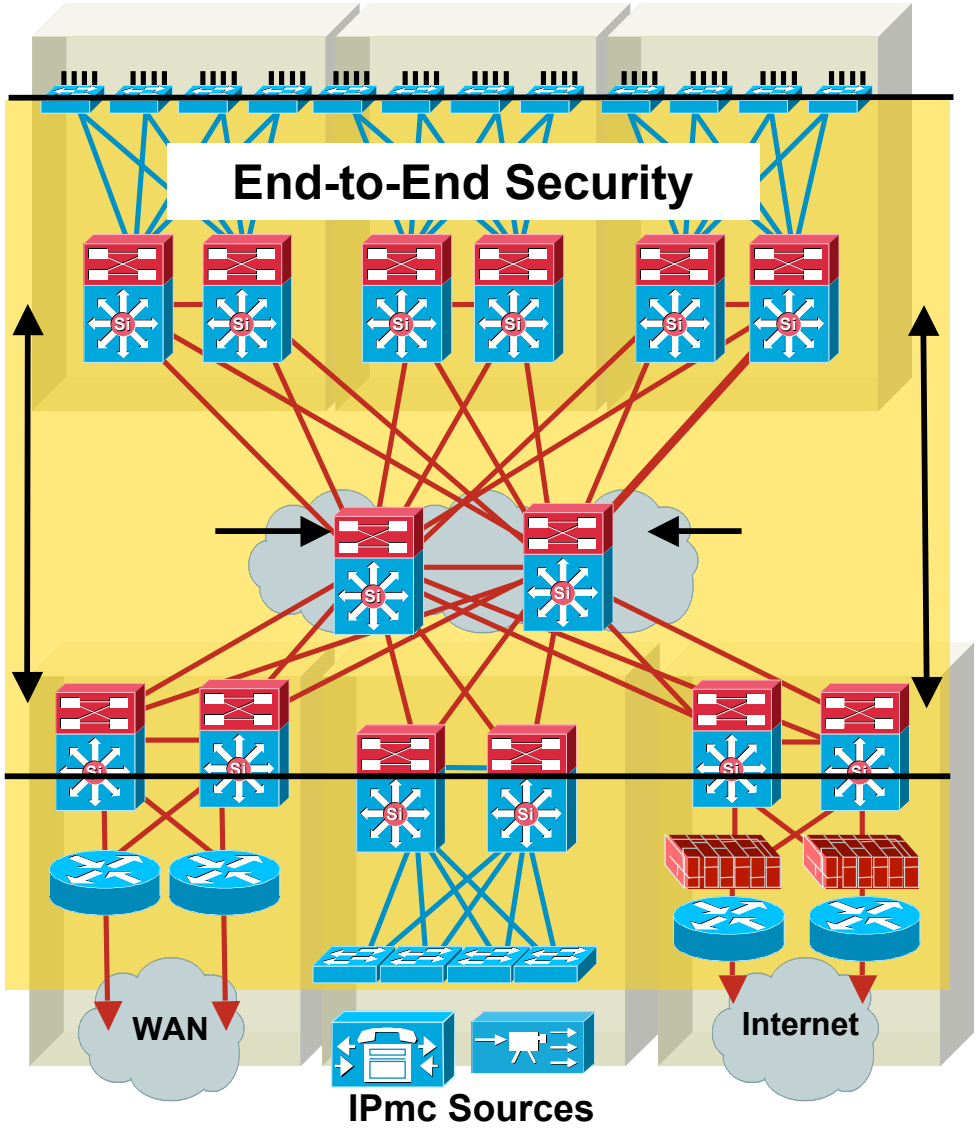
Campus Security - Best Practices

- **Catalyst Integrated Security Feature Set!**

  Dynamic Port Security, DHCP Snooping, Dynamic ARP Inspection, IP Source Guard

- Use SSH to access devices instead of Telnet
- Enable AAA and roles based access control (RADIUS/TACACS+) for the CLI on all devices
- Enable SYSLOG to a server. Collect and archive logs
- When using SNMP use SNMPv3
- Disable unused services:

  no service tcp-small-servers
  no service udp-small-servers
- Use FTP or SFTP (SSH FTP) to move images and configurations around – avoid TFTP when possible
- Install VTY access-lists to limit which addresses can access management and CLI services
- Enable control plane protocol authentication where it is available (EIGRP, OSPF, BGP, HSRP, VTP, etc.)
- Apply basic protections offered by implementing RFC2827 filtering on external edge inbound interfaces



BPDU Guard

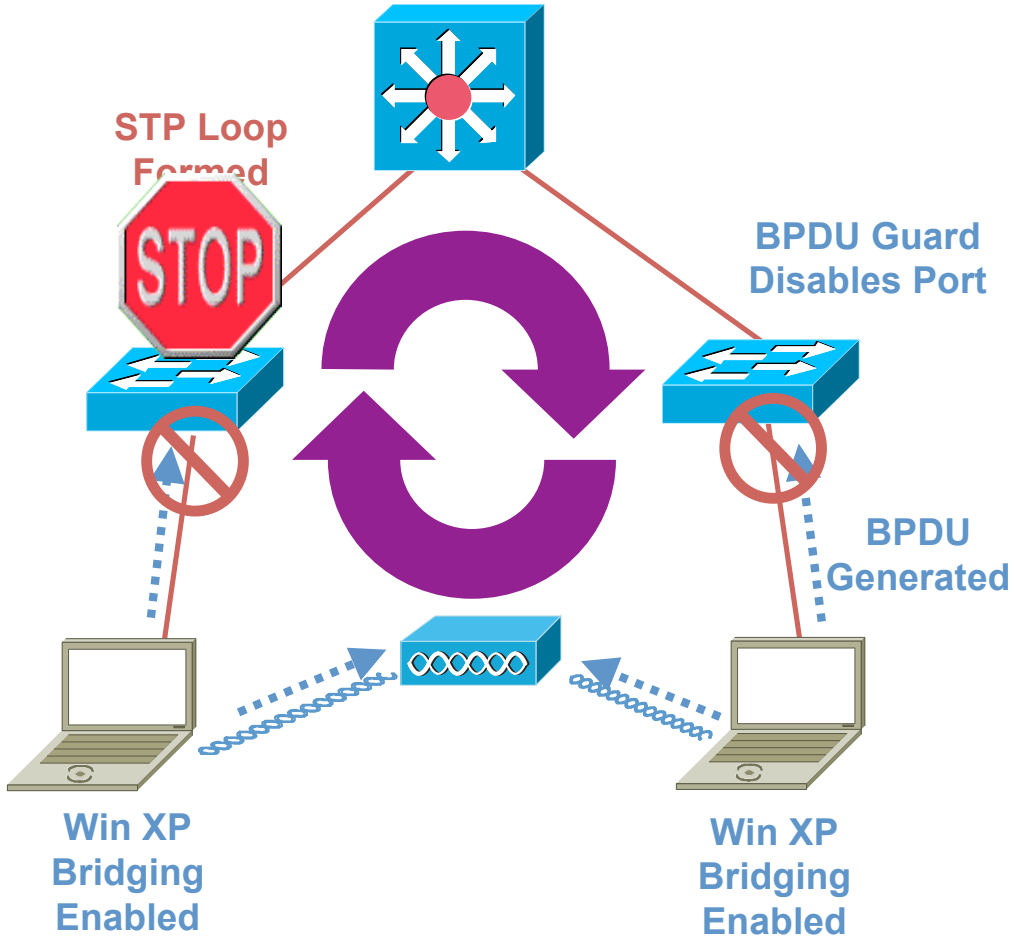
Prevent Loops via WLAN (Windows XP Bridging)

