Criticità dei servizi di telecomunicazione nella convergenza voce/dati

Colloquia sulla infrastrutture critiche
AIIC
Univ. Roma Tre, 27 Febbraio 2008

Agenda

- **Analisi introduttiva**
- **Univocità del problema “sicurezza-VoIP”**
- **Tassonomia delle vulnerabilità VoIP**
- **Contromisure e “best-practies”**
- **Architetture di riferimento**
- **Stato dell’arte dei prodotti e delle infrastrutture VoIP**
- **Conclusioni**

Analisi introduttiva

- **I protocolli e le tecnologie VoIP sono mature e robuste**
  - Esiste un grosso parco di offerta standardizzata
  - Iniziano a prendere il posto delle tecnologie TDM
  - Si avvantaggiano delle opportunità offerte dai servizi internet
- ***… ma da fonti Gartner:***
  - Gli utenti VoIP continueranno ad utilizzare terminali tradizionali (2011)
  - Le comunicazioni VoIP continueranno ad essere meno sicure delle TDM
  - Le tecniche di cifratura direttamente sui PBX-IP e sui terminali non saranno presenti fino alla fine di questo anno
  - Dal 2008 gli attacchi DOS potranno compromettere le comunicazioni Voice
  - Dal 2006 la convergenza delle reti Dati/Voce permetterà a virus e worms di attaccare i terminali VoIP

L’univocità del problema di sicurezza in VoIP

Le tecniche di messa in sicurezza delle comunicazioni VoIP differiscono dalle altre e sono sostanzialmente originali perché devono tenere in considerazione:

- garanzia di banda
- jitter e delay ridotti
- messaggi a priorità dei protocolli di segnalzione

Quando si mettono in sicurezza comunicazioni VoIP si devono tenere in considerazione tutti i problemi IP più gli specifici problemi VoIP

Mettere in sicurezza un sistema VoIP richiede un delicato bilancio fra QOS e contromisure

Le due facce di VoIP

- **La problematica VoIP si scompone in:**
  - setup della chiamata (segnalazione)
  - payload (pacchetti Voce)

- **Nel setup della chiamata il delay non è importante come nel trasporto dei pacchetti voce**
  - tolleranza delay setup = qualche secondo
  - tolleranza delay payload (G.114) = 150 ms (end to end), Max 250 ms

Tipi di vulnerabilità

- **Sia la segnalazione che il trasporto sono vulnerabili a tutti gli attacchi della suite IP compresi:**
  - virus, worm,spoofing, flooding, ManInTheMiddle, DoS
- **E' possibile classificare gli attacchi specifici di VoIP in:**
  - Registration Hijacking (+ problemi legali / privacy)
  - Impersonificazione di server / servizi
  - Abbattimento delle connessioni
  - Alterazione del corpo dei messaggi
  - DOS e DDOS

Tassonomia delle Vulnerabilità VoIP

- **Vulnerabilità Proprie**
  - guasti e malconfigurazioni si riflettono sulla rete IP
  - in assenza di alimentazione non sono assicurati neanche i servizi di emergenza
  - raddoppiano i target IP nella rete
- **Vulnerabilità Implementative**
  - “eavesdropping” e “vlan hopping”
  - “covert channel” e furto di banda
  - confidenzialità ed integrità non garantite da metodi di autenticazine forte e cifratura
- **Vulnerabilità DOS e Frodi**
  - sul protocollo di segnalazione
  - sul protocollo di trasporto
  - sul Voice-Gateway
  - “joyriding” VoIP / Wireless-LAN
- **Componenti Applicative**
  - call-manager e gate-keeper
  - unified-messages e VMAIL
  - softphone

