NETWORKERS

Cisco Systems

Network Security: Design and Attack Mitigation

Session SEC-201

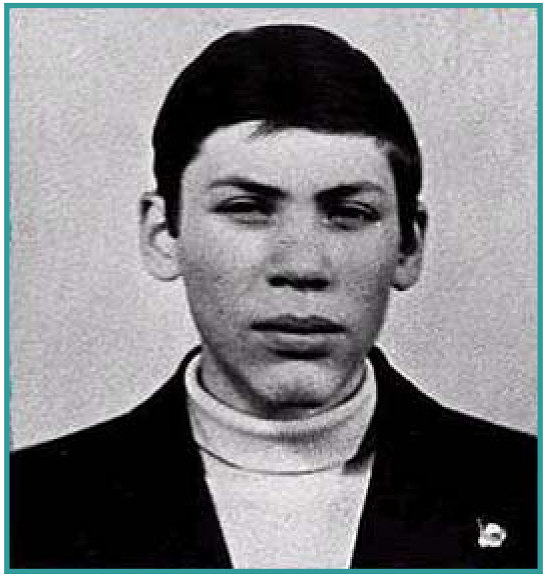
Agenda

- Security Design Overview
- Integrated Security Solution
- Distributed Security Solution
- High-End Resilient Security Solution
- Conclusion

Historical Hacks Sprinkled Throughout to Keep Everyone Awake!

History Hack #1:
Vladimir Levin and Citibank

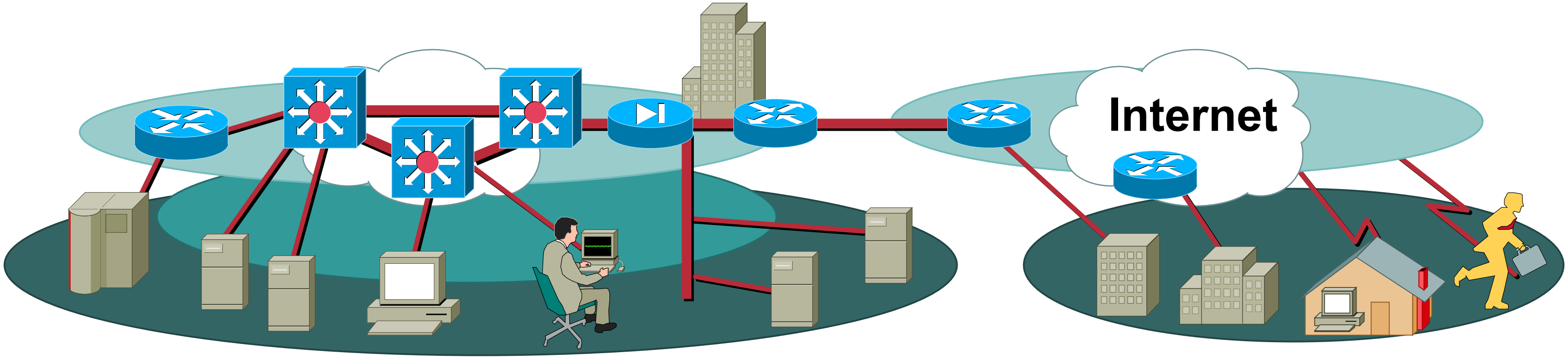
- In 1994 broke into Citibank's Customer Cash Management Account system and transferred funds to friends totaling up to around $4 million dollars over a period of 3 months ($10 million by some accounts)
- Broke in through phone system, not Internet, and apparently eavesdropped to capture PINS/passwords, then used them to gain access to accounts and conduct transactions
- Transfers conducted during off-hours for target accounts, and noticed by chance due to late night banking activity
- Rumors abound about insider involvement, though none proven
- Moral of the story? Secure identity systems matter



Vladimir Levin

Collage of Sources Including:
http://www.discovery.com/area/technology/hackers/levin.html
http://www.arraydev.com/commerce/JIBC/9601-07.htm

Overall Security Design Goals



- "Network security is a system"
- Security throughout the infrastructure
- Secure management and reporting
- Authentication of key users and operators
- Intrusion detection for critical areas
- Accommodation of emerging network apps

Functional Design Requirements

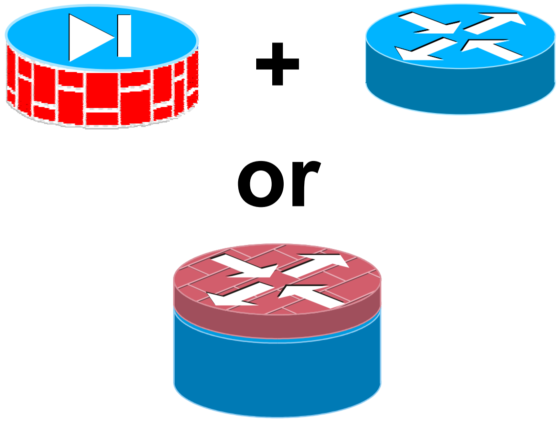
- **Solution should provide:**
  - Internet access
  - Site-to-site VPN
  - Remote access
  - Campus connectivity
  - Wireless LAN
  - IP telephony

Design Considerations

- General considerations
  - Integrated vs. dedicated security functions
  - Device specific
  - Network wide
  - IDS architecture
  - Logging architecture
- Wireless LAN
- IP telephony

Integrated vs. Dedicated

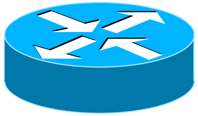
- Performance
  - Software vs. hardware
- Management
  - Net ops or Sec ops
- Risk mitigation
  - Multi-vendor, multi-device
  - Statistical probabilities
- Configuration
  - Routers and switches default open
  - Most security devices default closed
- Resilience considerations
- Complexity
  - Topology vs. device configuration



+

or

Device Specific Security: Routers



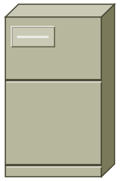
- Potentially a hacker's best friend
  - Effect availability of network, not just end-point services (DDoS)
  - Eavesdropping, man-in-the-middle
- Protection should include:
  - Constraining telnet access
  - SNMP read-only
  - Administrative access with TACACS+
  - ACLs to specify the management station
  - Turning off unneeded services
  - Logging unauthorized access attempts
  - Authentication of routing updates
  - Secure command and control where possible (SSH, IPSec)
- www.cisco.com/warp/public/707/21.html

Device Specific Security: Switches

- Protection needs are similar to routers
- VLANs create additional concerns:
  - Remove user ports from auto-trunking
  - Use non-user VLANs for trunk ports
  - Set unused ports to a non-routed VLAN
  - Ensure VLAN separation where appropriate
- Remember a switch is designed to enable communications

Device Specific Security: Hosts

- High visibility makes them easy targets (2001 CSI/FBI Survey)
  - 47% respondents offer WWW site for e-commerce
  - 23% respondents had unauthorized access or misuse to sites (27% don’t know)
  - 58% of these reported 10+ incidents
- Ensure that host components are compatible and at the latest version
  - Hardware platform
  - Operating system and updates
  - Standard applications, patches, and scripts
- Limit running services to only what’s necessary
- Audit trails matter
- Trust considerations
  - Between services on the host and between hosts
- Protect applications
  - Complexity of applications makes them prone to human error
  - Timely patching
  - Public domain, commercial, or self-developed?



Network Wide Security Considerations

- Contain IP spoofing

  Prevent inappropriate ingress of non-registered addressing (RFC 1918 and 2827)

  Filter valid IP addresses at the access and distribution layers

- DDoS attacks cannot be stopped by the victim network alone

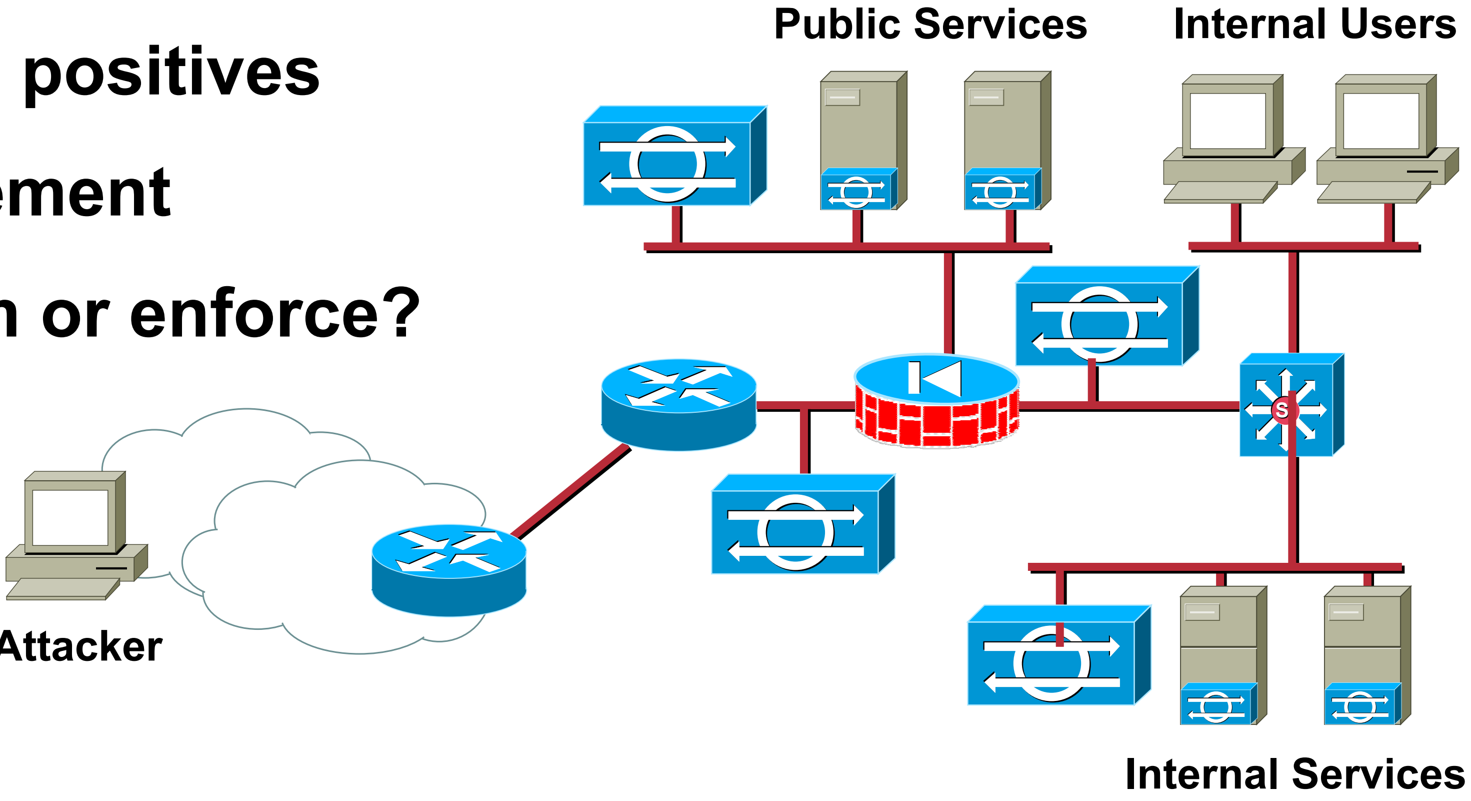
- Layer 2 considerations (switch vs. hub, ARP and MAC issues)

Intrusion Detection Systems

- Host and network

  Both have their place

- False positives
- Placement
- Alarm or enforce?



Logging Architecture

Cisco.com

- Device priority
- Where to log (multiple servers? One for historical, one for tactical? Tiered?)
- What to log (log levels)
- Some servers are log protocol and/or function specific (post office vs. syslog)
- Scaling considerations (per server, per network device, filtered display based on alarm level)

Design Considerations

- General considerations
- Wireless LAN
    - Wireless networks are targets
    - WLANs are weapons
    - AP security options
    - LEAP WLAN design
    - VPN WLAN design
- IP telephony

Wireless Networks Are Targets

- IT can’t keep up with deployments
- WLAN devices ship with all security features disabled
- Generic 802.11b devices don’t have effective security options
- WindowsXP informs users of available WLAN networks
- 2.4 GHz jamming is trivial (cordless phones, baby monitors, microwave ovens, bluetooth devices)
- Most WLAN APs have only clear-text management options

Wireless Networks Are Targets

- Access point security recommendations:

  Enable user authentication for the management interface

  Choose strong community strings for Simple Network Management Protocol (SNMP) and change them often

  Consider using SNMP read only if your management infrastructure allows it

  Disable any insecure and nonessential management protocol provided by the manufacturer

  Limit management traffic to a dedicated wired subnet

  Encrypt all management traffic where possible

  Enable wireless frame encryption where available

- Client security recommendations:

  Disable ad hoc mode

  Enable wireless frame encryption where available

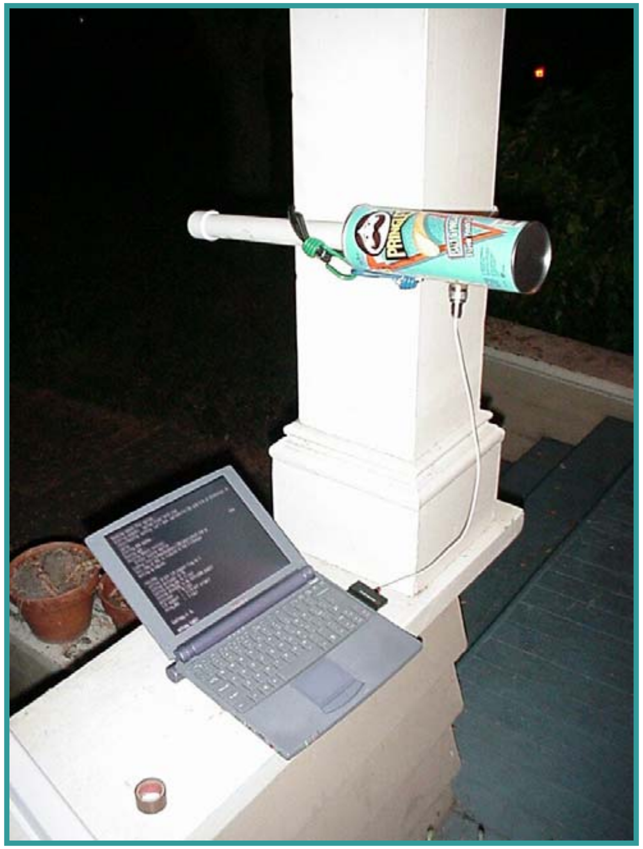
WLANs Are Weapons

- APs are small and cheap
- Physical building security is weak (tailgaters)
- Most buildings allow campus connectivity on all ports
- All this adds up to a cheap, effective, and anonymous hacking opportunity
- Consider the following:

    MAC address limitations on switches

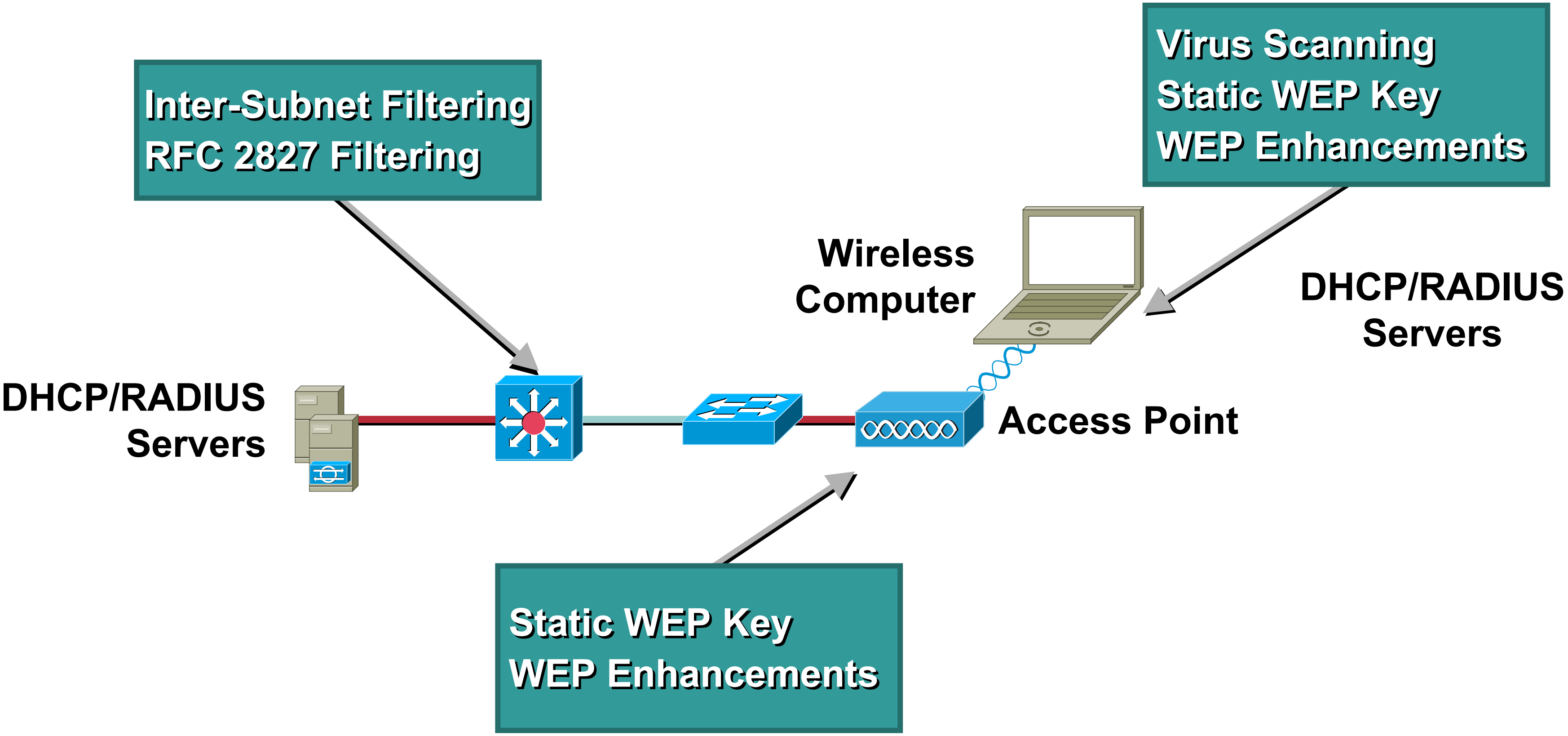
    Conference rooms use wireless access with authentication and privacy

    Perform regular physical and RF sweeps for APs



WEP WLAN Design

Be Aware of the Limitations

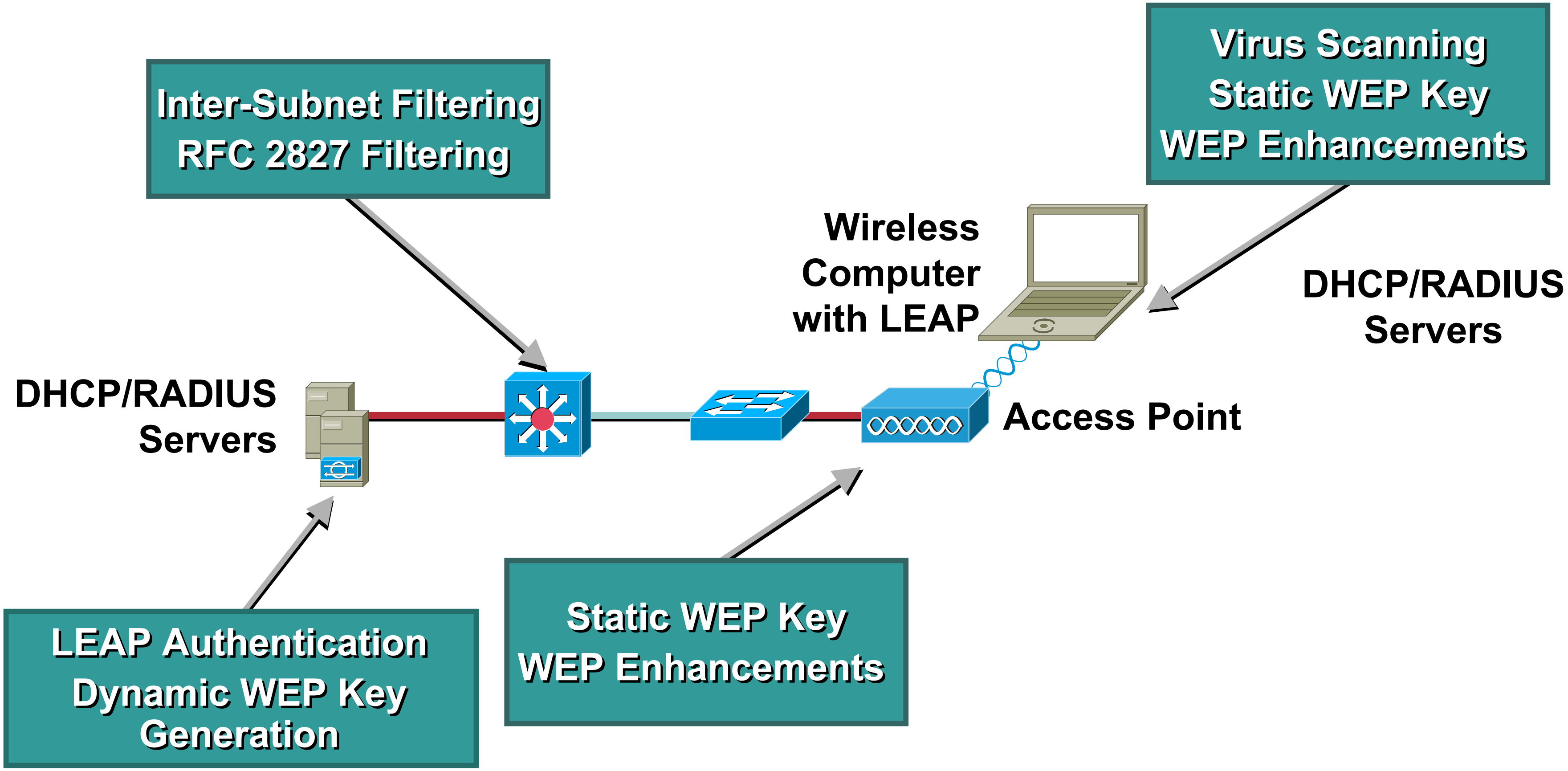


Inter-Subnet Filtering
RFC 2827 Filtering

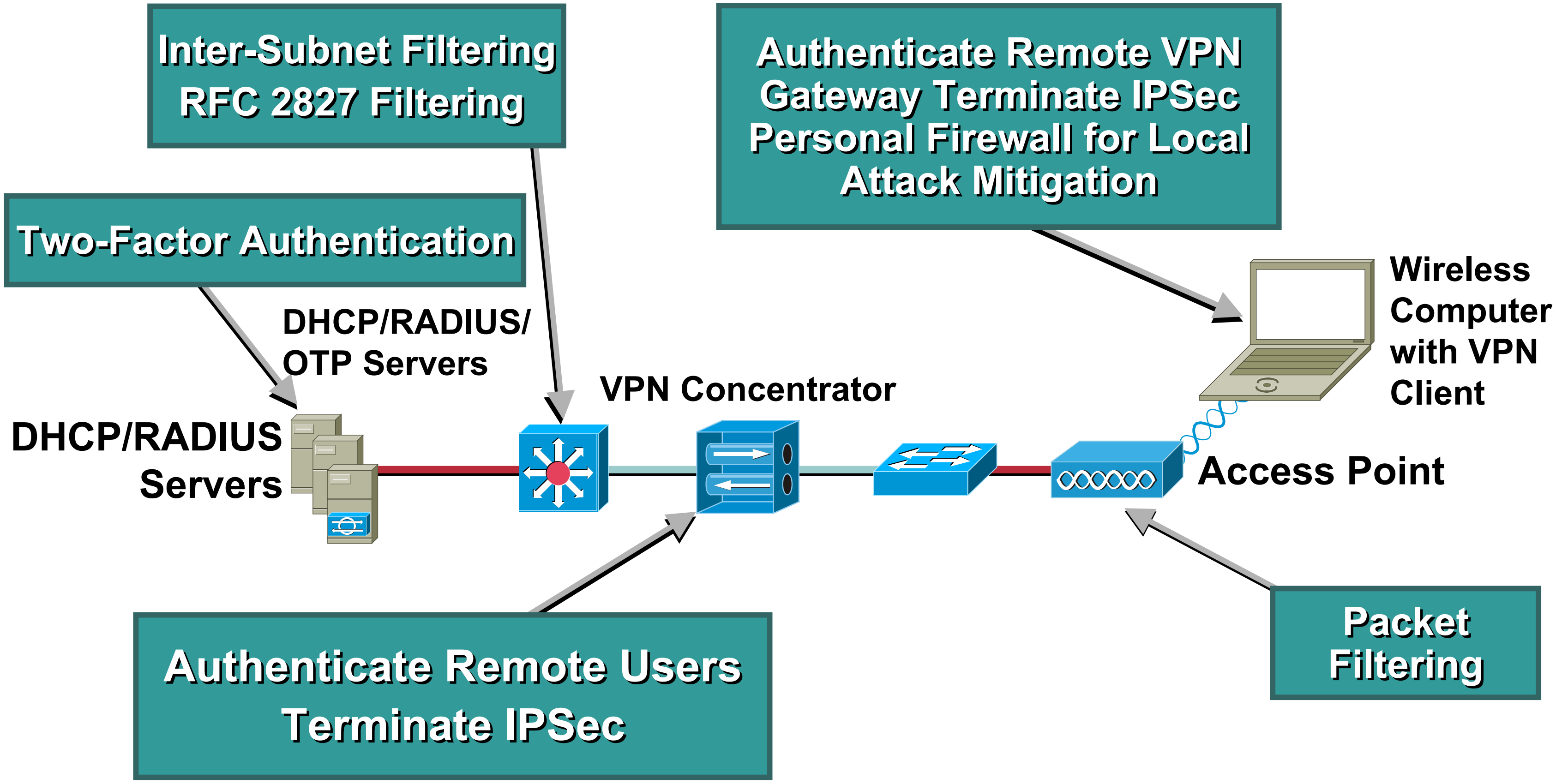
Virus Scanning
Static WEP Key
WEP Enhancements