- **Problem:**

  Multiple Windows XP machines can create a loop in the wired VLAN via the WLAN

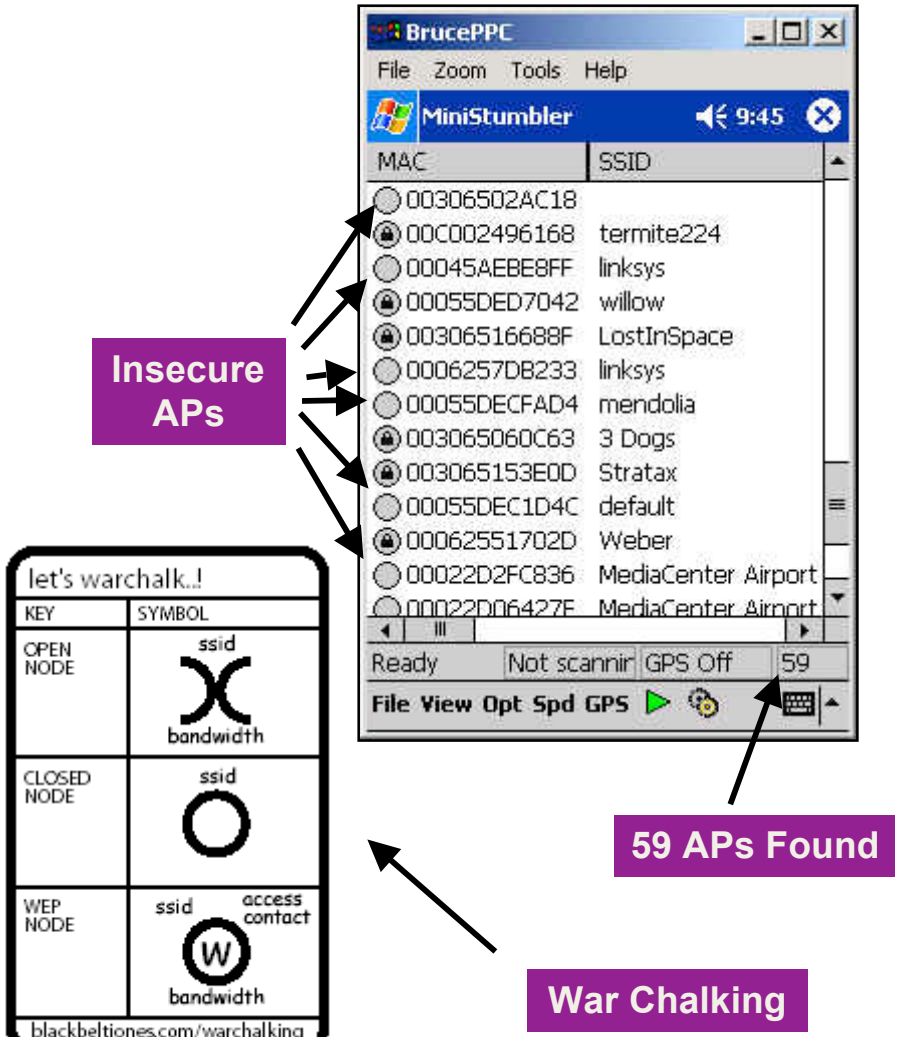
- **Solution:**

  BPDU Guard configured on all end station switch ports will prevent loop from forming



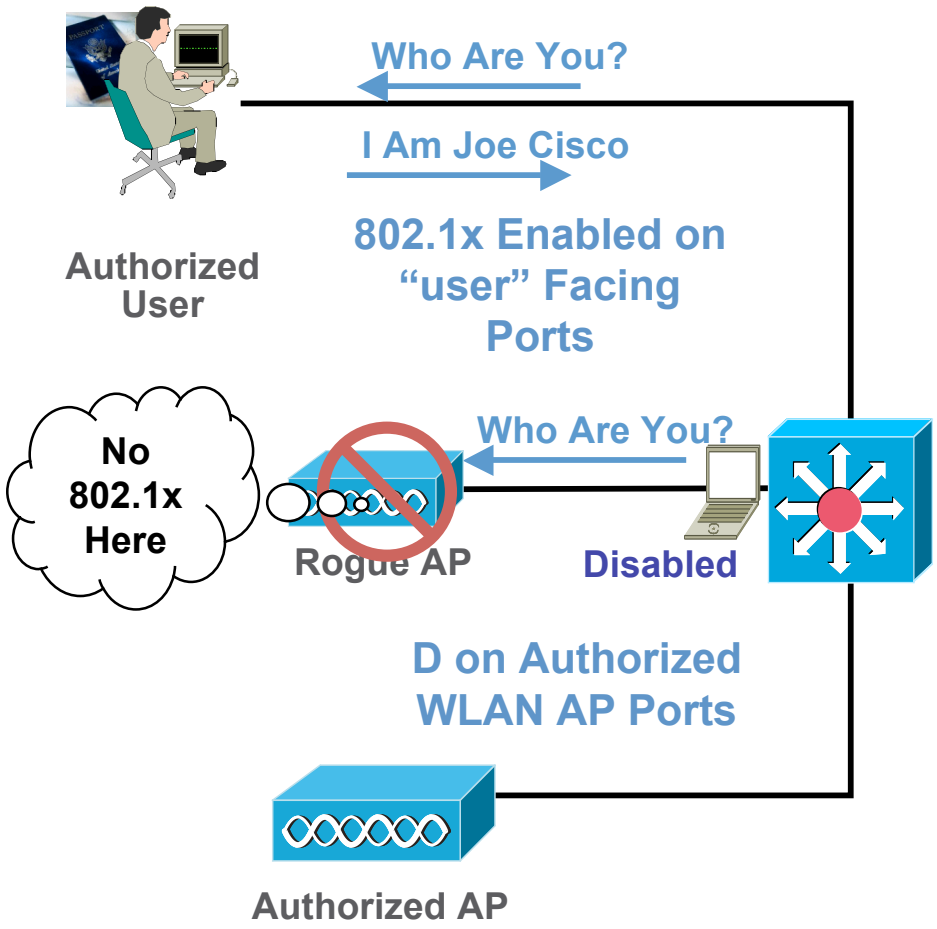
Problem: Prevalence of Rogue APs

- The majority of WLAN deployments are unauthorized by well intended employees (rogue APs)—many are insecure
- A daily drive to work taken within the car at normal speeds with a PDA running a freeware application (mix of residences and enterprises)
- Insecure enterprise rogue AP's are a result of:
  - Well intentioned staff install due to absence of sanctioned WLAN deployment
  - An infrastructure that is not "wireless ready" to protect against rogue AP's



Basic 802.1x Access Control

Controlling When and Where APs Are Connected



CatOS Configuration Example

```
set dot1x system-auth-control enable
set dot1x guest-vlan 250
set radius server 10.1.125.1 auth-port
1812 primary
set radius key cisco123
set port dot1x 3/1-48 port-control auto
```

Cisco IOS Configuration Example

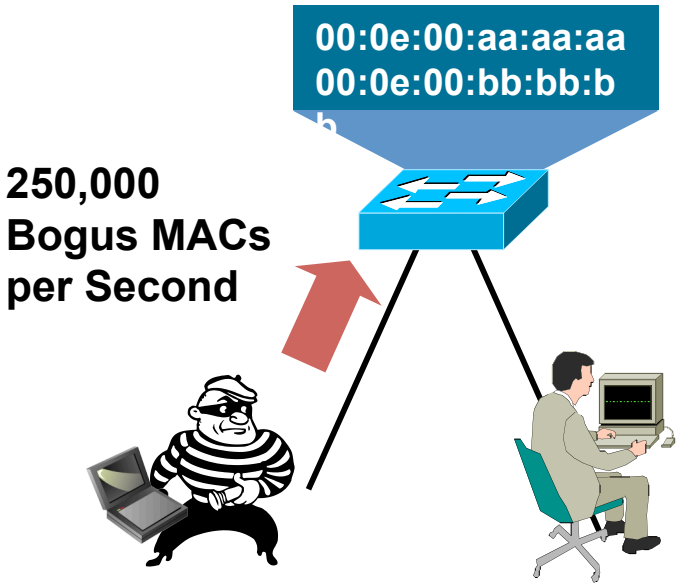
```
radius-server host 10.1.125.1
radius-server key cisco123
aaa new-model
aaa authentication dot1x default group
radius
aaa authorization default group radius
aaa authorization config-commands
dot1x system-auth-control
```