Tassonomia delle vulnerablità per livelli ISO/OSI

	Riservatezza	Integrità	Disponibilità
Layer 7 - Applicativo	Backdoor su Sistemi Operativi, Applicativi e Servizi		
Layer 5 - Sessione	Telephony DHCP spoofing		DOS su H323, SIP e MGCP/MEGACO
Layer 4 - Trasporto	Sniffing e TCP / UDP Spoofing	Man In the Middle	TCP flood e UDP fragment flood
Layer 3 – Rete	Attacchi e vulnerabilità IP e ICMP	CovertChannel	Attacchi DOS verso ROUTER che assicurano QOS
Layer 2 e 1 – data link e fisico	Eavesdropping	VLAN Hopping, ARP poisoning / flooding e MAC Spoofing	

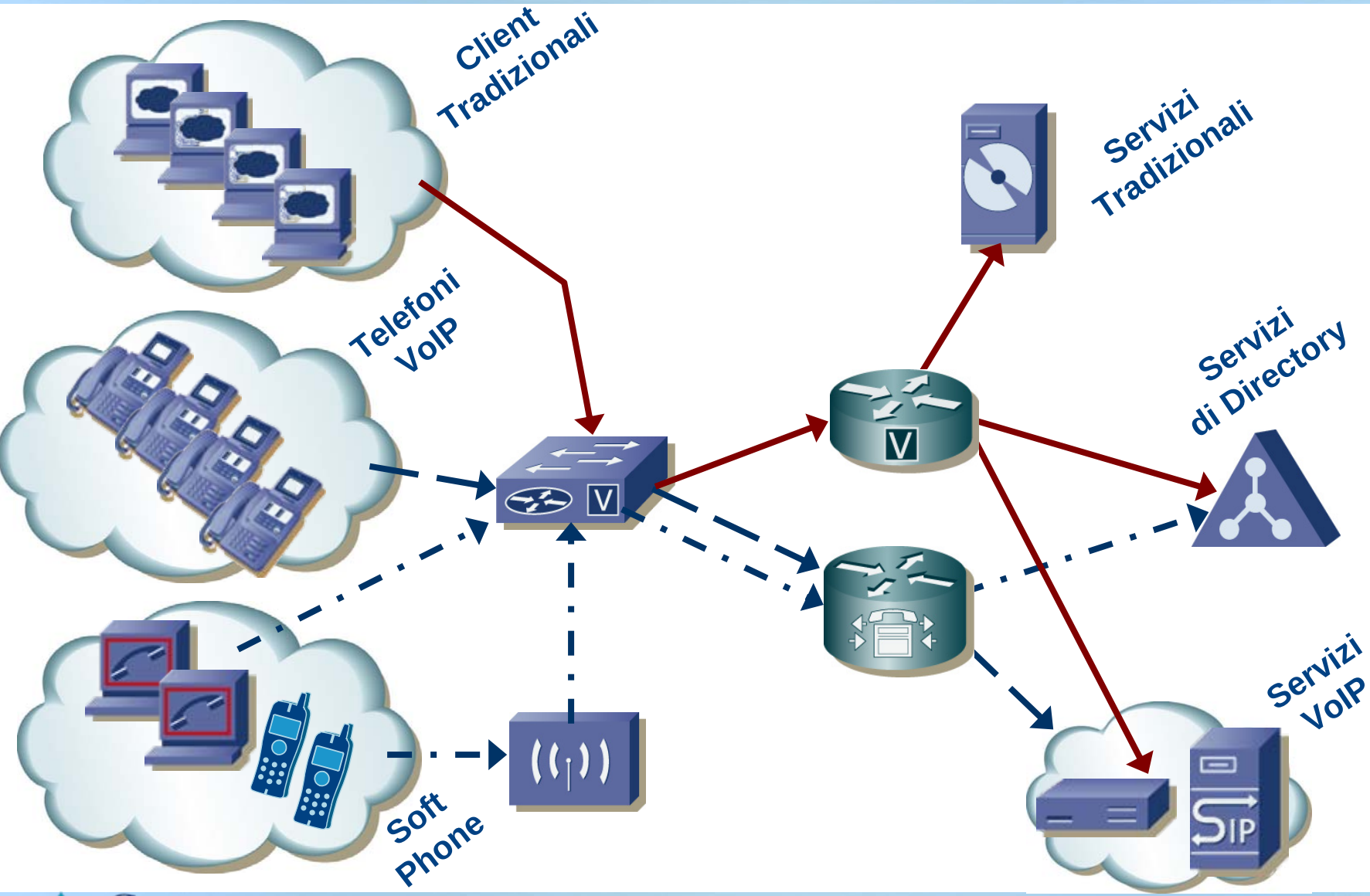
Tassonomia delle Contromisure VoIP

- **Contromisure Proprie**
  - separare dove possibile l'infrastruttura VoIP da quella dei servizi IP
  - prevedere sistemi di alimentazione secondaria anche per telefoni e apparati VoIP
  - configurare i terminali VoIP in VLAN dedicate con piani di indirizzamento separati
- **Contromisure Implementative**
  - utilizzo di sistemi di cifratura del traffico IP (IP-SEC)
  - sistemi di routing "policy-based"
  - utilizzo di sistemi di autenticazione dell'utente sui terminali e sul call-manager
- **Contromisure DOS e Frodi**
  - sistemi IDS e IPS VoIP-aware
  - sistemi di autenticazione del traffico verso l'esterno
  - utilizzo dei metodi di autenticazione per Access Point e terminali Wireless
- **Contromisure Applicative**
  - "hardening" call-manager e gate-keeper
  - restrizione protocolli unified-messages e VMAIL
  - "hardening" e sistemi di enforcement per softphone

