

Top VoIP Security Challenges



**Richard De Soto Director,
IP Telephony Solutions
Extreme Networks**

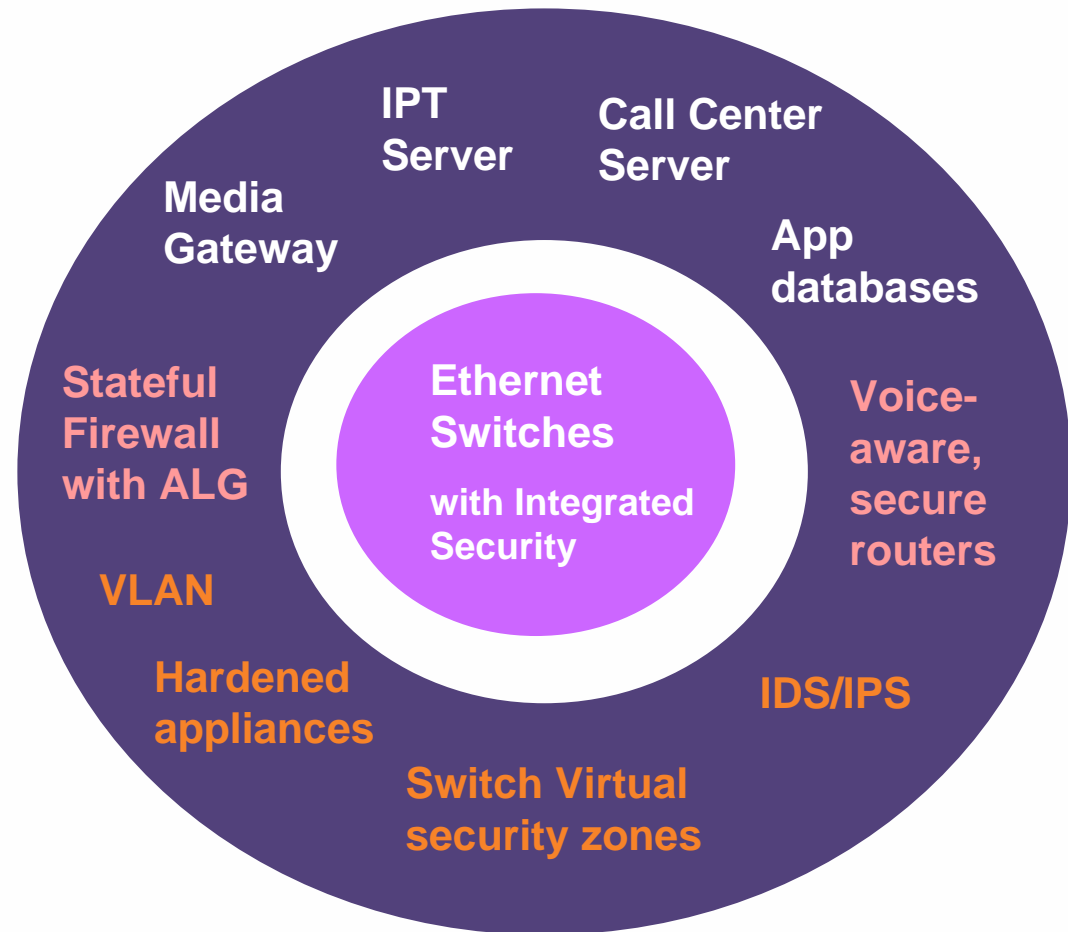
rdesoto@extremenetworks.com



Open Converged Networks

What is needed on the IP infrastructure for VoIP Security?

- ▶ VoIP security must be part of your overall security policy- it is an application on your IP network
- ▶ The more secure your network is, the harder it will be for attacker to eavesdrop, cause a DoS attack or break into an OS or VoIP app
- ▶ Involve your security group
- ▶ An IP Telephony system is not just an IP PBX- it is everything to make it work
- ▶ What provides QoS, network security, availability, routes calls on the LAN, device connectivity?...
Ethernet switches



