

CISCO SYSTEMS



Network Security

Fattore abilitante per le nuove tecnologie

Marco Misitano
Consulting Systems Engineer, Security
Cisco Systems Italy
misitano@cisco.com

Agenda

- **Securing a Wireless Network**
- **Securing a VoIP Network**
- **Infrastructure Security**

SAFE Wireless LAN Security Design

Design Objectives

- **Security and attack mitigation based on policy**
- **Authentication and authorization of wireless networks to wired network resources**
- **Wireless data confidentiality**
- **Access-point (AP) management**
- **Authentication of users to network resources**
- **Options for high availability (large enterprise only)**

SAFE WLAN Axioms

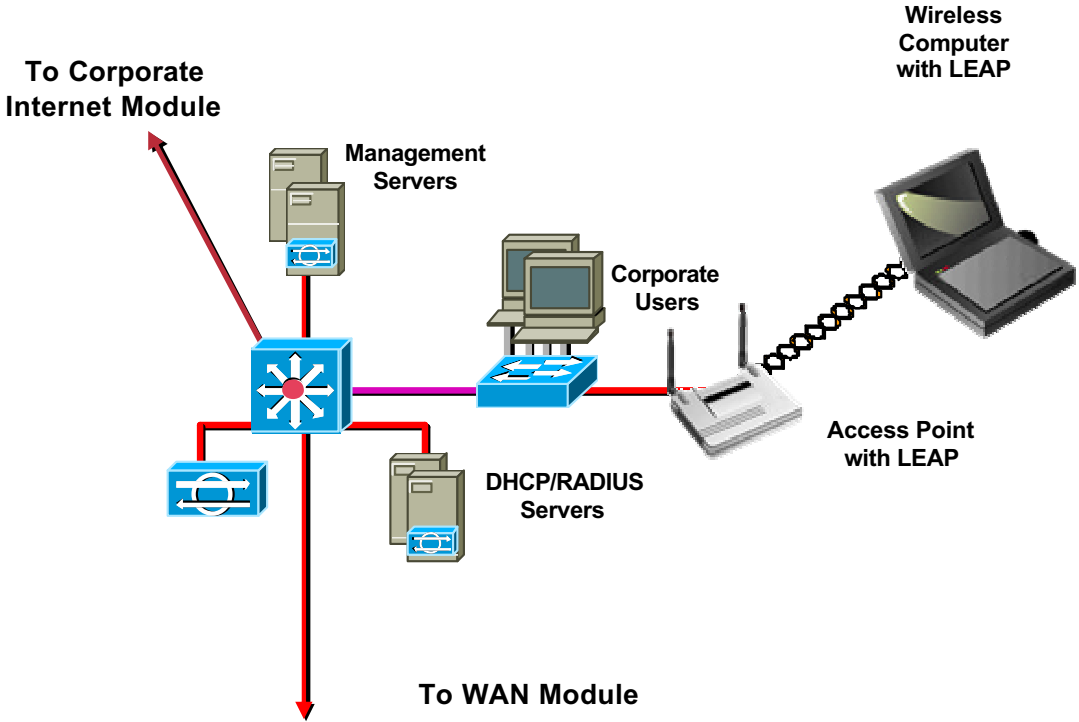
- **Wireless networks are targets**
- **Wireless networks are weapons**
- **802.11b is insecure**
- **Security extensions are required**
- **WLAN user differentiation challenges**