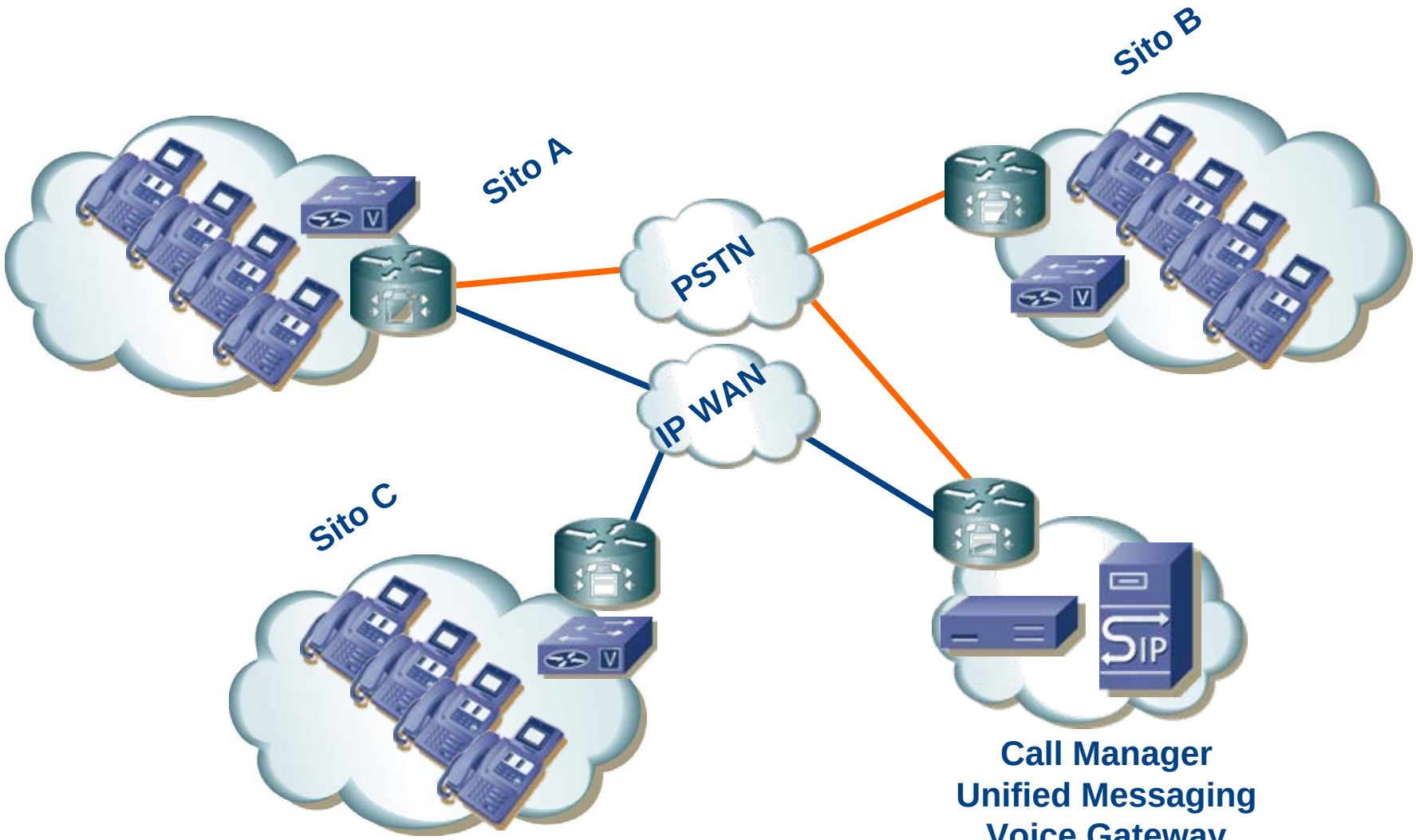
Tassonomia delle contromisure ISO/OSI

	Riservatezza	Integrità	Disponibilità
Layer 7 - Applicativo	“Hardening”, Firewall “Voip Aware”, Application Layer Gateway, IDS e IPS		
Layer 5 - Sessione	Fixing protocolli di segnalazione H323, SIP e MGCP/MEGACO e filtri Anti-spoofing Telephony DHCP		
Layer 4 - Trasporto	Chiavi di cifratura del payload e dei protocolli di segnalazione		Policing del traffico
Layer 3 – Rete	IPSec		
Layer 2 e 1 – data link e fisico	VLAN ACL, Dynamic ARP Inspection e Layer 2 DHCP snooping		

