VoIP Security

Andy Leung
Regional Security Product Manager
Email: aleung@juniper.net
Apricot 2005

Agenda

- VoIP general concept and components
- Security Framework
  - Protecting the core
  - Protecting the perimeter
  - Protecting the client
- Firewall and NAT
- Data Encryption
- References

General VoIP Concepts & Terminology

VOIP Major components

- IP PBX /Call Manager
  - Call Routing
  - Registering users / VOIP Phones
  - Signaling protocol used H.323, SIP, MGCP etc..
- VOIP Phone
  - Signaling protocol used SCCP, H.323, SIP
  - Voice transported using RTP over UDP/IP
- VOIP Gateway/Gatekeeper
  - Connection to PSTN and POTS
  - Signaling protocol used H.323, MGCP, SIP

H.323

- ITU standard for Real time media application
- VOIP H.323 implementation is typically vendor specific and not standard based, no multi vendor interoperability

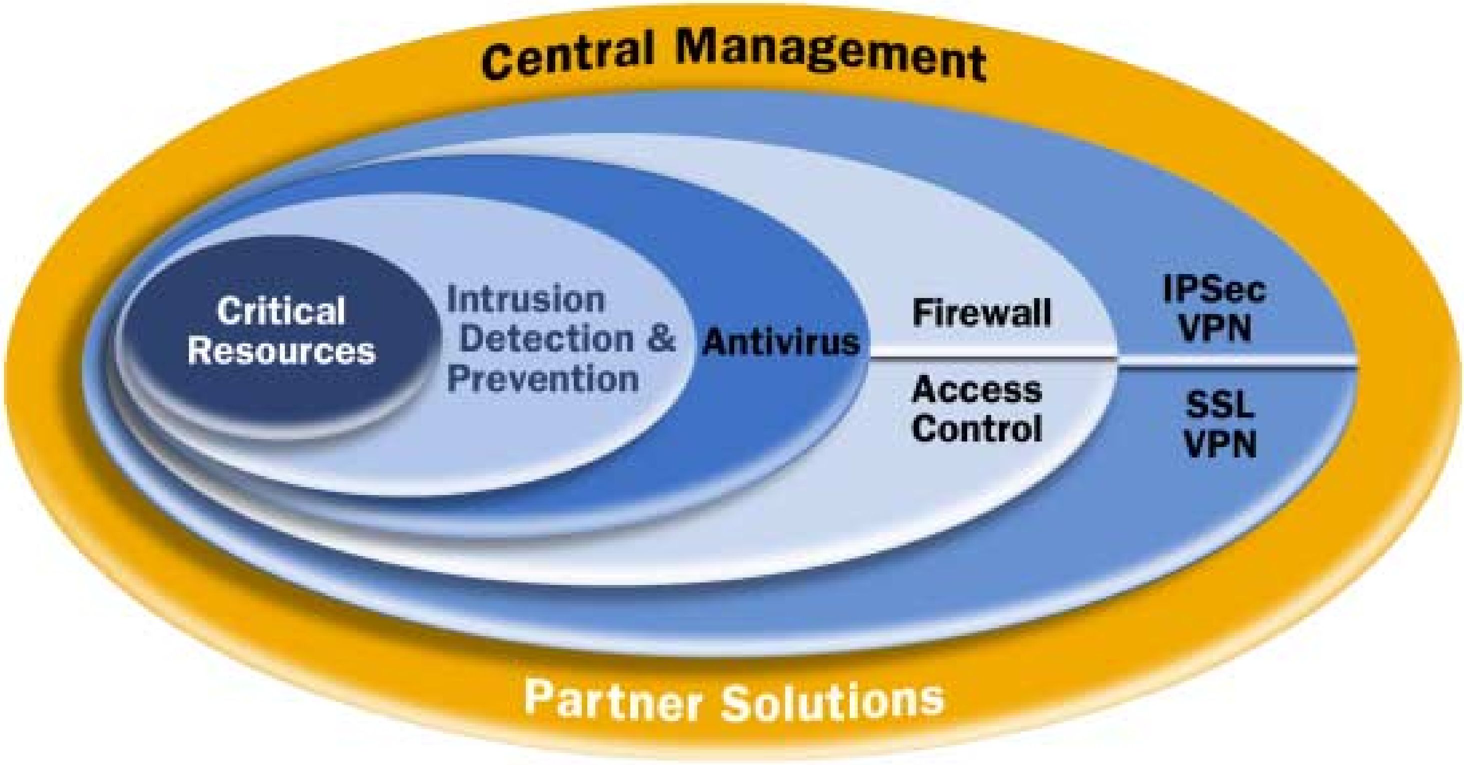
Session Initiation Protocol (SIP)

- Application layer signaling protocol to establish, maintain and terminate multimedia sessions involving audio, video and data
- SIP IP phone uses SIP Proxy (similar in concept as H.323 Gatekeeper) to establish multimedia session between end devices
- SIP is defined in IETF RFC 3261

SIP Components

- User agents (IP Phone, PC Clients)
  - Client – Initiates SIP requests and act as the user's calling agent
  - Server – Receives requests and return responses on behalf of user; act as the user called agent
- Network Servers
  - Proxy server – Acts on behalf of other clients and contain both client and server functions. A proxy server interprets and can re-write request headers before passing them on to other servers. This makes the proxy server as the initiator of the request and ensure that replies follow the same path
  - Redirect server – Accepts SIP requests and send