Static WEP Key
WEP Enhancements

LEAP WLAN Design



VPN WLAN Design



Inter-Subnet Filtering
RFC 2827 Filtering

Authenticate Remote VPN Gateway Terminate IPSec Personal Firewall for Local Attack Mitigation

Two-Factor Authentication

DHCP/RADIUS/
OTP Servers

VPN Concentrator

Wireless Computer with VPN Client

DHCP/RADIUS
Servers

Access Point

Authenticate Remote Users
Terminate IPSec

Packet
Filtering

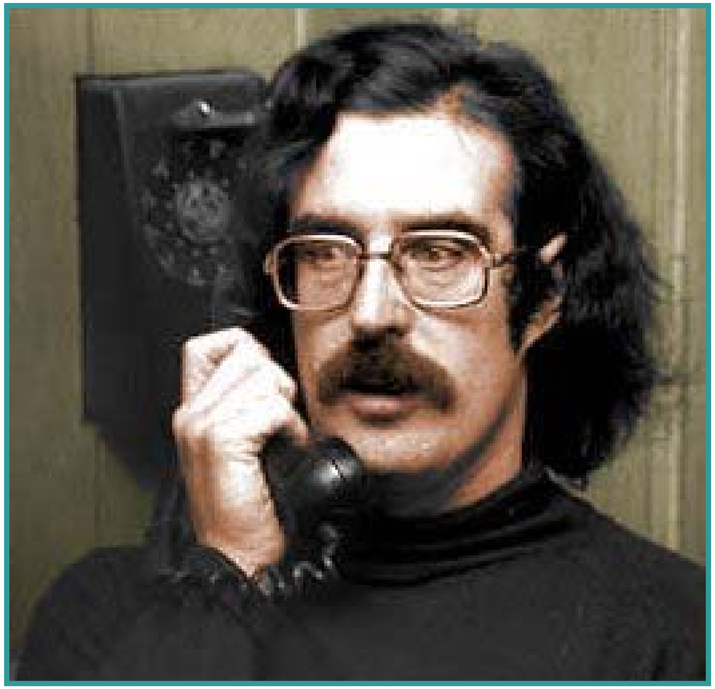
AP Security Options

Feature	LEAP	IPsec	WEP
Key Length (Bits)	128	168	128
Encryption Algorithm	RC4	3 DES	RC4
Packet Integrity	CRC32/MIC	MD5-HMAC/SHA-HMAC	CRC32/MIC
Device Authentication	None	Pre-Shared Secret or Certificates	None
User Authentication	Username/Password	Username/Password or OTP	None
User Differentiation	No	Yes	No
Transparent User Experience	Yes	No	Yes
ACL Requirements	None	Substantial	N/A
Additional Hardware	Authentication Server	Authentication Server and VPN Gateway	No
Per User Keying	Yes	Yes	No
Protocol Support	Any	IP Unicast	Any
Client Support	PCs and High End PDAs; Wide Range of OSs Supported From Cisco	PCs and High End PDAs ;Wide Range of OSs Supported from Cisco and 3rd Party Vendors	All Clients Supported
Open Standard	No	Yes	Yes
Time Based Key Rotation	Configurable	Configurable	No
Client Hardware Encryption	Yes	Available, Software is Most Common Method	Yes
Additional Software	No	IPSec Client	No

History Hack #2: Captain Crunch and the Origin of "2600"

- Back in the early 70s phone lines did both signaling and regular voice traffic over the same line
- Using a "Captain Crunch" cereal toy whistle it was possible to generate a sound at 2600Hz which allowed signaling data to be sent to "Ma Bell"
- Building on what was learned with the whistle, tones could then be sent using a "blue box" to call anywhere else for free
- Steve Wozniak even used a "blue box" to call the Pope posing as then Secretary of State Henry Kissinger
- Moral of the story? Security through obscurity is not security (unauthenticated control channels are bad)

http://www.webcrunchers.com/crunch



John T. Dryer

Design Considerations

- General considerations
- Wireless LAN
- IP telephony
  - The state of IP telephony
  - Voice attacks
  - Data and voice segmentation

The State of IP Telephony

- Today there is no single widely deployed standard for call signaling
    - Virtually all vendors rely on proprietary protocols
    - Standards-based protocols lack features or have feature disparity
- Voice protocols are still relatively new
    - Hackers are not familiar with them yet
    - There are not many documented attacks
- Security and IP telephony are in the initial integration phase
    - Most protocols today do not support confidentiality or strong device/user authentication features
    - However, there are many issues than we can address today with existing technologies

Voice Attacks

- Packet sniffing/call eavesdropping

  A rogue device has access to the voice stream between the two talking endpoints

  VOMIT or “voice over misconfigured Internet telephones” assembles tcpdumps of conversations into wave files

- Toll fraud

  A rogue user performs theft of telephony service

  Unattended valid IP phone

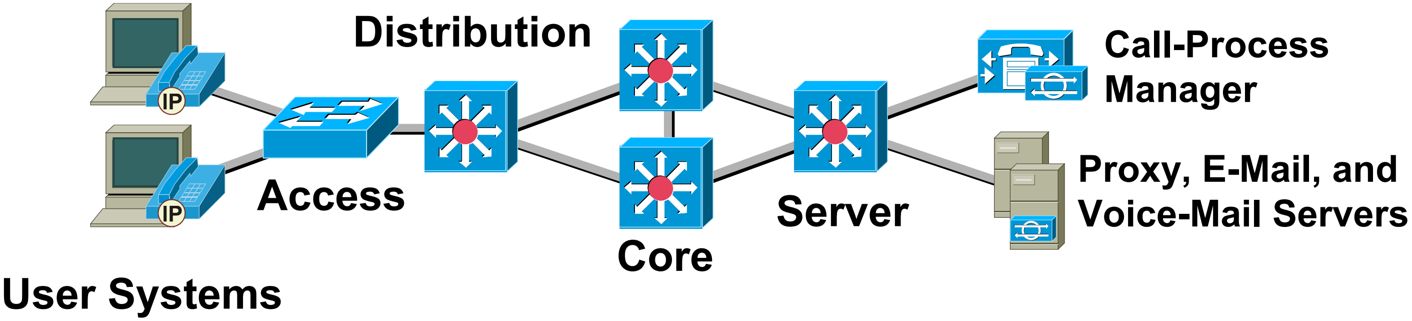
  Rogue IP phone placed in the network

  Rogue voice gateway placed in the network

Data and Voice Segmentation

- **Use the same access, core, and distribution layers for the two segments**

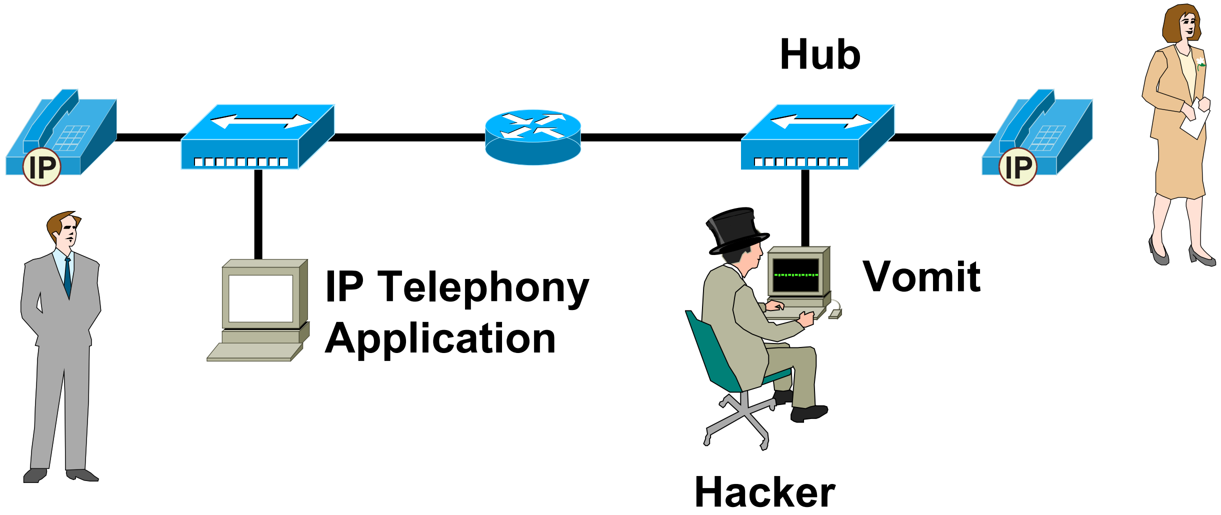
  Technologies such as layer 3 access control, stateful firewall, and VLANs make this possible



Let’s Talk about VOMIT

- **The majority of IP telephony devices don’t support confidentiality**

  Data-voice segmentation and a switched infrastructure will greatly reduce the likelihood of eavesdropping by tools such as Vomit



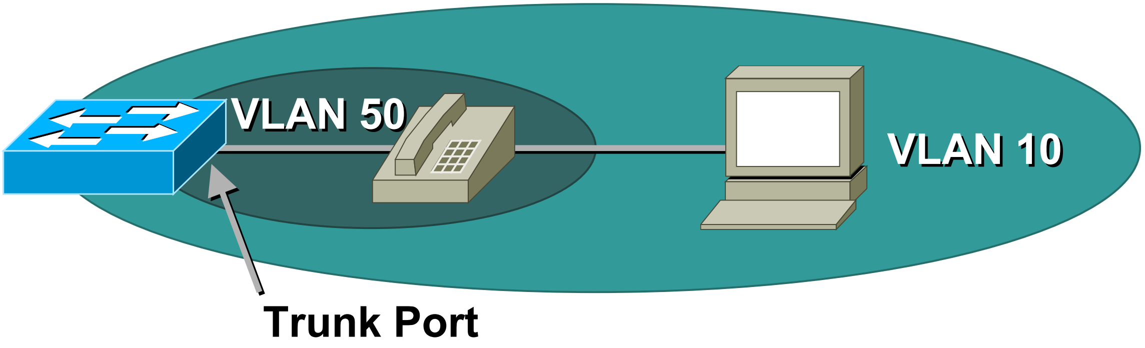
Data and Voice Segmentation II

- IP phones typically provide access to both segments

  IP phones support a “data port” for the local PC so that only a single cable is necessary

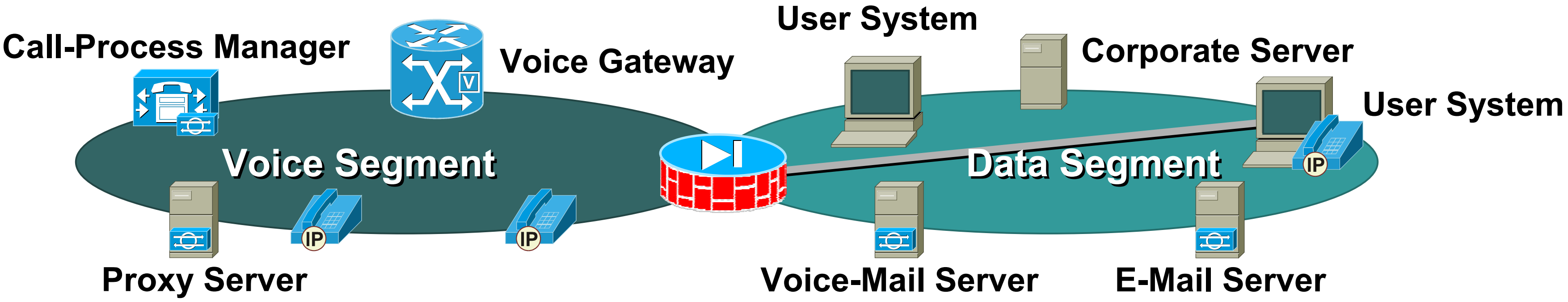
  Make sure that the phone supports separation of the two segments (e.g. via VLAN support)

  We don’t recommend you rely solely on VLANs for separation, in the interest of layered security you should also provide layer 3 filtering at the access layer



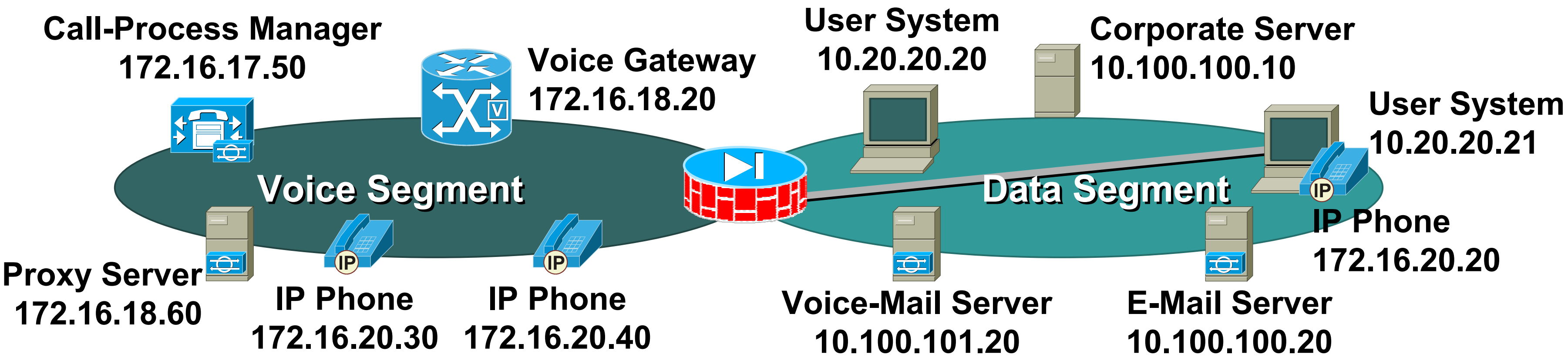
Data and Voice Segmentation III

- **Deploy a stateful firewall to broker the data-voice segment interaction**
  - Provides dynamic pinpoint access and mitigation against TCP connection starvation, UDP flood, and spoofing attacks
  - Feasible in front of voice services
  - Placement of voice and related services is key
  - Make certain the stateful firewall vendor you chose supports stateful inspection of the voice protocols you decided to deploy



Data and Voice Segmentation IV

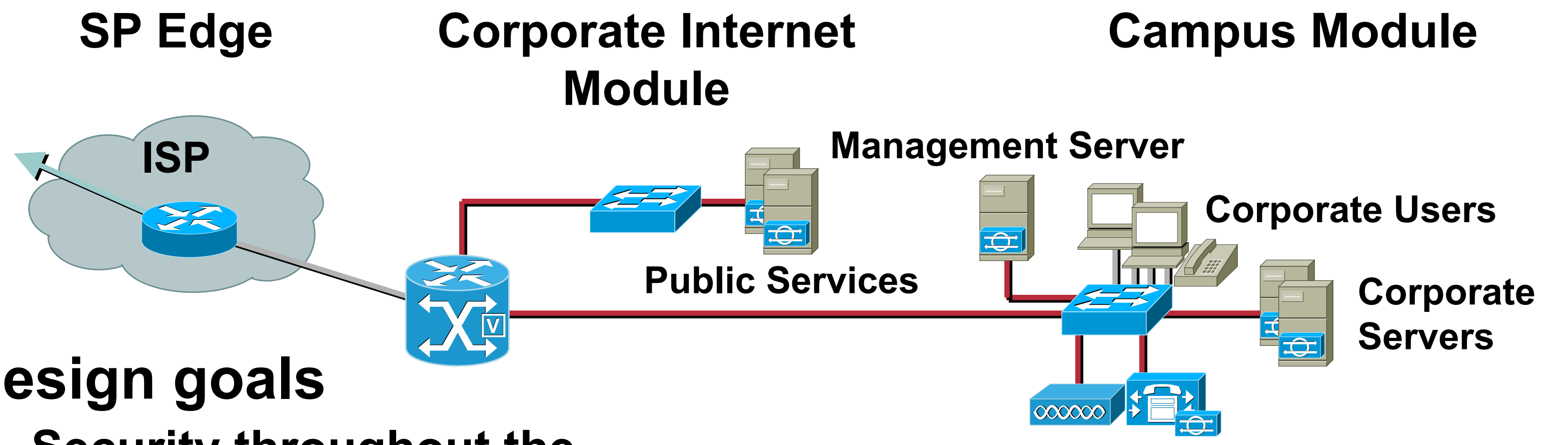
- **Use private address space for data-voice segments, such as RFC 1918**
  - Partitioned addressing facilitates filtering and recognition
  - 1918 is not routeable (well, most of the time) which reduces the likelihood of reconnaissance scans even if NAT is misconfigured
  - Spoof mitigation filtering virtually guarantees that hosts are who they claim to be in local segments
  - This also eases manageability and troubleshooting



Agenda

- Security Design Overview
- Integrated Security Solution
- Distributed Security Solution
- High-End Resilient Security Solution
- Conclusion

Integrated Detailed Model



- **Design goals**

  Security throughout the infrastructure

  Secure management and reporting

  Authentication of key users and operators

  Intrusion detection for critical areas

  Accommodation of emerging network apps (WLAN, IPT)

  Minimize cost

  Integration of features

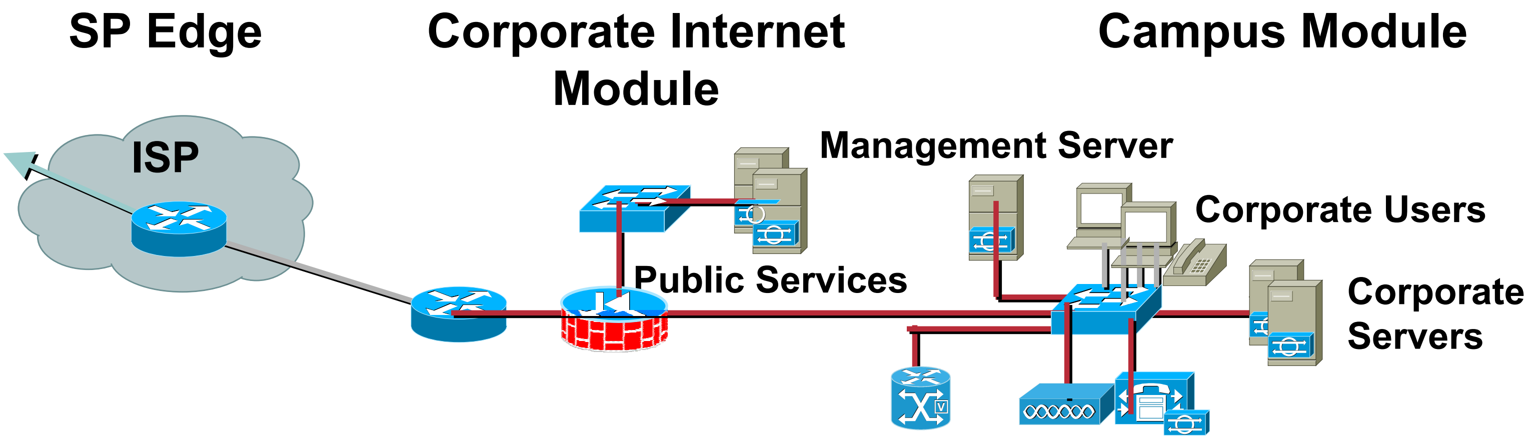
- **Design considerations**

  Performance

  Single point of security compromise

  Configuration complexity

Integrated Detailed Model—Appliance FW



- Common design
- General considerations

  Remote access VPN issues

  WAN considerations

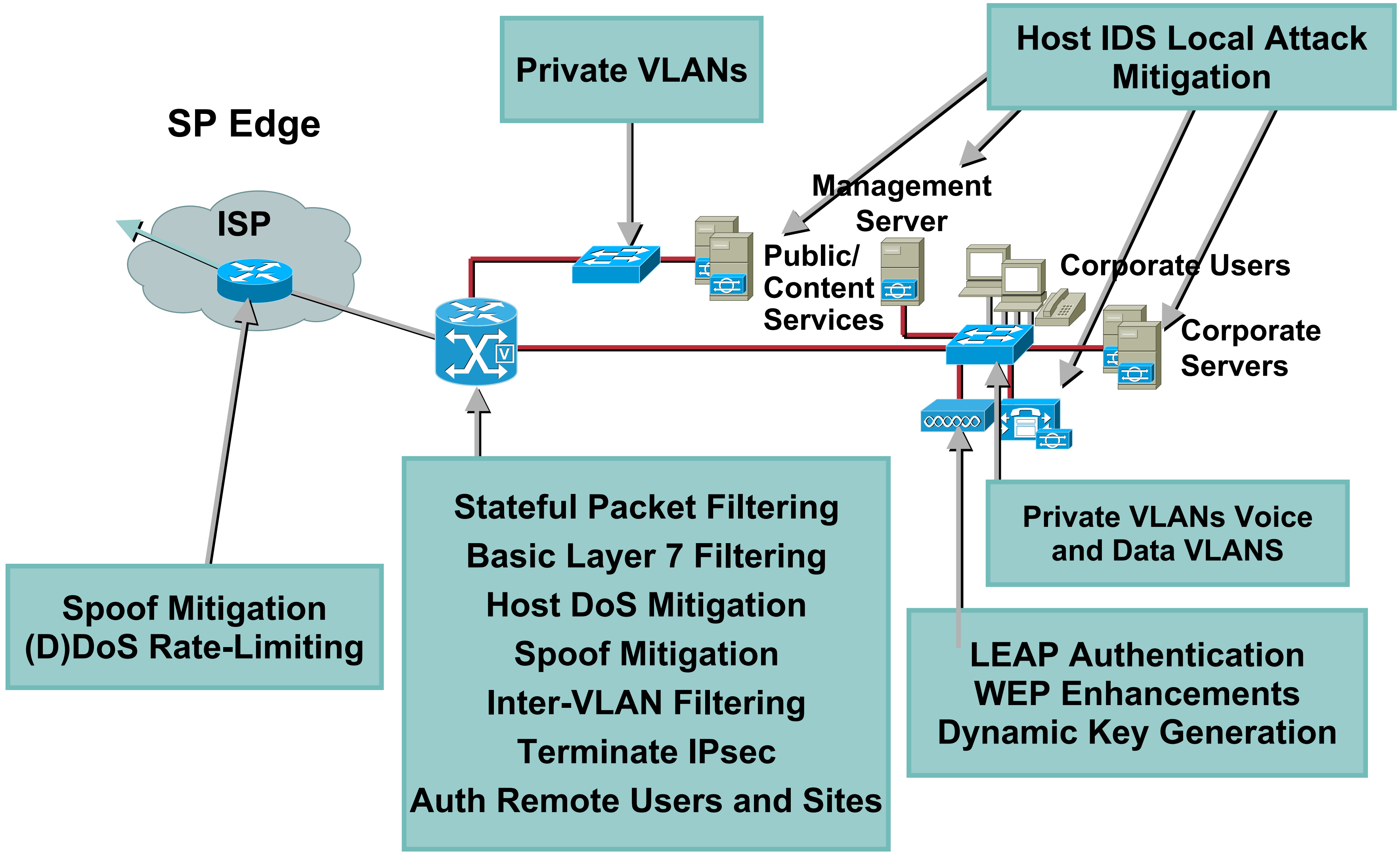
  Feature set

- When require voice, consider the following

  Voice needs inter-VLAN filtering, rarely available in low-end firewalls

  Note the router with stateful VoIP protocol support

Attack Mitigation



SP Edge

Private VLANs

Host IDS Local Attack Mitigation

Spoof Mitigation
(D)DoS Rate-Limiting

Stateful Packet Filtering
Basic Layer 7 Filtering
Host DoS Mitigation
Spoof Mitigation
Inter-VLAN Filtering
Terminate IPsec
Auth Remote Users and Sites

