

IPT Attack Mitigation

Jason Halpern

jhalpern@cisco.com

Cisco Systems



The foundation of any secure voice deployment is a secure underlying infrastructure.

The foundation of any deployment, of *any* application, is a secure underlying infrastructure.

Agenda

- **The Foundation**
 - Layer-2**
 - Layer-3/4**
 - Everything else**
- **Voice**
 - Services**
 - Endpoints**
 - Gateways**
- **Policy Throughout**
- **Designs**

Layer-2 Attack Mitigation

- **Typical attacks:**

**Good 'old
reconnaissance**

**Eavesdropping/Redirecti
on**

Dsniff, Ettercap

(D)DoS

- **Mitigation:**

**MAC limiting, ARP
controls**

**DHCP
intelligence/limiting**

IP address limiting

**L2 filtering, QoS (+trust),
802.1x, *ARPwatch***



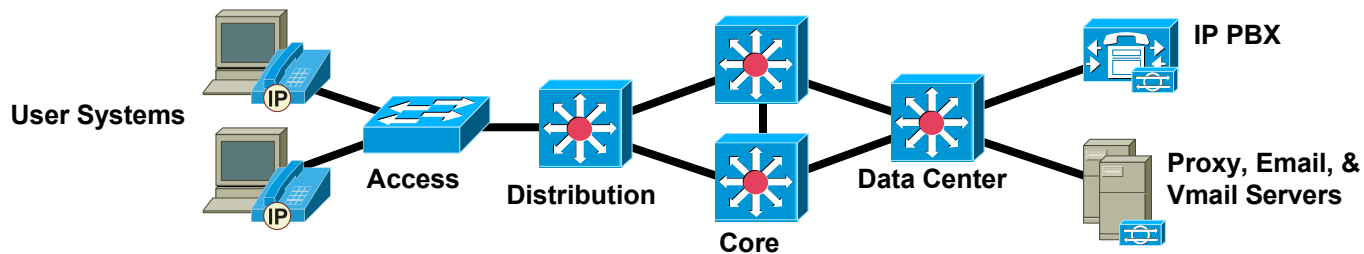
Dug Song, Author of dsniff

www.monkey.org/~dugsong/dsniff

<http://ettercap.sourceforge.net/>

Layer-3/4 Attack Mitigation

- **Typical attacks:**
 - Reconnaissance, crafted packets, (D)DoS Infrastructure, network services (e.g. voice, DHCP, AD)
- **Mitigation:**
 - **Segment DATA from VOICE**
Use the same IP infrastructure



Layer-3/4 Attack Mitigation II

- **Mitigation:**

- **Segment DATA from VOICE (continued)**

- Only allow interaction through firewalled access

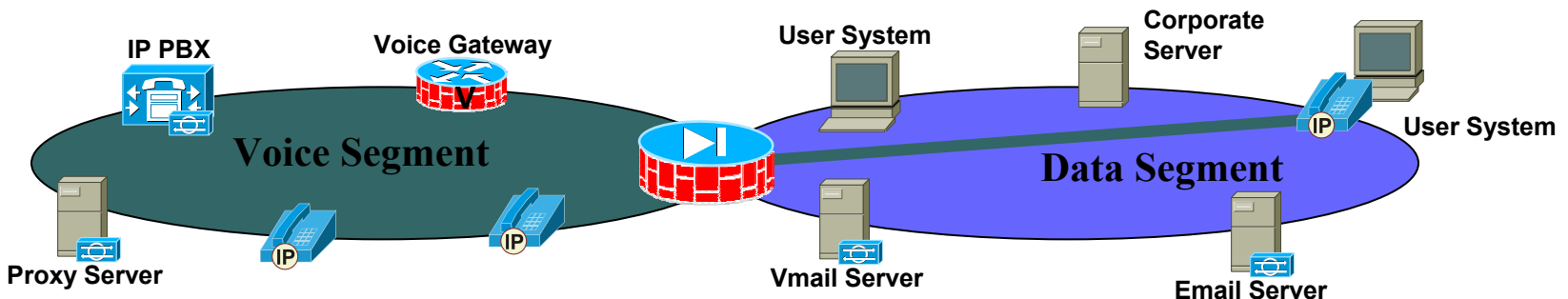
- Mitigates many IP and voice protocol attacks

- Make certain your vendor of choice supports voice protocols

- **Filter (ACL/FW) and rate-limit (QoS) traffic to known profiles**

- Endpoints don't need 100Mb rates to the IP PBX, limit flows on a per-port basis

- **Protect the network stack of any server – PFW/HIDS/HIPS/AV**



Everything Else

- **IDS/IPS**

Provides significant real-time monitoring of voice segments

Consider anomaly detection in addition to traditional IDS

- **QoS**

Traffic classification and policing ensures voice high availability and resilience in the campus (including WLAN) *and* over the WAN.