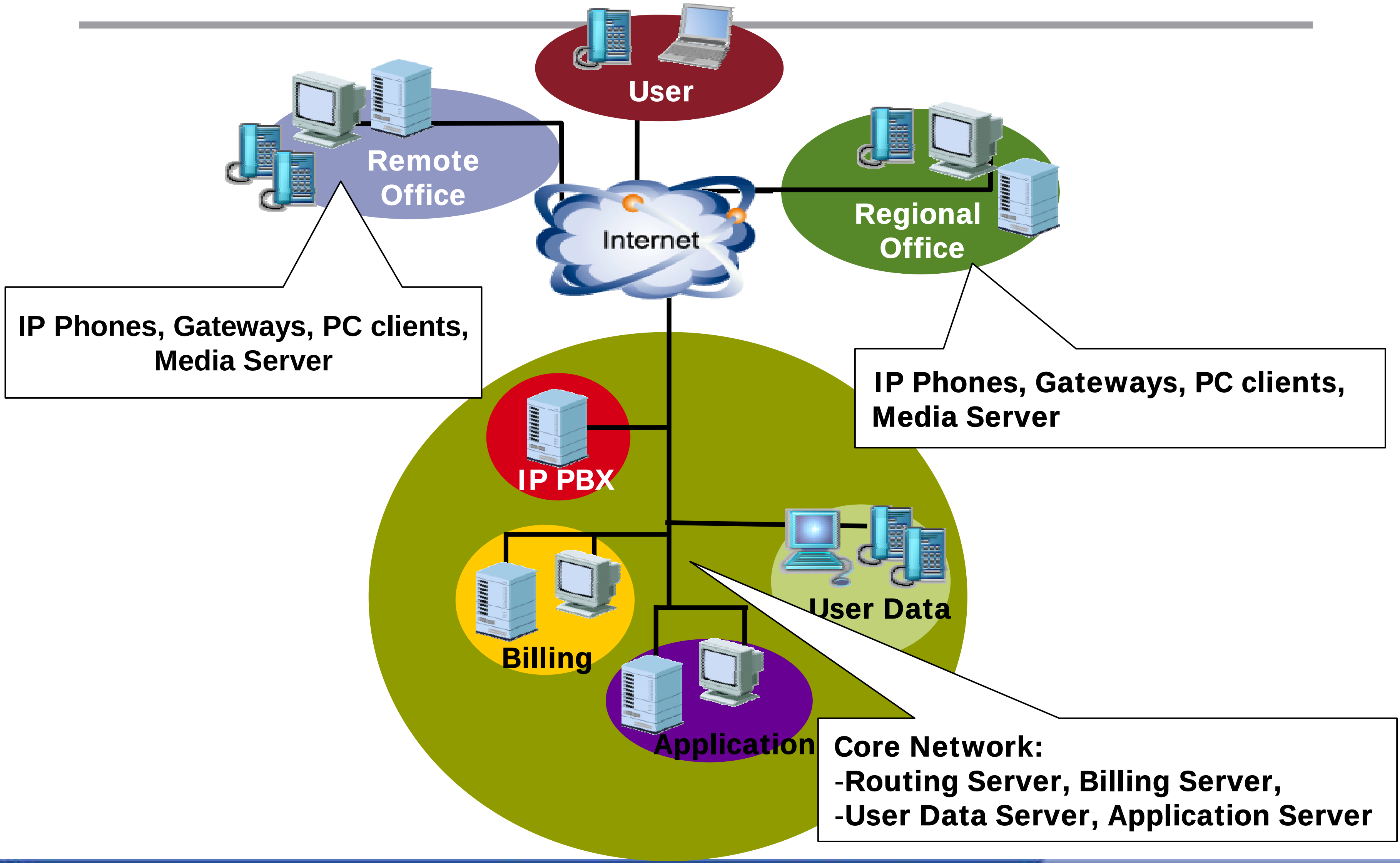
Layered Security Solutions



"Security professionals agree that network security requires a multi-layered defense. To meet the challenges posed by sophisticated and run-of-the-mill attacks, enterprises have been forced to deploy layers of security products."

International Data Corp.