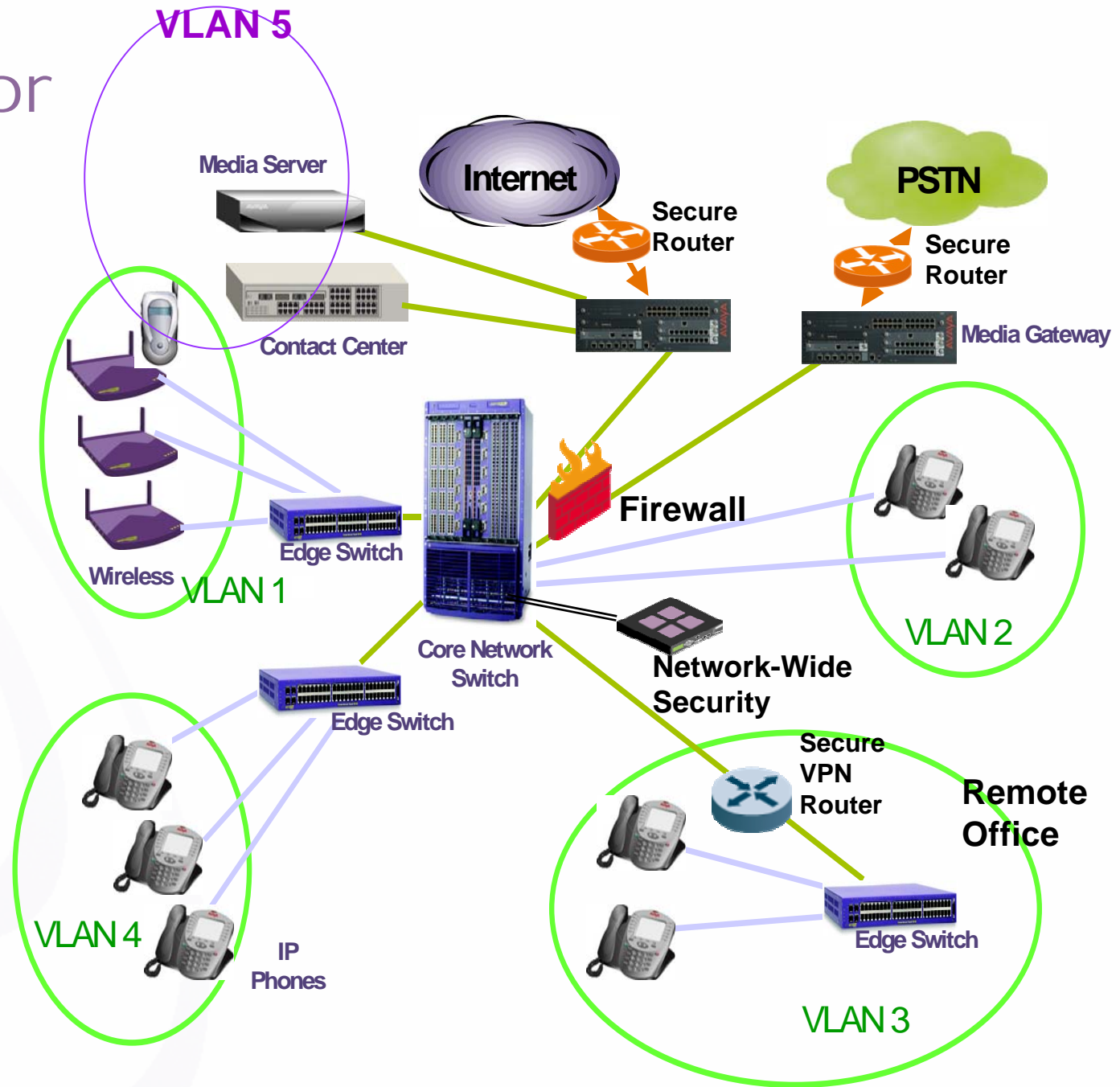
Top Threats to VoIP

The same as for data

- Denial of Service attacks
- Trojans, viruses, worms
- DHCP attacks (Eavesdroppers)
- Wireless VoIP rogue attacks
- Mobile workers plugging back into the network
- New VoIP threats: Voice spam, SPIT