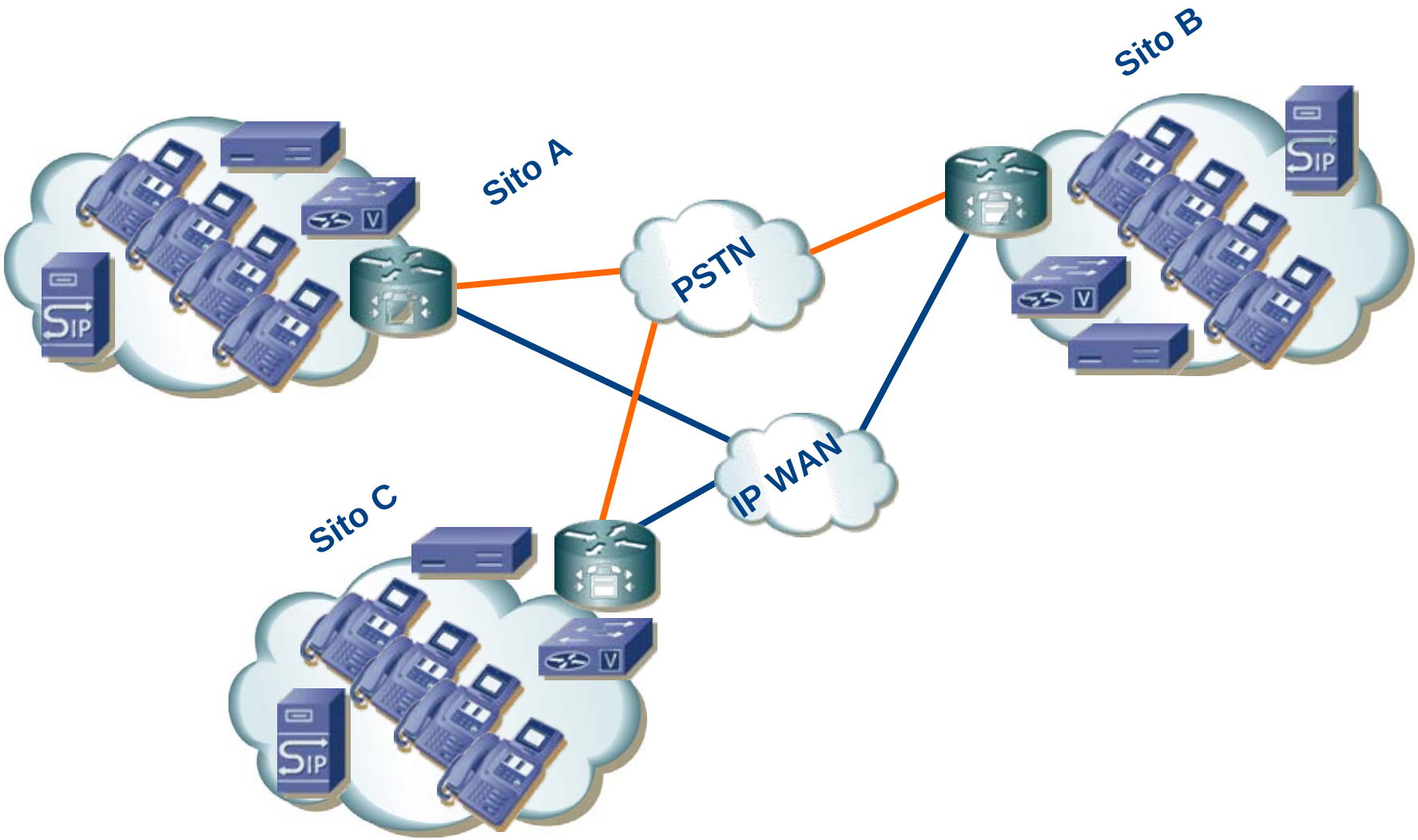
Un’architettura locale di riferimento