Private VLANs Voice and Data VLANS

LEAP Authentication
WEP Enhancements
Dynamic Key Generation

Agenda

- Security Design Overview
- Integrated Security Solution
- Distributed Security Solution
- High-End Resilient Security Solution
- Conclusion

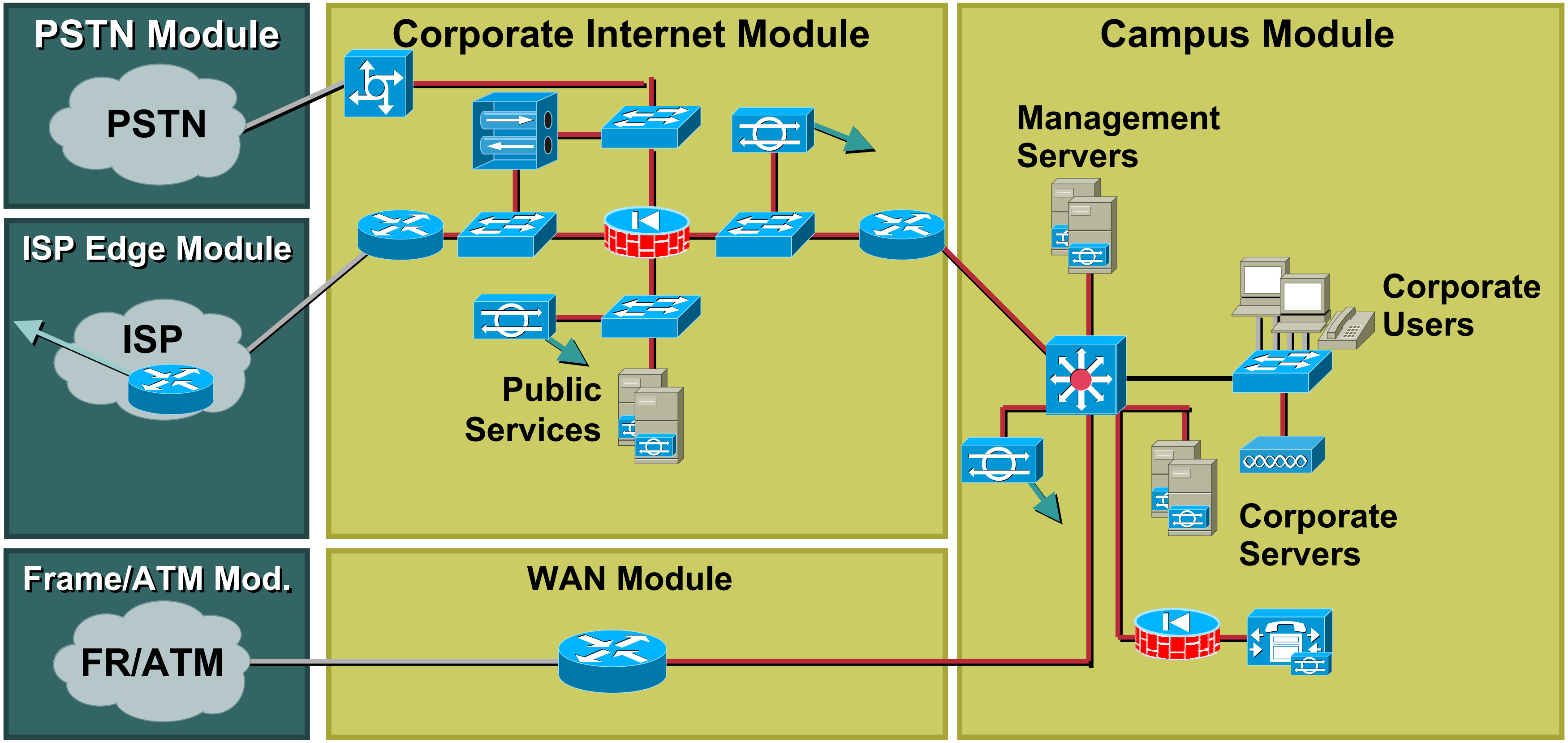
Distributed Security Design Goals

- Security throughout the infrastructure
- Secure management and reporting
- Authentication of key users and operators
- Intrusion detection for critical areas
- Accommodation of emerging network apps
- Performance
- Separation of security function
- No single point of total compromise

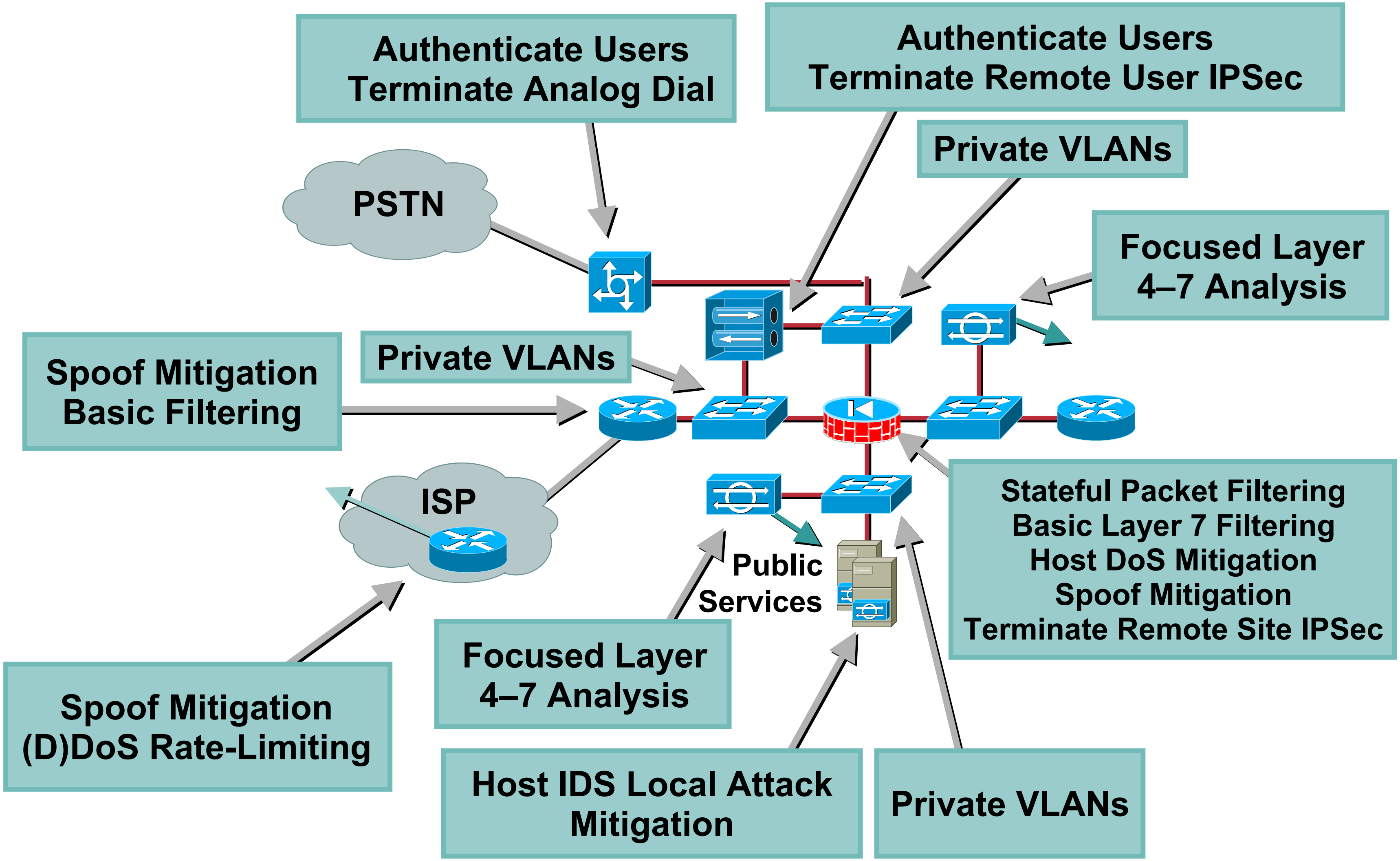
Distributed Security
Design Considerations

- Management
- Configuration complexity
- Cost

Distributed Security Detailed Model



Distributed Security Detailed Model: Corporate Internet



Authenticate Users
Terminate Analog Dial

Authenticate Users
Terminate Remote User IPSec

Private VLANs

Focused Layer 4–7 Analysis

Spoof Mitigation
Basic Filtering

Private VLANs

Stateful Packet Filtering
Basic Layer 7 Filtering
Host DoS Mitigation
Spoof Mitigation
Terminate Remote Site IPSec

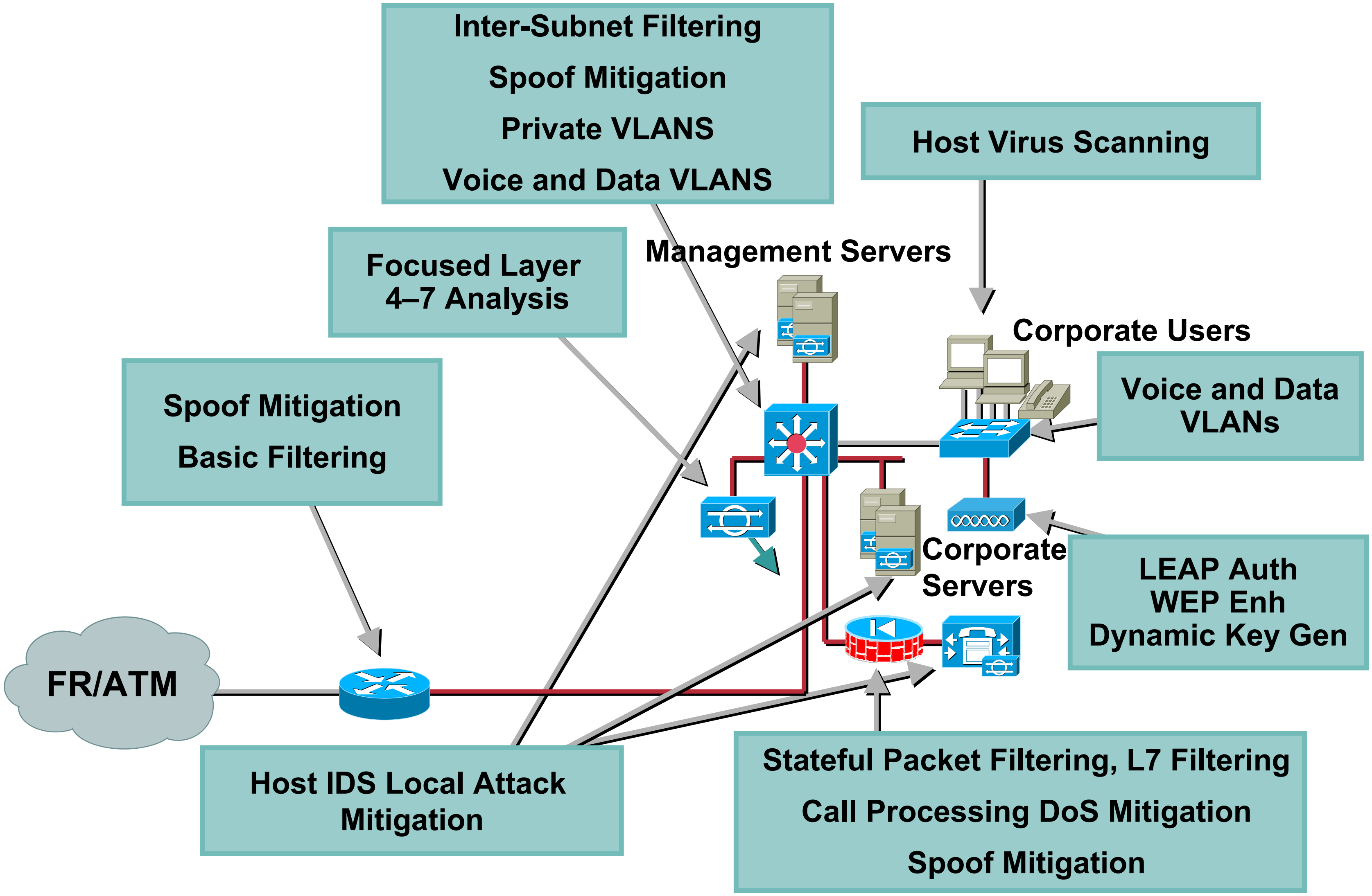
Spoof Mitigation
(D)DoS Rate-Limiting

Focused Layer 4–7 Analysis

Host IDS Local Attack Mitigation

Private VLANs

Distributed Security Detailed Model:
Campus and WAN



Agenda

- Security Design Overview
- Integrated Security Solution
- Distributed Security Solution
- High-End Resilient Security Solution
- Conclusion

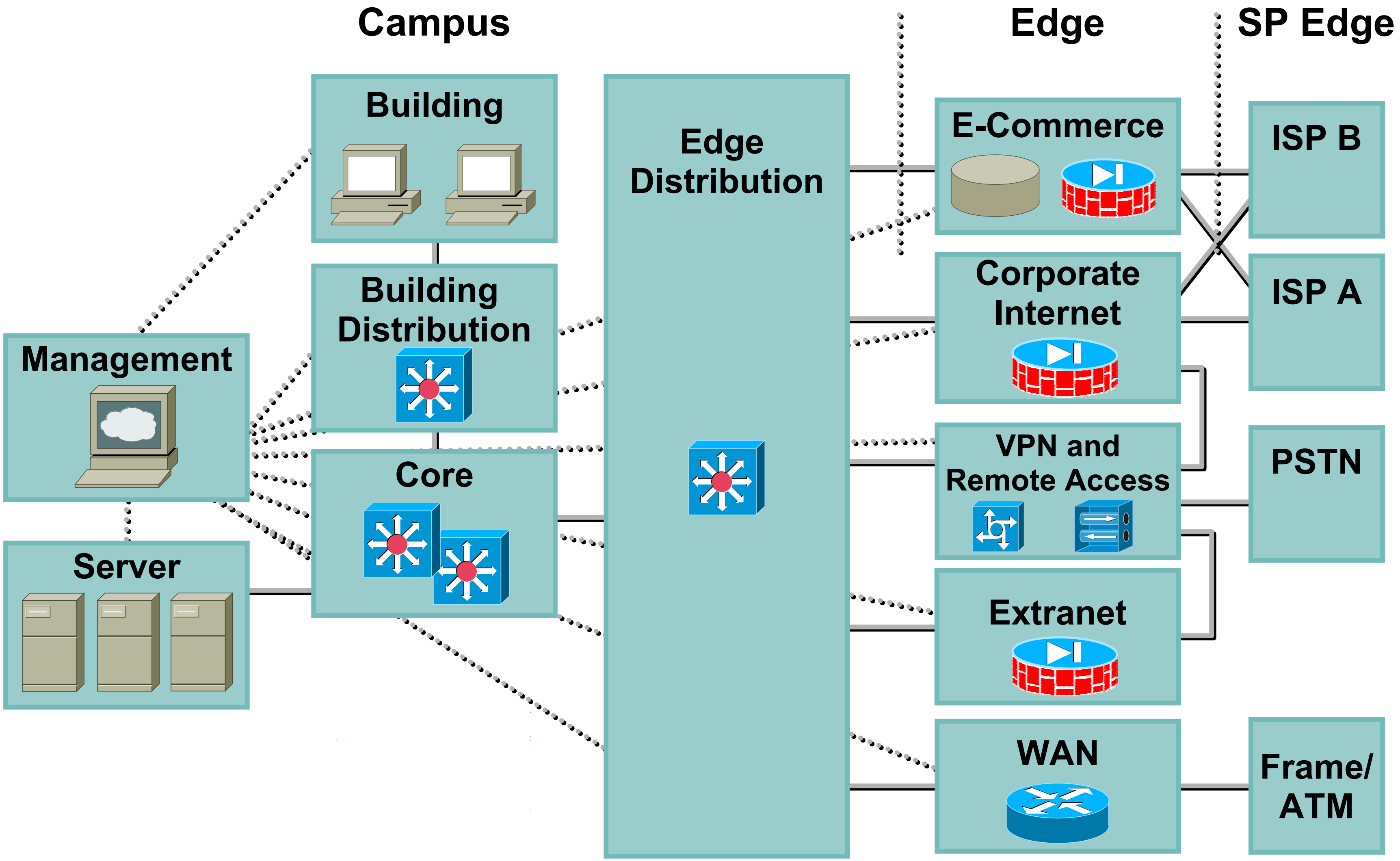
High-End Resilient Design Goals

- Security throughout the infrastructure
- Secure management and reporting
- Authentication of key users and operators
- Intrusion detection for critical areas
- Accommodation of emerging network apps
- Performance
- Resilience
- Scalability
- Out-of-band management
- No single point of total compromise
- Separation of security function

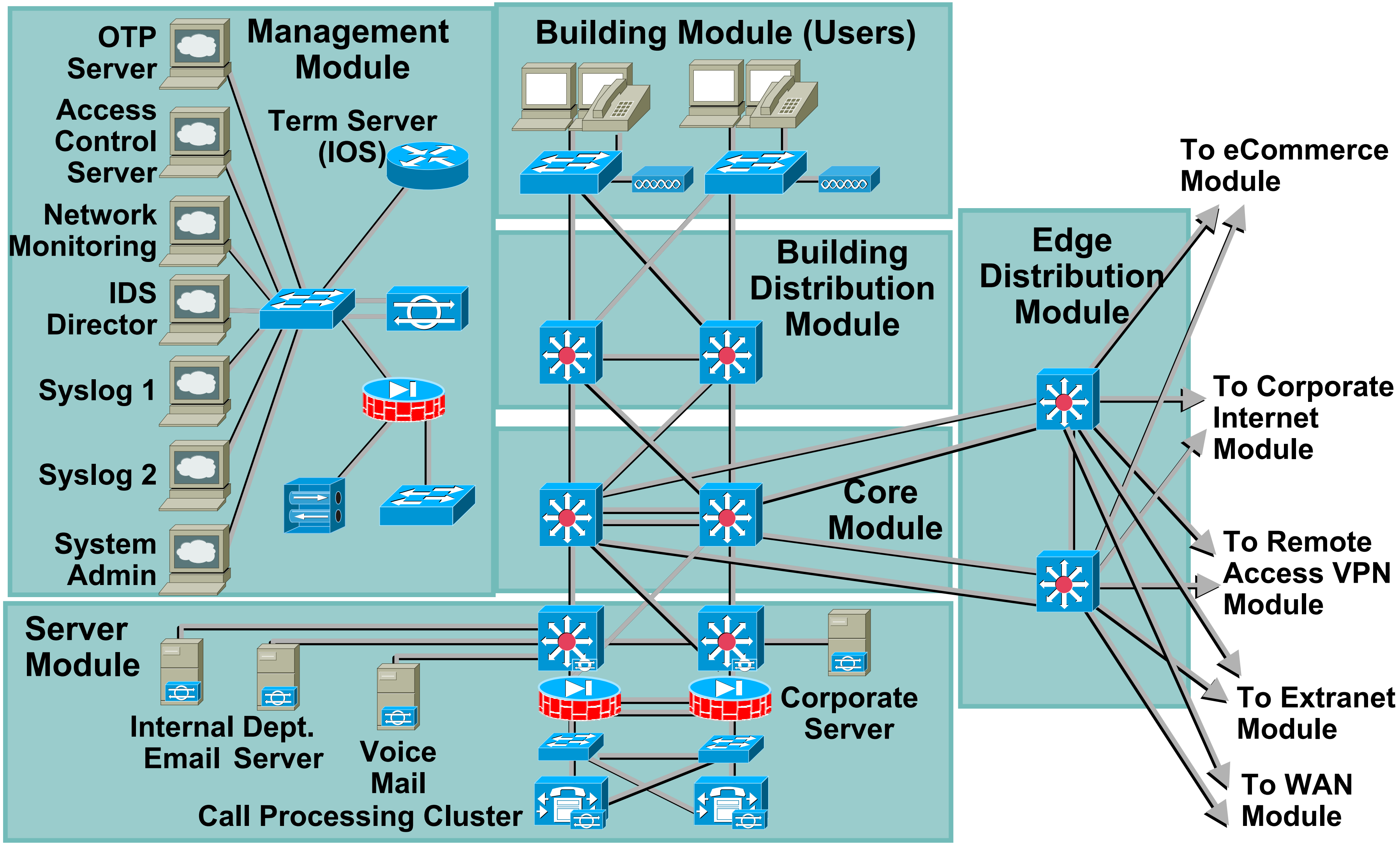
High-End Resilient Design Considerations

- Complexity of design
- Number of devices
- Asymmetric routing vs. state awareness
- Management infrastructure
- Administrative roles
- Cost

High-End Resilient Modules



High-End Resilient Campus Detail



History Hack #3:
Robert Morris's Internet Worm

- Self-replicating worm built to infect machines and replicate itself
- Took down 10% of the Internet in 1988 (about 6,000 hosts)
- Not malicious, but what if it was?
- Error in programming caused it to run more than once on the same system
- Took advantage of weaknesses in Sun 3 and VAX systems running 4 BSD UNIX
- http://www2.ncsu.edu:8010/eos/info/computer_ethics/abuse/wvt/worm/darby/worm.html
- Moral of the story? Patch apps, OSs and review code where possible

M. Okoniewski/AP File

Robert Morris's Internet Worm

- All the following events occurred on the evening of Nov. 2, 1988

  6:00 PM at about this time the worm is launched

  8:49 PM the worm infects a VAX 8600 at the University of Utah (cs.utah.edu)

  9:09 PM the worm initiates the first of its attacks to infect other computers from the infected VAX

  9:21 PM the load average on the system reaches 5 (load average is a measure of how hard the computer system is working; at 9:30 at night, the load average of the VAX is usually 1; any load average higher than 5 causes delays in data processing)

  9:41 PM the load average reaches 7

  10:01 PM the load average reaches 16

  10:06 PM at this point there are so many worms infecting the system that no new processes can be started; no users can use the system anymore

  10:20 PM the system administrator kills off the worms

  10:41 PM the system is reinfested and the load average reaches 27

  10:49 PM the system administrator shuts down the system; the system is subsequently restarted

  11:21 PM reinfestation causes the load average to reach 37

Campus Network Section

- Management module
- Building access and distribution
- Core and server modules
- Edge distribution module

Management Channel Security

- In-band in the clear
  - Optionally with strong authentication
- In-band secured
  - Application layer encryption (SSH, SSL)
  - Network layer encryption (IPSec)
    - Good for non config protocols
      - Syslog, TFTP, SNMP
- Out-of-band management
  - Strongest security
  - Beware topo sensitive NMS

Management Module Design Goals

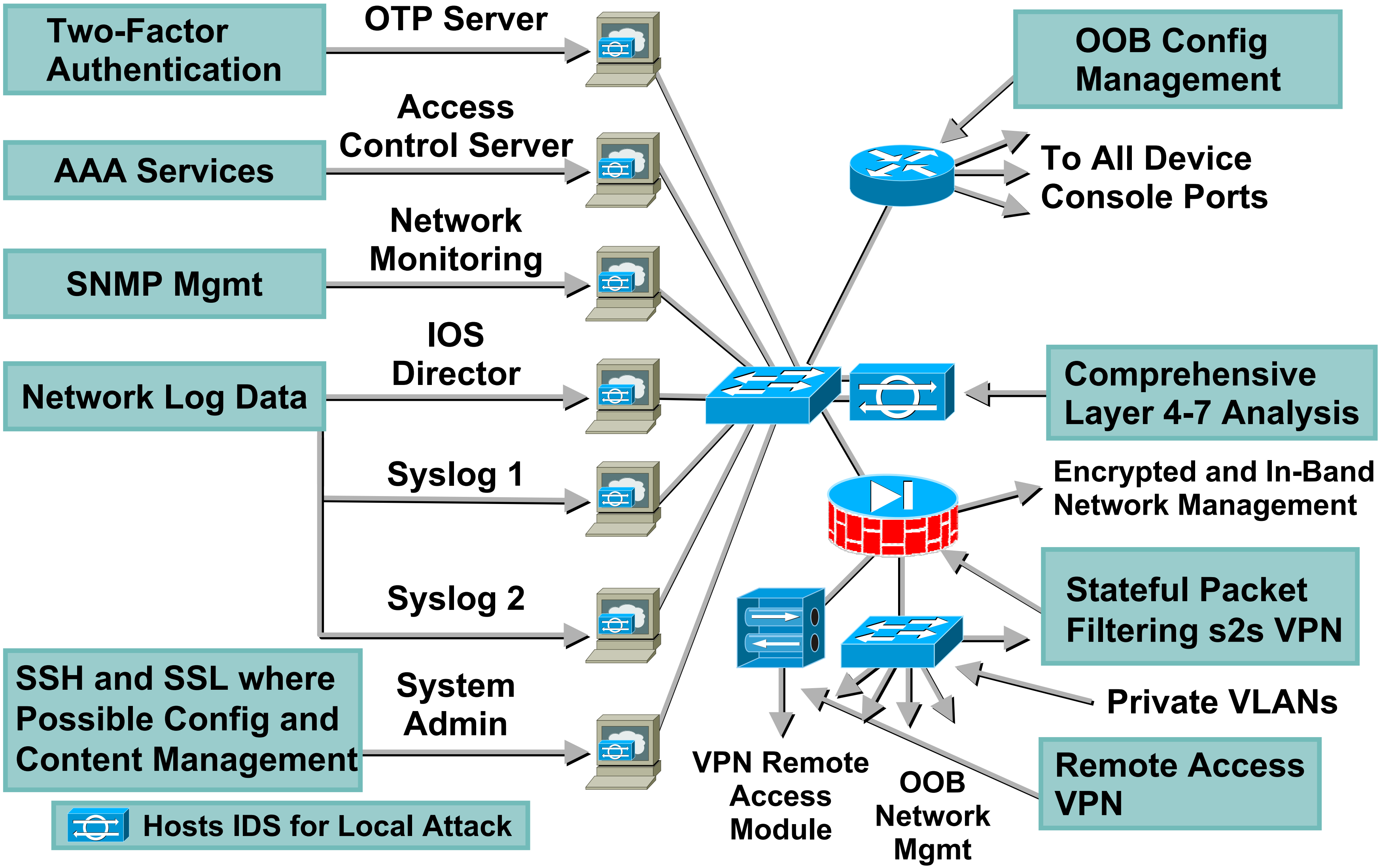
- Out-of-band management
  - Separate physical networks
  - Separate address space (i.e. 192.168.25x.xxx)
  - Use IPSec if physical separation is not possible
- Firewall between management subnet and managed-device subnet

Design Goals (Cont.)