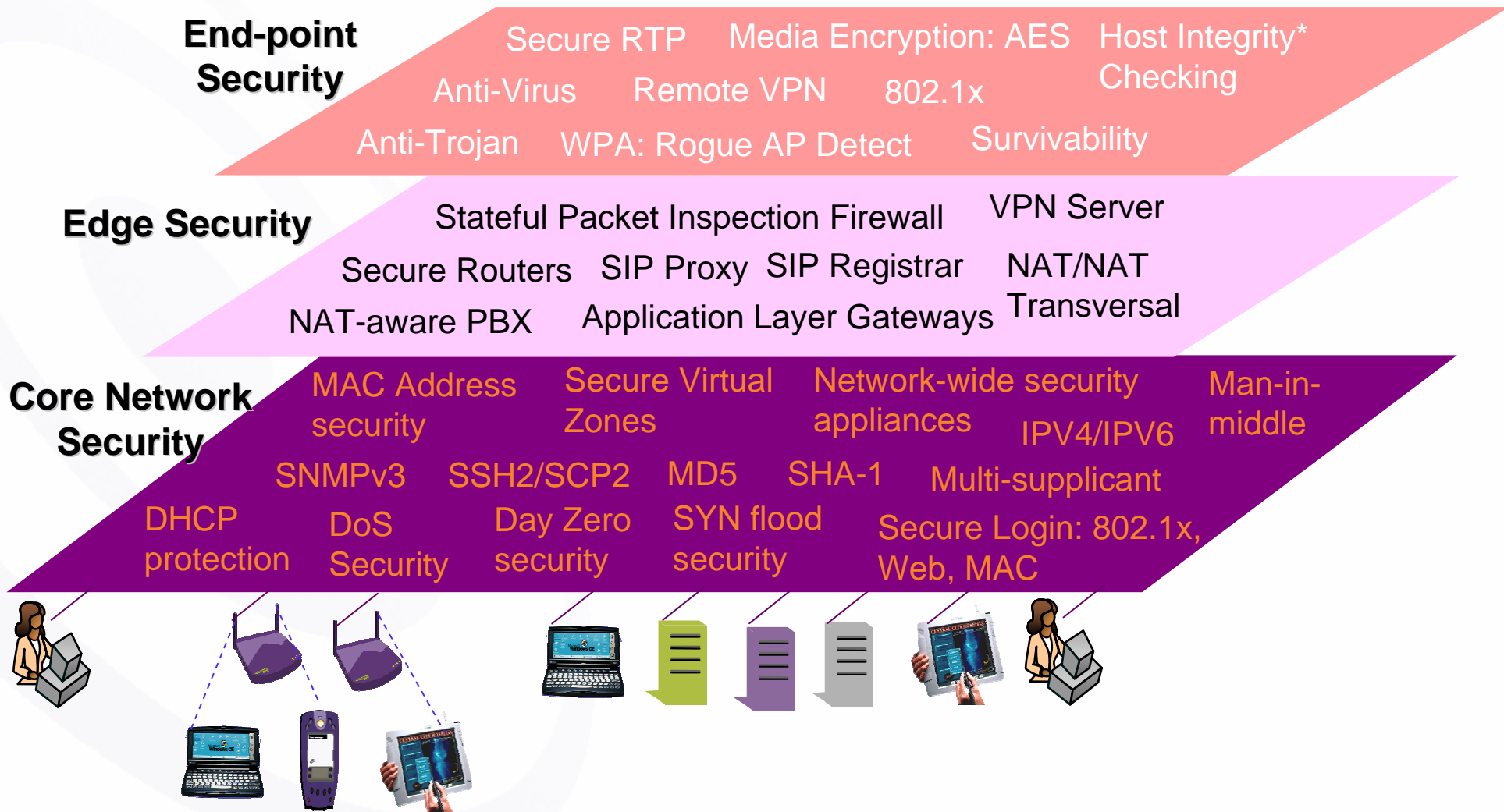
Safe Blueprint for VoIP

- Core Security on Ethernet Switches
- VLANs- separate security “islands” on IP networks
- Secure routers
- Voice-Aware Stateful Firewalls
- New Network-wide security
- IDS/IPS at critical points
- Hardened DHCP/DNS/RADIUS appliances
- Secure Login