VoIP Network Breakdown

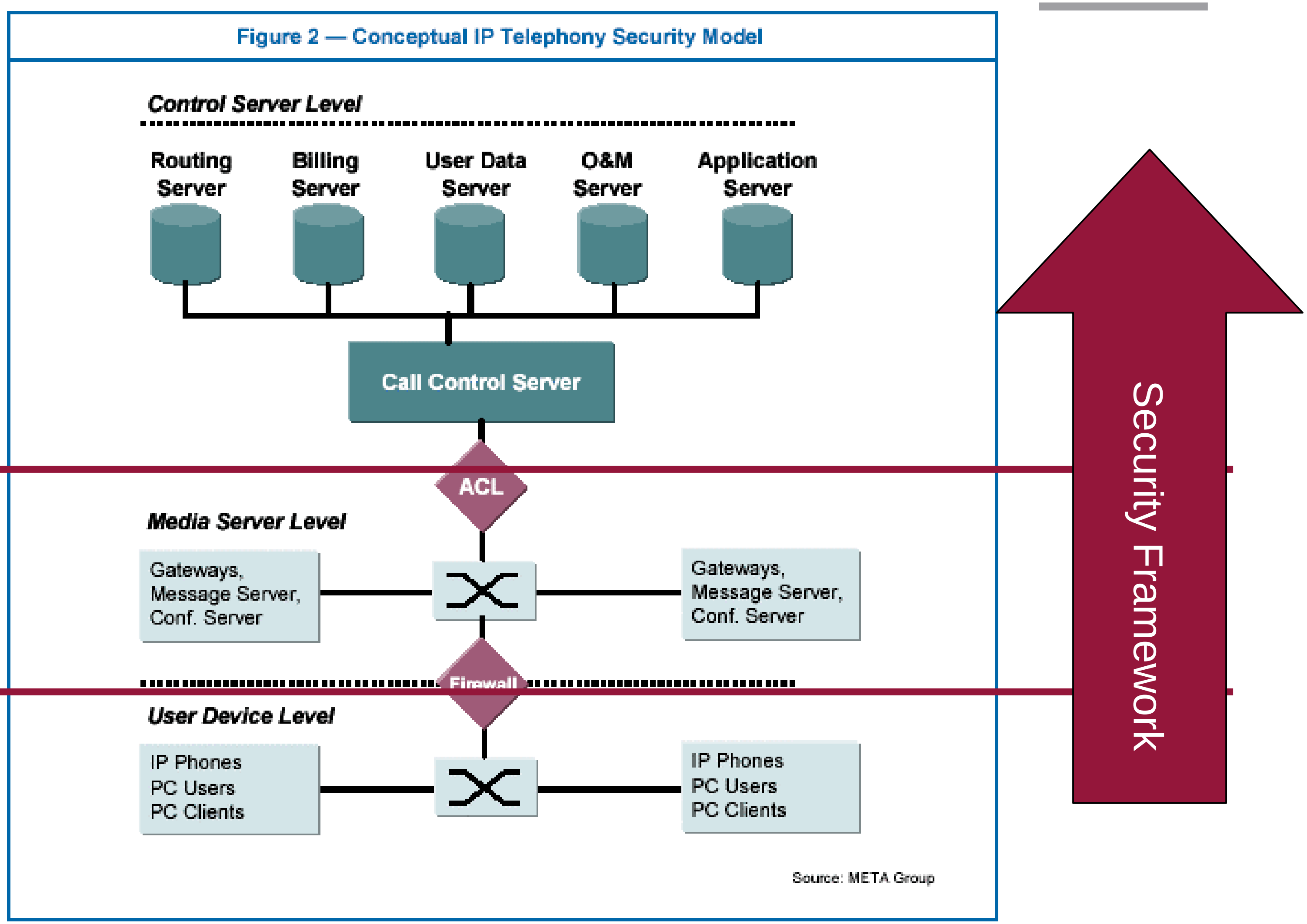


Conceptual IP Telephony Security Model

CORE

Perimeter

Client



Security Framework

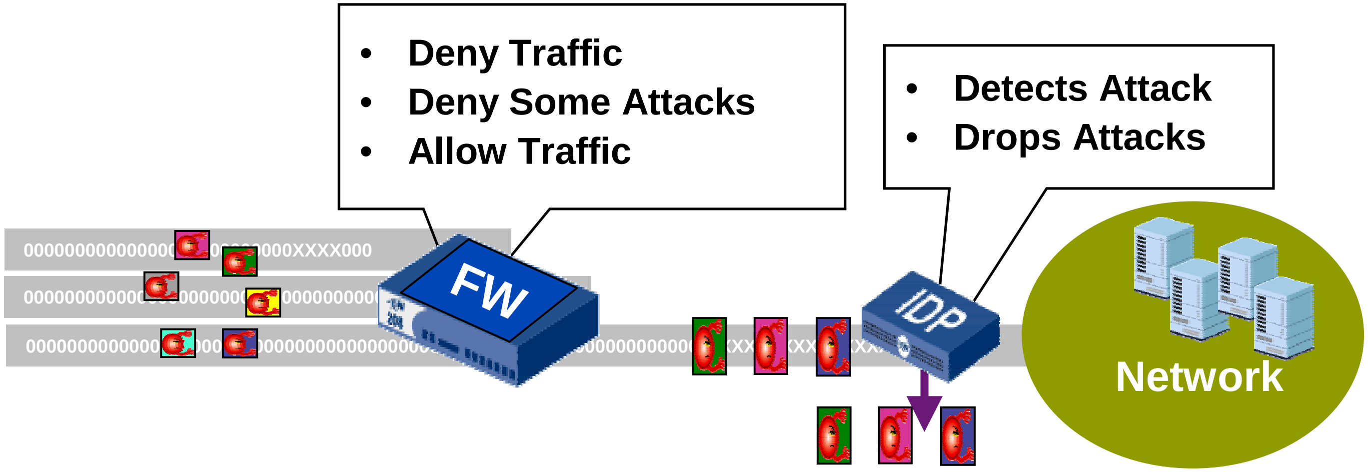
- Client devices
  - IP Phones, PC Clients
  - High risk domain
  - Chances for virus infections
  - Place none of VoIP services or control
- Gateways
  - Gateways, message or conference server
  - Medium risk domain
  - Access voice traffic by voice devices only
  - No user data or service critical data should be placed

Protecting the core network

- Core
  - All call handling related servers: call routing, call signaling, media, call statistics, etc …
  - Contains server critical and sensitive data.
  - Critical to protect against DOS.
  - Strong Authentication control
  - Use best practice from protecting an IP network

Core Network Security

- From Trust – Untrust model to Multiple zone concept.
- Use VLAN or multiple zones to define different security domains.
- Use IDP (Intrusion Detection and Protect) to stop intrusion.



Core Network Protection (cont.)

- Protecting the servers
  - Compromised IP telephony server may serve as a launching point for attacks on other servers in the network.
  - Keep the OS patches up-to-date.
  - Turn off all unused services.
  - Must support strong authentication for any configuration or software upgrade on the servers.

Protecting the Perimeter

Firewall in reference to VoIP

- FWs are passive device to VOIP communications , exception is when NAT in enabled
- VOIP signaling protocols are interpreted by FW to understand VOIP communication, but not modified, except in case of NAT
- FW do not interpret or participate RTP VOIP packets, but treat those packets as DATA packets

Problem with NAT

- NAT (Network address translation) could break VoIP implementation.
  - Call Registration: IP traversal from Private to Public domain
  - Dynamic port assignment by NAT
  - RTP / RTCP use dynamic ports (1024 – 65534)

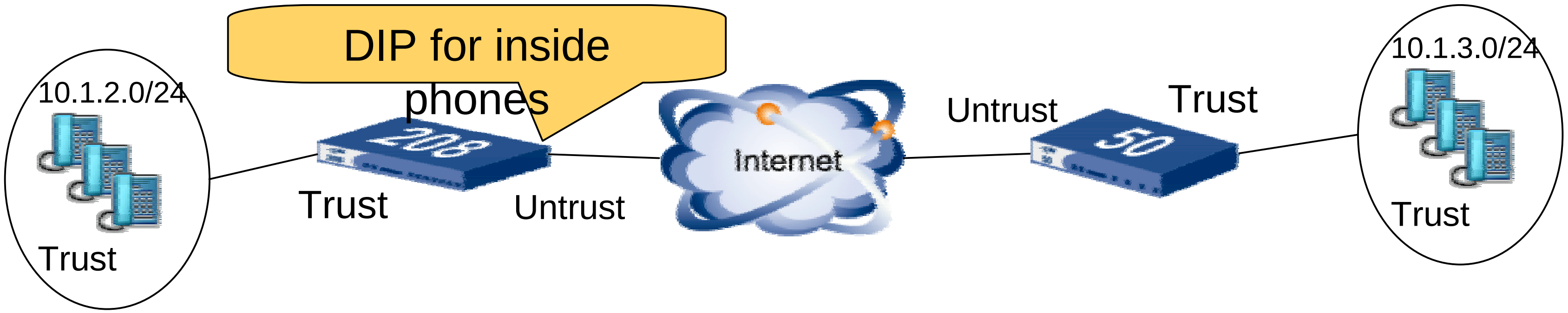
- Further complication
  - 2 ways, 3 ways calling
  - Both users are behind NAT