Cisco IOS Per-Port configuration

```
int range fa3/1 - 48
dot1x port-control auto
```

Securing Layer 2 from Surveillance Attacks

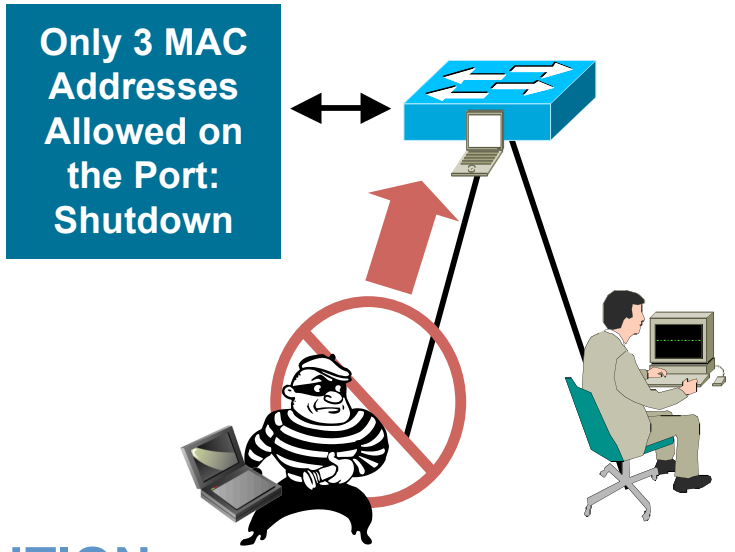
Cutting off MAC-Based Attacks



PROBLEM:

"Script Kiddie" Hacking Tools Enable Attackers Flood Switch CAM Tables with Bogus Macs; Turning the VLAN into a "Hub" and Eliminating Privacy

Switch CAM Table Limit Is Finite Number of Mac Addresses



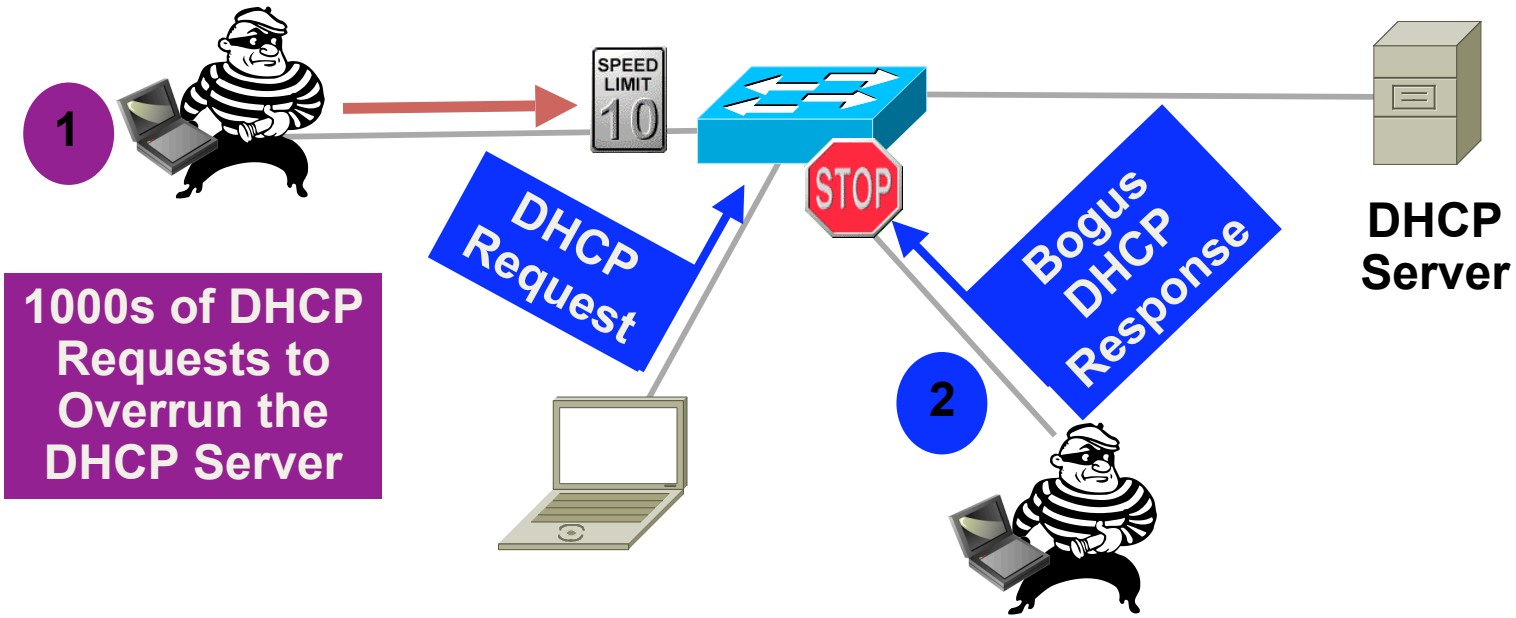
SOLUTION:

Port Security Limits MAC Flooding Attack and Locks down Port and Sends an SNMP Trap

```
switchport port-security
switchport port-security maximum 3
switchport port-security violation restrict
switchport port-security aging time 2
switchport port-security aging type inactivity
```

DHCP Snooping

Protection Against Rogue/Malicious DHCP Server

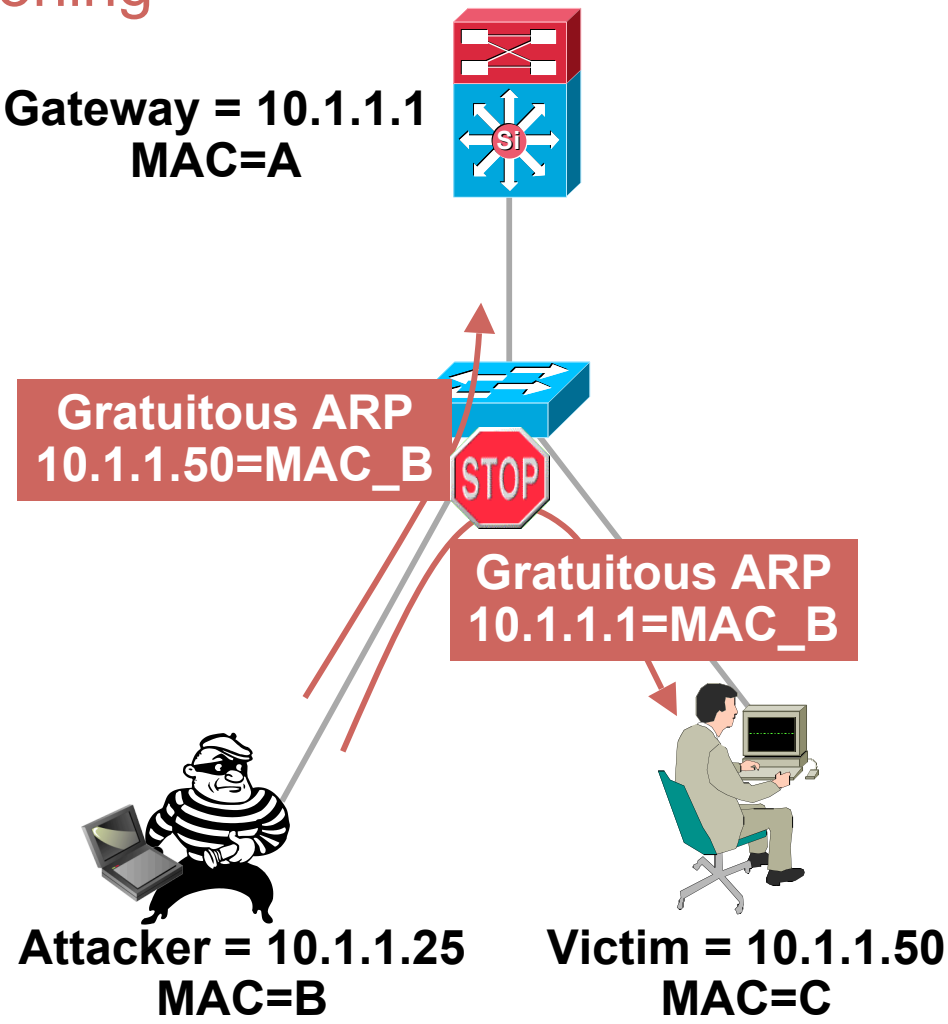


- DHCP requests (discover) and responses (offer) tracked
- Rate-limit requests on trusted interfaces; limits DOS attacks on DHCP server
- Deny responses (offers) on non trusted interfaces; stop malicious or errant DHCP server