VoIP Security must be in Layers

From the network infrastructure all the way to the user device

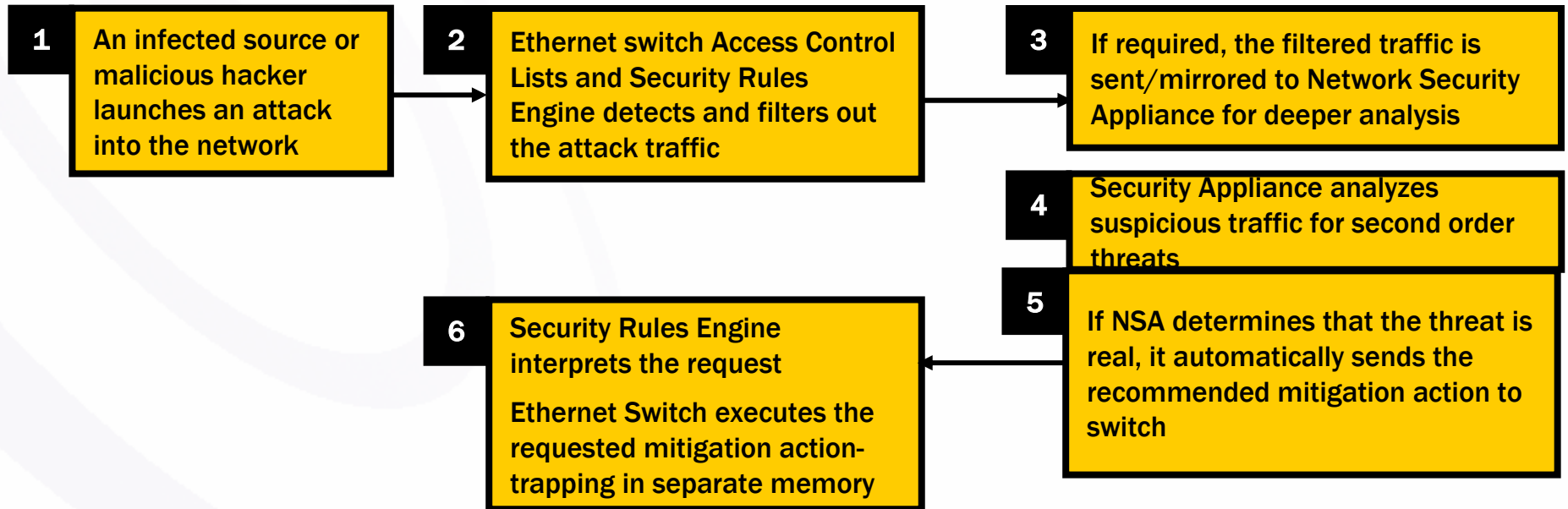
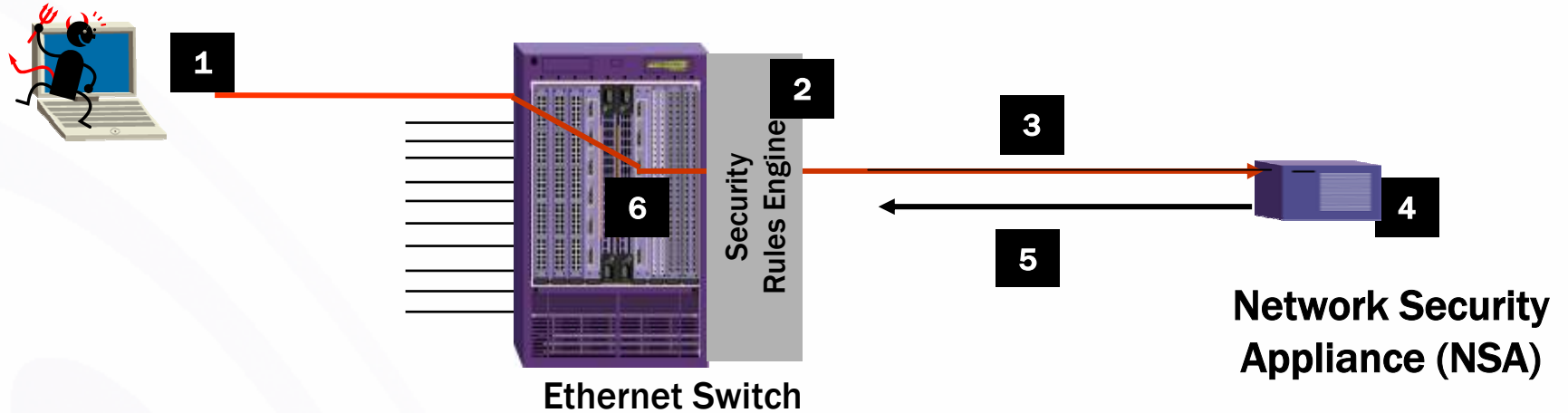


Ethernet Switch VoIP Security Methods

Ensure Ethernet switches have integrated protection against:

- **Syn Floods**
- **Denial of Service attacks-** detect an unusually large number of packets in the input queue- ACLs stop these packets from going anywhere. (IPDA-LPM, CPU DoS protection, programmable ACL's)
- **Man-in-the-middle attacks-** SNMPV3, SSH2, SCP
- **Rogue Access-** MAC lock-down, WAP for wireless
- **IP Address Security-** Spoofed address protection, DHCP enforcement via "Disable ARP", DHCP option 82, DHCP authentication, DHCP snooping
- **IP Telephony Security-** VLAN separation of voice/data: MAC-based VLANs (VoIP phone assigned to voice VLAN), PBX, Call Centers, Phones on VLANs
- **Secure Login-** MAC-based, Web-based, 802.1x
- **Virtual Security Zones on Switches-** to apply "firewalls" between zones (between acctg and sales, etc.)