- Isolate managed ports to minimize impact of compromised device
- NIDS and HIDS on the management subnet
- One-time passwords for authentication of administrators
- SNMP read-only

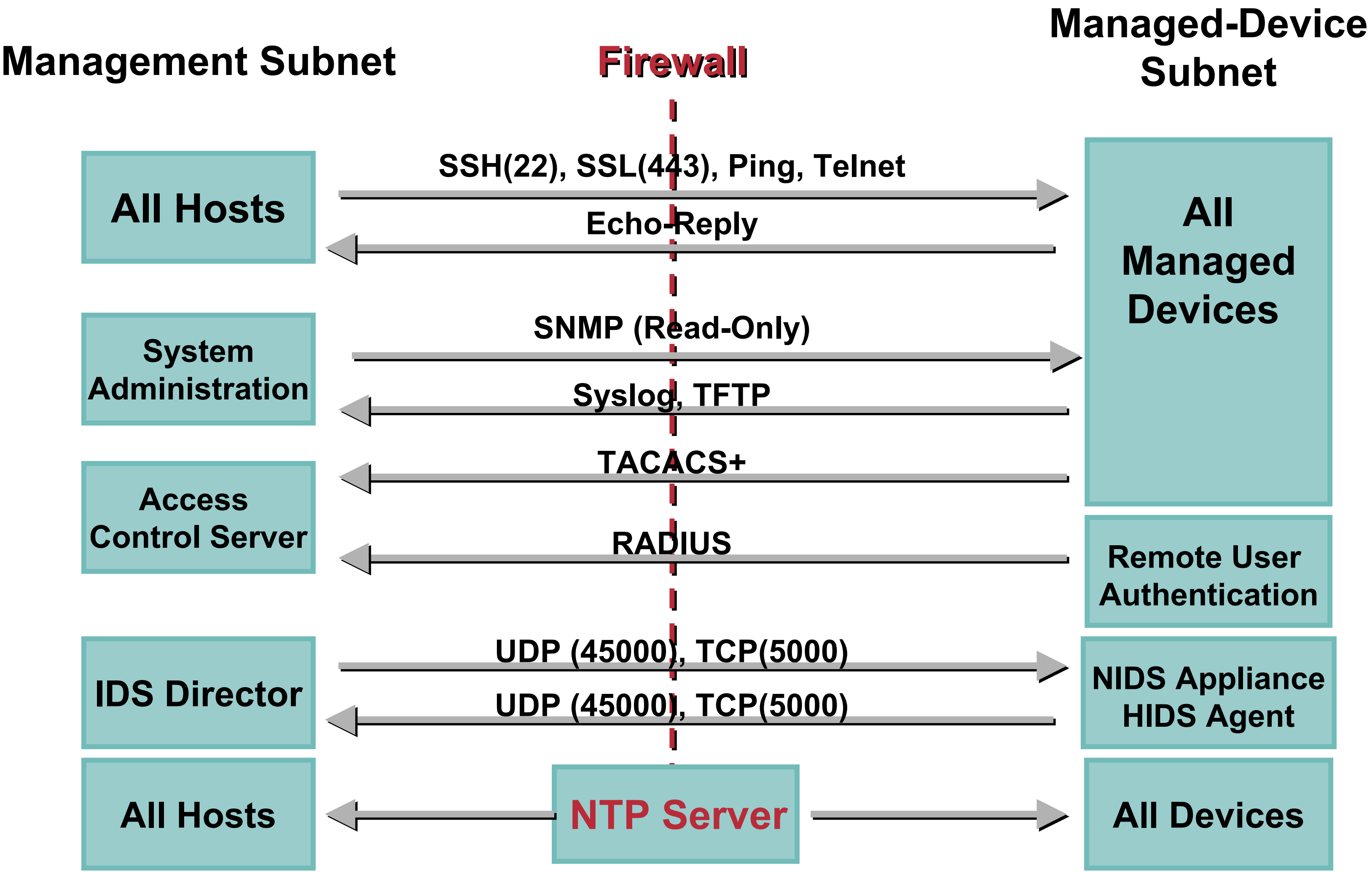
```
snmp-server community Txo~QbW3XM RO 98

access-list 98 permit host
192.168.253.51
```

Attack Mitigation Roles for Management Module



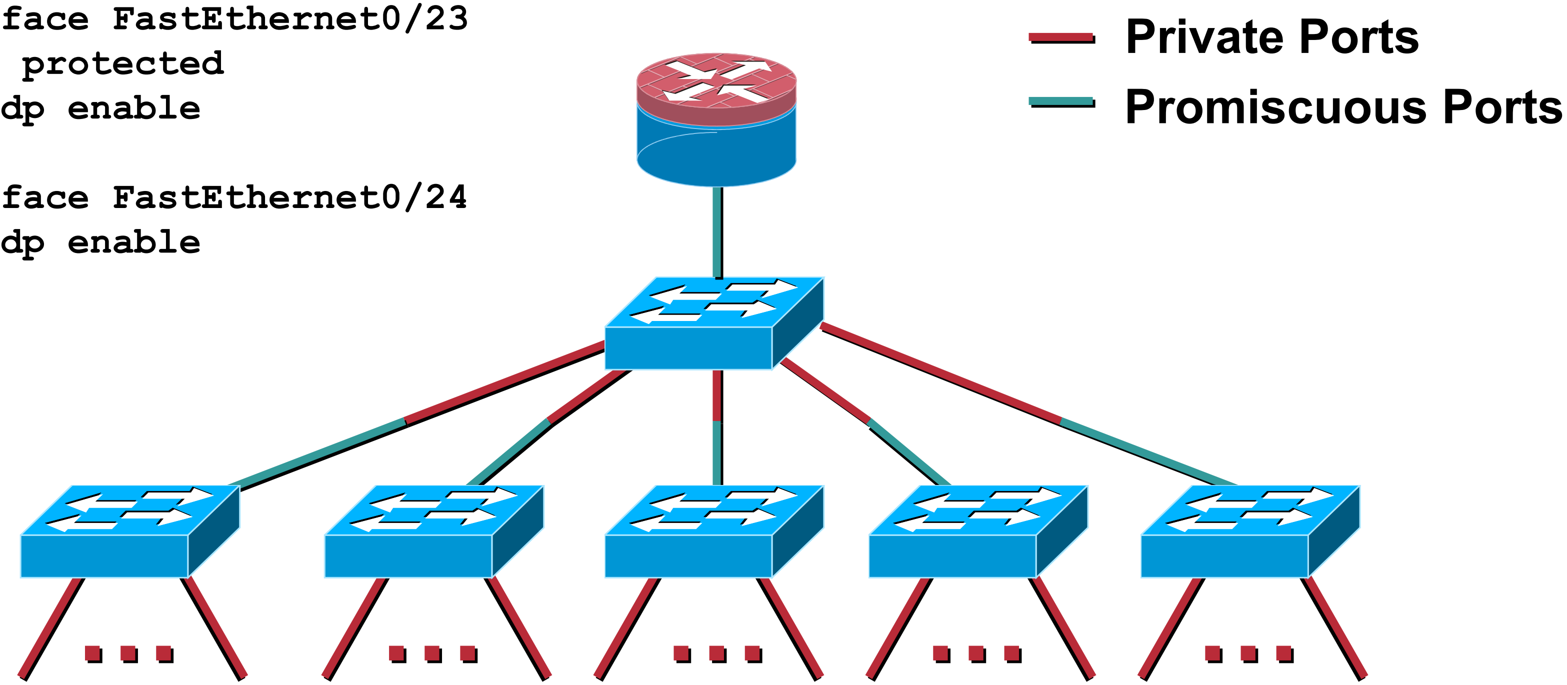
Two-Factor Authentication
OTP Server
AAA Services
Access Control Server
SNMP Mgmt
Network Monitoring
Network Log Data
IOS Director
Syslog 1
Syslog 2
SSH and SSL where Possible Config and Content Management
System Admin
Hosts IDS for Local Attack
OOB Config Management
To All Device Console Ports
Comprehensive Layer 4-7 Analysis
Encrypted and In-Band Network Management
Stateful Packet Filtering s2s VPN
Private VLANs
Remote Access VPN
VPN Remote Access Module
OOB Network Mgmt

Management Firewall— Stateful Packet Filtering



Managed Device Subnet

```
interface FastEthernet0/23
 port protected
 no cdp enable
!
interface FastEthernet0/24
 no cdp enable
```



To Dedicated Management LAN Port on Each Device

OOB Mgmt Access Control

```
! Access control configuration for all managed routers
!
! Inbound ACL
access-list 101 permit icmp any any
! Required for Tacacs+
access-list 101 permit tcp 192.168.253.0 0.0.0.255 host 192.168.254.13 established
! Required for TFTP
access-list 101 permit udp 192.168.253.0 0.0.0.255 host 192.168.254.13 gt 1023
! Other Management Access
access-list 101 permit tcp 192.168.253.0 0.0.0.255 host 192.168.254.13 eq telnet
access-list 101 permit udp host 192.168.253.51 host 192.168.254.13 eq snmp
access-list 101 permit udp host 192.168.253.53 host 192.168.254.13 eq tftp
access-list 101 permit udp host 192.168.254.57 host 192.168.254.13 eq ntp
access-list 101 deny   ip any any log
! Outbound ACL (local router isn’t affected by ACLs)
access-list 102 deny   ip any any log

! Management Interface Settings
interface FastEthernet0/0
 ip address 192.168.254.13 255.255.255.0
 ip access-group 101 in
 ip access-group 102 out
 no cdp enable
```

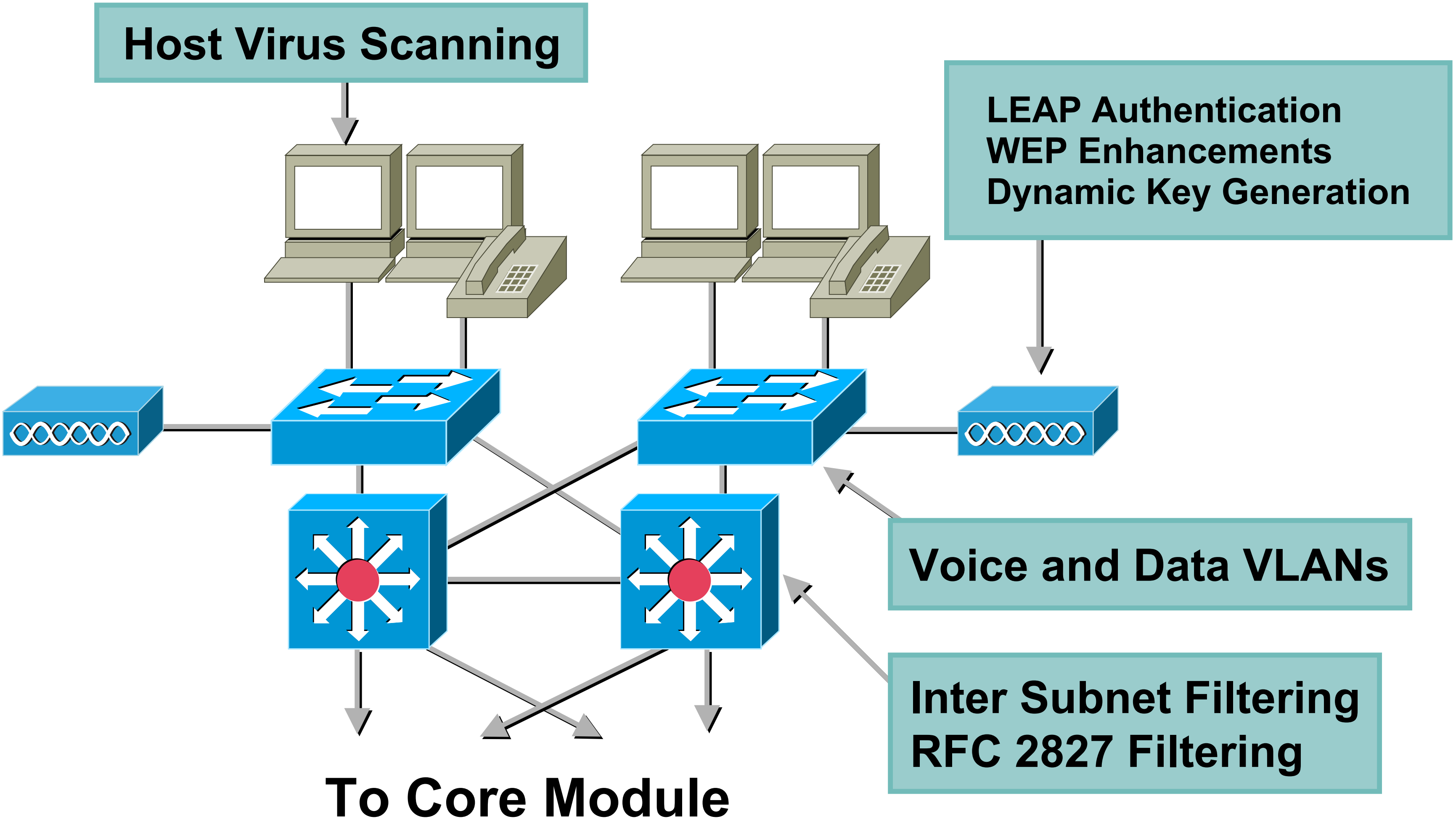
Campus Network Section

- Management module
- Building access and distribution
- Core and server modules
- Edge distribution module

Building and Distribution Design Goals

- Using VLANs, layer 2 separation for:
  - Data and voice ports
  - Ports between corporate departments
- Host virus scanning
- Layer 3 access-control at distribution prevents IP spoofing and filters traffic

Attack Mitigation Roles for Building and Distribution Modules



Host Virus Scanning

LEAP Authentication
WEP Enhancements
Dynamic Key Generation

Voice and Data VLANs

Inter Subnet Filtering
RFC 2827 Filtering

To Core Module

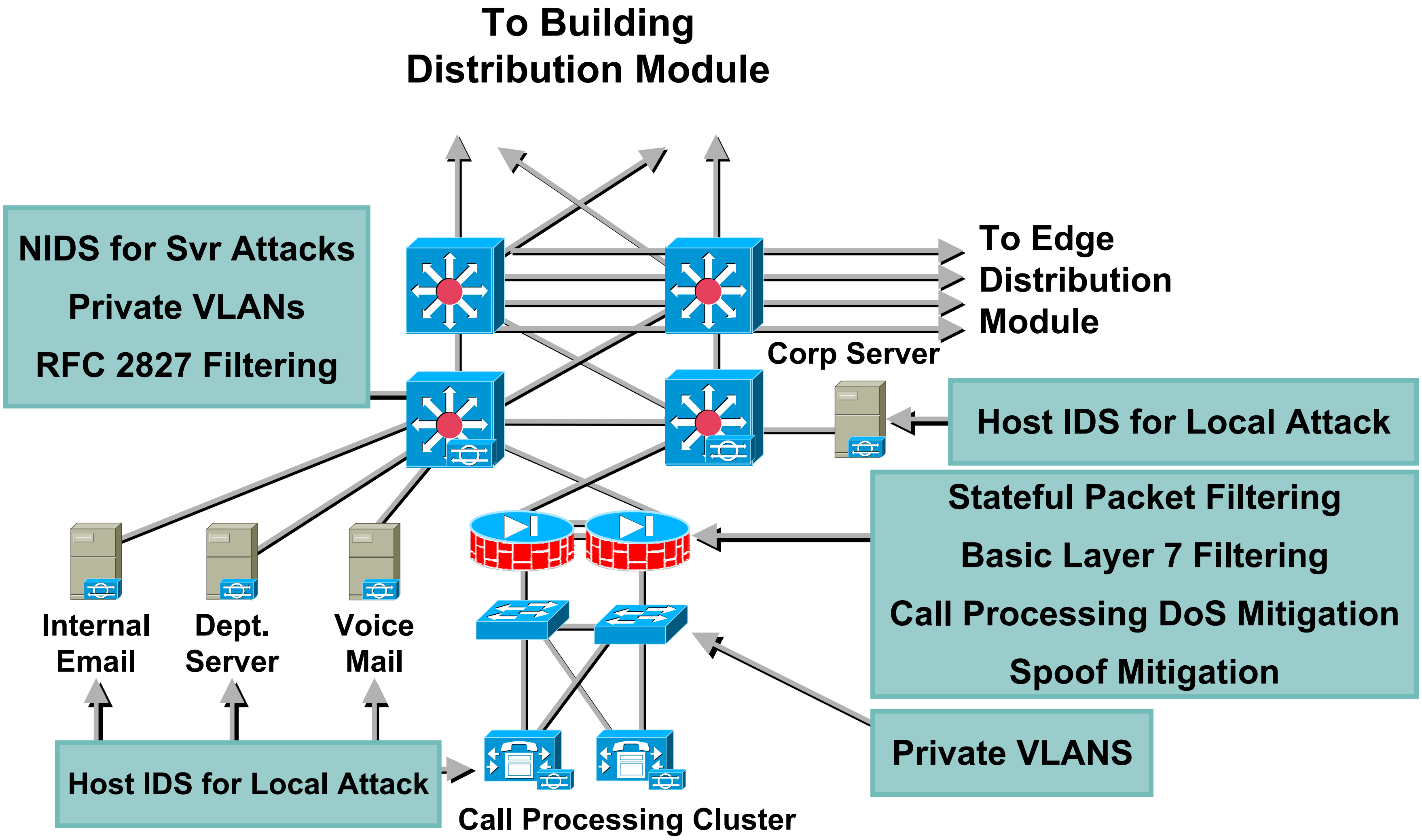
Campus Network Section

- Management module
- Building access and distribution
- Core and server modules
- Edge distribution module

Core and Server Module Design Goals

- L3 switching with authenticated routing protocol
- Private VLANs between servers that do not need communication
- Layer 3 access control
- HIDS and NIDS to protect server resources

Attack Mitigation Roles for Core and Server Modules



To Building Distribution Module

To Edge Distribution Module

NIDS for Svr Attacks

Private VLANs

RFC 2827 Filtering

Host IDS for Local Attack

Stateful Packet Filtering

Basic Layer 7 Filtering

Call Processing DoS Mitigation

Spoof Mitigation

Private VLANS

Host IDS for Local Attack

Campus Network Section

- Management module
- Building access and distribution
- Core and server modules
- Edge distribution module

Edge Distribution Module Design Goals

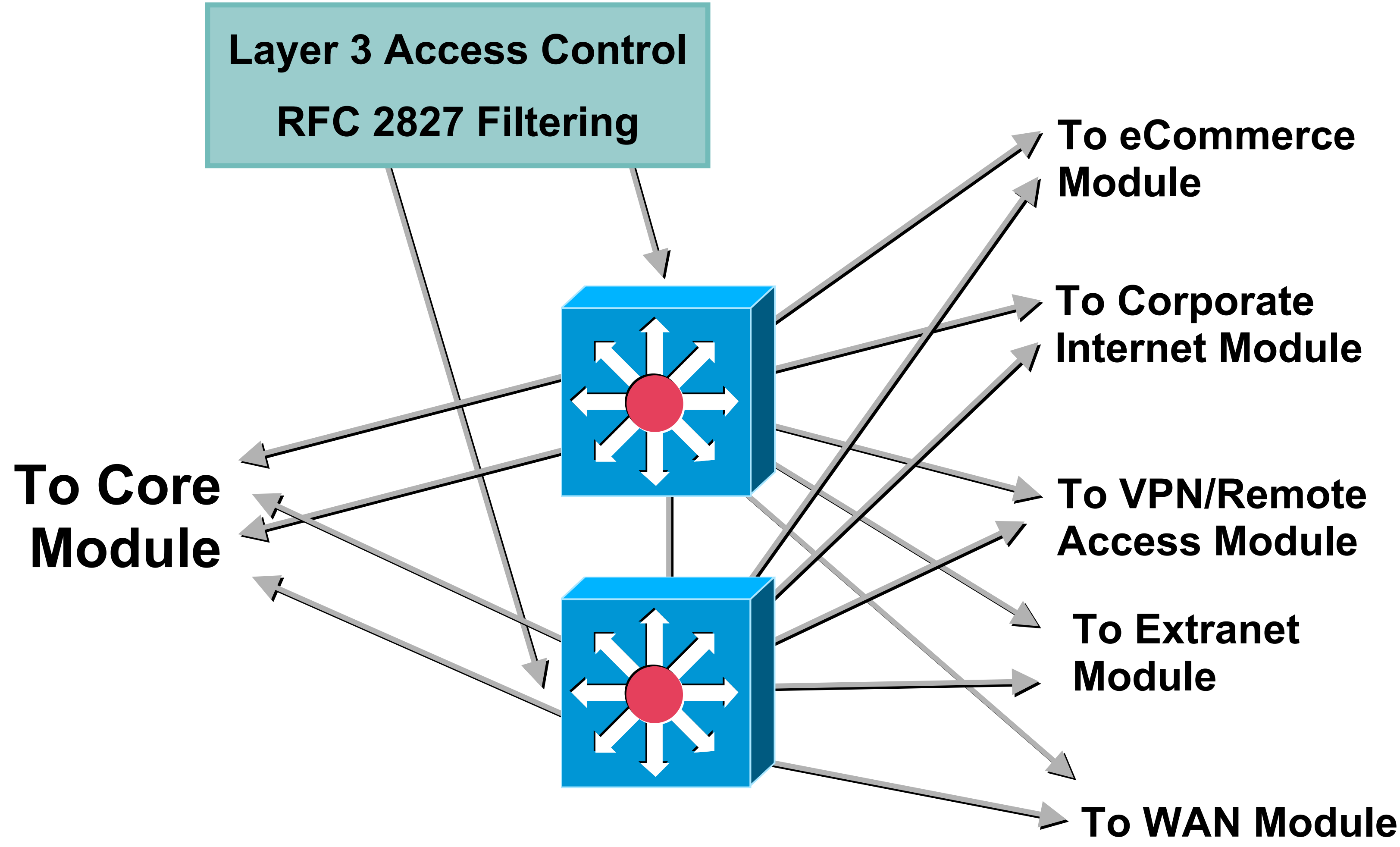
- Aggregation of four edge functions
- Similar to building distribution except:

    Layer 3 filtering can be more extensive since types of access are different

    Can partially rely on firewall functions in edge functional areas

- Last line of defense prior to reaching campus resources

Attack Mitigation Roles for Edge Distribution Module



Layer 3 Access Control

RFC 2827 Filtering

To eCommerce Module

To Corporate Internet Module

To VPN/Remote Access Module

To Extranet Module

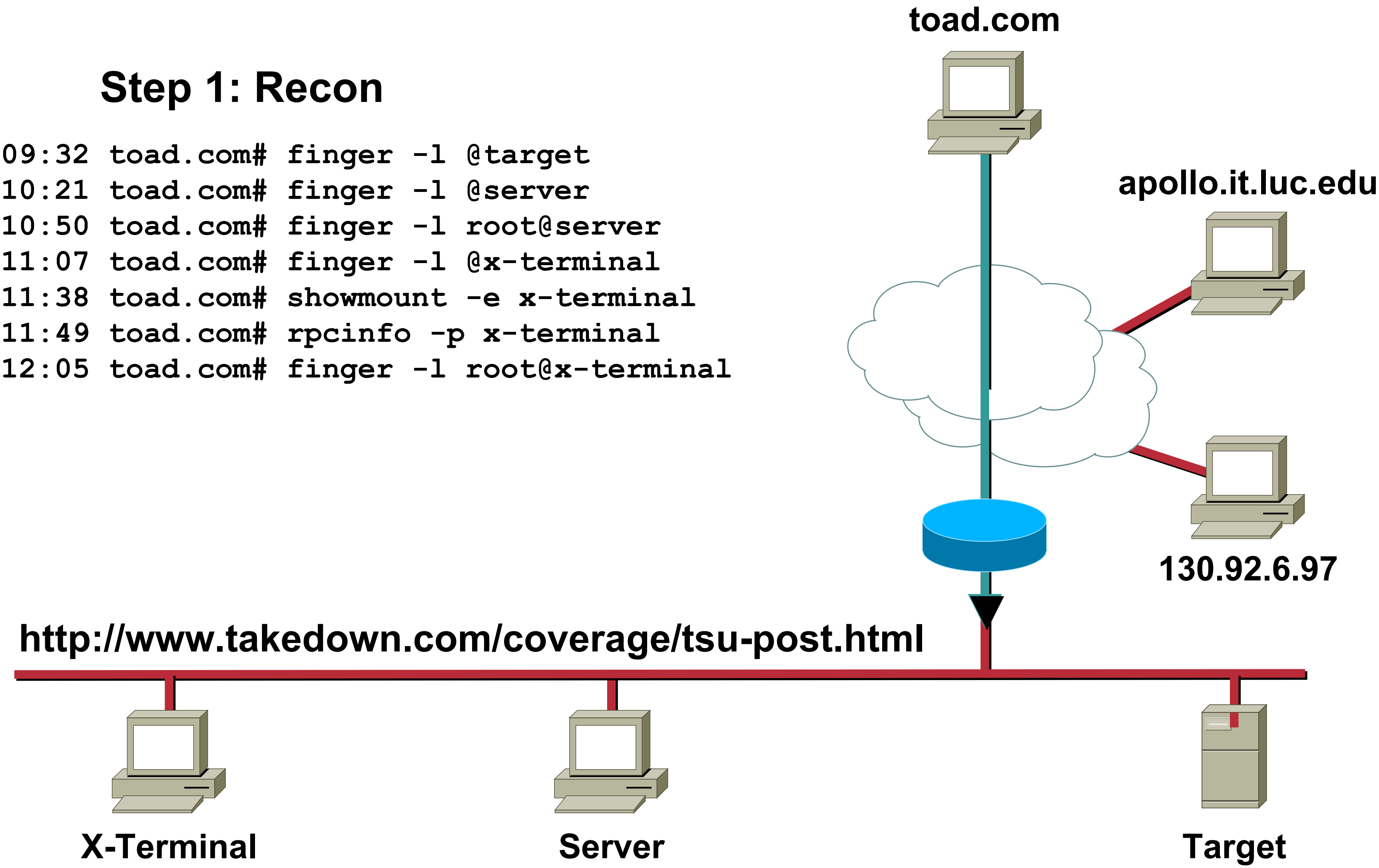
To WAN Module

To Core Module

History Hack #4:
Kevin Mitnick vs. Tsutomu Shimomura

Step 1: Recon

```
14:09:32 toad.com# finger -l @target
14:10:21 toad.com# finger -l @server
14:10:50 toad.com# finger -l root@server
14:11:07 toad.com# finger -l @x-terminal
14:11:38 toad.com# showmount -e x-terminal
14:11:49 toad.com# rpcinfo -p x-terminal
14:12:05 toad.com# finger -l root@x-terminal
```

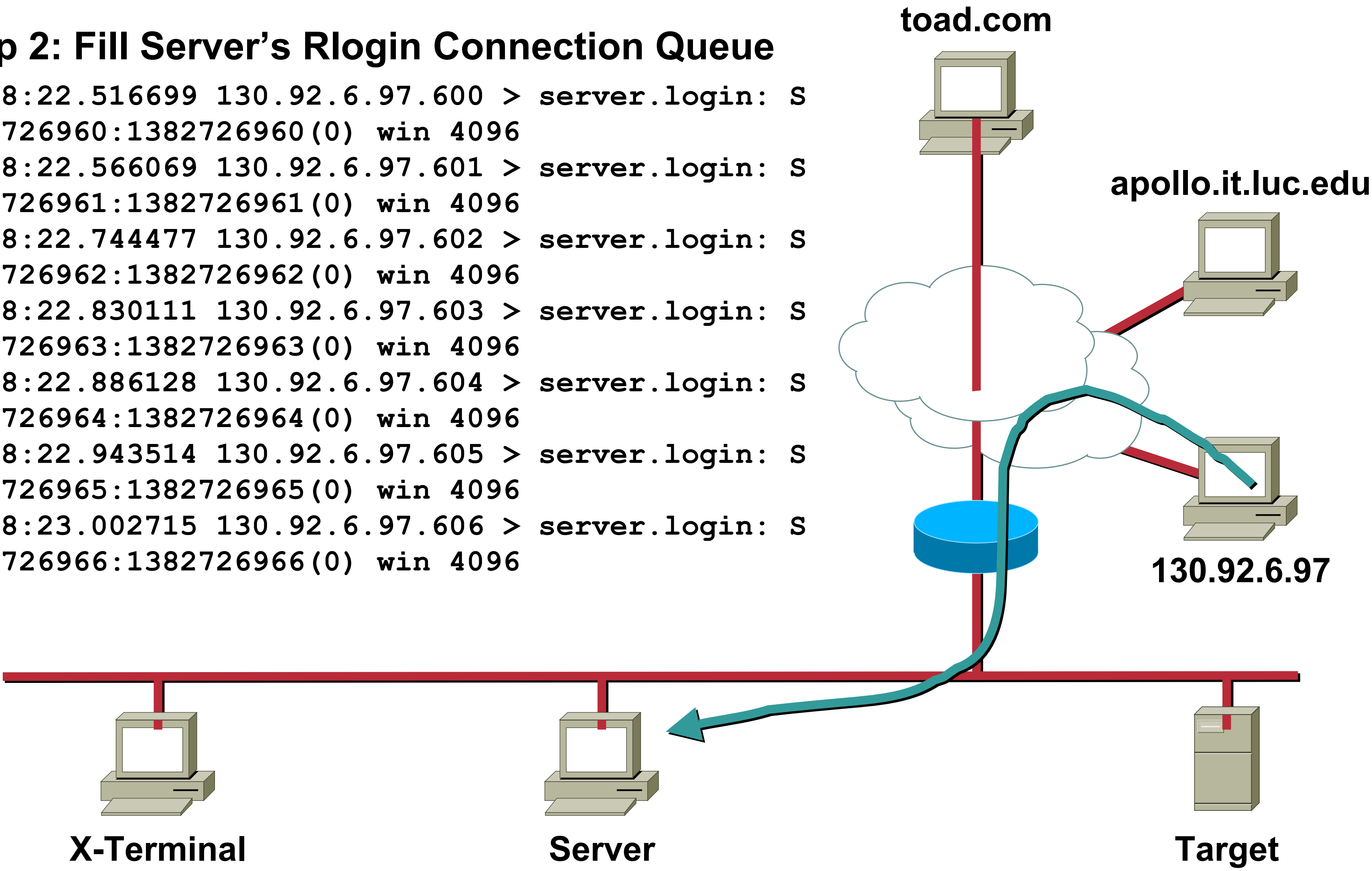


http://www.takedown.com/coverage/tsu-post.html

History Hack #4:
Kevin Mitnick vs. Tsutomu Shimomura

Step 2: Fill Server's Rlogin Connection Queue

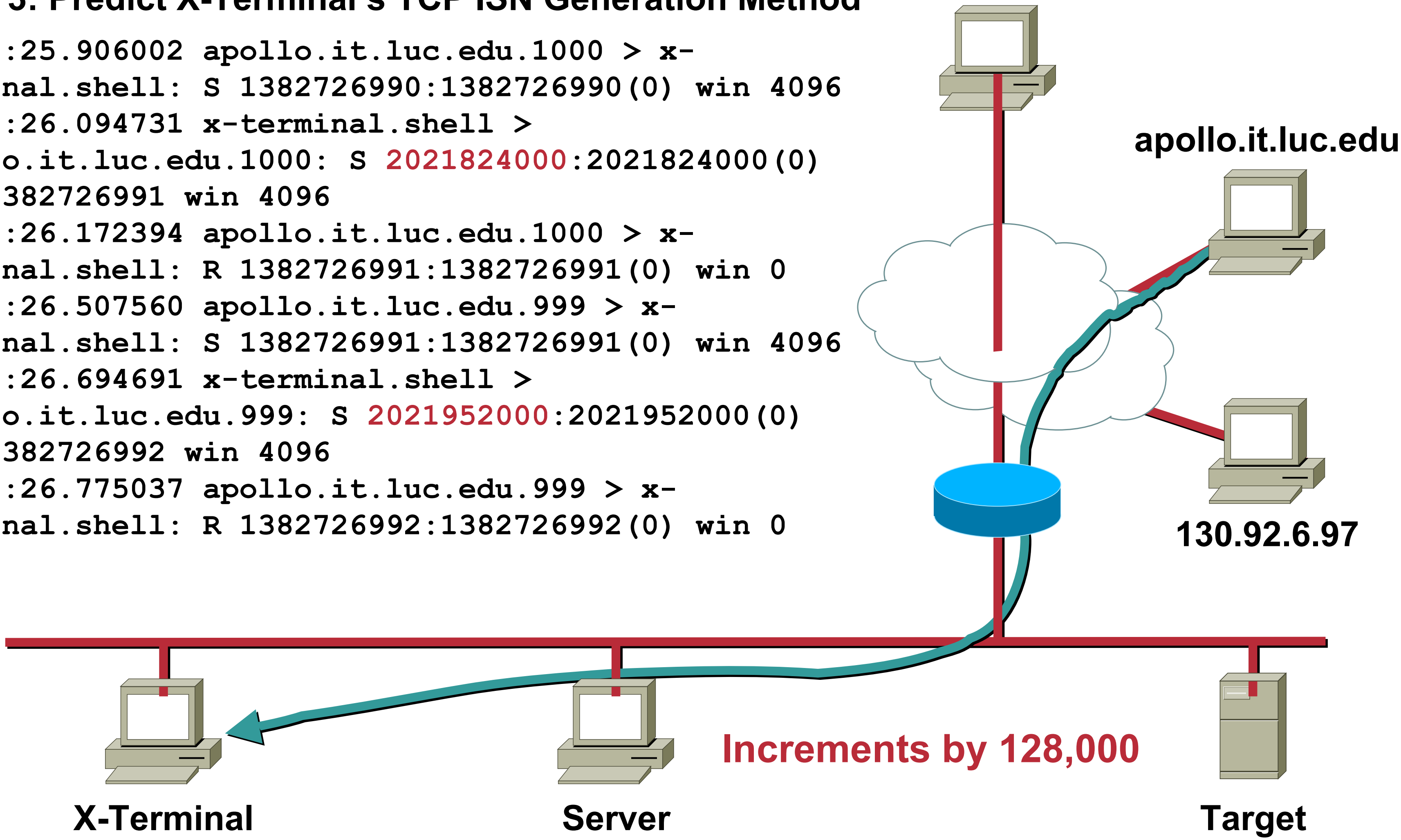
```
14:18:22.516699 130.92.6.97.600 > server.login: S
1382726960:1382726960(0) win 4096
14:18:22.566069 130.92.6.97.601 > server.login: S
1382726961:1382726961(0) win 4096
14:18:22.744477 130.92.6.97.602 > server.login: S
1382726962:1382726962(0) win 4096
14:18:22.830111 130.92.6.97.603 > server.login: S
1382726963:1382726963(0) win 4096
14:18:22.886128 130.92.6.97.604 > server.login: S
1382726964:1382726964(0) win 4096
14:18:22.943514 130.92.6.97.605 > server.login: S
1382726965:1382726965(0) win 4096
14:18:23.002715 130.92.6.97.606 > server.login: S
1382726966:1382726966(0) win 4096
```



History Hack #4: Kevin Mitnick vs. Tsutomu Shimomura

Step 3: Predict X-Terminal’s TCP ISN Generation Method

```
14:18:25.906002 apollo.it.luc.edu.1000 > x-
terminal.shell: S 1382726990:1382726990(0) win 4096
14:18:26.094731 x-terminal.shell >
apollo.it.luc.edu.1000: S 2021824000:2021824000(0)
ack 1382726991 win 4096
14:18:26.172394 apollo.it.luc.edu.1000 > x-
terminal.shell: R 1382726991:1382726991(0) win 0
14:18:26.507560 apollo.it.luc.edu.999 > x-
terminal.shell: S 1382726991:1382726991(0) win 4096
14:18:26.694691 x-terminal.shell >
apollo.it.luc.edu.999: S 2021952000:2021952000(0)
ack 1382726992 win 4096
14:18:26.775037 apollo.it.luc.edu.999 > x-
terminal.shell: R 1382726992:1382726992(0) win 0
```



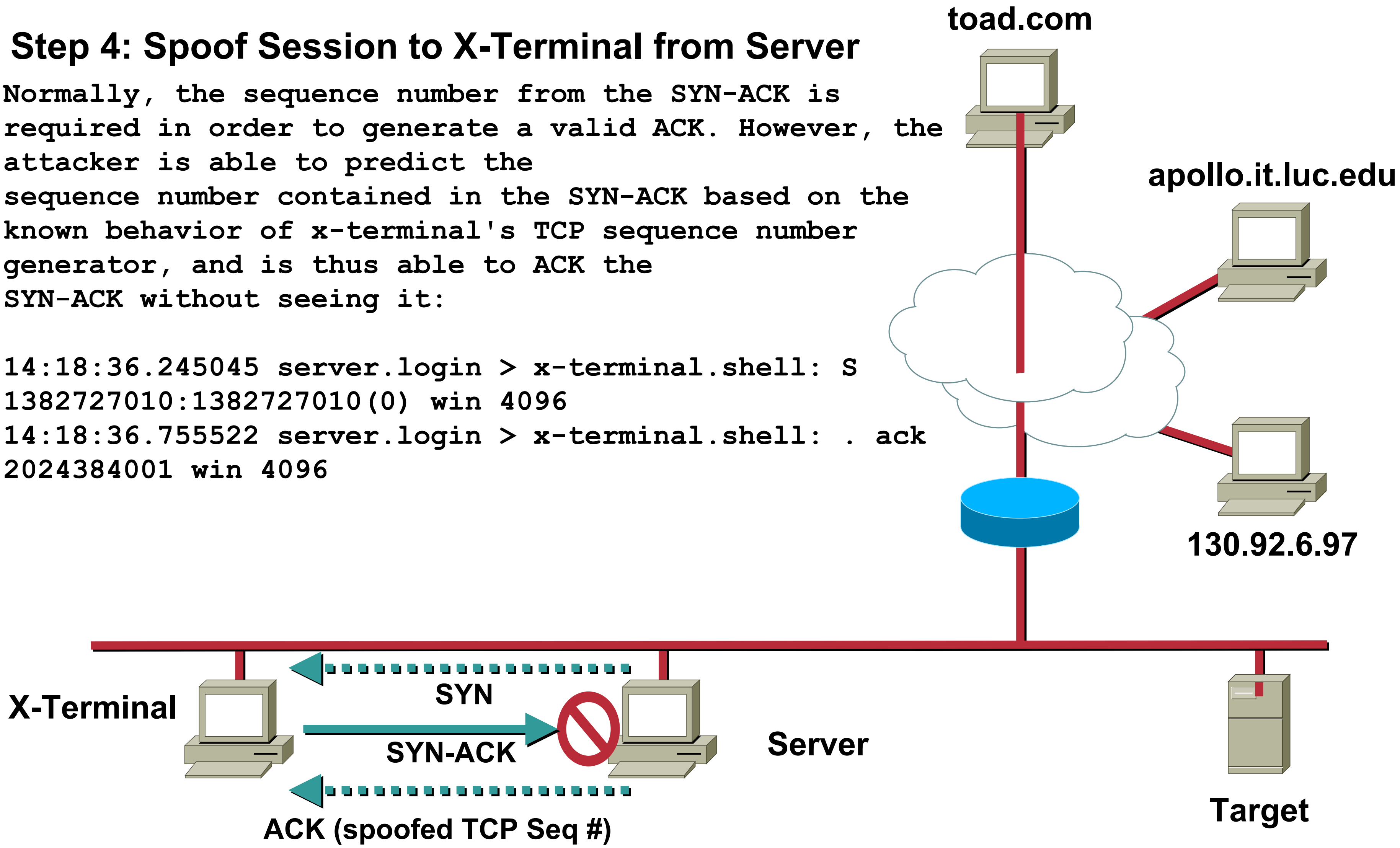
Increments by 128,000

History Hack #4:
Kevin Mitnick vs. Tsutomu Shimomura

Step 4: Spoof Session to X-Terminal from Server

Normally, the sequence number from the SYN-ACK is required in order to generate a valid ACK. However, the attacker is able to predict the sequence number contained in the SYN-ACK based on the known behavior of x-terminal's TCP sequence number generator, and is thus able to ACK the SYN-ACK without seeing it:

```
14:18:36.245045 server.login > x-terminal.shell: S
1382727010:1382727010(0) win 4096
14:18:36.755522 server.login > x-terminal.shell: . ack
2024384001 win 4096
```



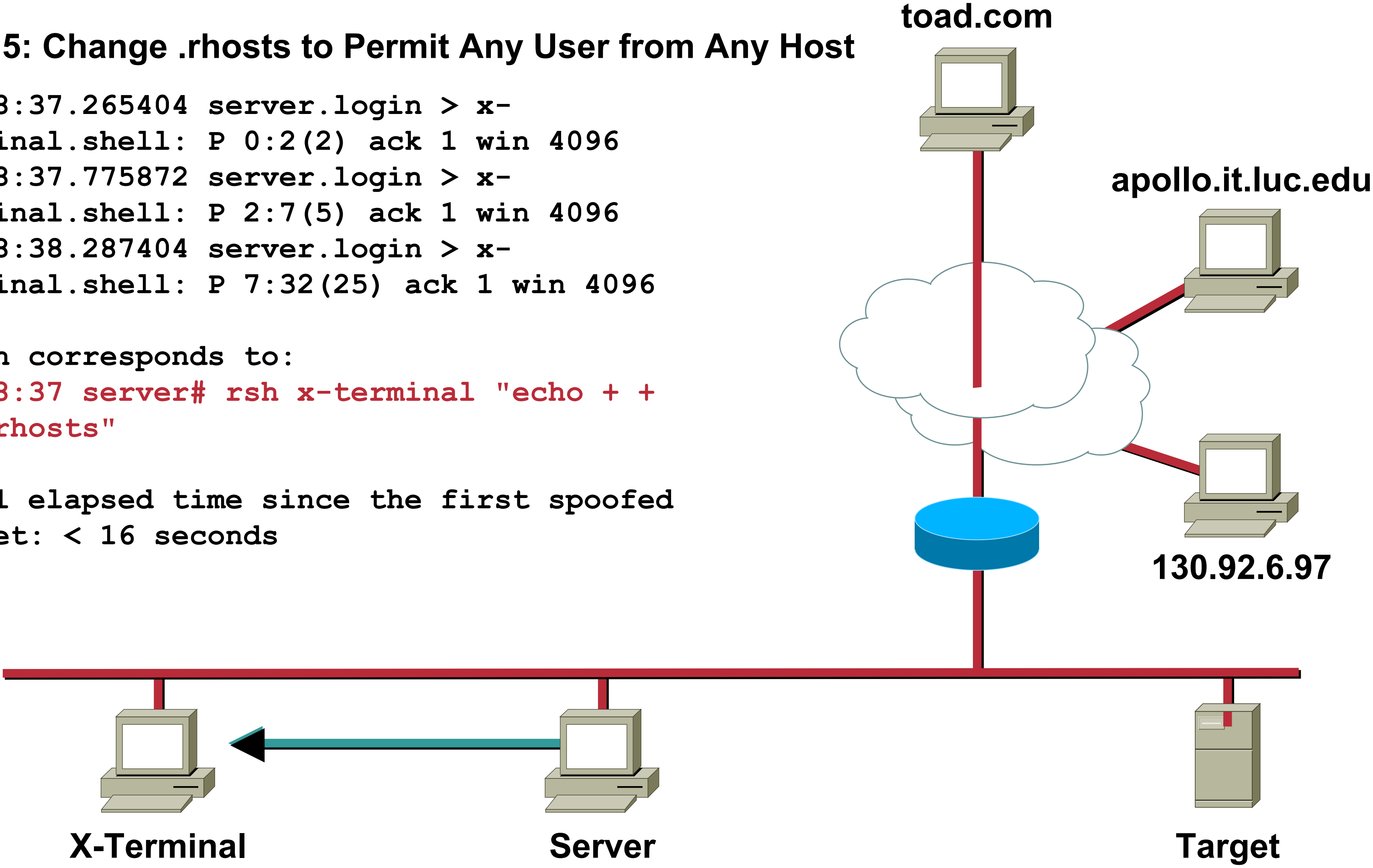
History Hack #4:
Kevin Mitnick vs. Tsutomu Shimomura

Step 5: Change .rhosts to Permit Any User from Any Host

```
14:18:37.265404 server.login > x-
terminal.shell: P 0:2(2) ack 1 win 4096
14:18:37.775872 server.login > x-
terminal.shell: P 2:7(5) ack 1 win 4096
14:18:38.287404 server.login > x-
terminal.shell: P 7:32(25) ack 1 win 4096
```

```
which corresponds to:
14:18:37 server# rsh x-terminal "echo + +
>>/.rhosts"
```

```
Total elapsed time since the first spoofed
packet: < 16 seconds
```