Everything Else II

- **VPN (IPsec)**

For intra-cluster security over WANs (MGCP, H323)

Provides inter-site security for control and bearer channels for private and public networks

Allows secure connectivity between sites to create a virtual private IP-enable telephony environment

- **SSL/SSH**

Provides secure management of voice infrastructure and endpoints

Consider SSL off-loaders that support centralized authentication databases

Voice Services (All)

- **Turn off unneeded services, harden remaining services**
 - Patch OS, services, & applications
- **Segment services**
 - Registration, configuration, management, database
- **PFW/HIDS/HIPS/AV** – *more than one* for worms, viruses, trojans, and implementation-specific exploits

Voice Services II

- **Change default passwords**
- **Implement strong password policy**
- **Enable SSL/SSH**
- **Consider Out-Of-Band (OOB)**

Toll Fraud

- Many commonly exploited area codes.
- The following list is just a start and may not apply to your organization...

Research the problem for your particular area

Country	Area Code	Blocked CM Pattern
Bahamas	242	9.1242xxxxxxx
Anguilla	264	9.1264xxxxxxx
Antigua/ Barbuda	268	9.1268xxxxxxx
Barbados	246	9.1246xxxxxxx
Bermuda	441	9.1441xxxxxxx
British Virgin Is	284	9.1284xxxxxxx
Cayman Islands	345	9.1345xxxxxxx
Dominica	767	9.1767xxxxxxx
Dominican Repub	809	9.1809xxxxxxx
Grenada	473	9.1473xxxxxxx

Jamaica	876	9.1876xxxxxxx
Montserrat	664	9.1664xxxxxxx
Puerto Rico	787	9.1787xxxxxxx
St. Kitts & Nevis	869	9.1869xxxxxxx
St. Lucia	758	9.1758xxxxxxx
St. Vincent & the Grenadines	784	9.1784xxxxxxx
Toll Charge	900 976	9.1900xxxxxxx 9.1976xxxxxxx
Trinidad & Tobago	868	9.1868xxxxxxx
Turks & Caicos Is	649	9.1649xxxxxxx
U.S. Virgin Islands	340	9.1242xxxxxxx

Voice Services: IP PBX/Call-Process Manager/Call Agent

- **Call forward, transfer, and social engineering exploits (toll fraud)**
 - Constrain country codes**
 - Policy - educate user base**
- **Disable autoregistration & only associate authenticated endpoints with strong credentials**
 - Mitigate rogue devices**

Voice Services: IP PBX/Call-Process Manager/Call Agent II

- **Provide signed images and configurations for endpoints**
 - Mitigates MITM attacks against voice endpoints**
- **Password policy protects user speed dials/call-forwarding**
 - Encryption hides data over other channels (DTMF)**

Voice Services: Voicemail

- **Same voice services best practices (slide 7)**
- **Call forward exploits**
- **Password policy protects against unauthorized voicemail access (stealing messages, changing greeting) and call-forward exploits**
- **Consider SSL for management interface**

Endpoints

- **IP phones**

Harden - configuration, data port, packet handling (+QoS)

Enforce data/voice segmentation (802.1q)

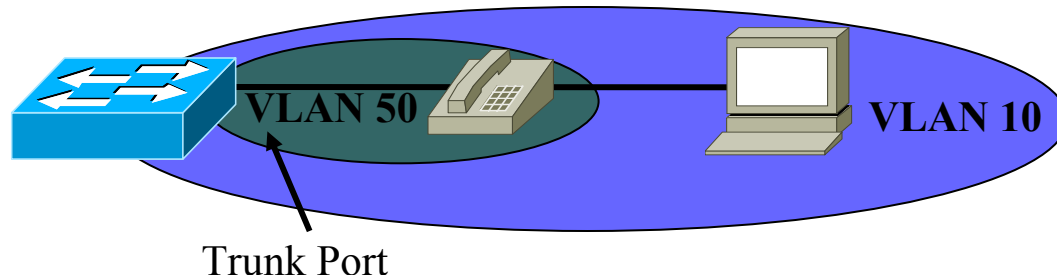
Authentication, encryption, integrity

Consider a secure control channel mode to IP PBX

e.g. TLS over your signaling/control protocol of choice, mitigates rogue IP PBXs

Consider a secure bearer channel mode to other endpoints (gateways, phones, IP PBXs, etc.)