Network-Wide Protection against Major Threats: *Worm Storms, Day Zero Attacks*



Secure Login to prevent Unauthorized Access

▶ **Unauthorized MAC access**

- **MAC lockdown-** enables switch blocking access to any Ethernet port when the MAC address of a station attempting to access the port is different from the configured MAC address
 - used to “lock down” a device like an IP telephone, an AP or a server to a specific port
- **Limit Dynamic MAC addresses-** for flexibility

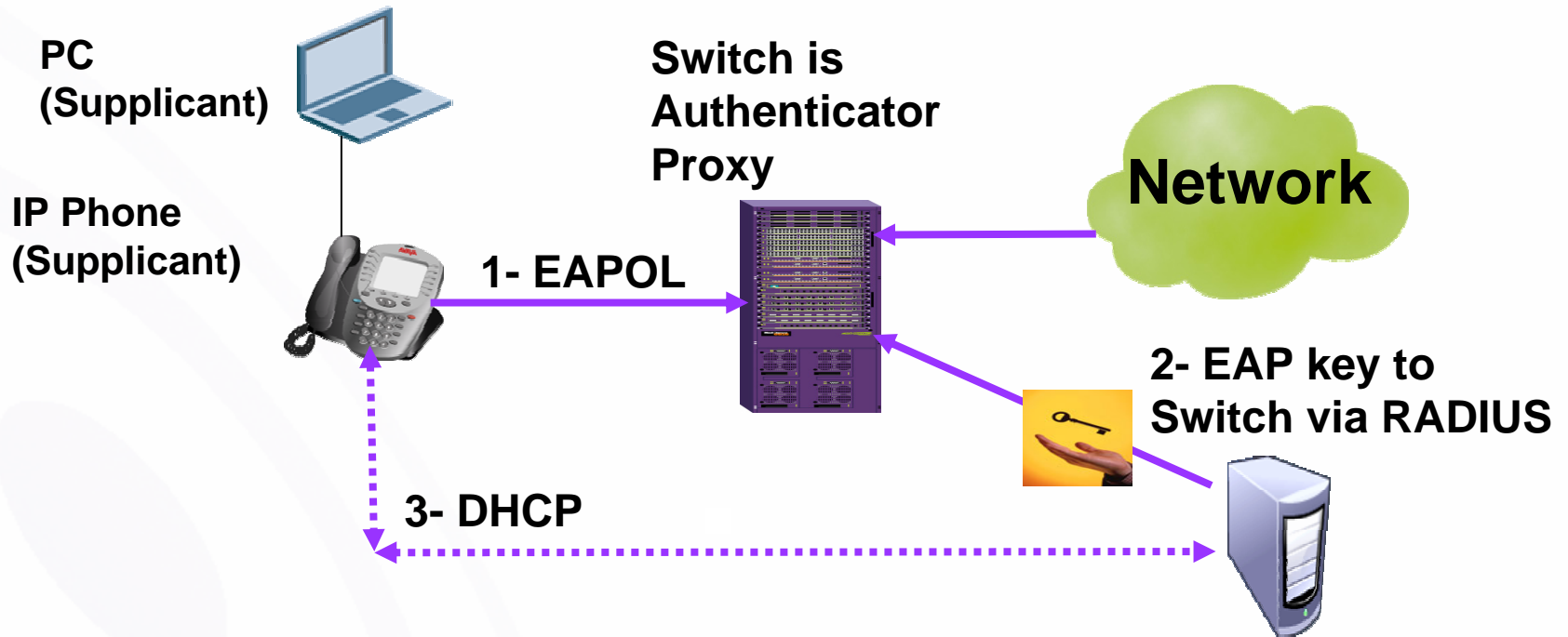
▶ **Web login-** for clients without 802.1x