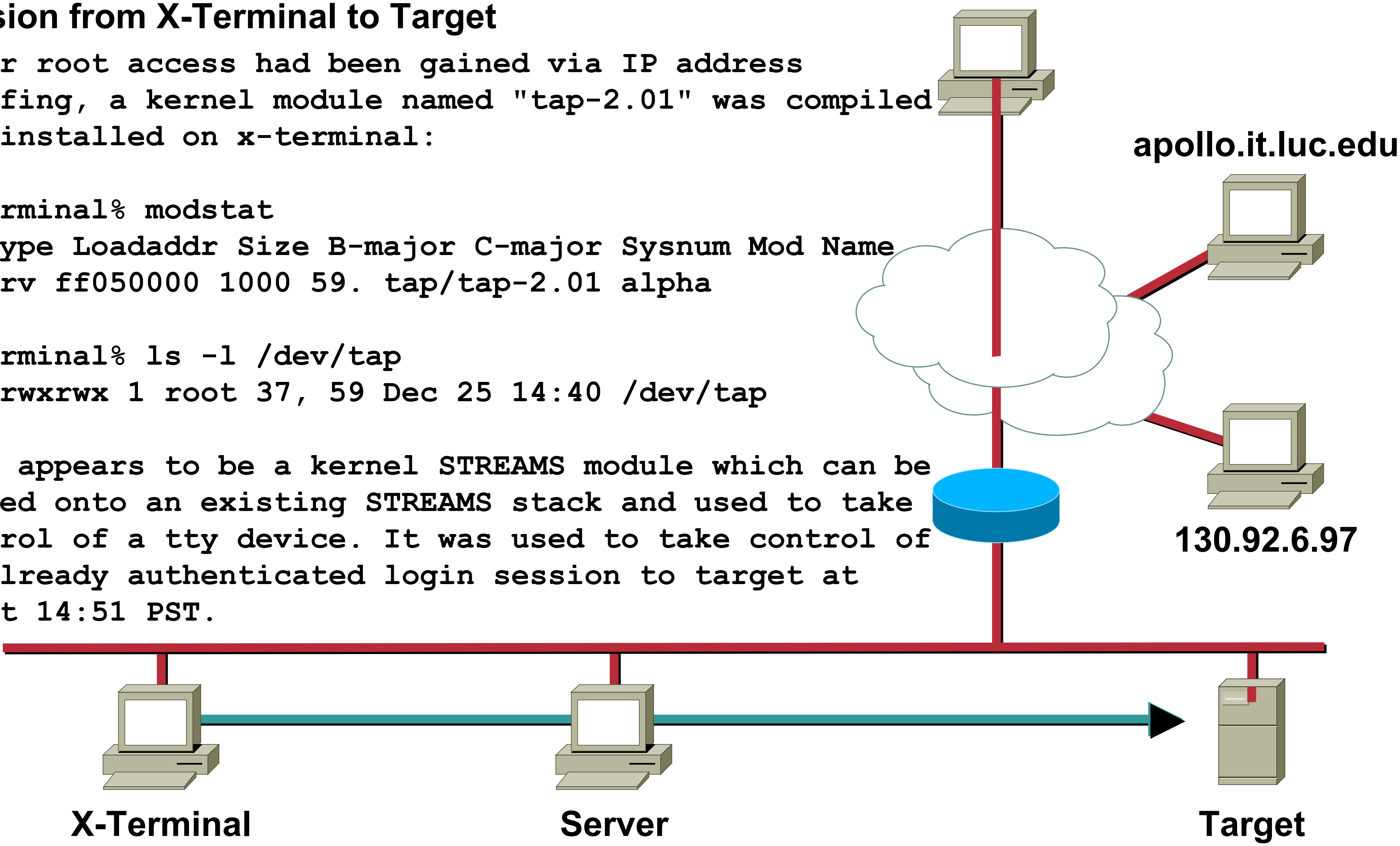
History Hack #4:
Kevin Mitnick vs. Tsutomu Shimomura

Step 6: Install Tool to Grant Access to Pre-Authenticated Session from X-Terminal to Target

After root access had been gained via IP address spoofing, a kernel module named "tap-2.01" was compiled and installed on x-terminal:

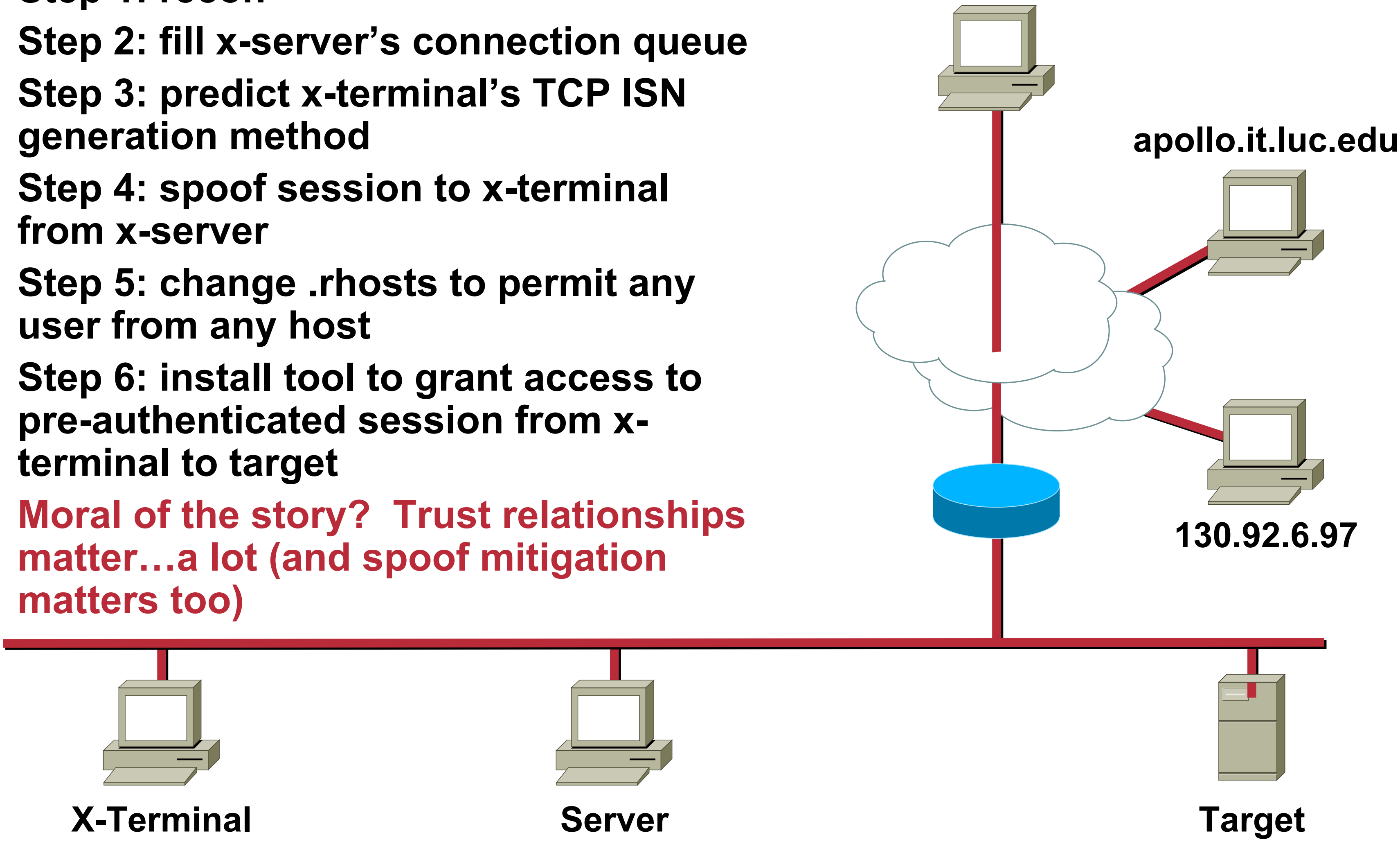
```
x-terminal% modstat
Id Type Loadaddr Size B-major C-major Sysnum Mod Name
1 Pdrv ff050000 1000 59. tap/tap-2.01 alpha

x-terminal% ls -l /dev/tap
crwxrwxrwx 1 root 37, 59 Dec 25 14:40 /dev/tap
```

This appears to be a kernel STREAMS module which can be pushed onto an existing STREAMS stack and used to take control of a tty device. It was used to take control of an already authenticated login session to target at about 14:51 PST.

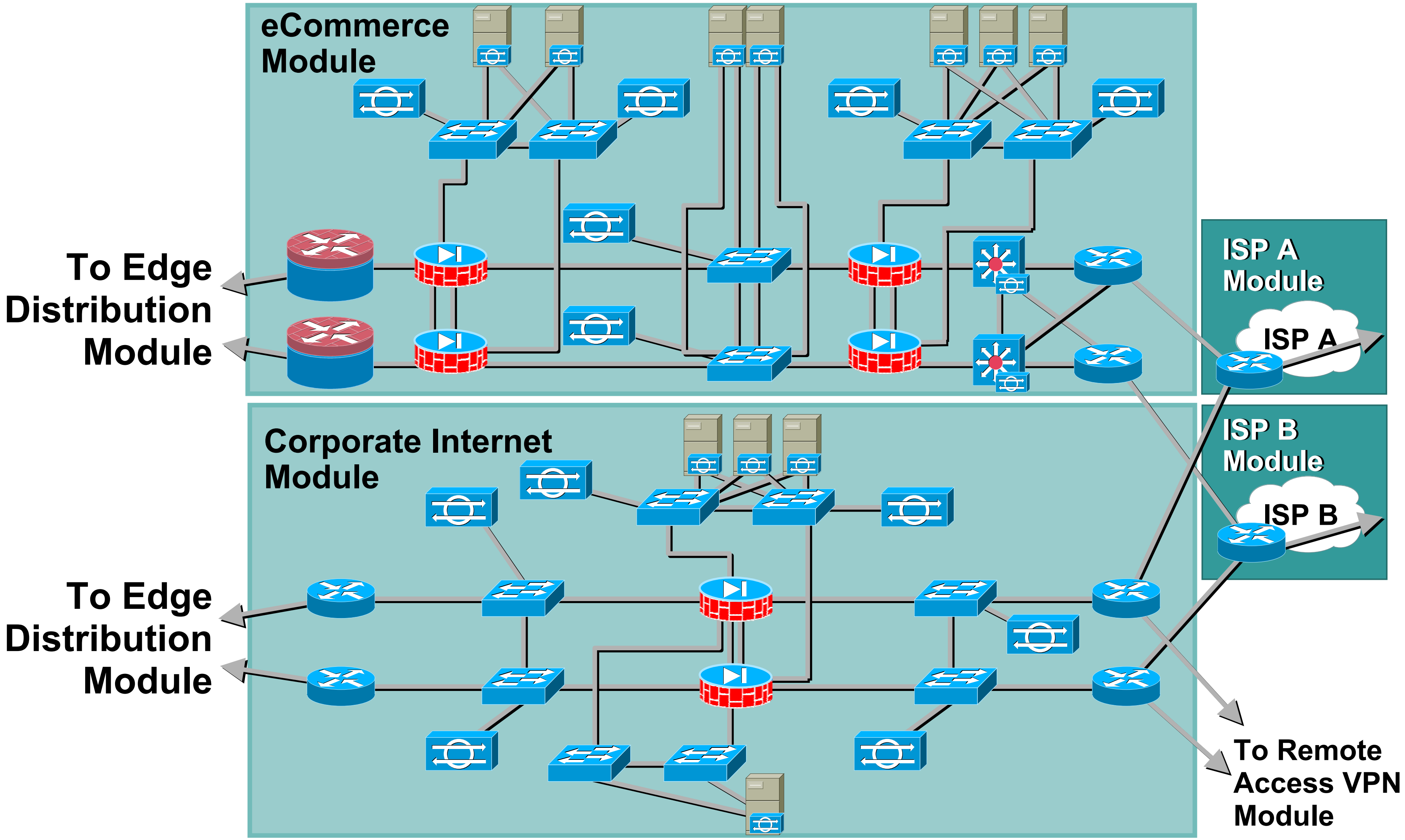


History Hack #4:
Kevin Mitnick vs. Tsutomu Shimomura

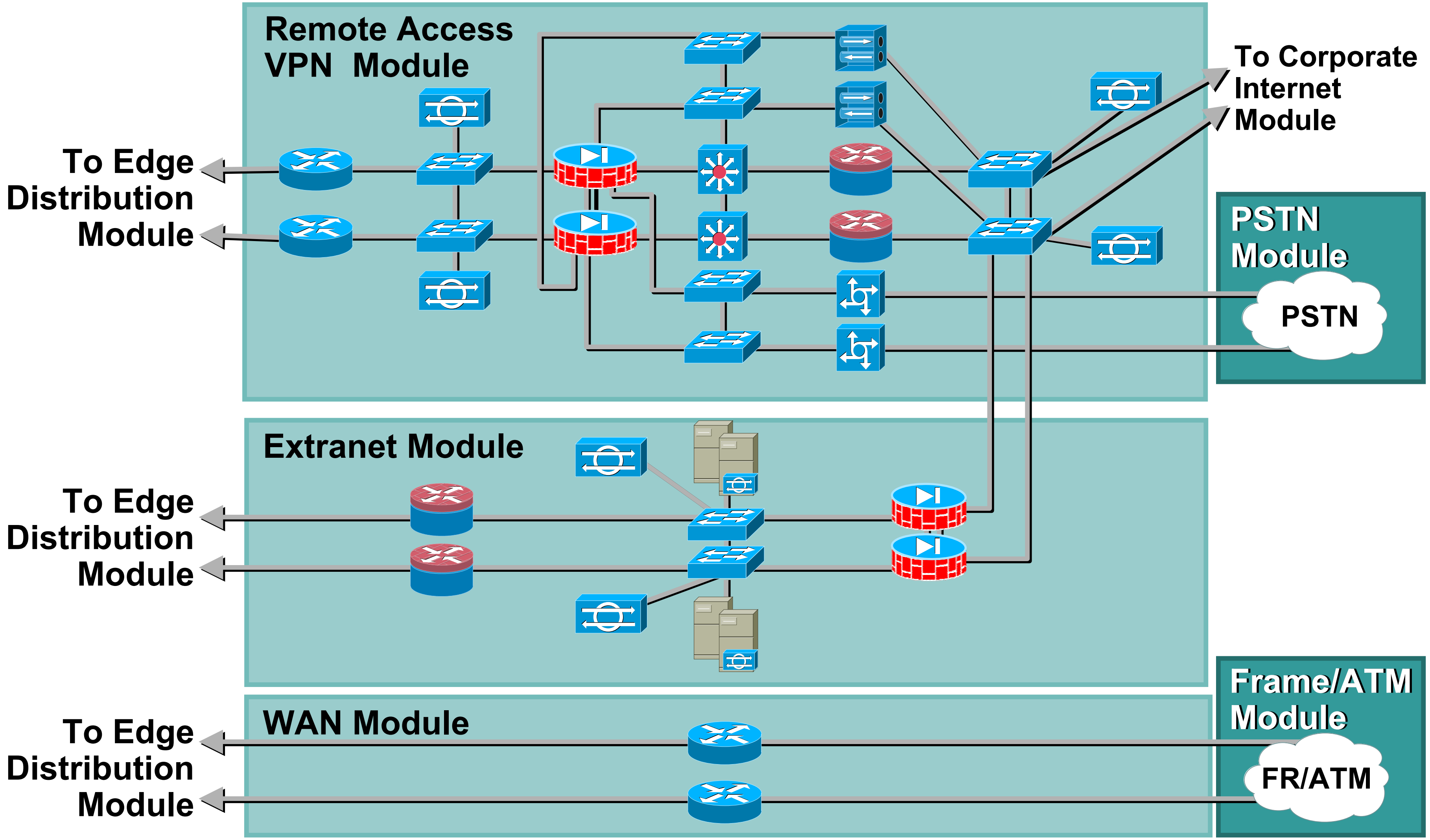
- Step 1: recon
- Step 2: fill x-server's connection queue
- Step 3: predict x-terminal's TCP ISN generation method
- Step 4: spoof session to x-terminal from x-server
- Step 5: change .rhosts to permit any user from any host
- Step 6: install tool to grant access to pre-authenticated session from x-terminal to target
- Moral of the story? Trust relationships matter…a lot (and spoof mitigation matters too)



Enterprise Edge Detail—Part 1


eCommerce Module
To Edge Distribution Module
ISP A Module
ISP A
Corporate Internet Module
ISP B Module
ISP B
To Edge Distribution Module
To Remote Access VPN Module

Enterprise Edge Detail—Part 2


Remote Access VPN Module
To Corporate Internet Module
To Edge Distribution Module
PSTN Module
PSTN
Extranet Module
To Edge Distribution Module
WAN Module
To Edge Distribution Module
Frame/ATM Module
FR/ATM

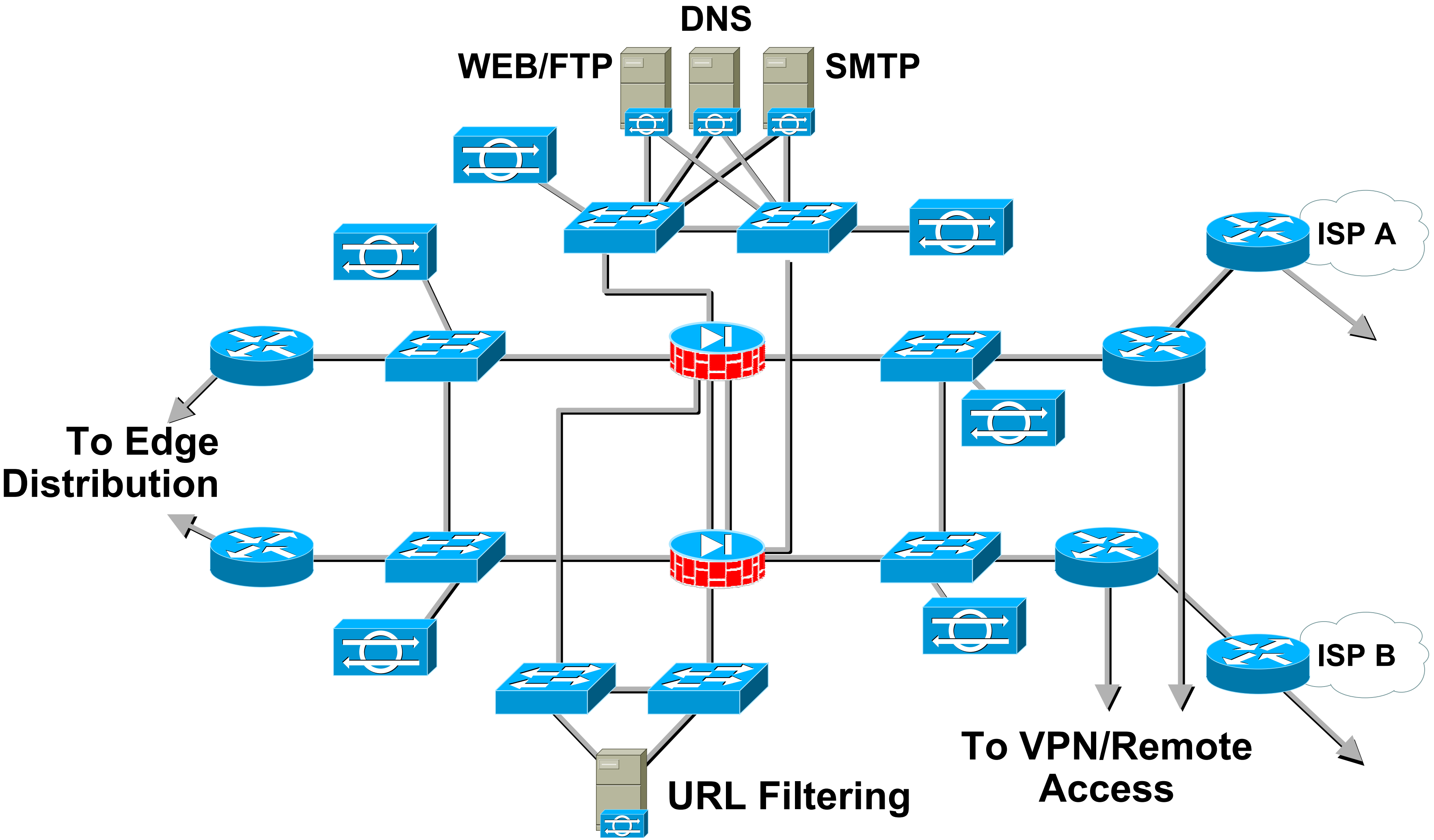
Edge Network Section

- Corporate Internet module
- Remote access VPN module
- Extranet module
- WAN module
- E-commerce module

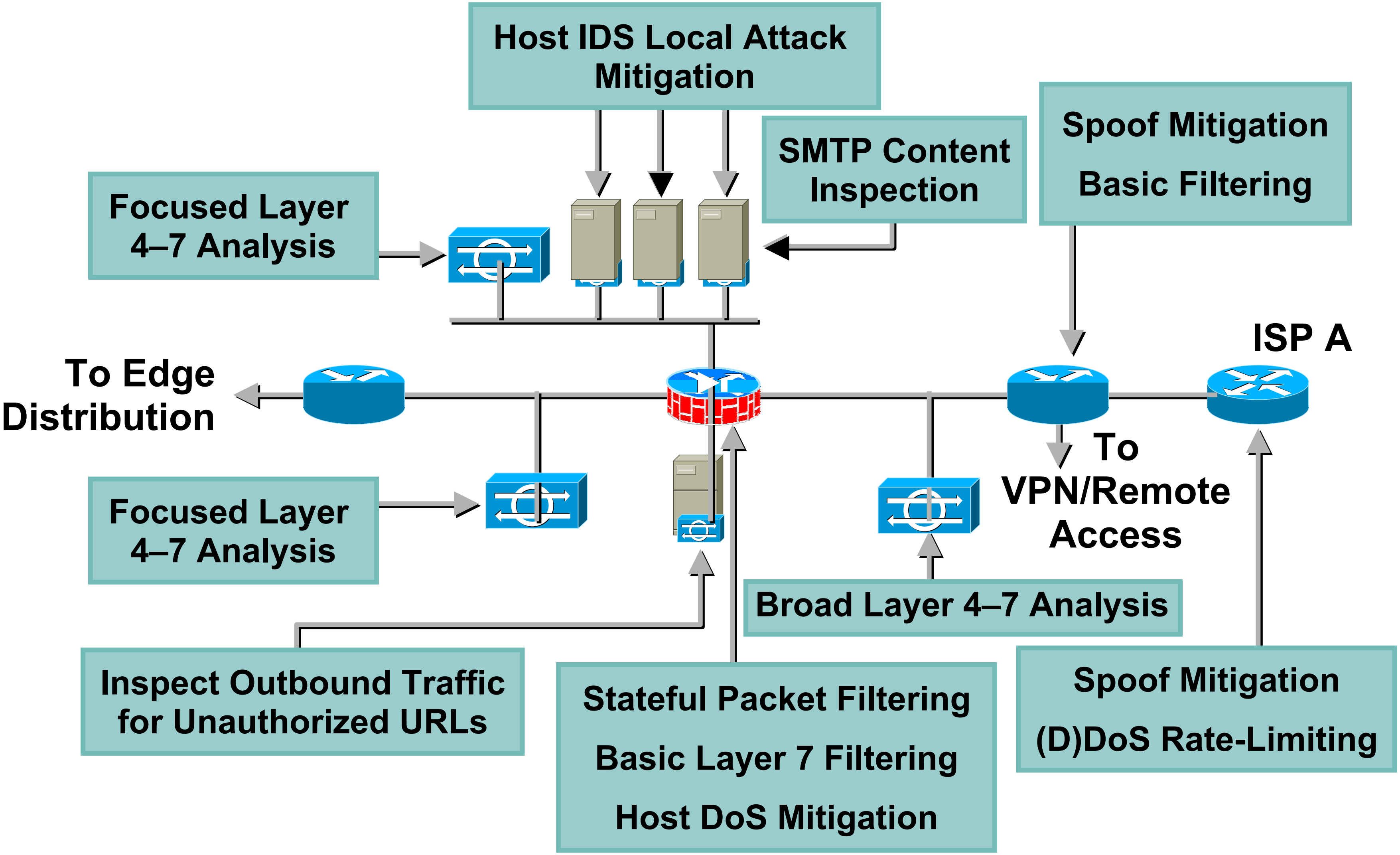
Corporate Internet Module Design Goals

- Resilient firewall pair
- Three security points
  - Ingress from ISP
  - Public host DMZ
  - Internal corporate network
- Security applications
  - SMTP content filtering
  - URL inspection