Securing Layer 2 from Surveillance Attacks

Protection Against ARP Poisoning

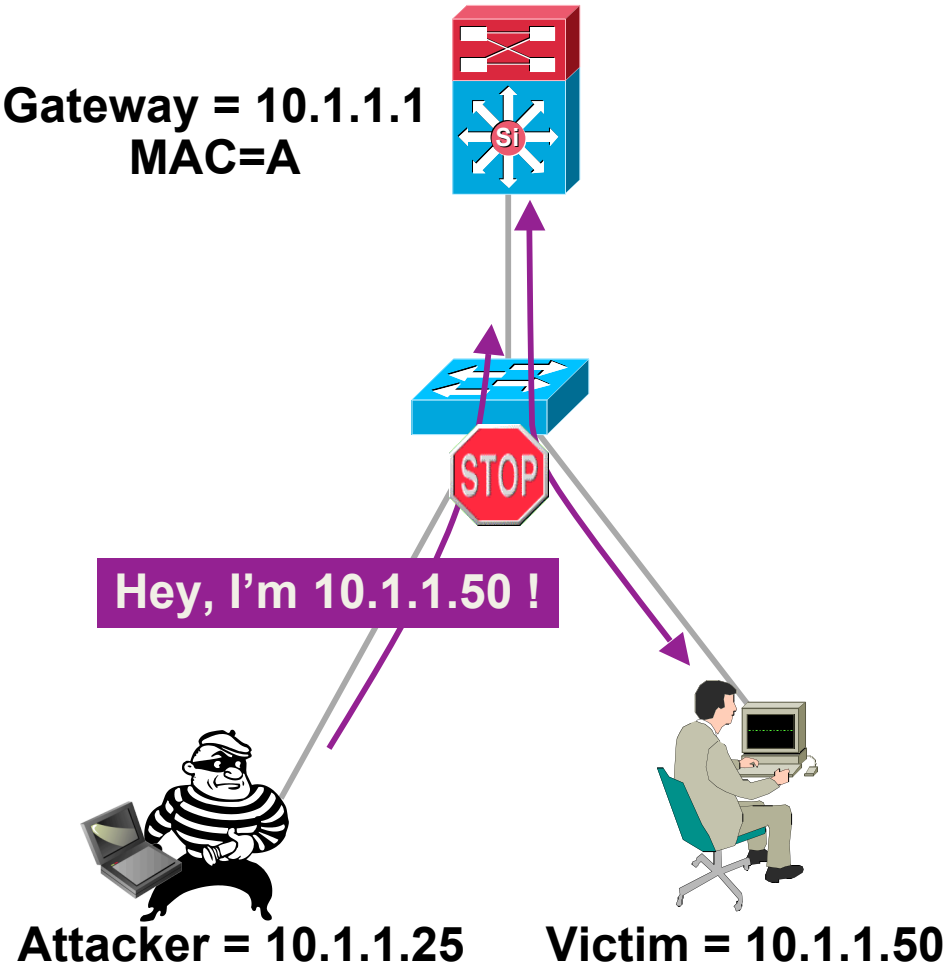
- Dynamic ARP inspection protects against ARP poisoning (ettercap, dsnif, arpspoof)
- Uses the DHCP snooping binding table
- Tracks MAC to IP from DHCP transactions
- Rate-limits ARP requests from client ports; stop port scanning
- Drop BOGUS gratuitous ARPs; stop ARP poisoning/MIM attacks



IP Source Guard

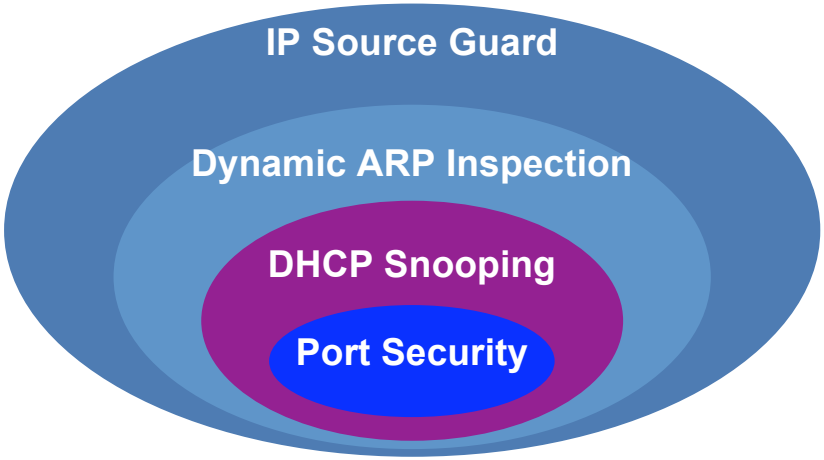
Protection Against Spoofed IP Addresses

- IP source guard protects against spoofed IP addresses
- Uses the DHCP snooping binding table
- Tracks IP address to port associations
- Dynamically programs port ACL to drop traffic not originating from IP address assigned via DHCP



Catalyst Integrated Security Features

Summary Cisco IOS



- Port security prevents MAC flooding attacks
- DHCP snooping prevents client attack on the switch and server
- Dynamic ARP Inspection adds security to ARP using DHCP snooping table
- IP source guard adds security to IP source address using DHCP snooping table

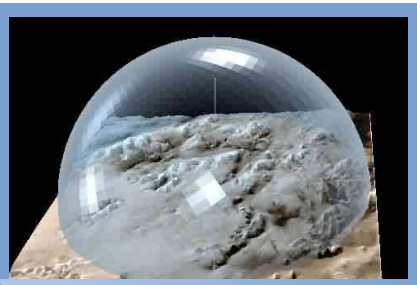
```
ip dhcp snooping
ip dhcp snooping vlan 2-10
ip arp inspection vlan 2-10
!
interface fa3/1
switchport port-security
switchport port-security max 3
switchport port-security violation
restrict
switchport port-security aging time 2
switchport port-security aging type
inactivity
ip arp inspection limit rate 100
ip dhcp snooping limit rate 100
ip verify source vlan dhcp-snooping
!
Interface gigabit1/1
ip dhcp snooping trust
ip arp inspection trust
```

Place II
The Data Center

Secure Data Center

Data Protection

- Perimeter Protection
- Encryption Services
- Virtualized data inspection services
- XML Security



Service Resilience

- Load sharing and acceleration
- Application protection
- SSL Offload and load balancing
- e-Mail spam prevention

Compliance Issues

- SOX
- PCI
- HIPAA
- Gramm-Leach-Bliley Act (GLBA

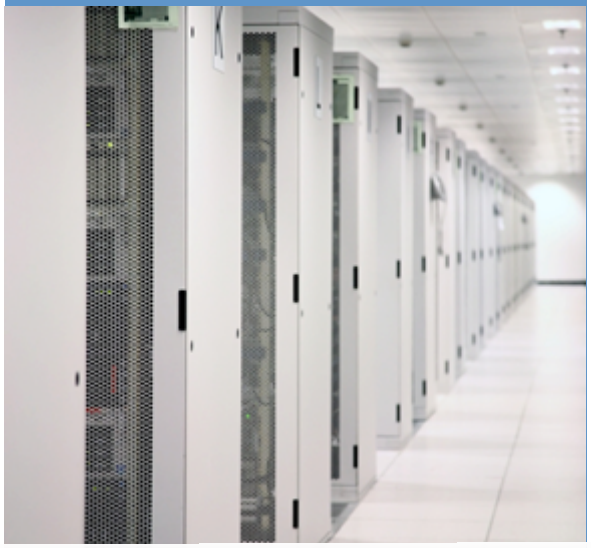
Business Continuity

- Effective crisis management
- Protected data redundancy
- Improved global access to core critical services and data