- No client required

▶ **802.1x login**

802.1X Authentication for Voice

Standard for wireless and wired security



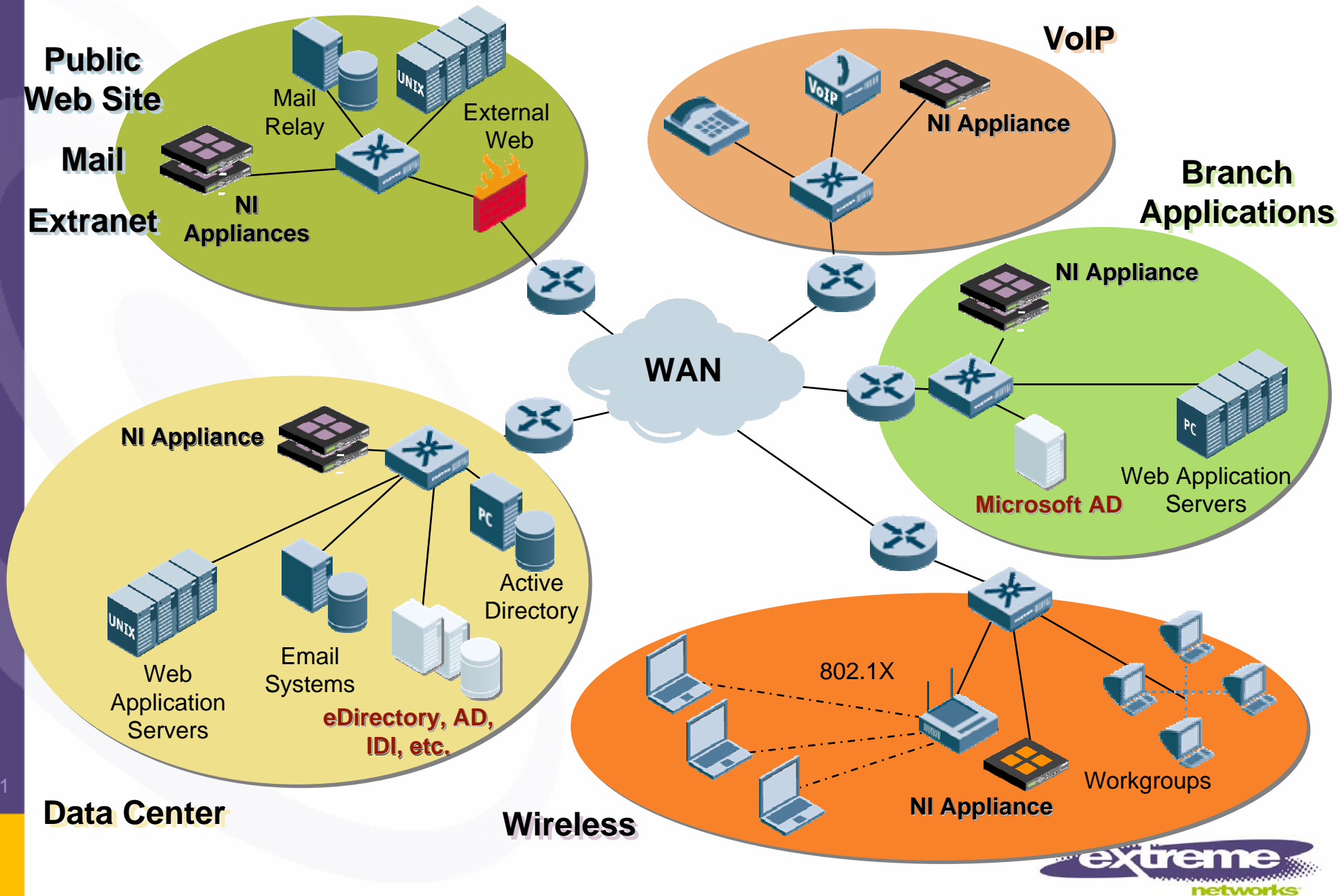
Controls the admission of user packets into a network by giving addresses only to users that are properly authenticated

- ▶ Supplicant (client) generates EAPOL authentication request to Authenticator Switch
- ▶ Switch interacts with RADIUS server for end user authentication- EAP key passed to Switch. Switch provides controlled access to the port the Supplicant is connected
- ▶ DHCP activated
- ▶ Multiple supplicants are supported