LEAP, IPsec, Static WEP

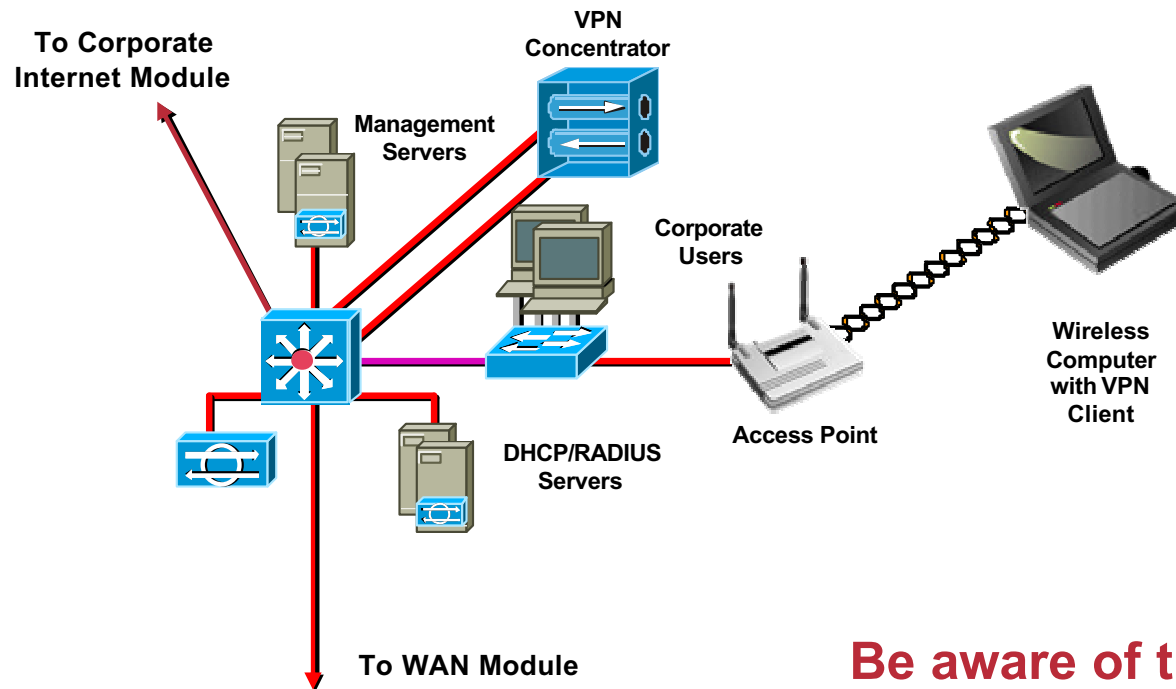
Cisco.com

	LEAP	IPsec	WEP
Key length (bit)	128	168	128
Encryption algorithm	RC4	3DES	RC4
Packet Integrity	CRC32/MIC	MD5-HMAC/SHA-HMAC	CRC32/MIC
Device Authentication	no	Pre-shared secret/certificates	no
User authentication	username/password	username/password, OTP	no
Transparent to user	yes	no	yes
Additional hardware	Auth server	Auth Server, VPN gateway	no
Protocol support	any	IP Unicast	any
Open standard	no	yes	yes