Three Tiers of Data Center Security

1

Features of a typical data center design



2

Higher level of protection from DDoS and malicious traffic

3

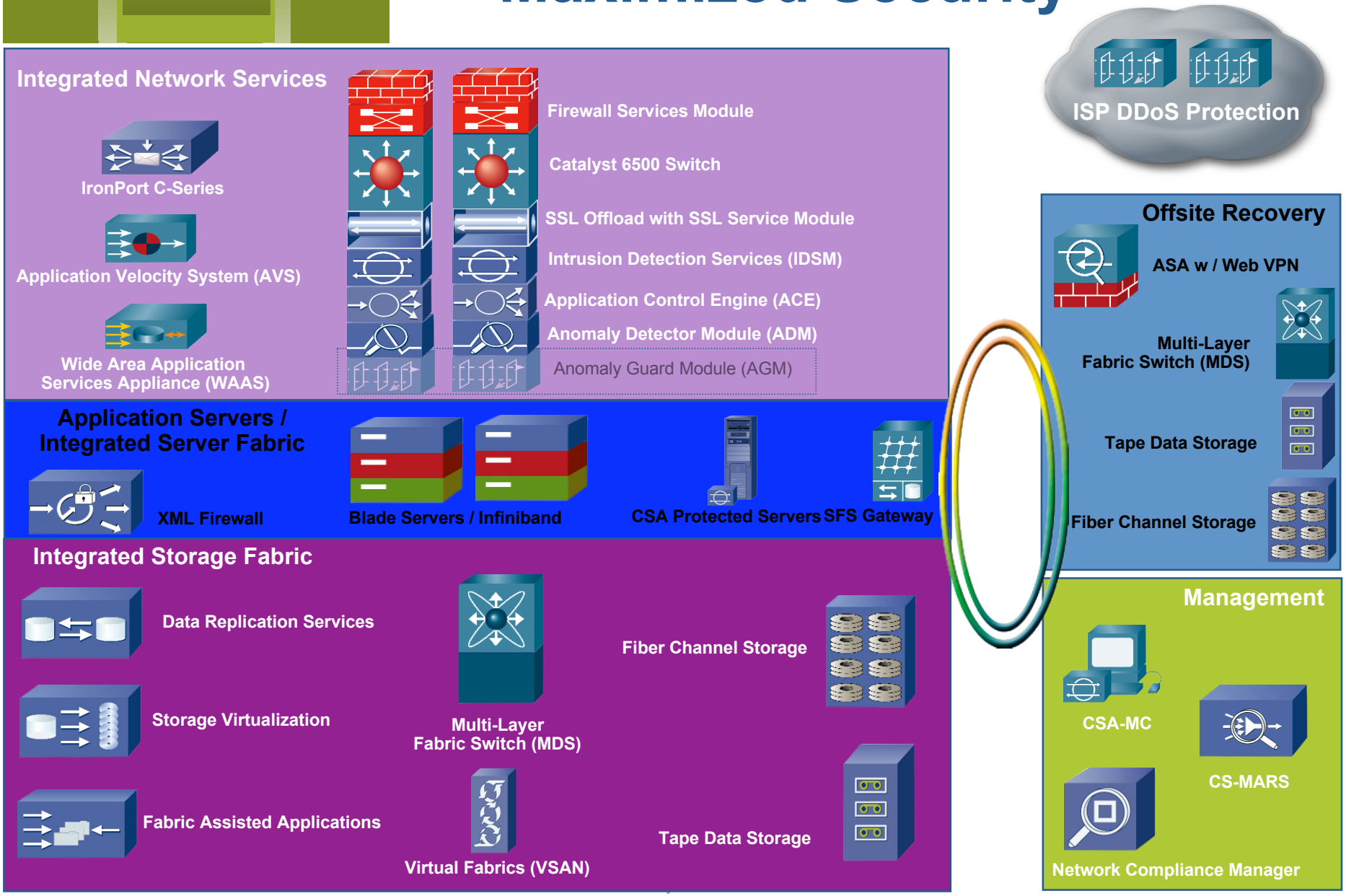
Maximum protection at the application and data layers

Data Center Security - In a Nutshell

- Security considerations for Data Center must address
  - Business Continuity
  - Regulatory Compliance
  - Mitigating risk to service availability, service integrity and service confidentiality
- Secure Data Center Designs leverage breadth and depth of defense
  - NETWORK-WIDE not PRODUCT NARROW
- Services Layer design critical to delivery of Virtualized and High-touch security services
- Differentiate technologies based on customer requirements and placement within the Data Center
- Deliver Secure Data Center designs based:
  - Scalable network
  - Agile services
  - Highly Available
  - Validated approach

DC

Maximized Security



Secure Data Center

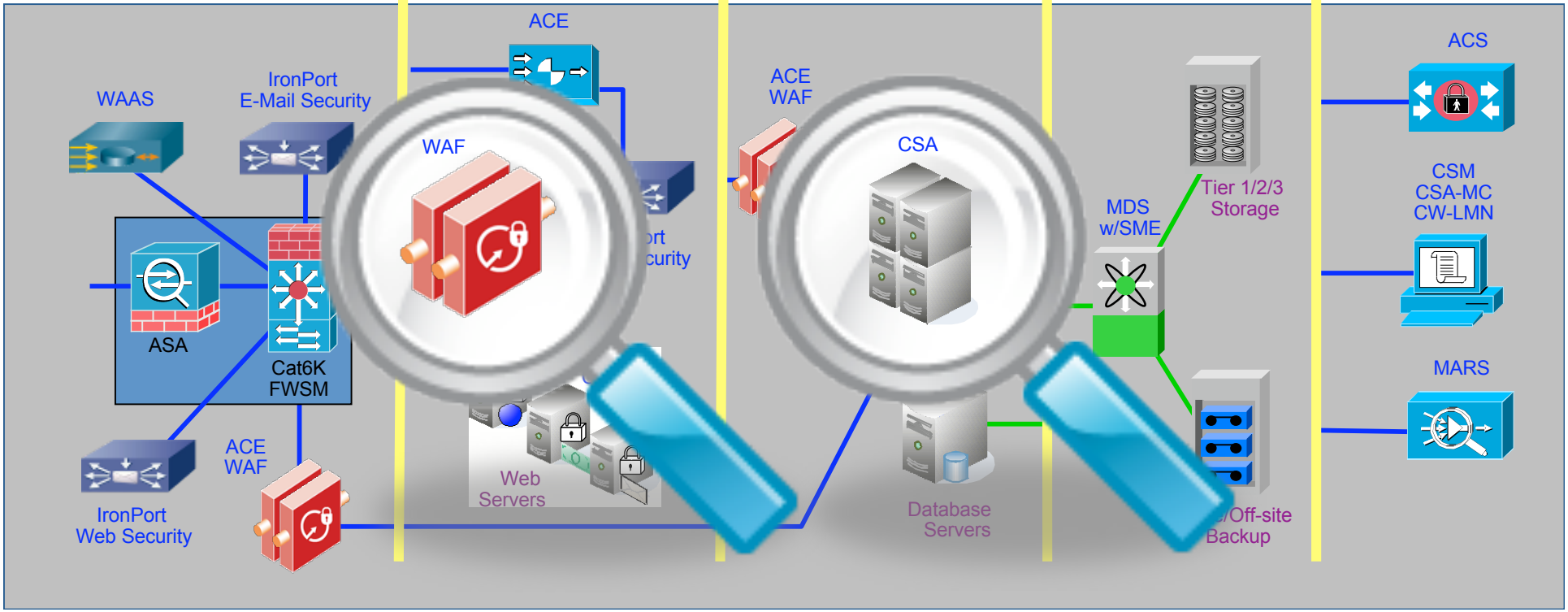
Data Center Edge
- Firewall & IPS
- DOS Protection
- App Protocol Inspection
- Web Services Security
- VPN termination
- Email & Web Access control