The next weak link- DHCP

- ▶ DHCP used to assign IP addresses to IP phones
- ▶ IPT servers, Ethernet switches may use hardened OS but how is DHCP usually deployed?...Windows servers
- ▶ Solutions in Ethernet switches:
 - DHCP option 82- uses switch as proxy for inbound DHCP requests and forwards screened input onto real DHCP server
 - Disable ARP learning- only can learn IP address via DHCP
 - Source IP lockdown- allows traffic only from valid DHCP address
 - Trusted DHCP support- set of ports for valid DHCP server responses
 - Gratuitous ARP protection- prevents Man-in-the-Middle attacks from attacker pretending to be a router
 - DHCP snooping- allows switch to protect the network from rogue DHCP servers
 - DHCP Secured ARP- prevents dynamic IP hijacking
 - ❖ Builds table of valid IP/MAC bindings via DHCP snooping
 - ❖ Compares ARP packets with table

Hardened Network Identity Appliances (with DHCP/DNS/RADIUS) Integrate Into Existing Network



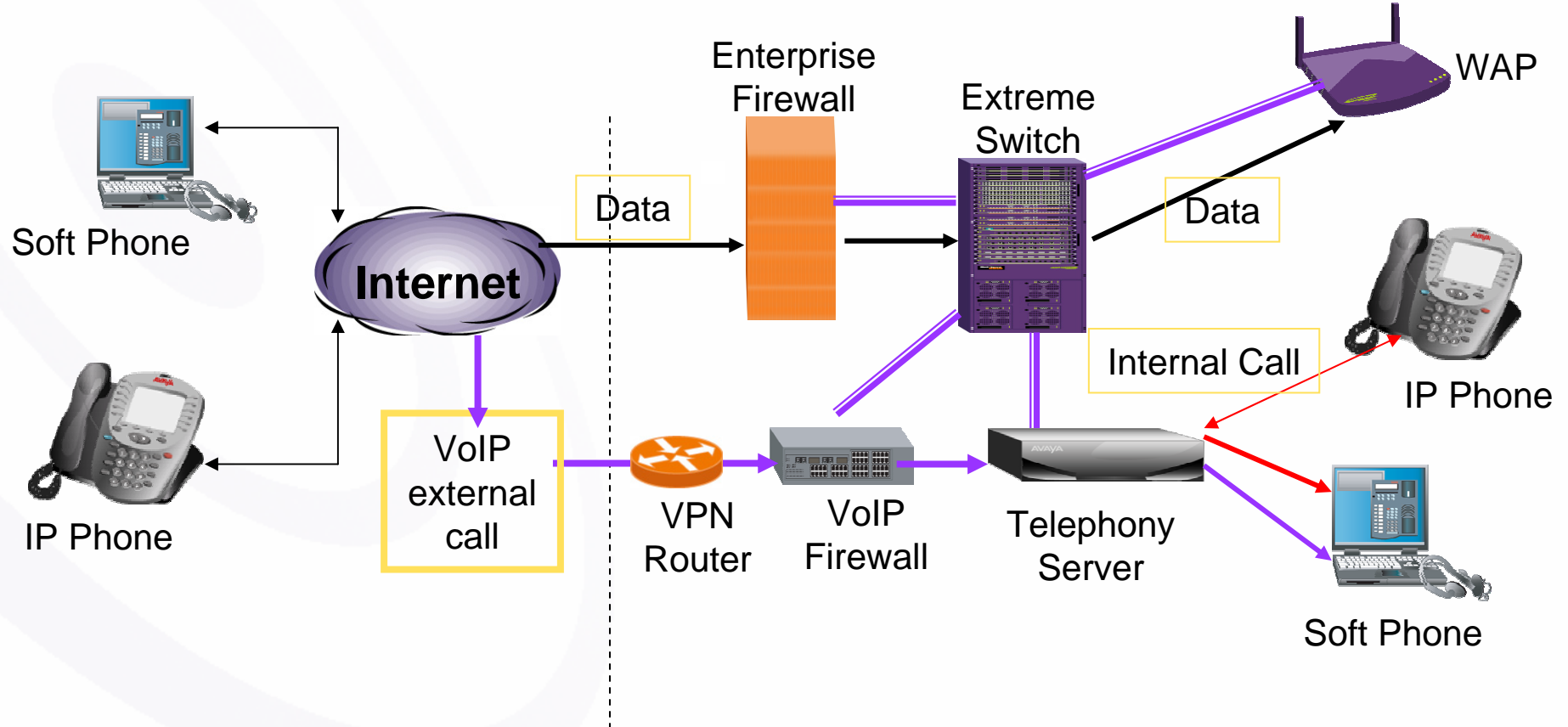
Edge Security

Firewalls, Session Border Controllers, Routers, Gateways

Stateful Packet Inspection Firewall VPN Server
Application Layer Gateways NAT/NAT Transversal
Secure Routers SBCs SIP Proxy
NAT-aware PBX SIP Registrar