Simple network LEAP WLAN Design

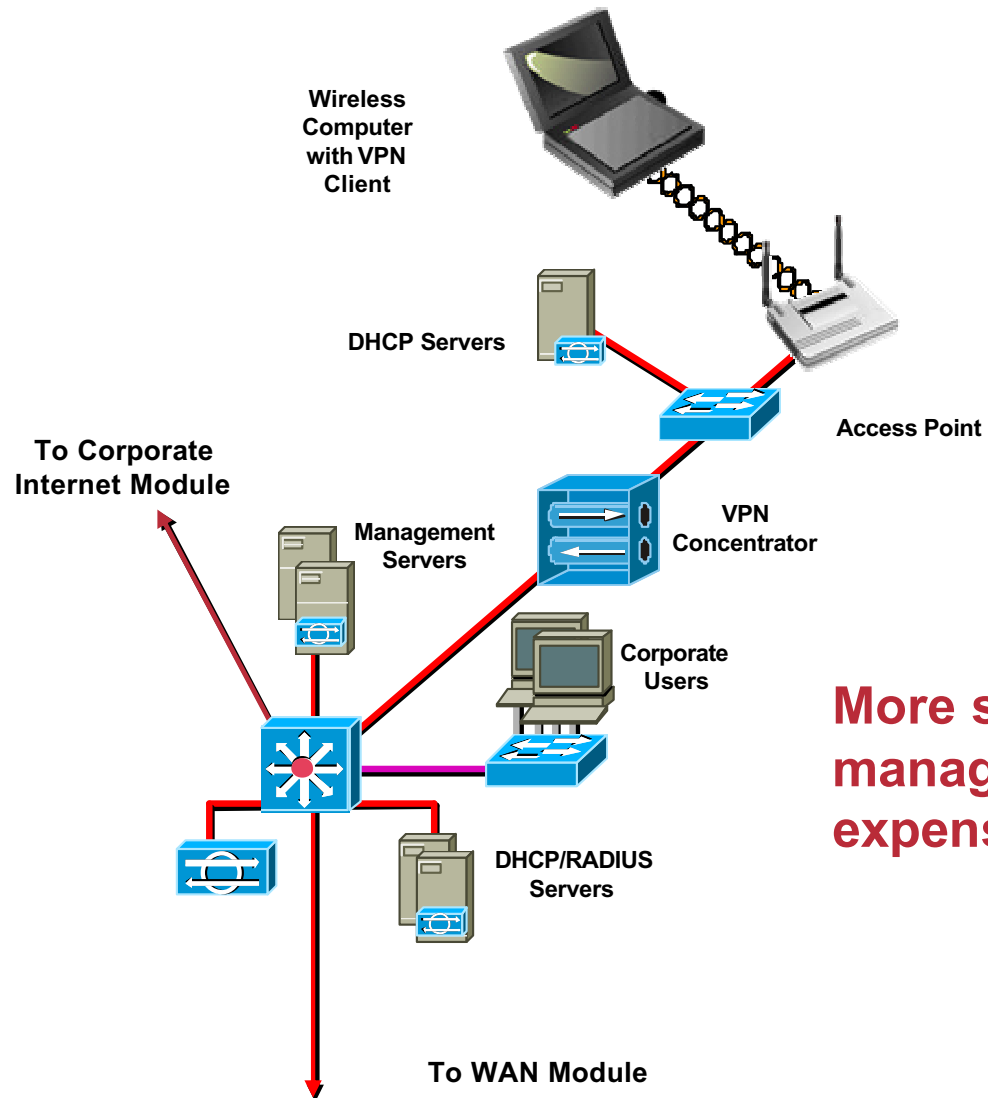


Simple network VPN WLAN Design



Be aware of the reliance on VLANs in this design!

Simple network VPN WLAN Design Option



More secure, but harder to manage and more expensive.

SAFE WLAN Gotchas

- **AP management**
- **Physical/VLAN Issues**
- **VPN 3000 throughput**
- **Back-end service resiliency (DHCP/DNS/RADIUS)**
- **AP Filters and L3 switch ACLs**