Web Access
- Web Security
- Application Security
- Application Isolation
- Content Inspection
- SSL Encryption/Offload
- Server Hardening

Apps and Database
- XML, SOAP, AJAX Security
- XDoS Prevention
- App to App Security
- Server Hardening

Storage
- Data Encryption
  - •In Motion
  - •At Rest
- Stored Data Access Control
- Segmentation

Mgmt
- Tiered Access
- Monitoring & Analysis
- Role-Based Access
- AAA Access Control



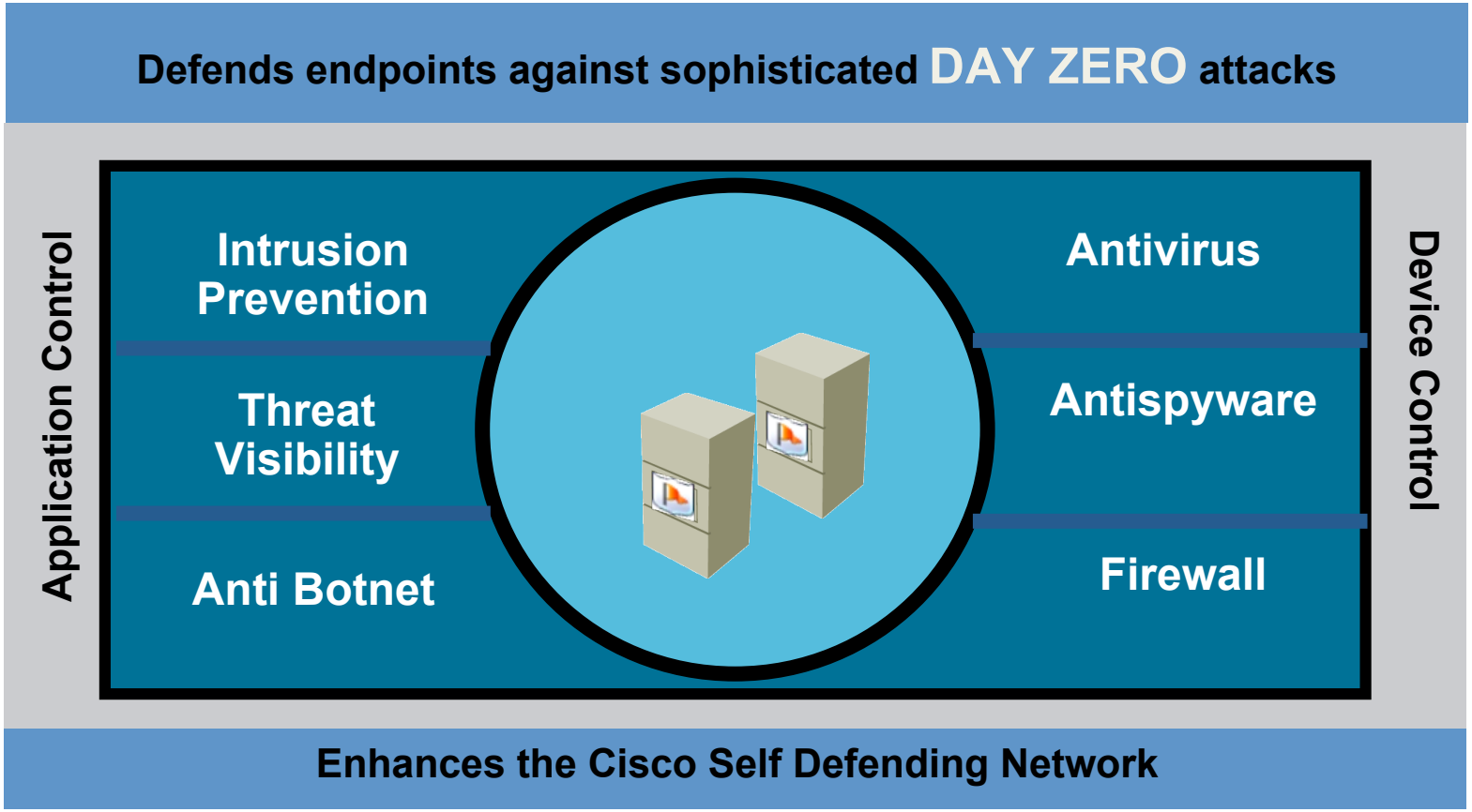
The Effect of Application Attacks

Web Application Threats

- Cross-site scripting
- SQL injection
- Command injection
- Cookie and session poisoning
- Parameter and form tampering
- Buffer overflow
- Directory traversal and forceful browsing
- Cryptographic interception
- Cookie snooping
- Authentication hijacking
- Error-message interception
- Attack obfuscation
- Application platform exploits
- DMZ protocol exploits
- Security management attacks
- Day-zero attacks

- **Theft of customer data**
- **Access to unpublished pages**
- **Unauthorized application access**
- **Password theft**
- **Modification of data**
- **Disruption of service**
- **Website defacement**
- **Recovery and cleanup**

Endpoint Security for Servers



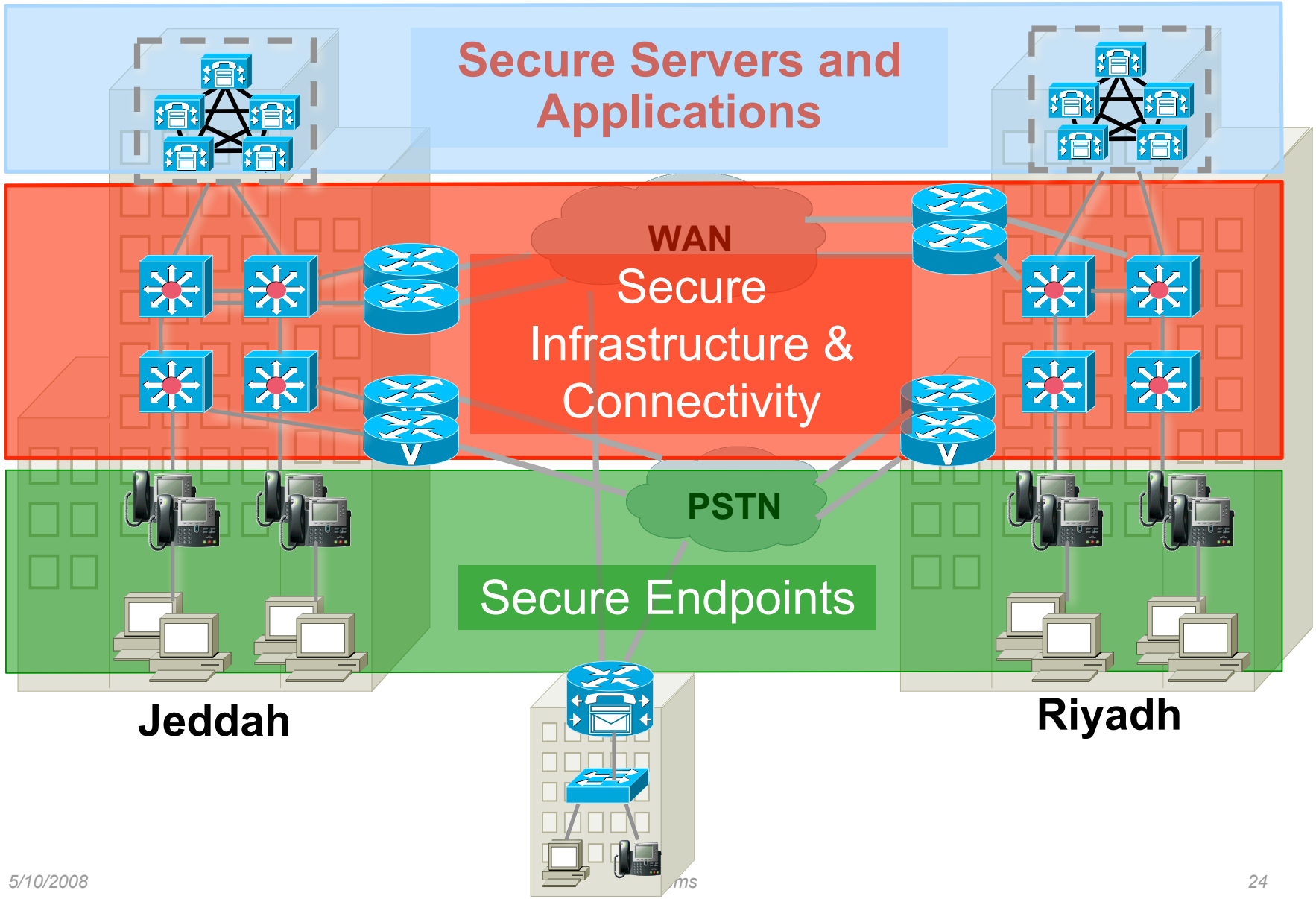
Securing the Layers
Defense in Depth - Best Practices