Working with NAT

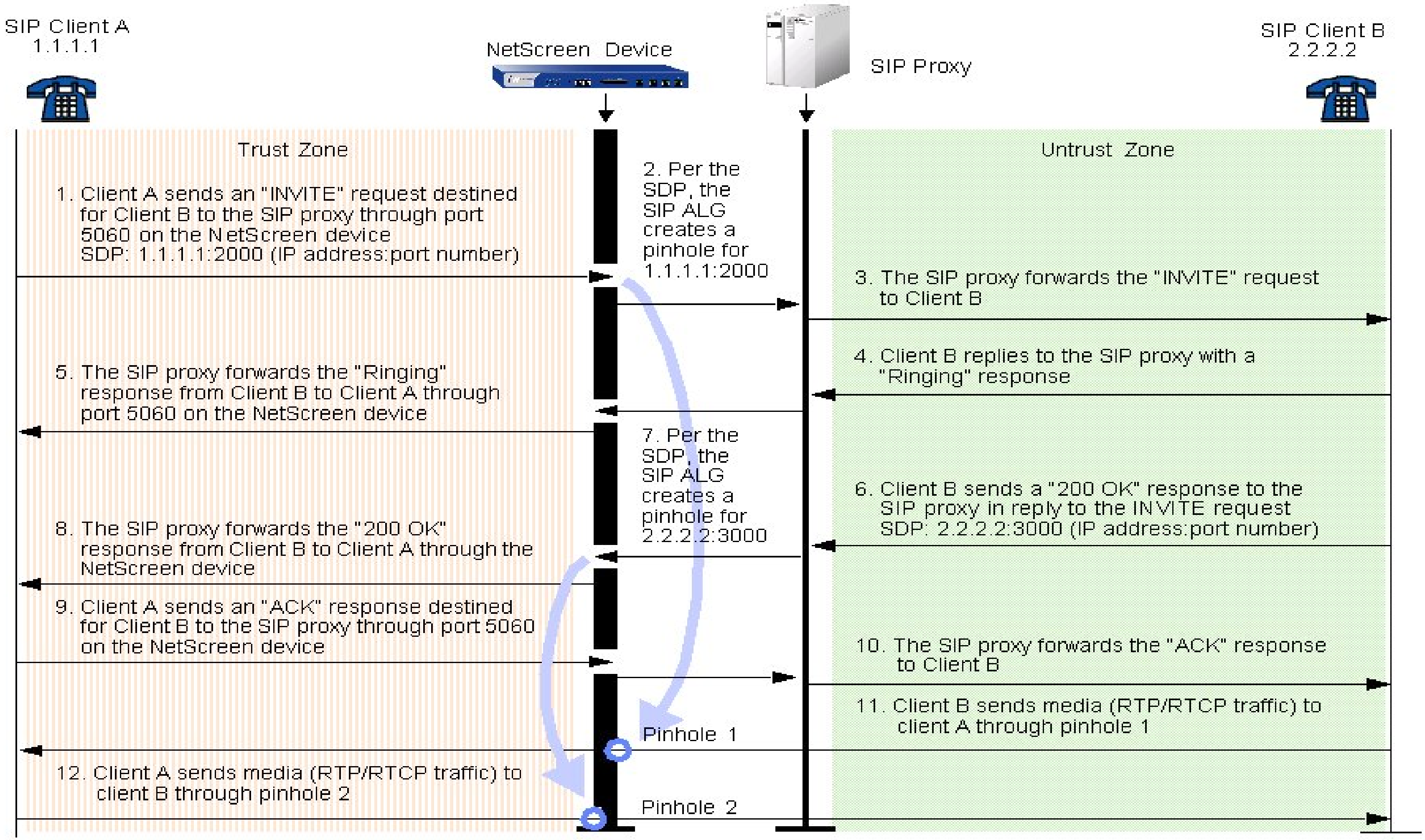
- ALG
- Others implementations
  - Middle box solution
  - SBC (Session Board Controller)
  - Firewall Traversal Protocol (STUN, TURN ..)

VoIP ALG - Behavior

- ALGs are invoked by default on the protocol standard ports (SIP: 5060, H.323: 1718-1720)
- Benefits:
  - Allow better traffic classification (service: H.323/SIP)
  - Perform NAT on the application payload (layer 7)
  - Open dynamic pinholes for Media
  - Perform application level security



SIP ALG Example



*Assumes bidirectional policies created allowing port 5060 signal flow

VoIP DOS Protection

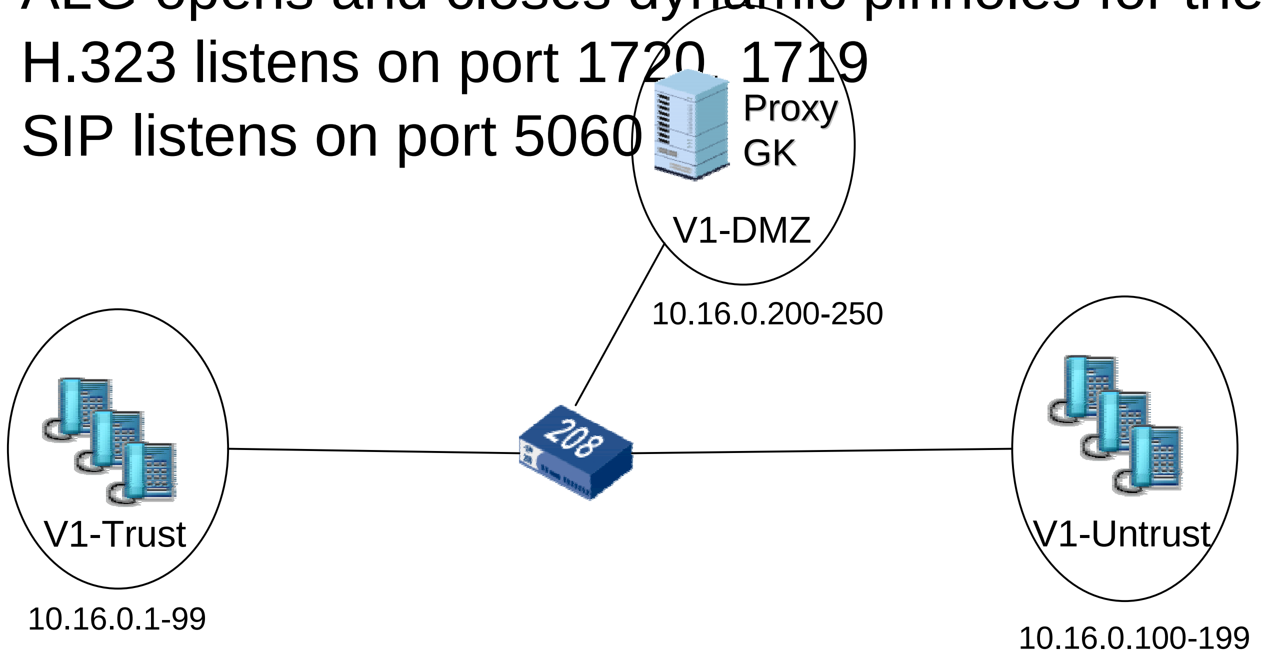
- DoS protection for VoIP applications
  - UDP Flooding Threshold
    - Enables customer to limit the number of requests over UDP
      - As VoIP gains widespread adoption, hackers will spend more time creating attacks exploiting VoIP deployments
      - Both of these provide application specific Denial of Service protection originating from SIP endpoints
  - Source Limiting
    - Enables customer to limit call setup originating from an unknown source
      - Prevents unwanted “spamming” for VoIP calls
  - Attack Protection
    - Prevents a client from making multiple SIP requests to a server that has already denied the initial request