SAFE: IP Telephony Security in Depth

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

The State of IP Telephony II

- **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

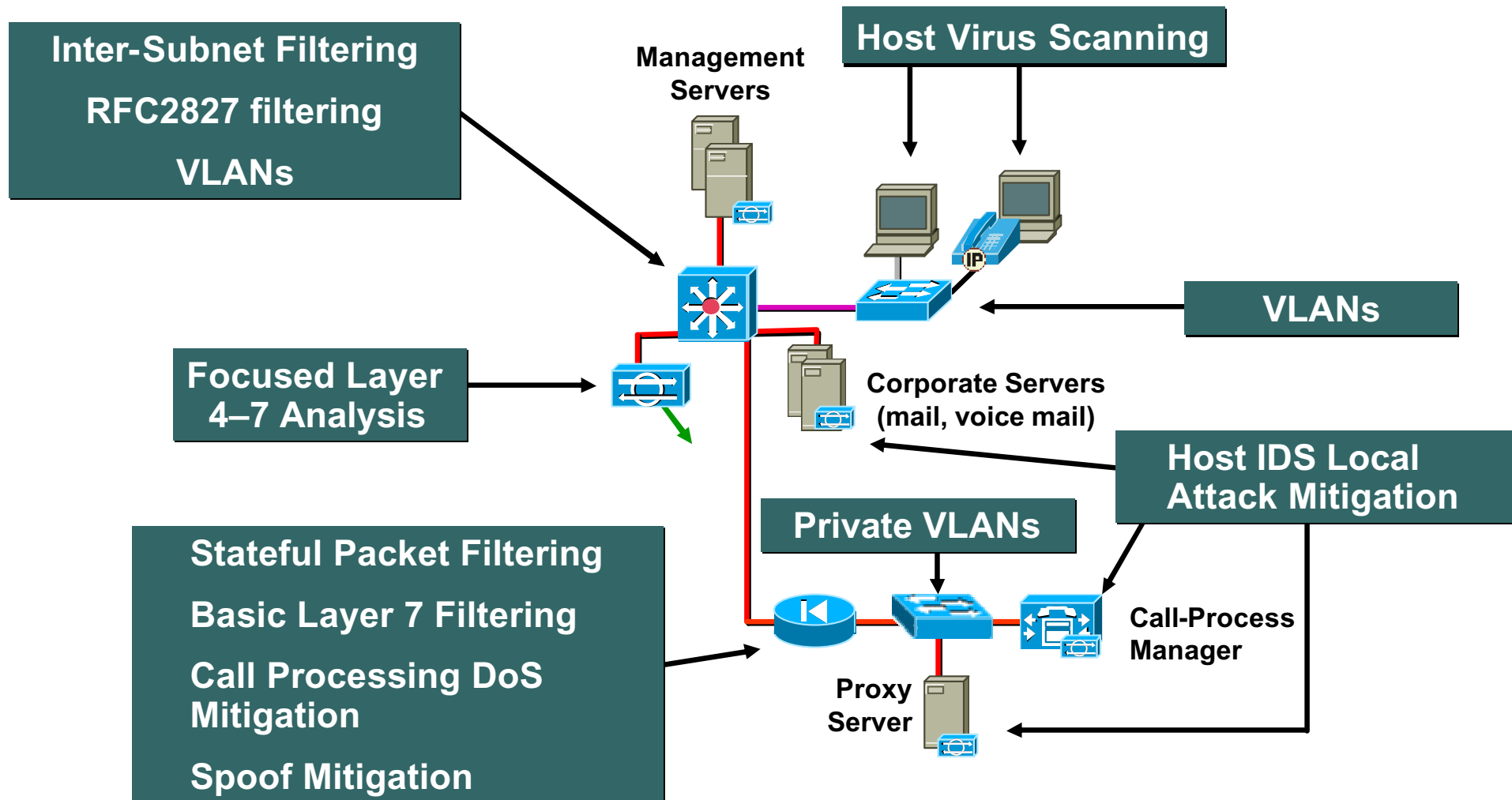
Design Objectives

- **Security and attack mitigation based on policy**
- **Quality of Service**
- **Reliability, performance, and scalability**
- **Authentication of users/devices to network resources**
- **Secure management**
- **Options for high availability in large environments**

SAFE IP Telephony Axioms

- **Voice networks are targets**
- **Data and voice segmentation is key**
- **Telephony devices don't support confidentiality**
- **IP phones provide access to the data-voice segments**
- **Pc-based IP phones require open access**
- **Pc-based IP phones are especially susceptible to attacks**
- **Controlling the voice-to-data segment interaction is key**
- **Establishing identity is key**
- **Rogue devices pose serious threats**
- **Secure and monitor all voice servers and segments**