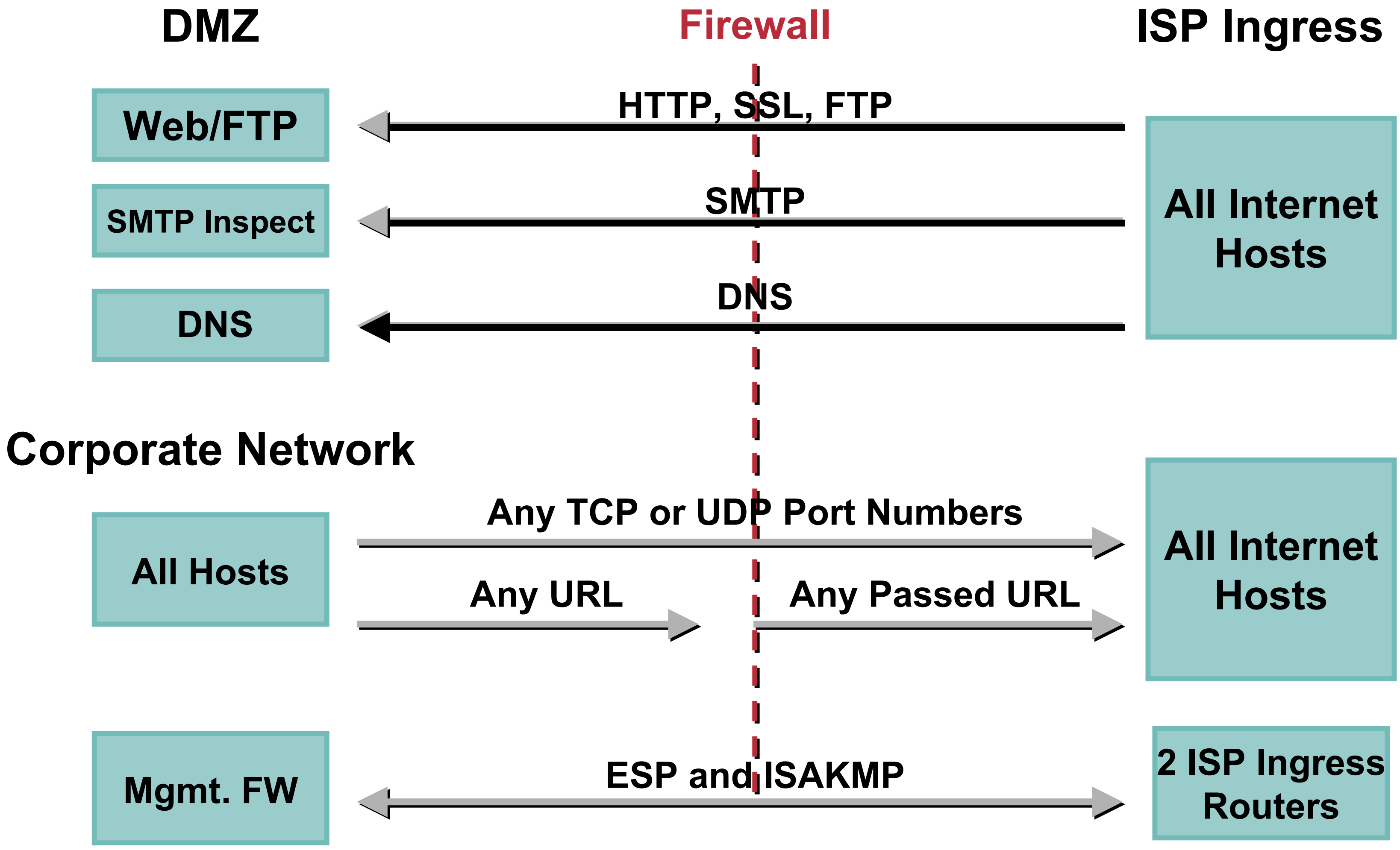
Corporate Internet Module—Detail



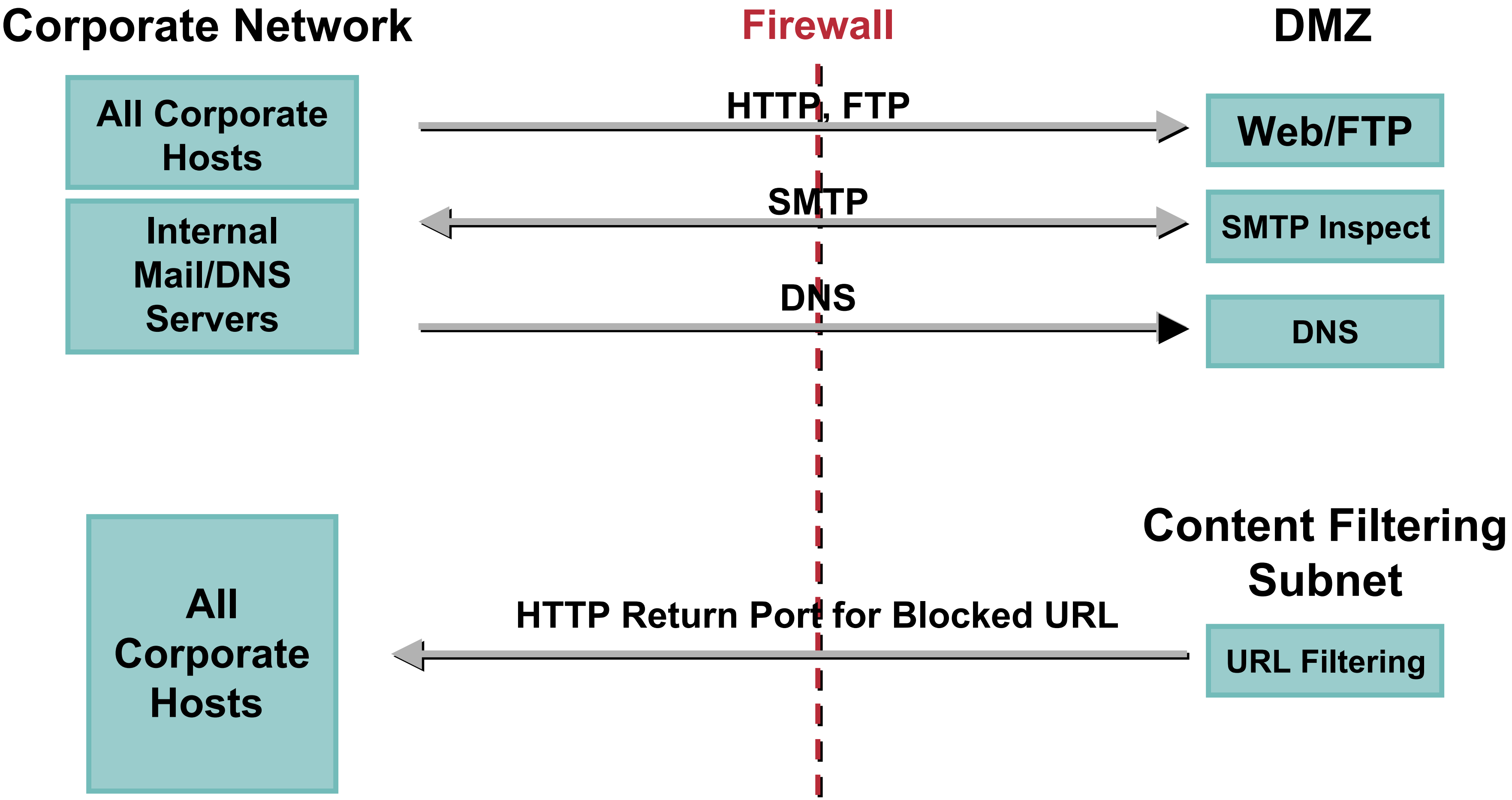
Attack Mitigation Roles for Corporate Internet Module



Stateful Packet Filtering:
Internet to DMZ, Corporate Network



Stateful Packet Filtering:
Corporate Network to DMZ and URL Filter


Corporate Network

Firewall

DMZ

All Corporate Hosts

Internal Mail/DNS Servers

HTTP, FTP

SMTP

DNS

Web/FTP

SMTP Inspect

DNS

Content Filtering Subnet

All Corporate Hosts

HTTP Return Port for Blocked URL

URL Filtering

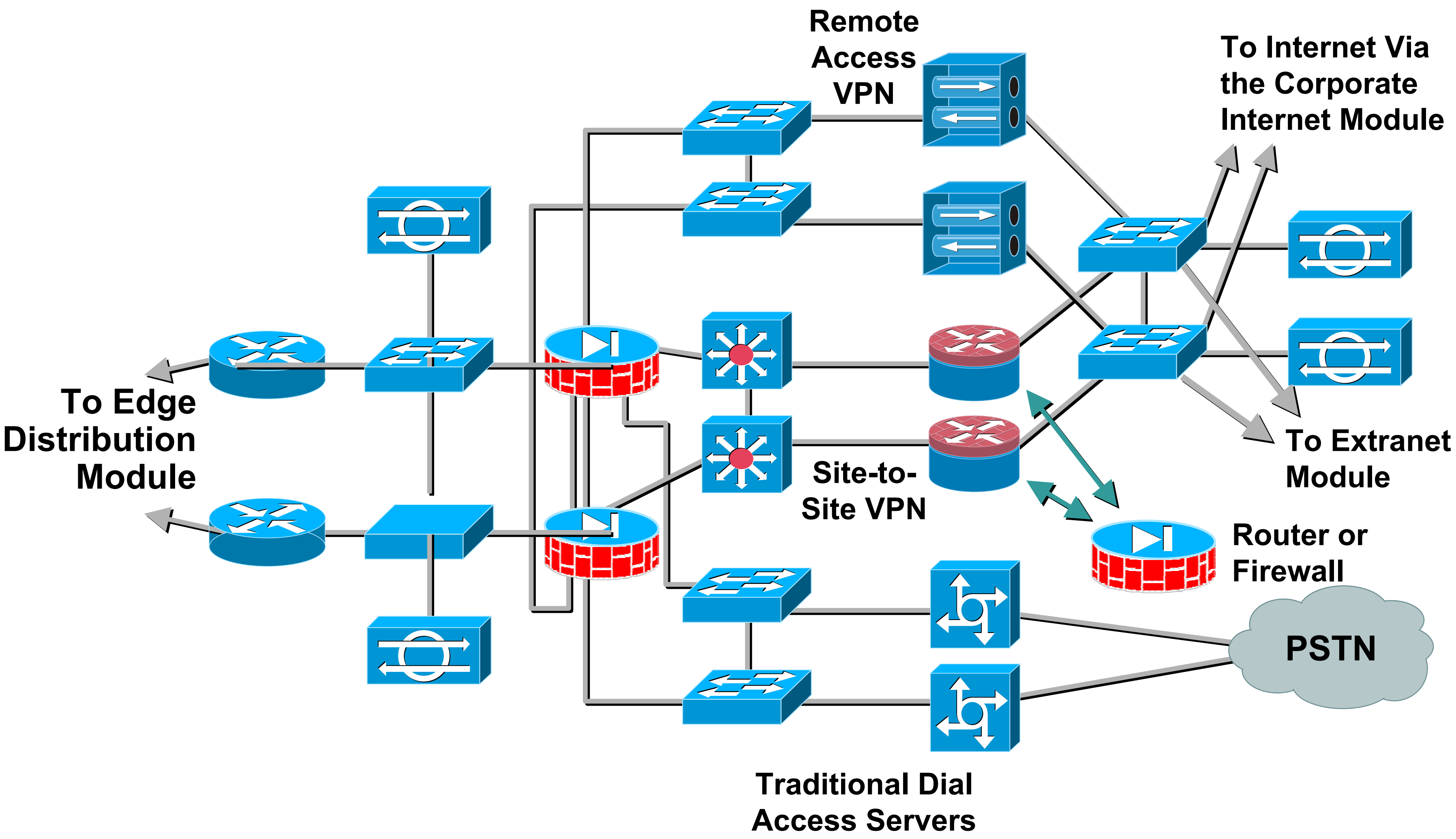
Edge Network Section

- Corporate Internet module
- Remote access VPN module
- Extranet module
- WAN module
- E-commerce module

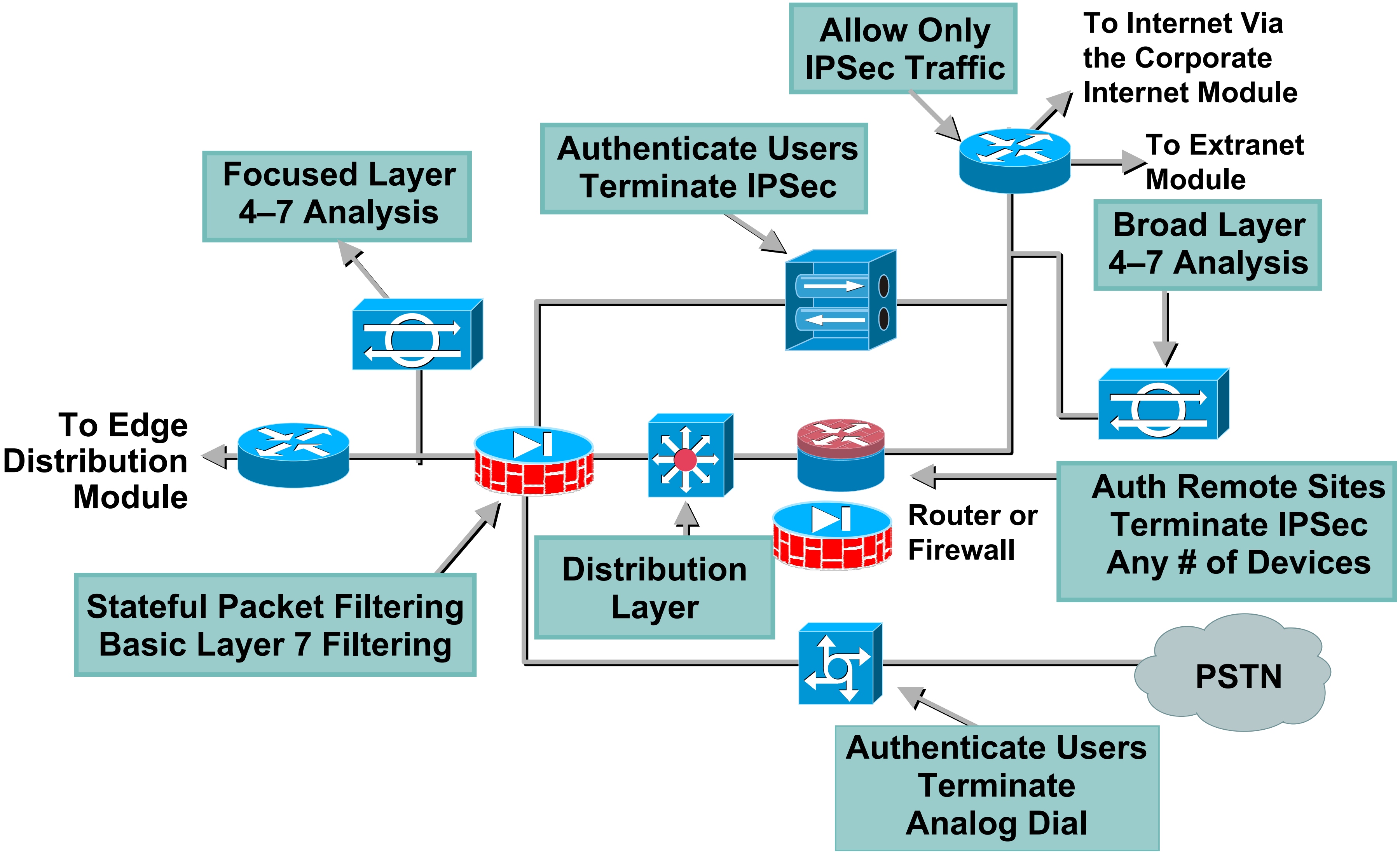
Remote Access VPN Module Design Goals

- Resilient firewall pair
- Three different security requirements
  - Classic (PSTN) remote access
  - VPN remote access
  - Site-to-site VPN connectivity

Remote Access VPN Module—Detail


Remote Access VPN
To Internet Via the Corporate Internet Module
To Edge Distribution Module
To Extranet Module
Site-to-Site VPN
Router or Firewall
PSTN
Traditional Dial Access Servers

Attack Mitigation Roles for Remote Access VPN Module


Allow Only IPSec Traffic
To Internet Via the Corporate Internet Module
To Extranet Module
Authenticate Users Terminate IPSec
Focused Layer 4–7 Analysis
Broad Layer 4–7 Analysis
To Edge Distribution Module
Router or Firewall
Auth Remote Sites Terminate IPSec Any # of Devices
Stateful Packet Filtering Basic Layer 7 Filtering
Distribution Layer
PSTN
Authenticate Users Terminate Analog Dial

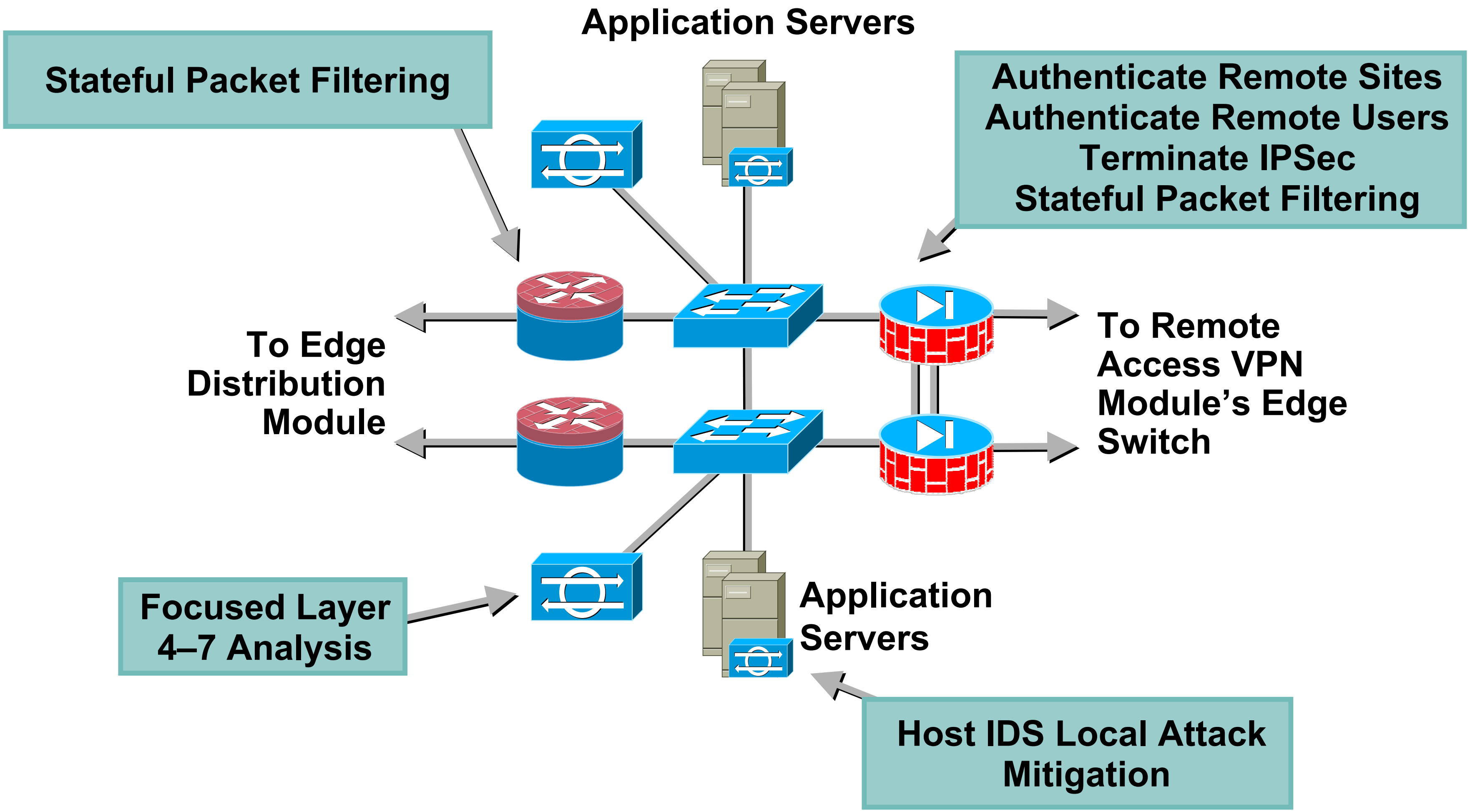
Edge Network Section

- Corporate Internet module
- Remote access VPN module
- Extranet module
- WAN module
- E-commerce module

Extranet Module Design Goals

- Terminate business partner connections
  - Remote access IPsec
  - Site to site IPsec
- Mitigate application server attacks
- Prevent extranet as launch-point into campus

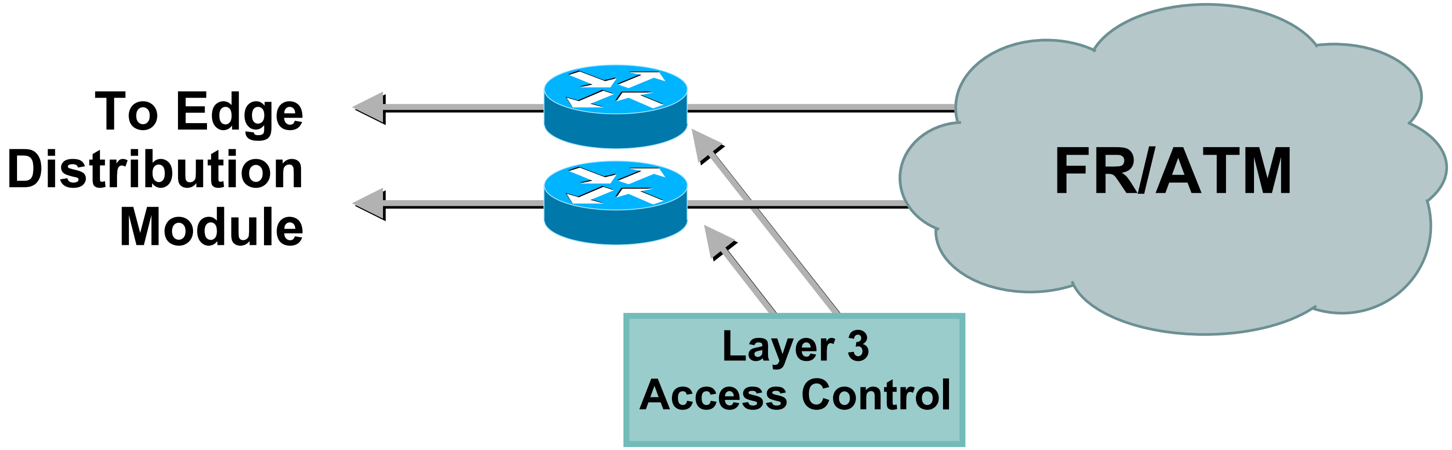
Extranet Module—Detail


Application Servers
Stateful Packet Filtering
Authenticate Remote Sites
Authenticate Remote Users
Terminate IPSec
Stateful Packet Filtering
To Edge Distribution Module
To Remote Access VPN Module's Edge Switch
Focused Layer 4–7 Analysis
Application Servers
Host IDS Local Attack Mitigation

Edge Network Section

- Corporate Internet module
- Remote access and VPN module
- Extranet module
- WAN module
- E-commerce module

Classic WAN Module:
Detail and Attack Mitigation



- **Classic WAN not often addressed in security context**
- **ISP initiated man-in-the-middle attacks can be mitigated by several IOS features:**