VoIP Deployment

- Firewall Deployment
  - Transparent
  - Route
  - NAT
  - Topology Hiding
- Encryption

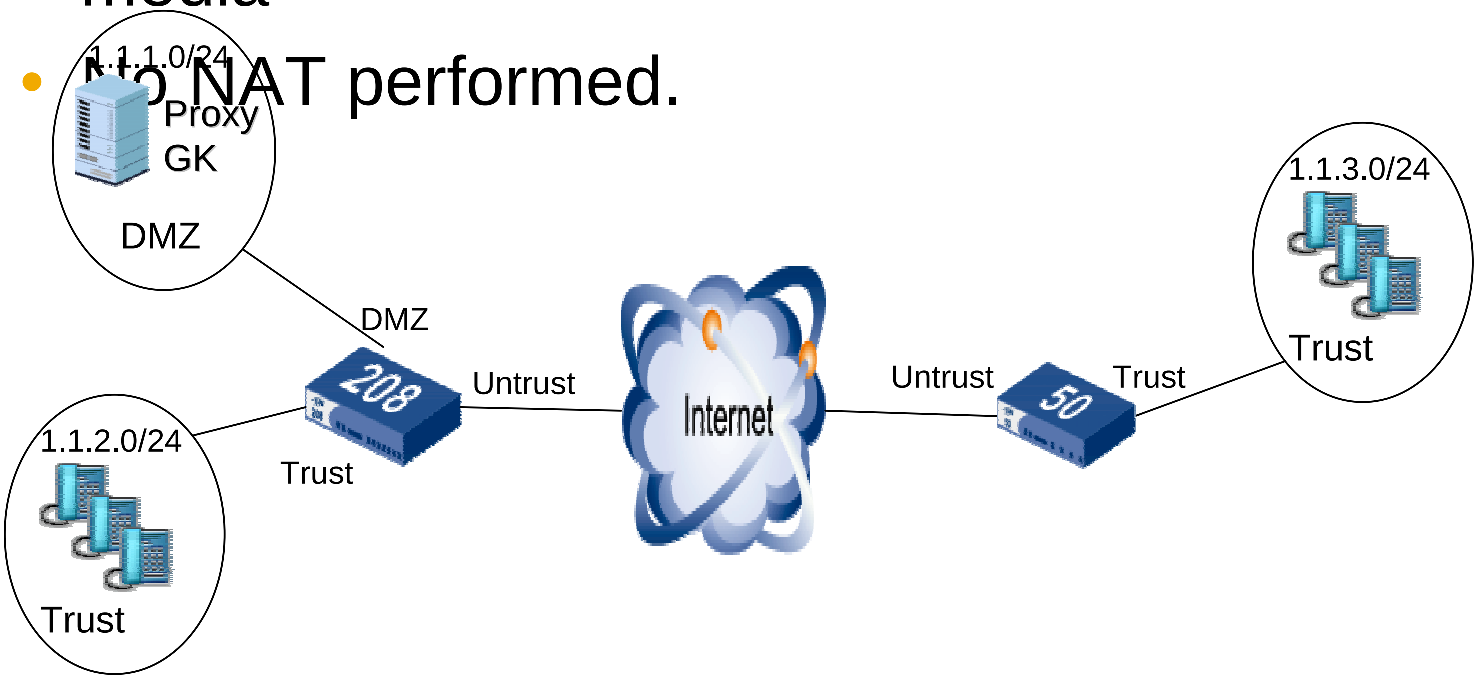
Deploy FW in Transparent Mode

- No change to existing IP architecture
- Implement security in existing network.
- H.323 & SIP ALGs are invoked even in Layer 2 (transparent mode):
  - ALG opens and closes dynamic pinholes for the media
  - H.323 listens on port 1720, 1719
  - SIP listens on port 5060