- Secure Management-Plane
  - -Secure communications to Nodes
  - -Ensure CLI Access available at all times
- Secure Control-Plane
  - -Shield network from direct attack and from collateral damage
- Secure Data-Plane
  - -Block malicious packets at the Edge of the network
- Services-Plane
  - -Managed Security Services
  - -Application Security
  - -Virtualization

- CORE/AGGREGATION
  - -Secure Bandwidth resources
  - -Segmentation (VLAN, PVLAN, VRF)
- ACCESS
  - -Secure Server to Server traffic
  - -Traffic Marking and Policing
  - -L2 Edge Filtering
- SANs
  - -Secure Access to storage resources
  - -Segmentation (VSANS)

Securing Services
Unified Communications

Secure Unified Communications



Building A Secure UC System
Protecting all elements of the UC system

Infrastructure

Secure connectivity and transport

Endpoints

Authenticated IP phones, soft clients and other devices

Call Control

Secure Protocols for Call Management Features

Applications

Auto-attendant, Messaging, and Customer Care

Network as the Platform

Secure UC Threats and Risks Examples

- **Eavesdropping**

  Listening/Recording to audio or video conversations

  Risk: Loss of Privacy (Regulatory Issues, Reputation)

- **Denial of Service (Internal)**

  Loss of service

  Risk: Loss of Productivity, Safety and Security impact (#999)

- **Compromised System Integrity**

  Hacker control of applications or call control infrastructure

  Risk: Financial (Toll Fraud), Data Theft, Regulatory Issues (Loss of Privacy)

- **Compromised UC Clients (e.g. Softphones)**

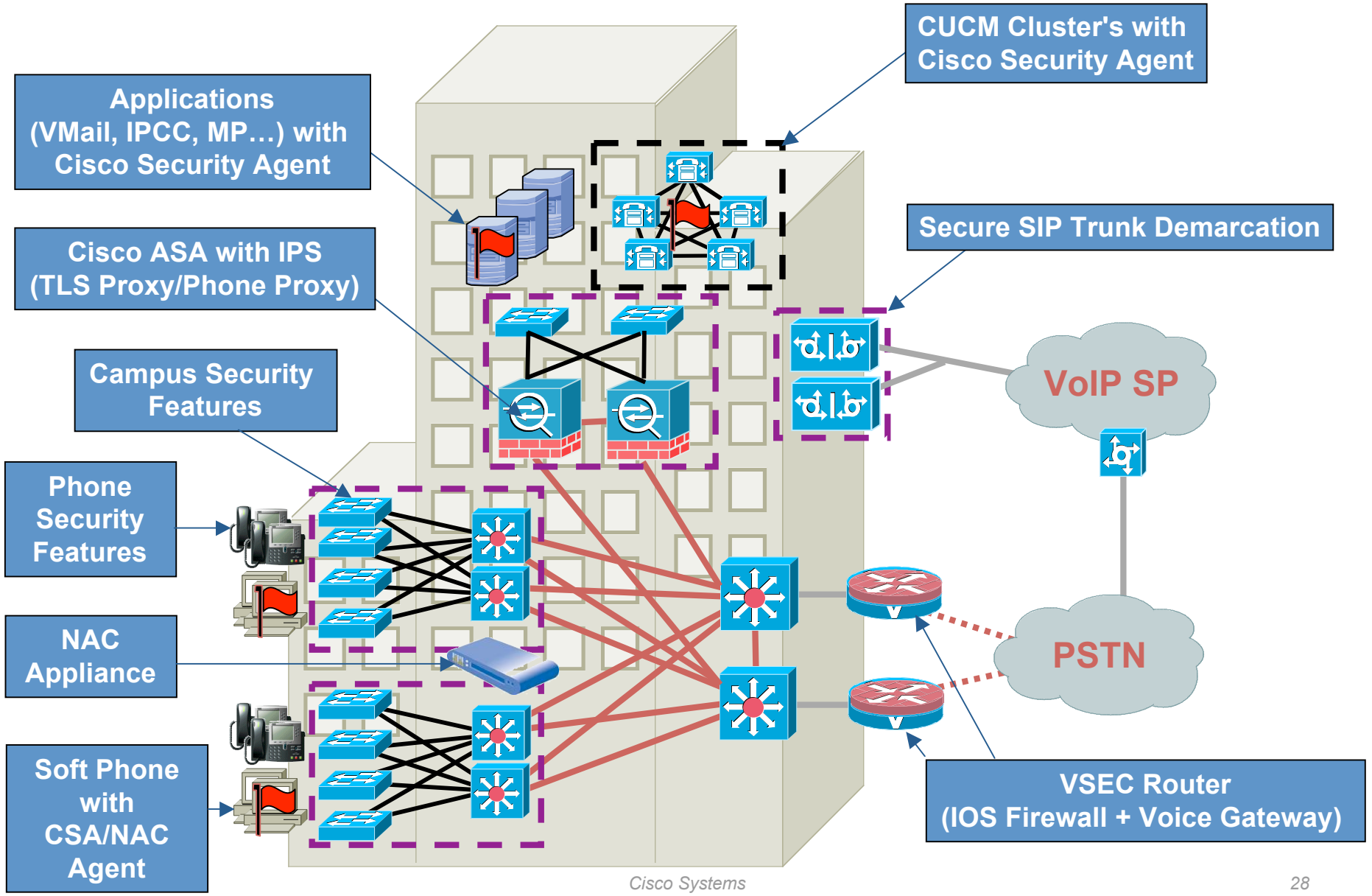
  Hacker control of platforms that are UC Clients

  Risk: Financial (Toll Fraud), Data Theft (egg Customer Information - IPCC Agent Desktop)