Simple Standalone Campus Module

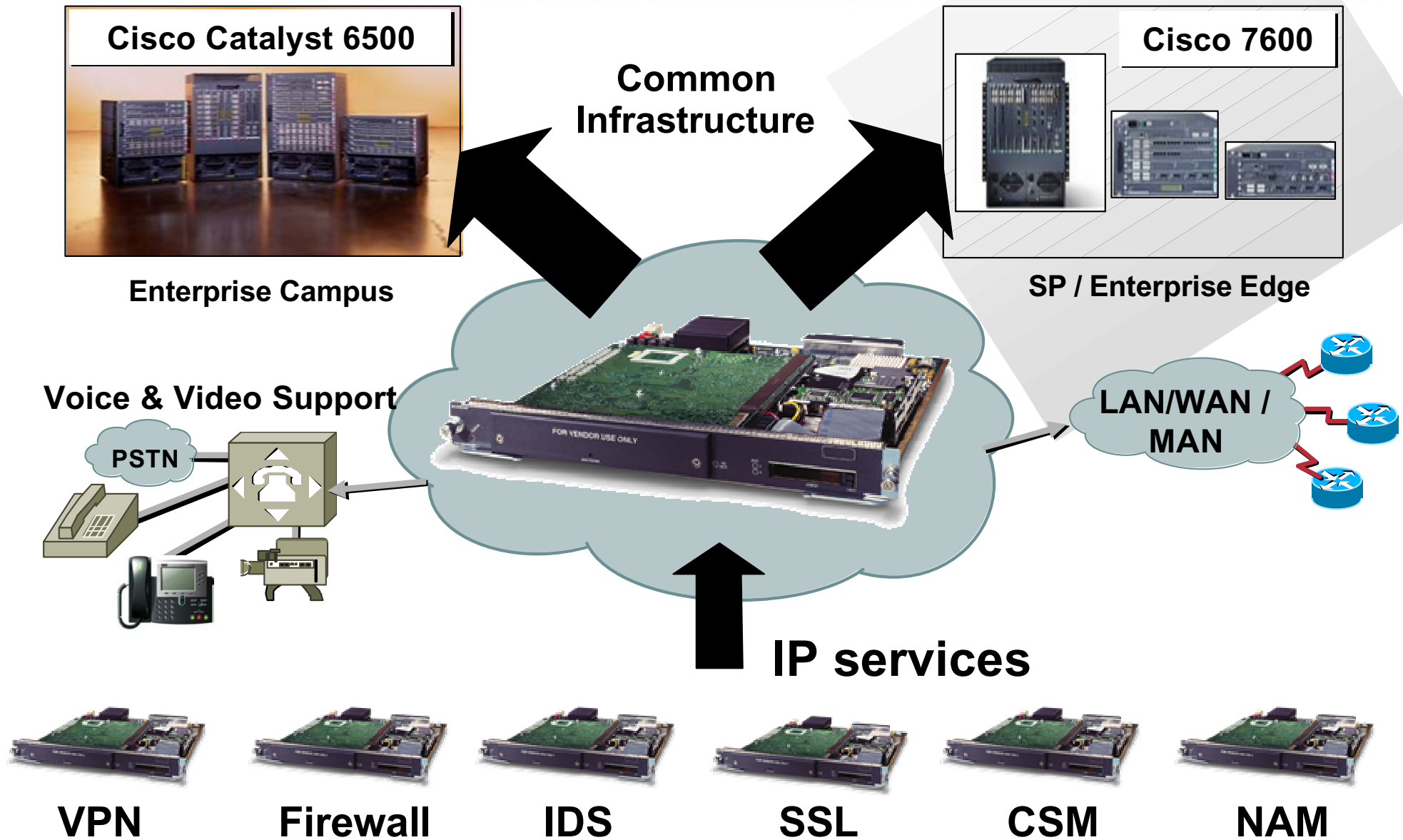


Security and IP Telephony Integration Issues

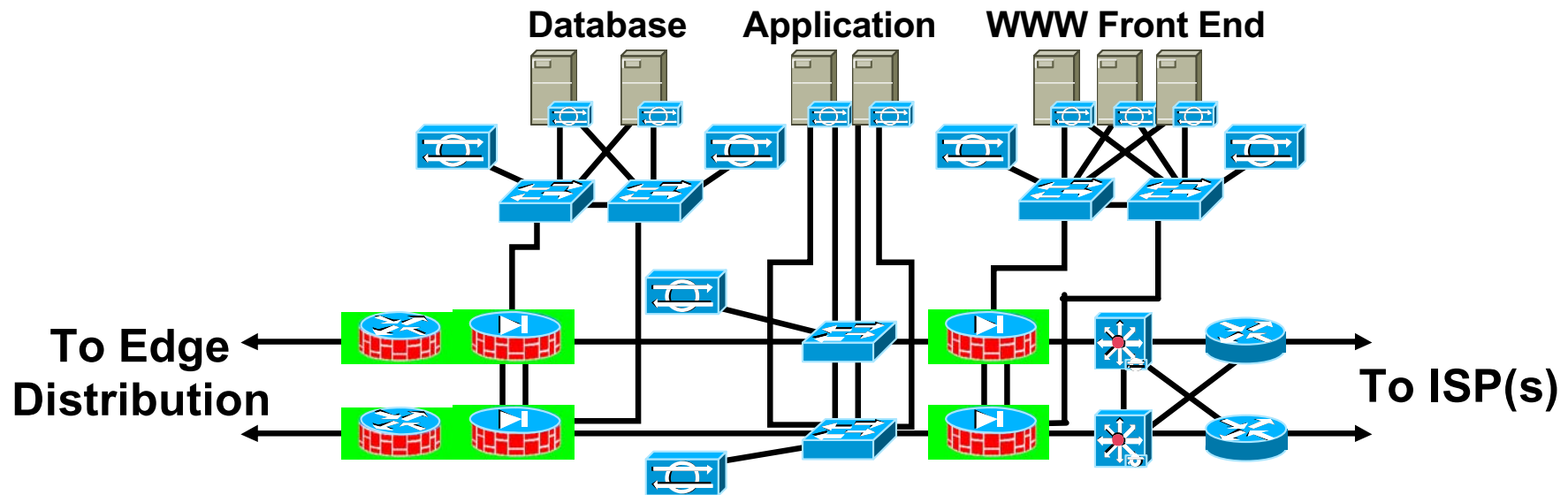
- **The standards**
- **Server secure management**
- **Port security and trunking**
- **MAC-based device authentication**
- **PC-based IP phones**
- **Voice/VPN/QoS**