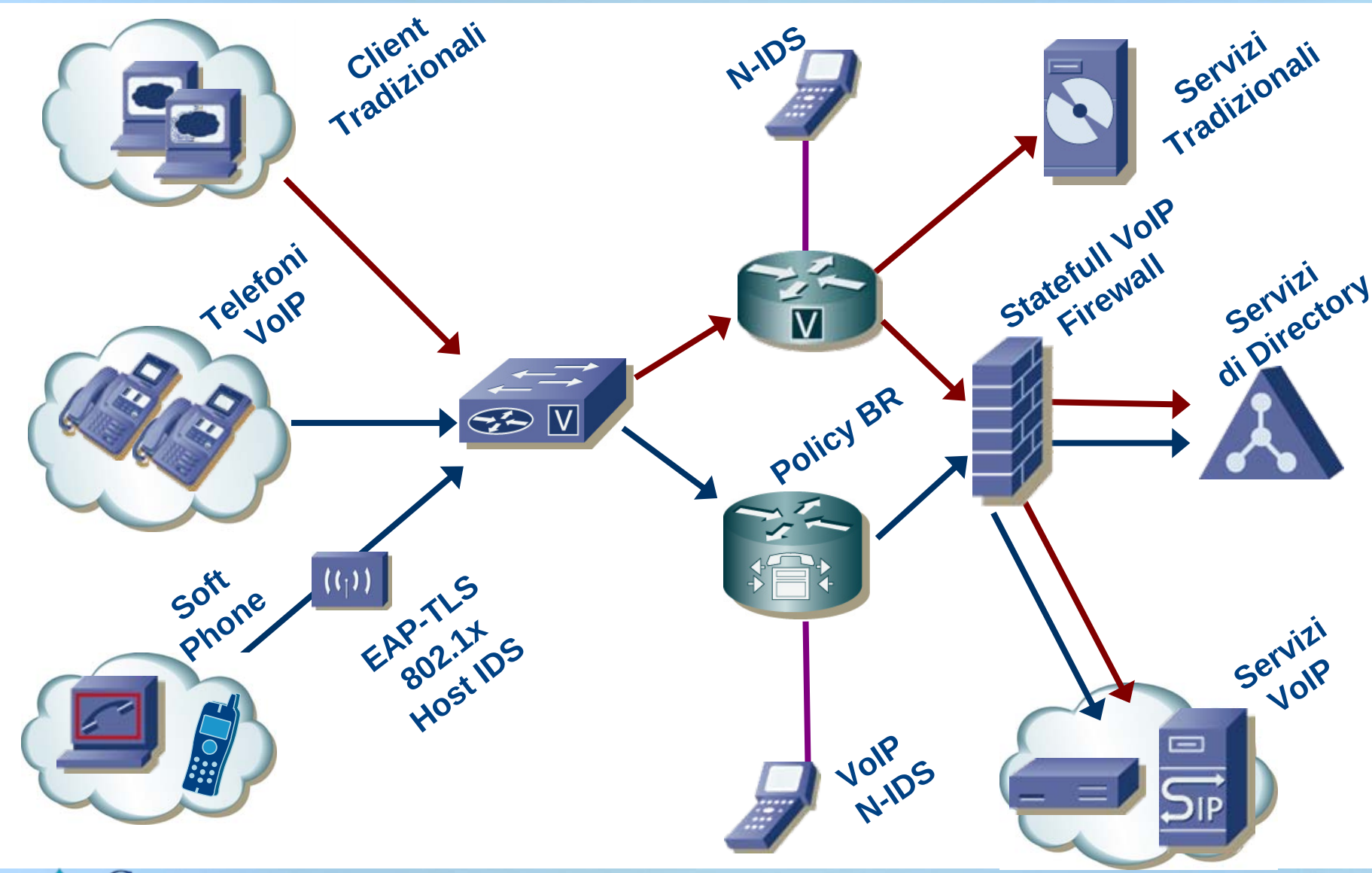
Usciamo dalla LAN
Infrastruttura centralizzata