  Layer 3/4 access-control

  IPSec encryption—needed if level of trust for layer 2 WAN technology is not high

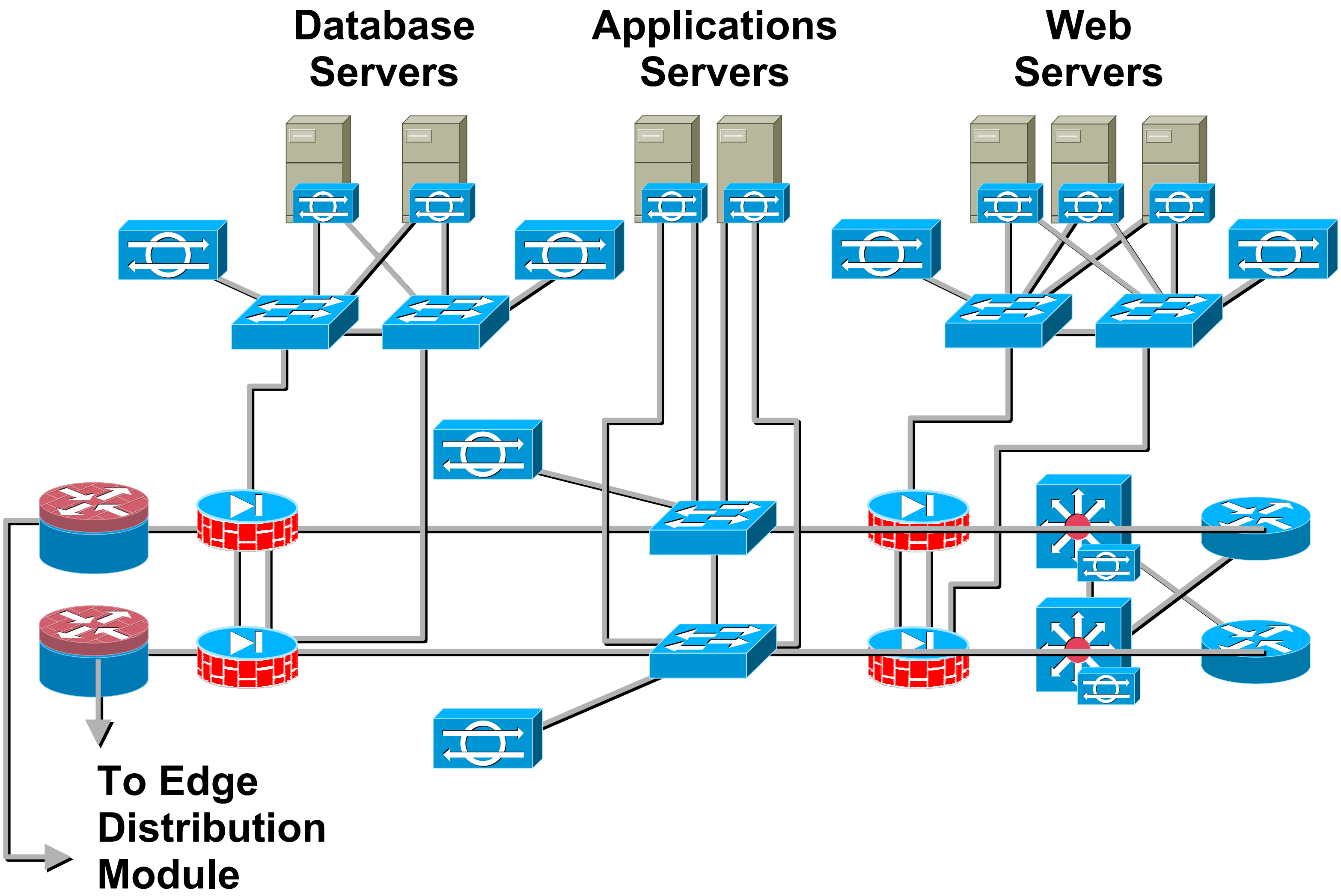
Edge Network Section

- Corporate Internet module
- Remote access and VPN module
- Extranet module
- WAN module
- E-commerce module

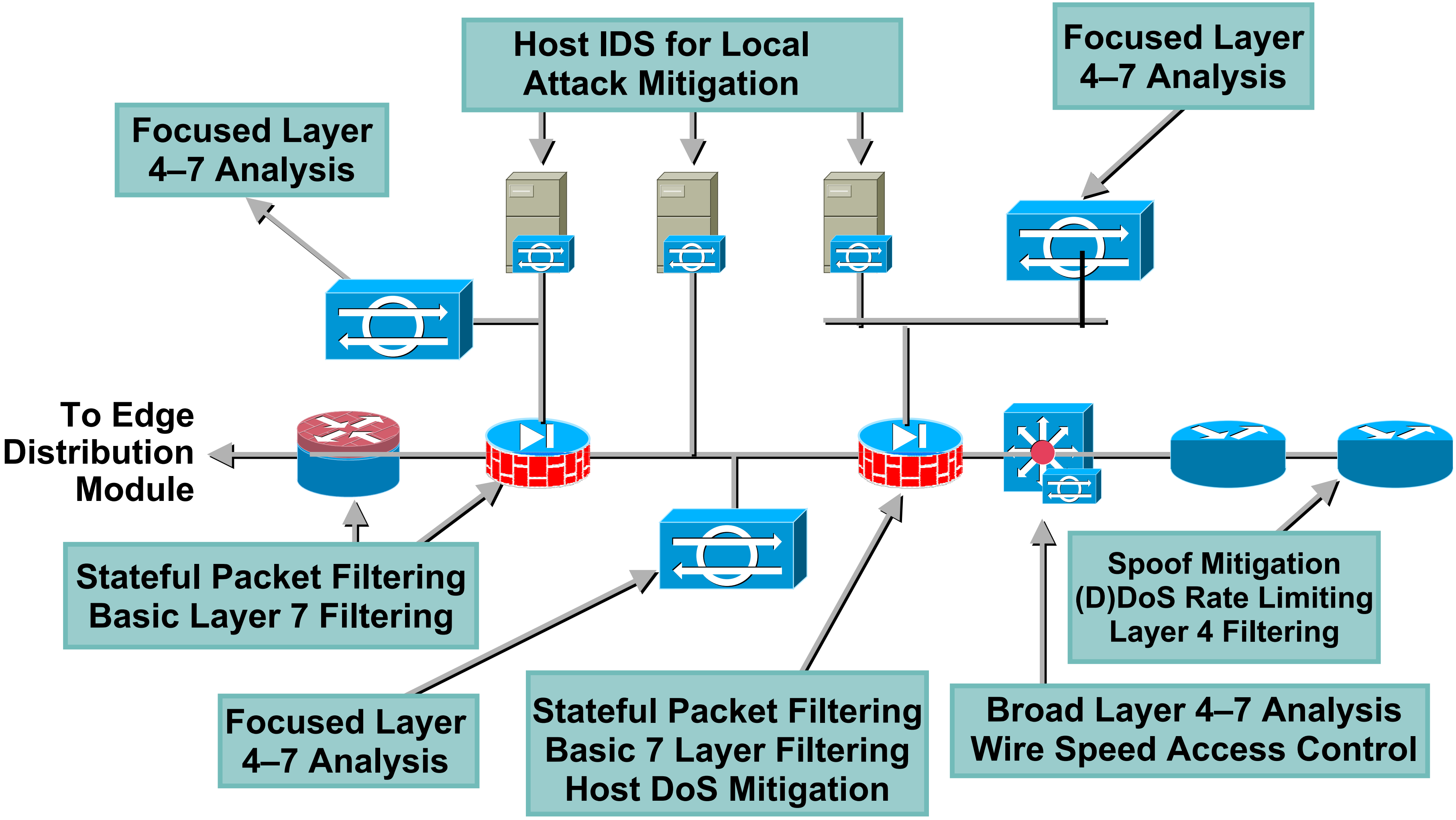
E-Commerce Module Design Goals

- Highest visibility = largest attack target
- Tiered resilient FW design
- Layered host and network IDS
- Proper trust model

E-Commerce Module—Detail

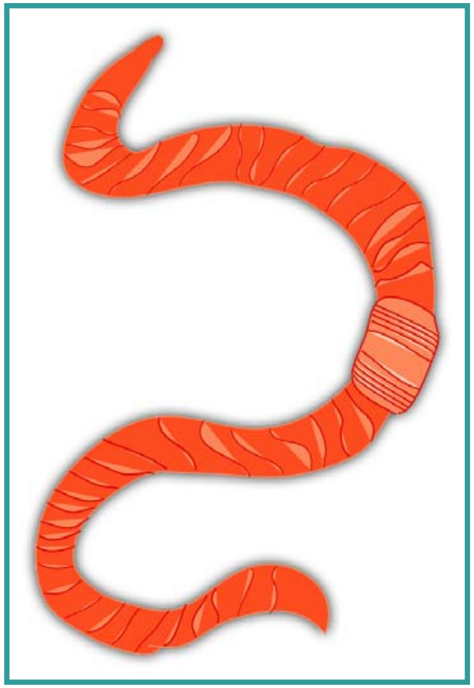


Attack Mitigation Roles for E-Commerce Module


Host IDS for Local Attack Mitigation
Focused Layer 4–7 Analysis
Focused Layer 4–7 Analysis
To Edge Distribution Module
Stateful Packet Filtering
Basic Layer 7 Filtering
Spoof Mitigation
(D)DoS Rate Limiting
Layer 4 Filtering
Focused Layer 4–7 Analysis
Stateful Packet Filtering
Basic 7 Layer Filtering
Host DoS Mitigation
Broad Layer 4–7 Analysis
Wire Speed Access Control

History Hack #5: Code Red

- **Who: 359,104 hosts in 13 hours**
- **What: Internet worm affecting IIS web servers**
- **Where: Everywhere**
- **When: July 19**
- **How: Buffer overflow attack in Microsoft's Index Server (a part of IIS)**
- **$1.2 billion in damages; estimates from Computer Economics (Carlsbad, CA)**



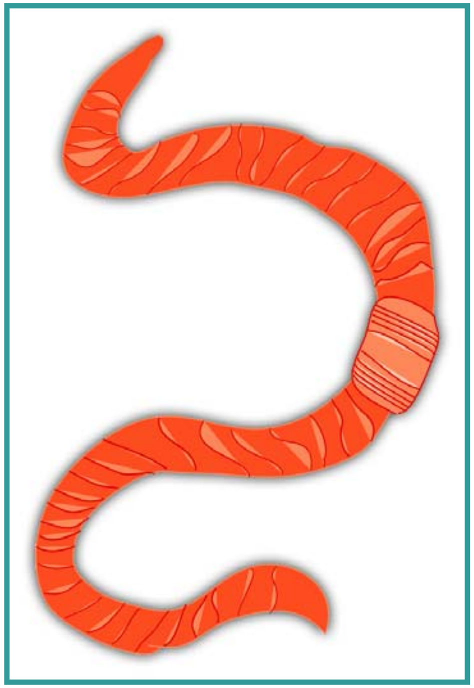
History Hack #5: Code Red

- **Two versions: CRv1 and CRv2—both affect WIN2K and NT**

  CRv1—used random number generator using static seed to generate new IP addresses; static seed meant that limited number of machines would be hit

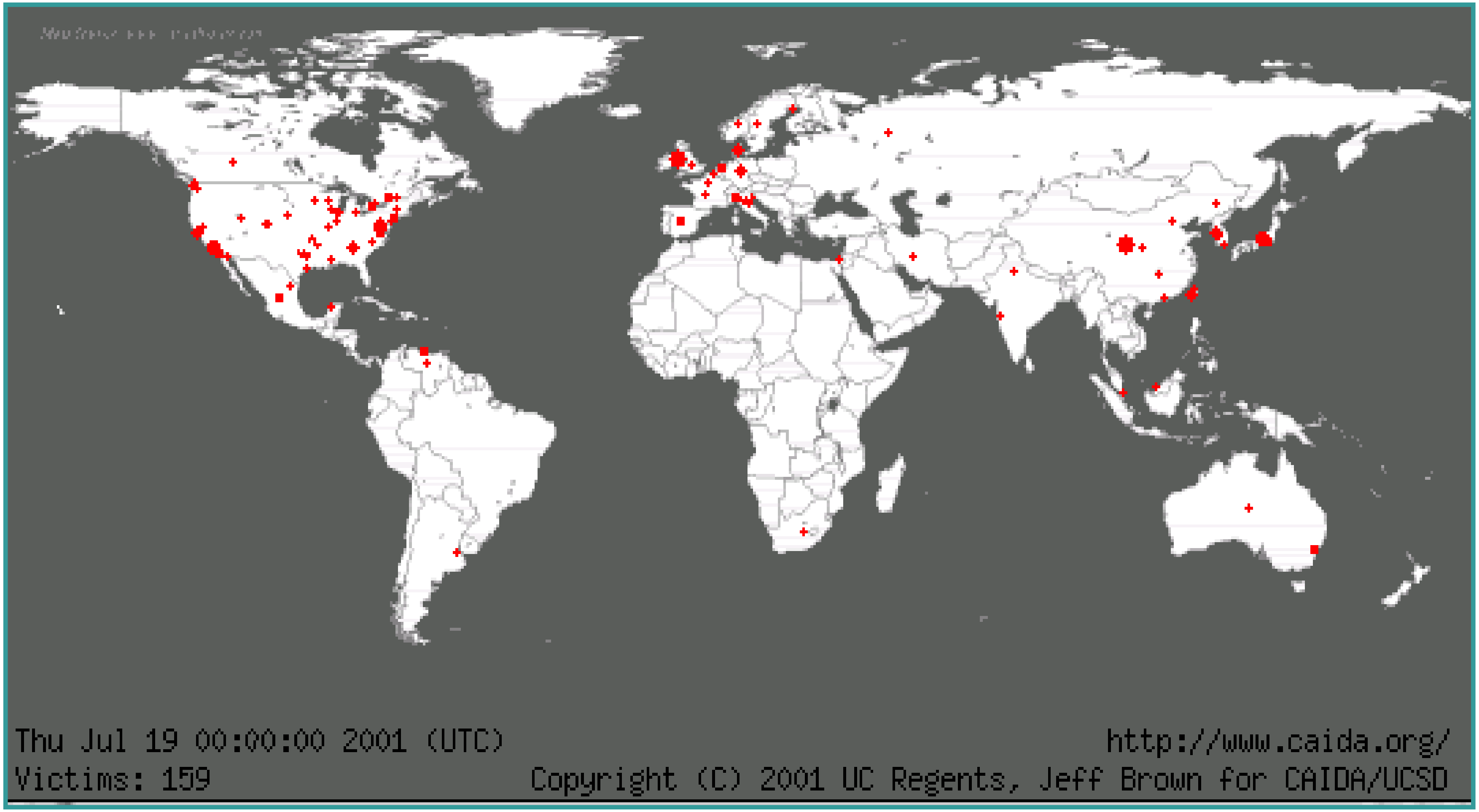
  CRv2—better random number generator; more machines hit; at peak, CRv2 infected 2,000 hosts/minute

- **Code-Red II—affects only WIN2K; more likely to attack systems that shared portion of infected system's IP address; installed minimal back-doors into systems (copies of cmd.exe, new file shares, etc.)**

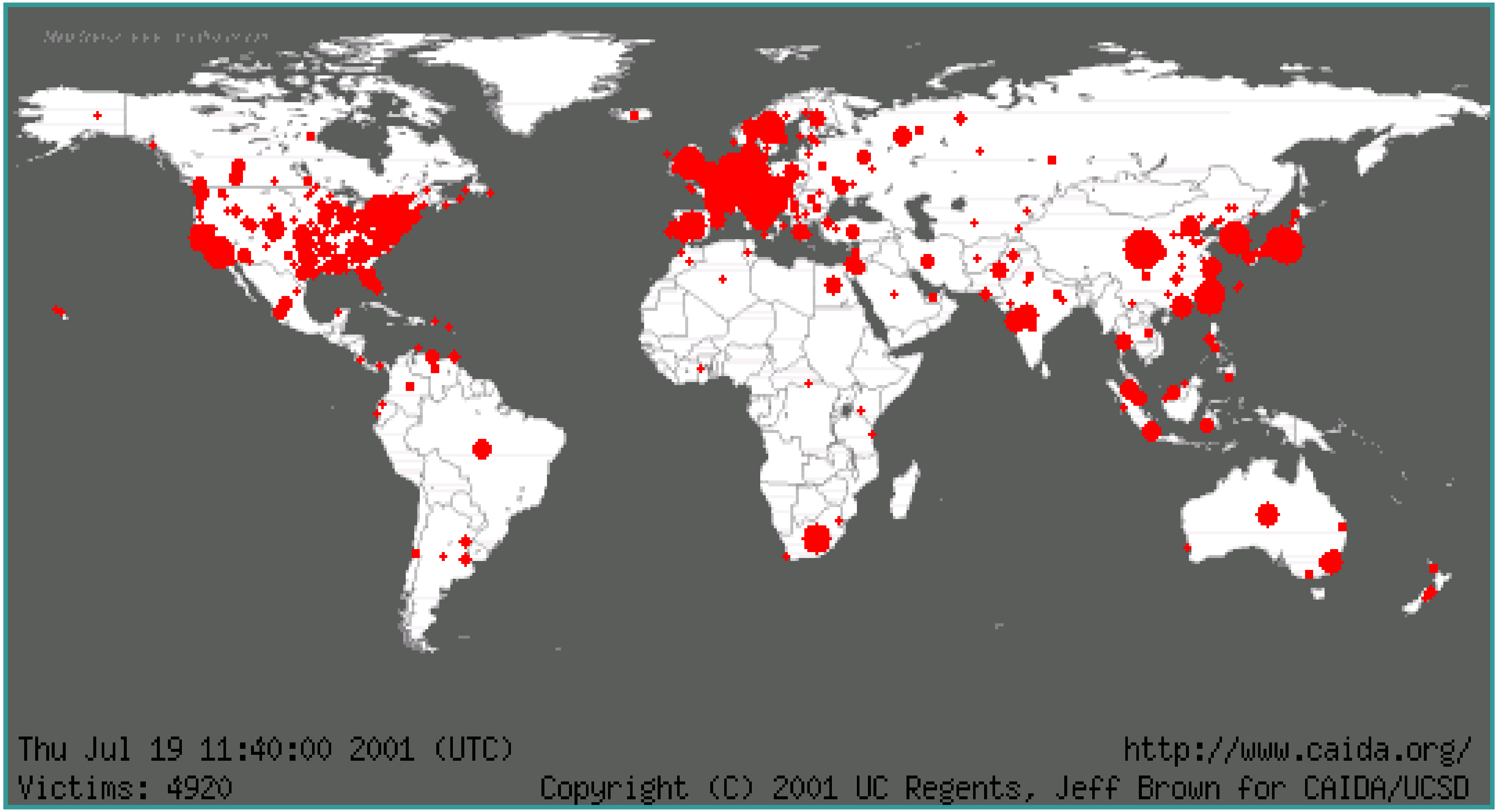


History Hack #5: Code Red

Cisco.com


Thu Jul 19 00:00:00 2001 (UTC)
Victims: 159
http://www.caida.org/
Copyright (C) 2001 UC Regents, Jeff Brown for CAIDA/UCSD

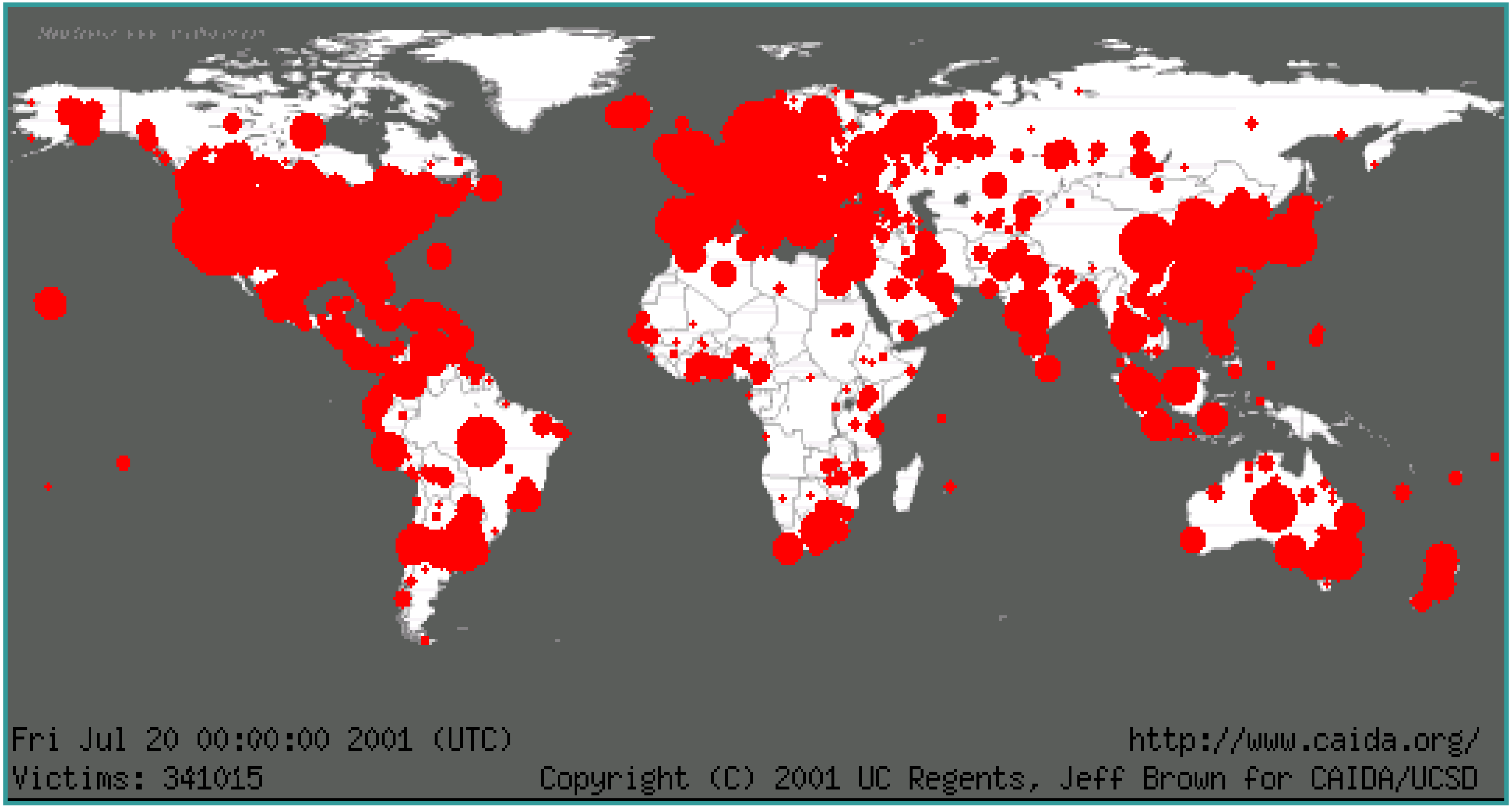
History Hack #5: Code Red



Thu Jul 19 11:40:00 2001 (UTC)
Victims: 4920

http://www.caida.org/
Copyright (C) 2001 UC Regents, Jeff Brown for CAIDA/UCSD

History Hack #5: Code Red



Fri Jul 20 00:00:00 2001 (UTC)

Victims: 341015

http://www.caida.org/

Copyright (C) 2001 UC Regents, Jeff Brown for CAIDA/UCSD

Crunchy on the Outside… Crunchy in the Middle

Implementing Security: Where Do I Start?

- "Network security is a system"
- Develop a security policy based on business requirements and likely threats
- Perform a network vulnerability analysis
- Use a modular approach to designing and deploying a security solution
- Maintain security posture through disciplined system and network administration

Other Sessions of Interest

- Risk and Threat Model —SEC-200
- Security on Ethernet Switches – SEC-307
- Security on Routers—SEC-211
- Understanding and Deploying Intrusion Detection Systems—SEC-204
- Advanced Concepts in Security Threats—SEC-400
- Surviving a DoS Attack—SEC 301

Further Reading

- http://www.cisco.com/warp/public/cc/so/cuso/epso/sqfr/safe_wp.htm

  www.cisco.com/go/safe

  www.cisco.com/go/security

  www.cisco.com/go/evpn

  www.cisco.com/go/securityassociates

  Networking Professionals Connection (forums.cisco.com)

  Improving Security on Cisco Routers

  http://www.cisco.com/warp/public/707/21.html

  Essential IOS Features Every ISP Should Consider

  http://www.cisco.com/warp/public/707/EssentialIOSfeatures_pdf.zip

  Increasing Security on IP Networks (oldie but a goodie)

  http://www.cisco.com/cpress/cc/td/cpress/ccie/ndcs798/nd2016.htm

Cisco.com

Network Security: Design and Attack Mitigation

Session SEC-201

Please Complete Your Evaluation Form

Session SEC-201

Cisco Systems

Empowering the Internet Generation