Getting security **IN** the fabric

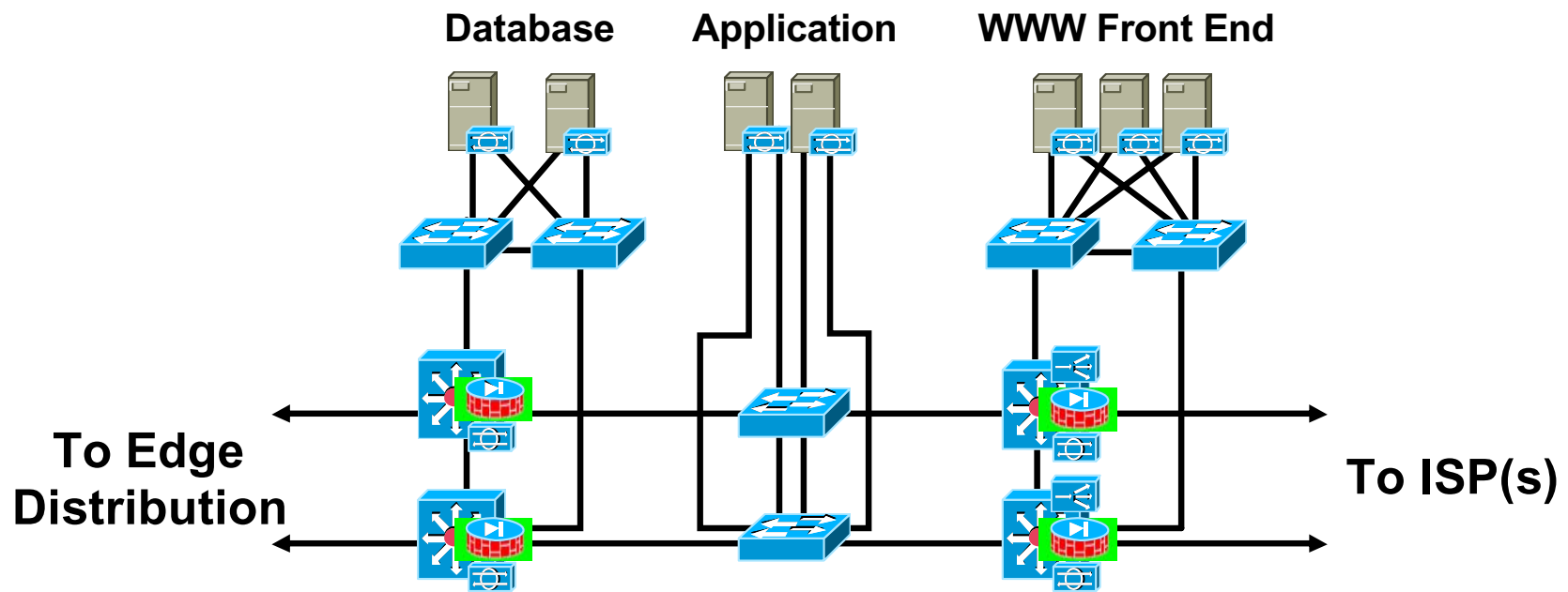
Cisco Catalyst 6500 and Cisco 7600



E-Commerce (BEFORE)



E-Commerce (AFTER)





Cisco.com

Conclusions

- **Technology gets complex**
- **New Technologies especially**
- **There are Security Issues**
- **Don't minimize, be aware.**
- **There are SAFE solutions**
- ***<http://cisco.com/go/safe>***

CISCO SYSTEMS



EMPOWERING THE
INTERNET GENERATION