e.g. SRTP, mitigates eavesdropping



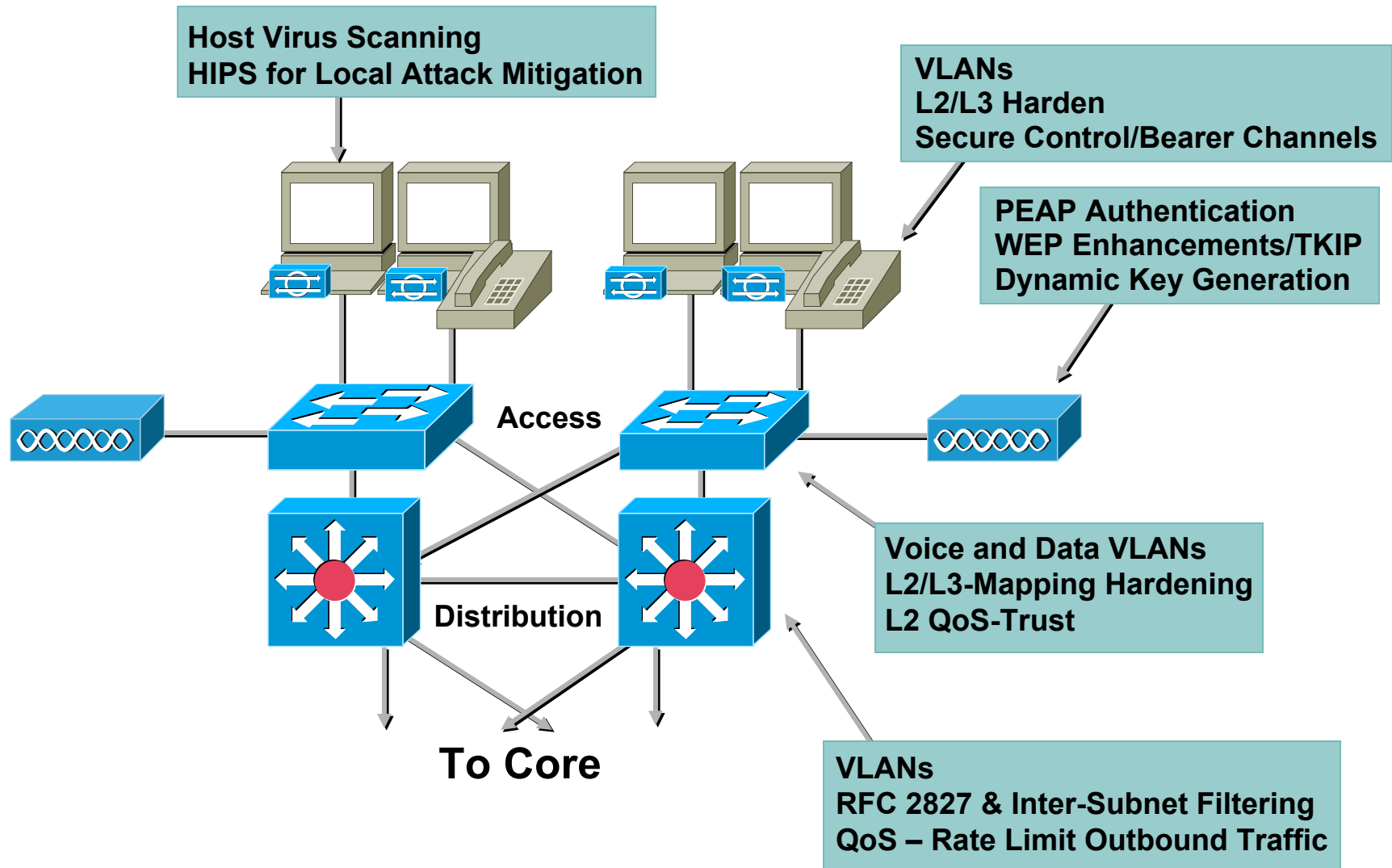
- **Softphones or other applications**

Reside in data segments, not