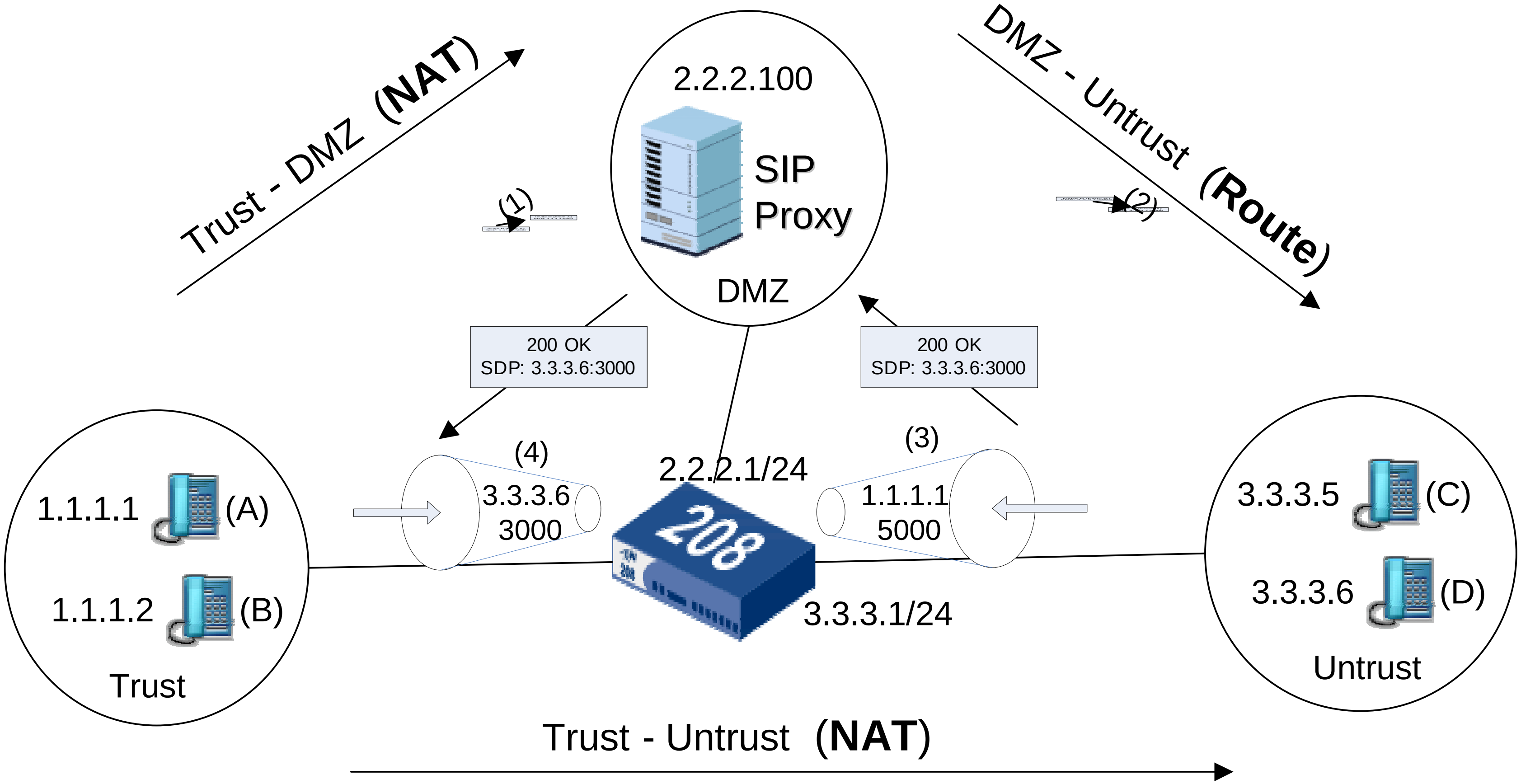


VoIP - In Route Mode

- H.323 & SIP ALGs invoked for the same reasons as in transparent mode
  - ALG opens and closes dynamic pinholes for the media
  - No NAT performed.