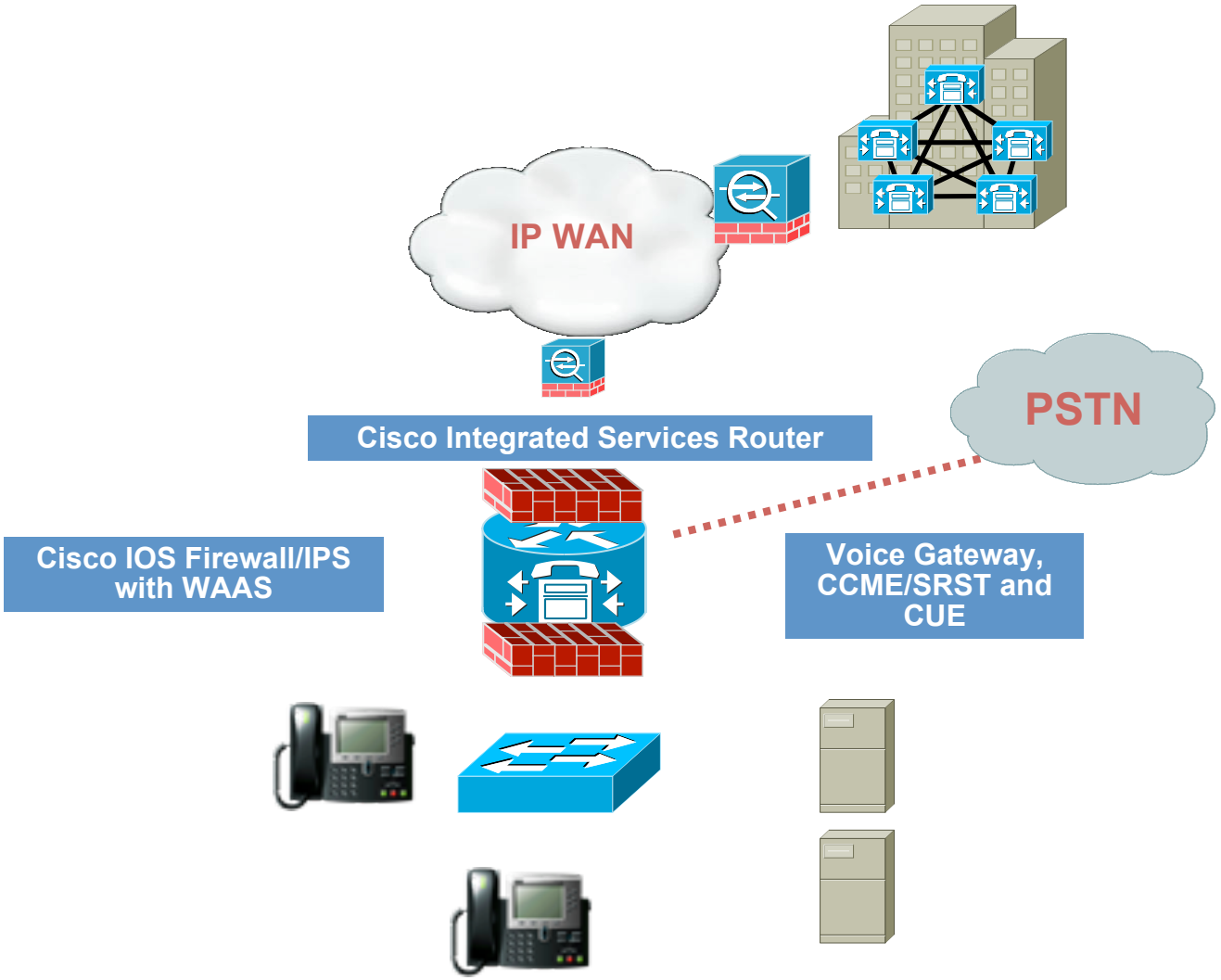
Best Practice for Secure Unified Communications

Base	Intermediate	Advanced
Basic Layer 3 ACL's	Firewalls with stateful inspection	Firewall with advanced application inspection (and encrypted VoIP support)
Separate voice/data VLANS	Rate Limiting	NAC / 802.1X
Standalone Cisco Security Agent (CSA)	Limit MAC Address Learning	TLS / SRTP to Phones
Approved Antivirus	Dynamic ARP Inspection	IPSec/TLS & SRTP to Gateways
Disable Gratuitous ARP	IP Source Guard	TLS/SRTP to applications (Unity)
Smart Ports (Auto QoS)	Dynamic Port Security	Encrypted Config Files
Signed Firmware and Configs	DHCP Snooping	Advanced O/S Hardening
Classes of restriction (Toll Fraud prevention)	Managed CSA	
Cisco Patches	Intrusion prevention services	

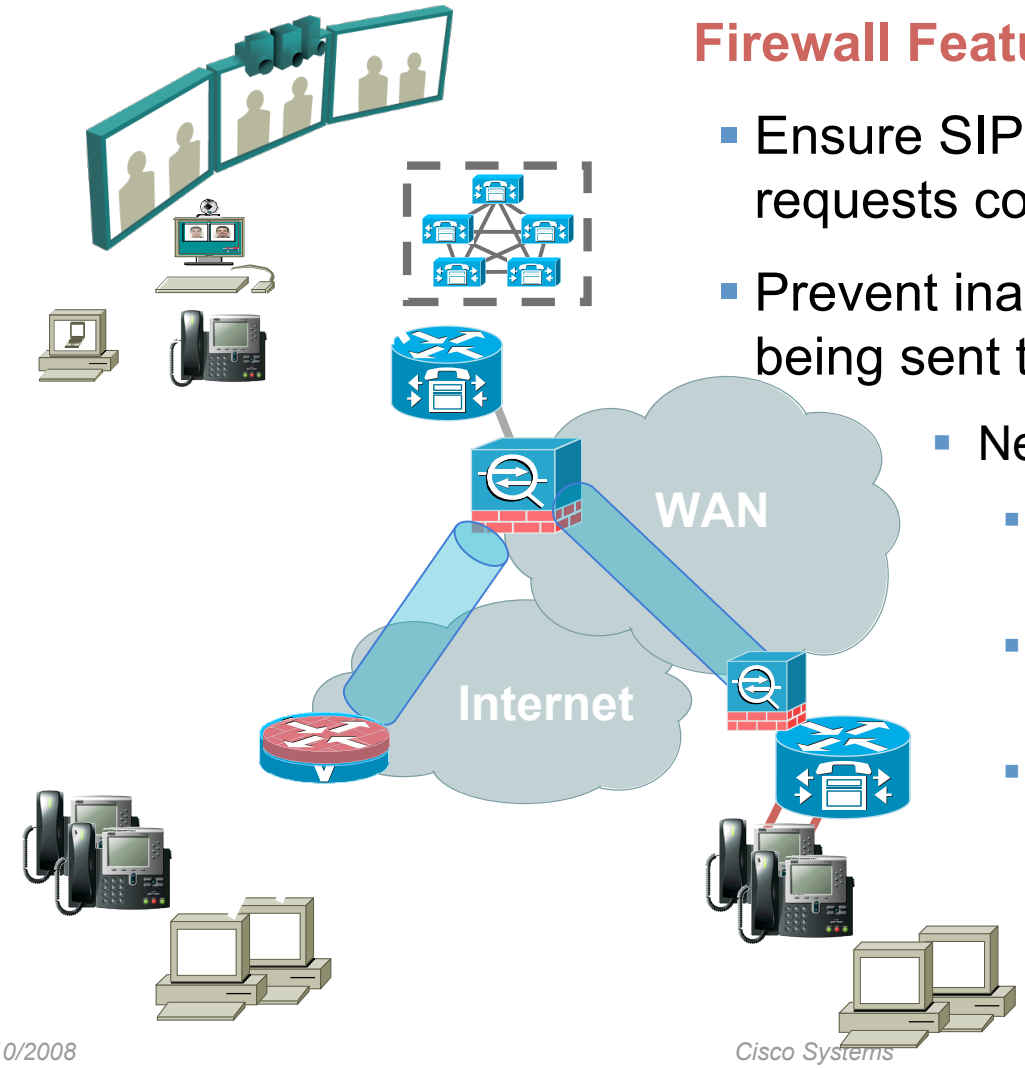
Secure UC Campus



Secure UC Branch



ASA for Secure Unified Communications
Protecting the Telephony Infrastructure and enabling UC Services



Firewall Features:

- Ensure SIP, SCCP, H.323, MGCP requests conform to standards
- Prevent inappropriate SIP Methods from being sent to Communication Manager
  - Network Rate Limit SIP Requests
    - Policy enforcement of calls (white list, blacklist, caller/called party, SIP URI)
    - Dynamic port opening for Cisco applications
    - Enable only “registered phones” to make calls
      - Enable inspection of encrypted phone calls

Links to Resources

- **Cisco Security Center**
  http://www.cisco.com/security
- **Open Web Application Security Project (OWASP)**
  http://www.owasp.org
- **SANS Institute**
  http://www.sans.org


CISCO