much to do from configuration aspect

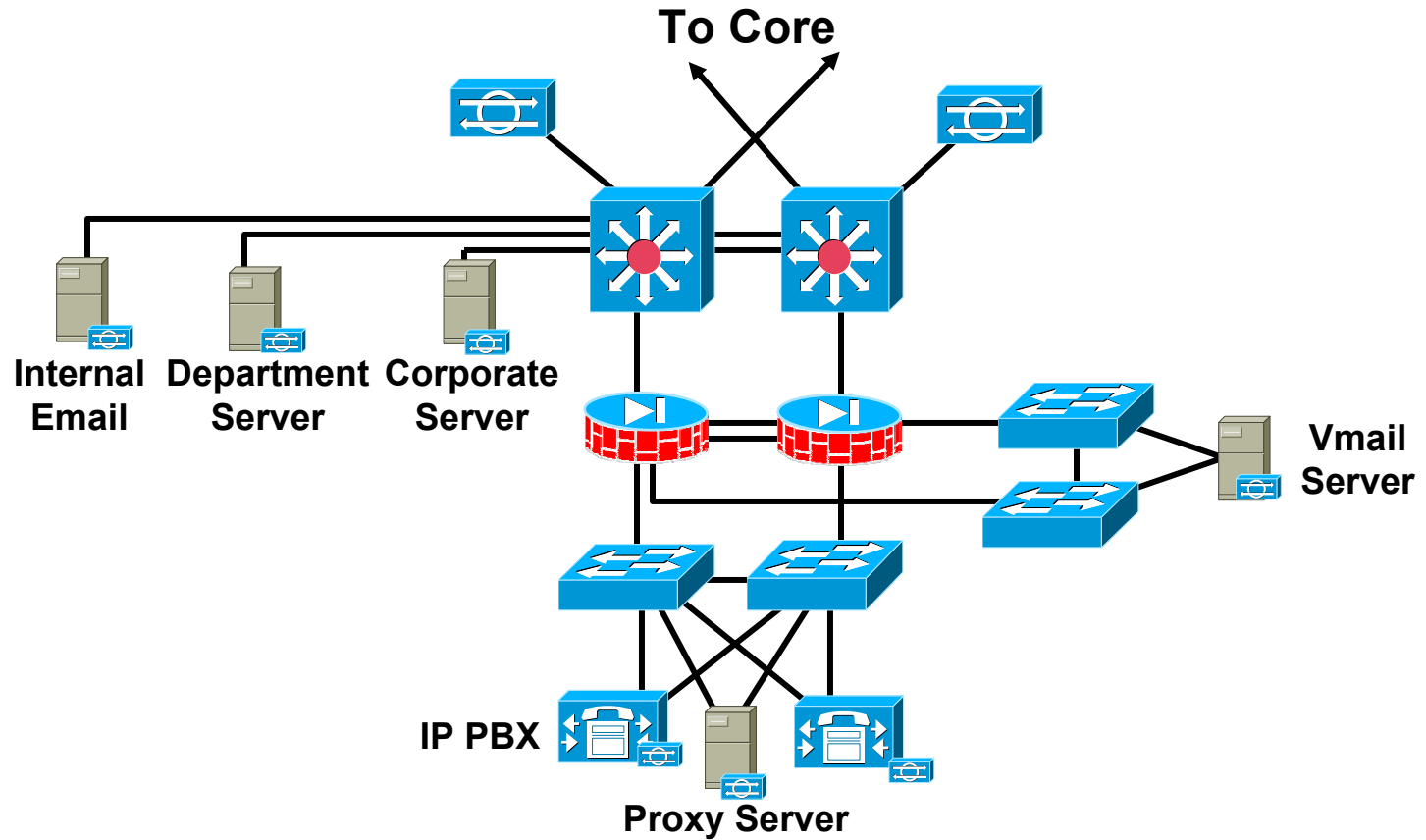
Secure the endpoint (PFW/HIDS/HIPS/AV) else realize the consequences