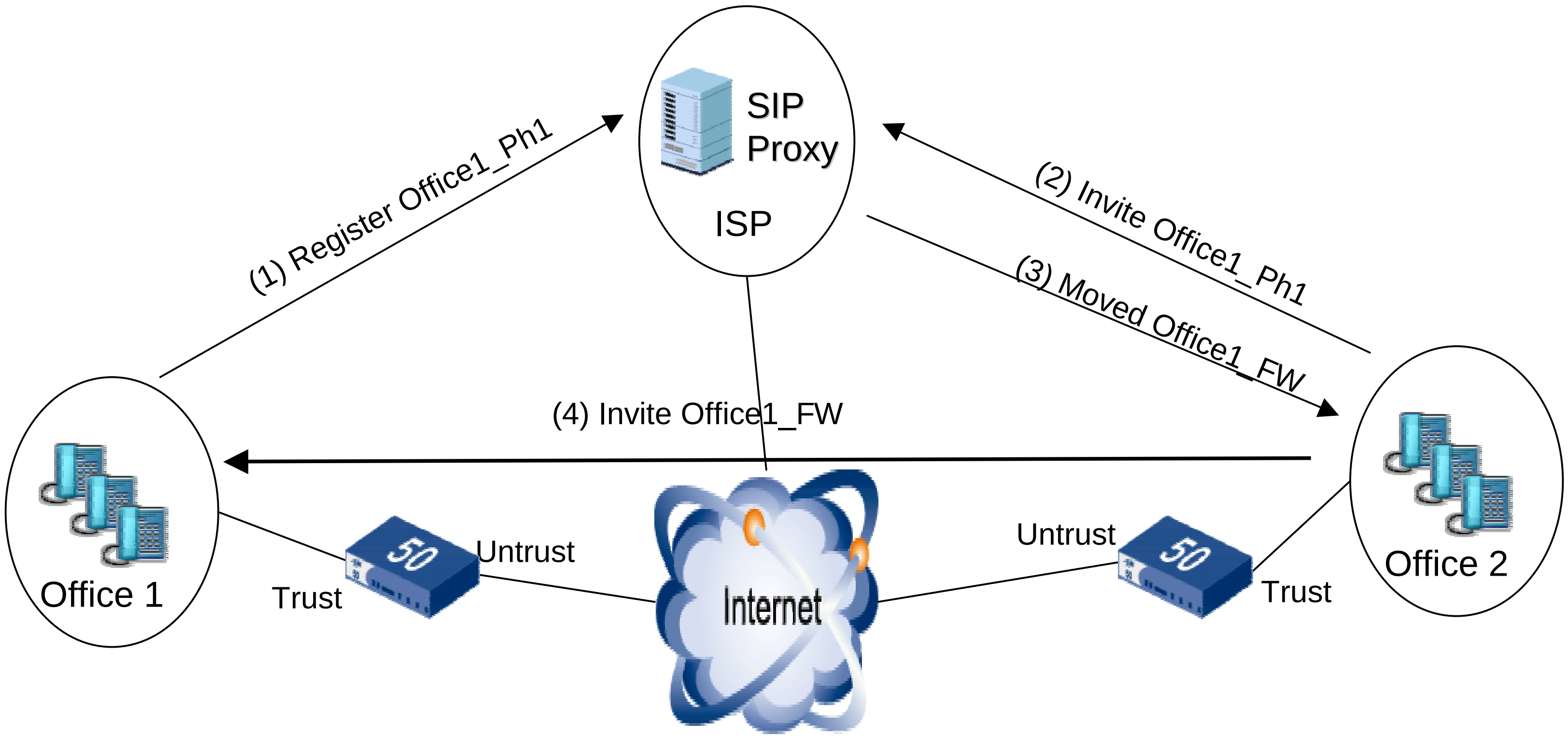
SIP – 3-Zone Architecture



* (A) calls (D) through the SIP Proxy

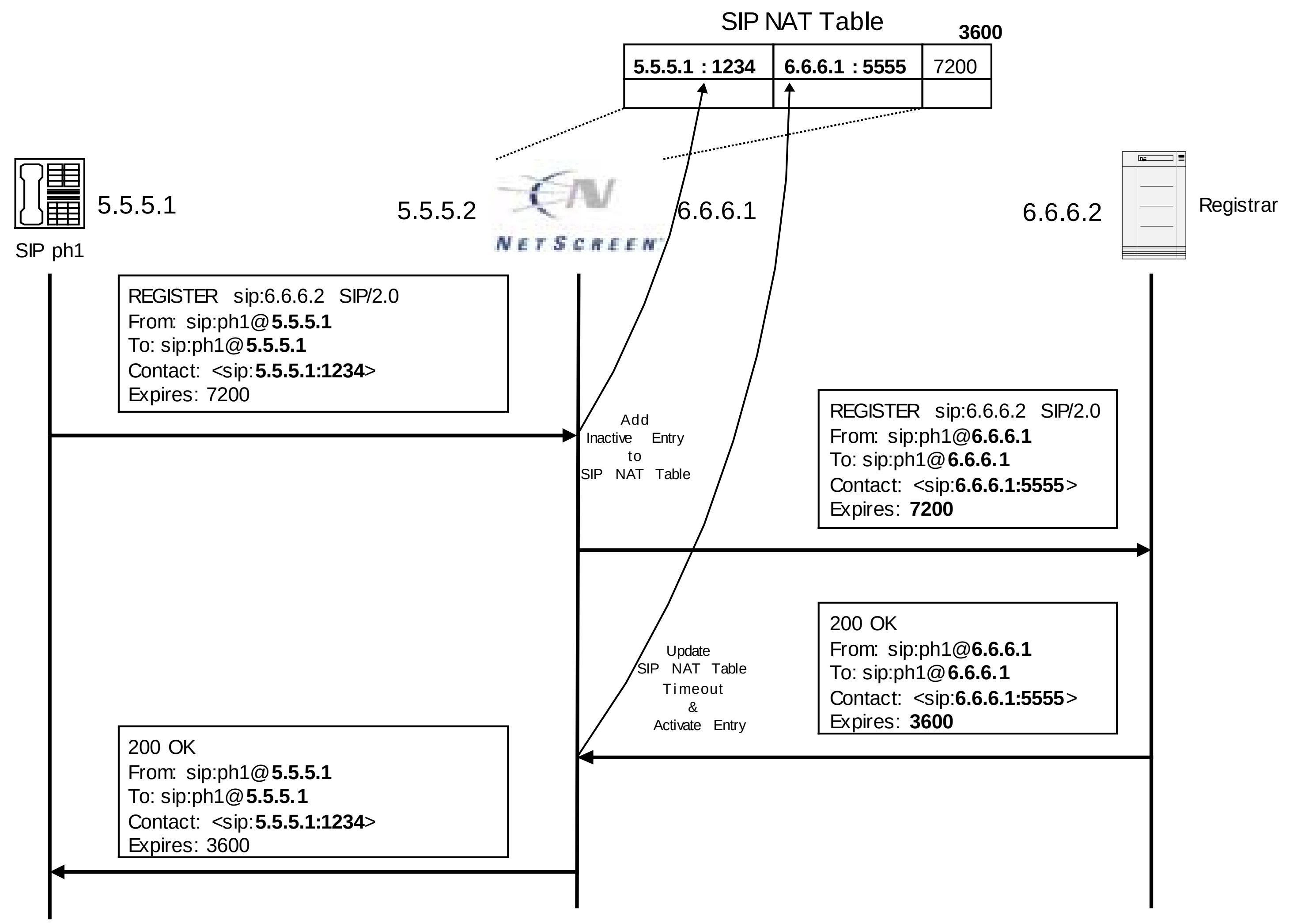
Incoming NAT - SIP Example

- Allows phones in Private Zone to be reached from the Public Zone.
  - New Inbound Dip table for Private-to-Public IP mappings



* (A) calls (D) through the SIP Proxy

Incoming NAT – Incoming DIP Table



SIP – Topology Hiding

- Removes “Via” and “Record-Route” headers from the SIP payload when packets leave the private domain.

INVITE sip:user@work.com SIP/2.0
Via: SIP/2.0/UDP server1.work.com
Via: SIP/2.0/UDP server2.work.com
Via: SIP/2.0/UDP server.home.com
Record-Route: <sip:user@server1.work.com>
Record-Route: <sip:user@server2.work.com>
From: Alice<sip:alice@home.com>
To: User<sip:user@work.com>
Call-ID: 123442@station1.home.com
CSeq: 1 INVITE
Contact: Alice<sip:alice@home.com>

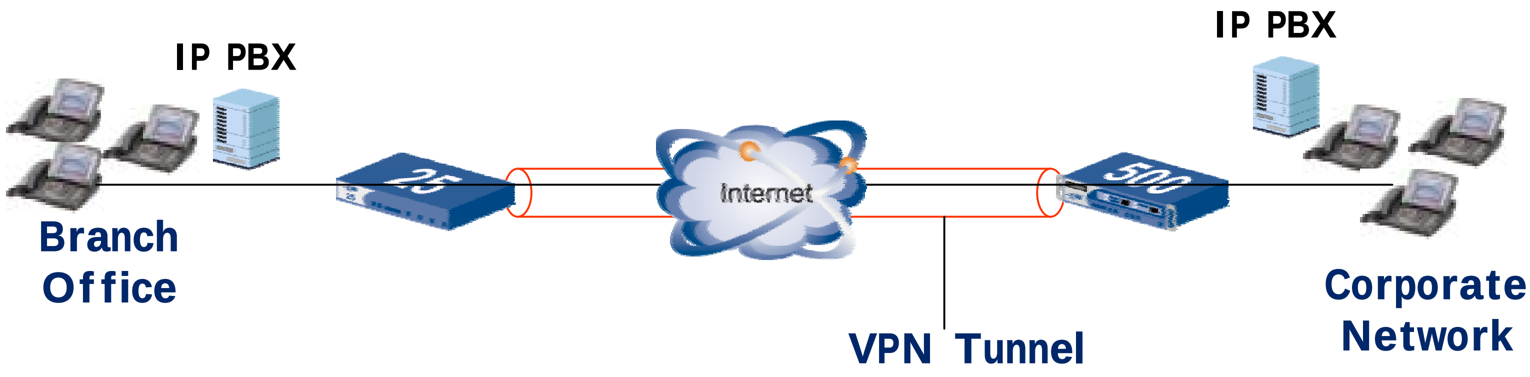
Private 192.168.1.2 →  → Public 212.24.2.56