VoIP/SIP Firewalls

- ▶ Protect against hijackers, Anti-voice Spam, Voicemail bombs, Call Eavesdropping, Crashing IP PBXs
- ▶ Application Layer Gateways- dynamic opening and closing of ports- understanding VoIP protocol data
 - Examples: Juniper, SecureLogix, BorderWare, NFR Security



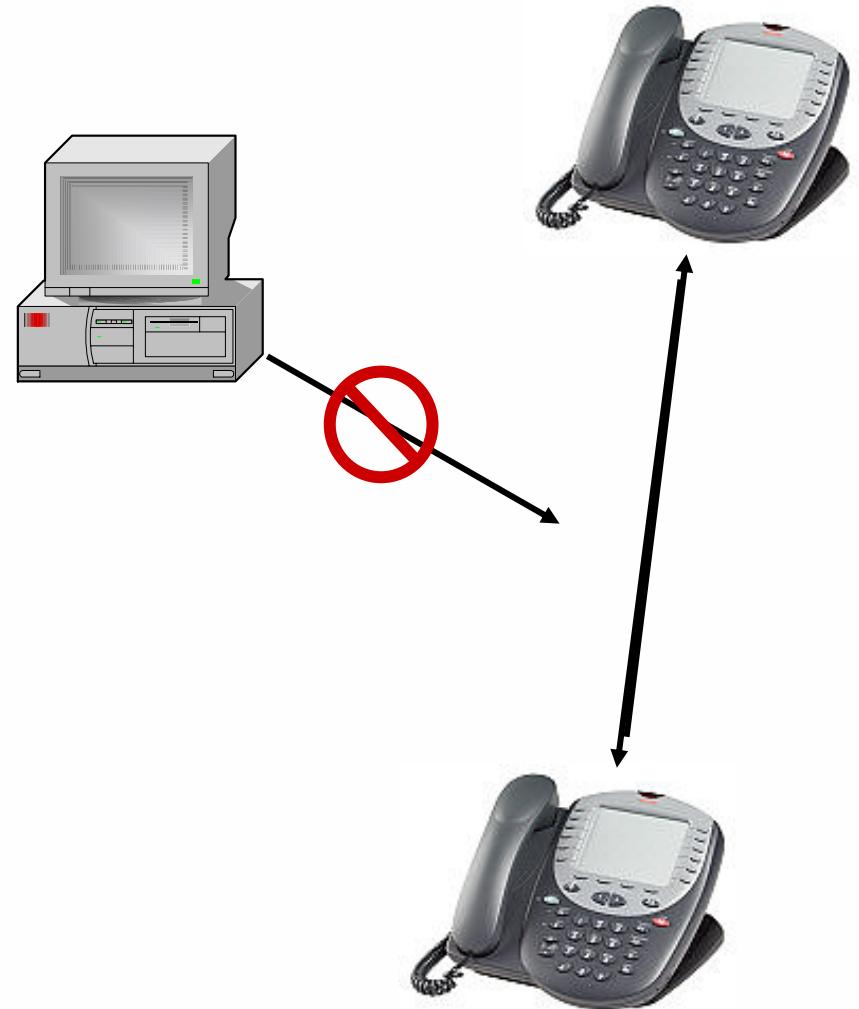
End-point Security

IP Phones, PDA's, Wireless APs

Secure RTP Media Encryption: AES Host Integrity*
Anti-Virus Remote VPN 802.1x Checking
Anti-Trojan WPA: Rogue AP Detect Survivability

Secure IP Phones

- ▶ Call processing can be isolated from production network if desired
- ▶ Signaling for endpoints and gateways is encrypted
- ▶ Operating system is hardened and includes intrusion detection
- ▶ IP Endpoints do not include web server functionality
- ▶ Endpoint registration is based on user authentication, not MAC address



Summary- VoIP Security

1. VoIP security must be part of your overall security policy- for known/unknown threats
2. Multiple layers (Core, Edge, Endpoints)
3. Implement VLANs
4. Core network security by Ethernet switch vendor
5. IDS/IPS at critical points
6. Supplement with Network-Wide protection
7. Consider new hardened DHCP/DNS/RADIUS appliances
8. Use VPN for remote access
9. Use Dynamic Packet Inspection/Voice-Aware Firewalls