Enforce application-layer strong password policy

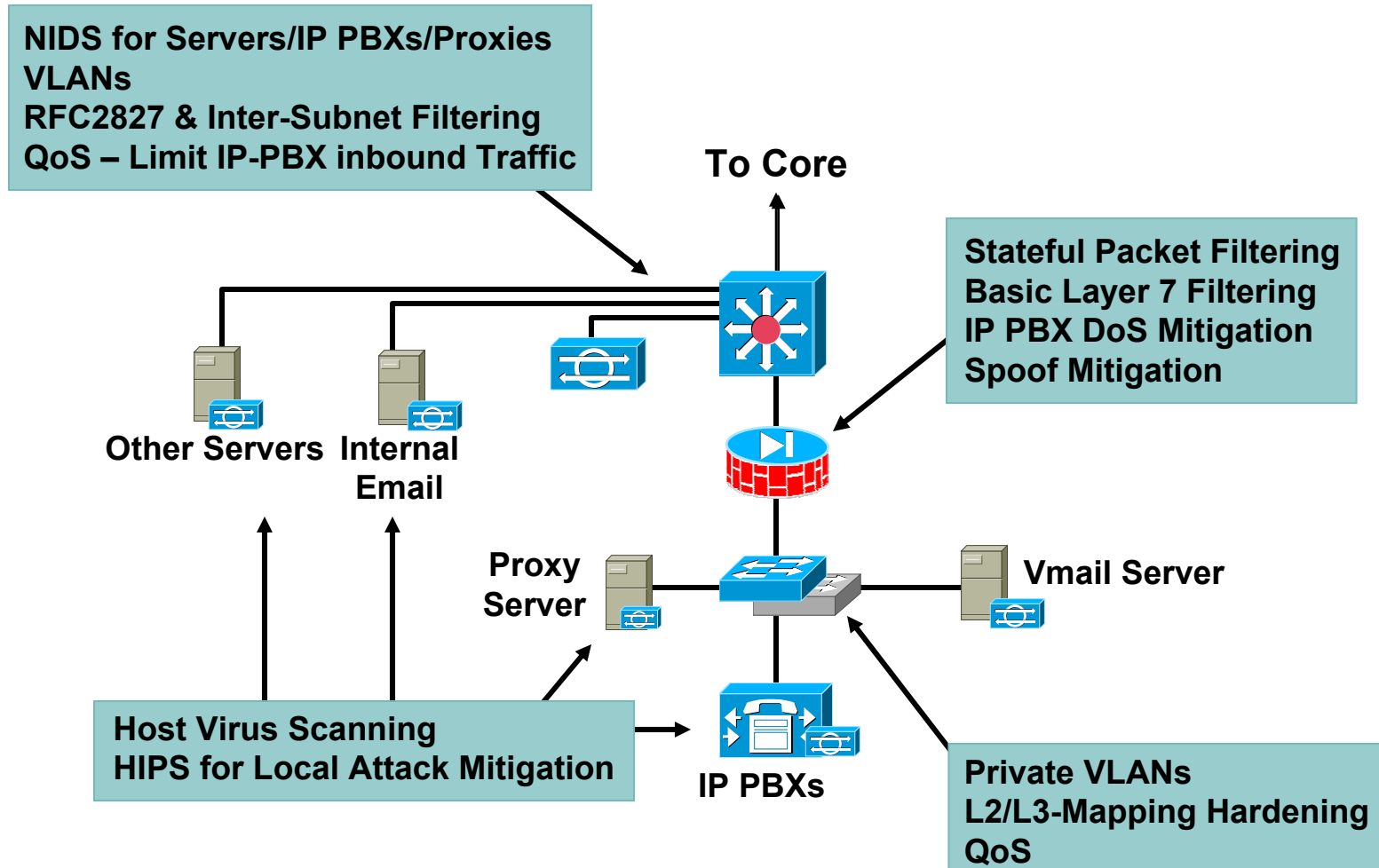
Attack Mitigation Roles for Building and Distribution Segments



Data Center Model



Attack Mitigation Roles for Data Center



Walkaways

- **Job #1: Physical security**
- **Job #2: A secure underlying infrastructure**
- **Job #3: Policy enforcement**
- **Realize: It's IP, it's only a matter of time for the good and bad**

- ***ET can phone home***

Questions?

- **Consider the SAFE IPT white paper**
www.cisco.com/go/safe
(V2 update soon)