INVITE sip:user@work.com SIP/2.0
Via: SIP/2.0/UDP **212.24.2.56:4023**
Record-Route: **212.24.2.56:4023**
From: Alice<sip:alice@home.com>
To: User<sip:user@work.com>
Call-ID: 123442@station1.home.com
CSeq: 1 INVITE
Contact: Alice<sip:alice@home.com>

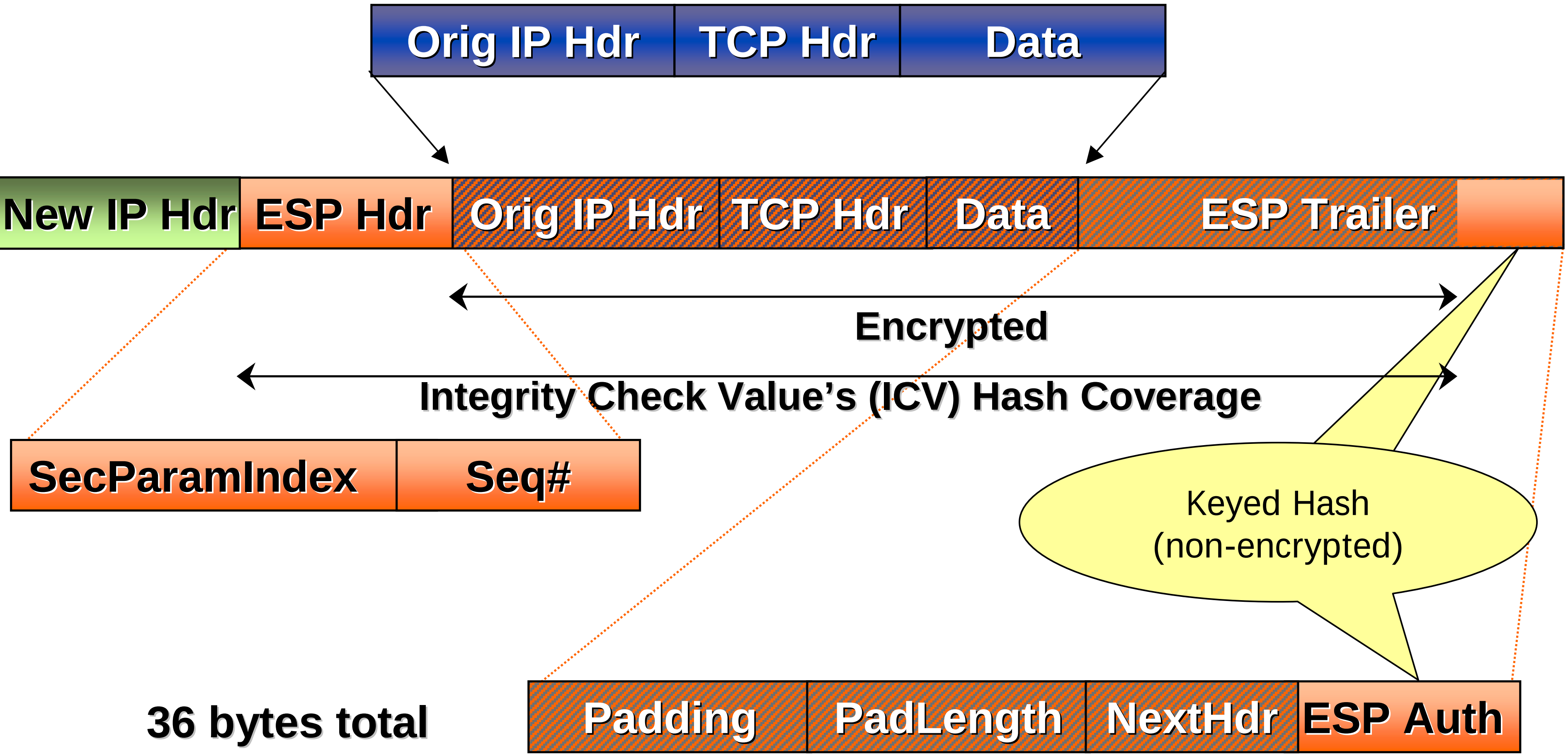
Juniper your Net

Ensure Privacy of VoIP Calls

- VoIP Security Challenge
  - Protecting VoIP calls from Eavesdropping
  - Encrypt VoIP connections with site-to-site VPN (DES, 3DES, AES) to prevent eavesdropping
  - IPSec: Transport mode vs. Tunnel mode



ESP Tunnel Mode Packet Transform



Other considerations

Common VoIP Security Performance Challenge		Solutions
VoIP traffic consists of very small packet sizes that are intolerant to latency or jitter	→	Purpose-built systems deliver predictable performance, low latency solutions ideal for VoIP applications
VoIP networks always needs to be available to match expectations of traditional telephony networks	→	Full-range of high availability options ensures availability and reduces chance for failure
Need a high availability solution to ensure no calls are dropped or missed	→	Support for multiple Call managers ensure higher call completion rate – utilize second Call manager if one lacks the resources
Solution needs to be able to scale easily and grow as the business grows	→	Capacity to handle the number of concurrent calls and achieve the calls per second set up rate required by large deployments

Reference

- Security Considerations for Voice over IP network
  - http://csrc.nist.gov/publications/nistpubs/800-58/SP800-58-final.pdf
- Deploying Secure IP Telephony in the Enterprise network
  - http://www.juniper.net/solutions/literature/white_papers/#02
- Juniper Firewall Concept and Examples Guide
  - http://www.juniper.net/techpubs/
- IP Telephony and Network Address Translation
  - http://www.networkmagazine.com/showArticle.jhtml?articleID=17602009
- Voice over IP security issues
  - http://www.sans.org/rr/whitepapers/voip/

Thank You