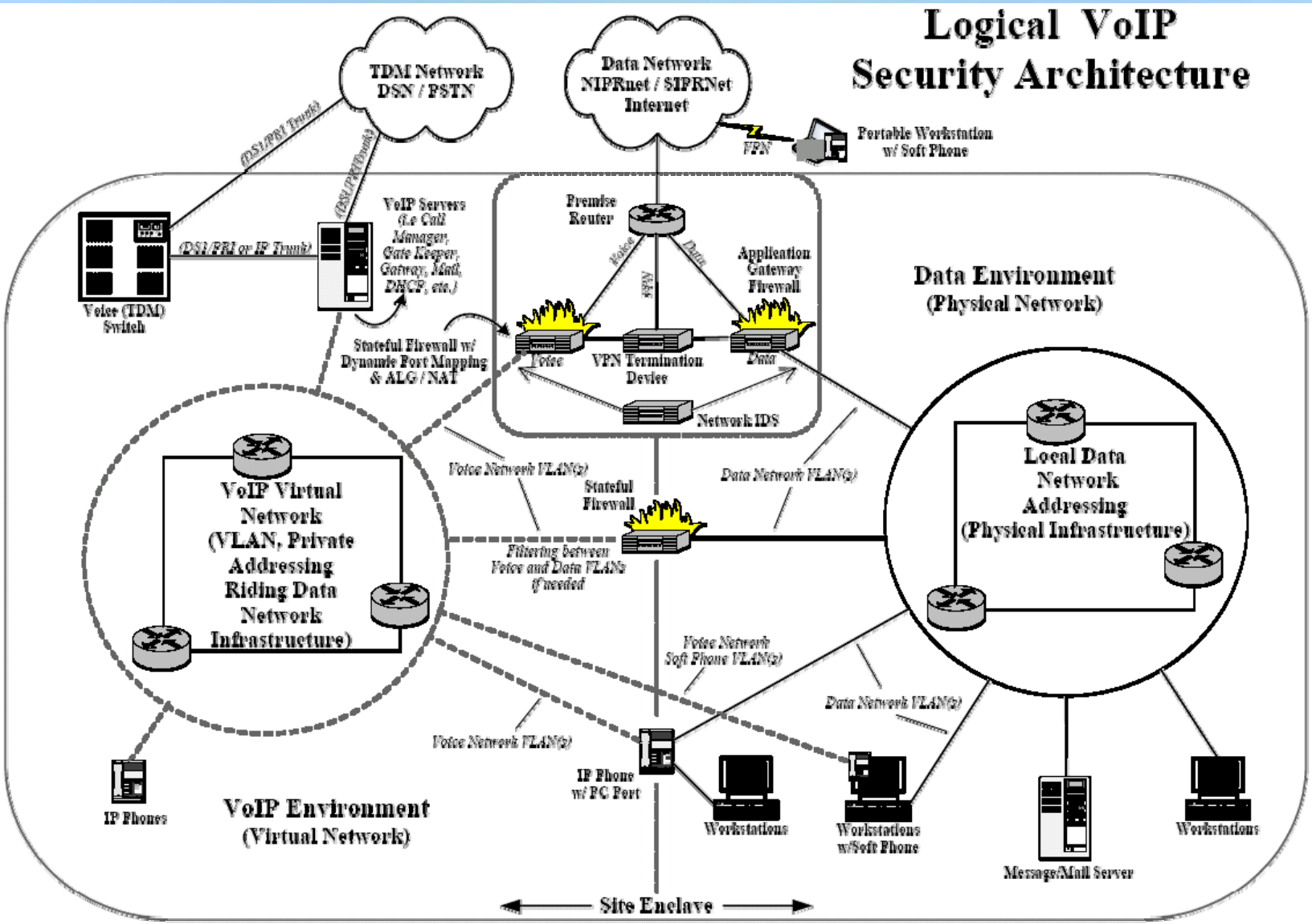
Usciamo dalla LAN
Infrastruttura distribuita



Servizi + Voce in sicurezza nella LAN



La visione “DISA” della sicurezza VoIP



Le funzionalità correnti e future dei prodotti VoIP

	IP PBX	IP Contact Center	VoIP Phone	Soft Phone	EMG	Signailing GW	MS	BSG FW	VoIP Appl.
Cifratura	😐	😐	☺	☺	☺	😐	☺	☺	😐
IP SEC	😐	😐	☹	☹	😐	😐	😐	☺	☺
TLS	😐	😐	☺	😐	😐	😐	😐	☺	😐
S-MIME	😐	☹	☹	☹	☹	☹	☹	☺	☹
Auth HTTP Digest	😐	☹	☺	☹	☹	**NA**	☹	☺	☺
Secure RTP	😐	😐	😐	😐	😐	**NA**	😐	☹	☹

Fornitori di “sicurezza” VoIP

Figure 1 Leading Service Providers For IPT Managed Services And Security

	Major IPT partners	IPT security services	Security team	Comments
AT&T Business Services	Cisco, Avaya, Nortel Networks, Alcatel, Siemens	Managed security services, business continuity, IP PS	Integrated into all PS teams across all products	Comprehensive services on multi-IPT products; consultative approach
Avaya	Avaya/others on multivendor network platforms	Secure access control and managed security	Dedicated services for voice security	Partners with VeriSign, SecureLogix, and McAfee; broad voice experience
IBM Global Services	Major partner Cisco; also Avaya, Nortel Networks, Alcatel	Managed and outsourced IPT services	Combines security specialists with IPT teams	Extensive managed services across life cycle; customized offerings
INS	Primarily Cisco, but vendor-neutral	Consulting firm provides a full range of services	More than 120 consultants with CISSP certification	For internal-based solutions that offer a full range of network value-added services
NetSolve	Primarily Cisco; also partners with IBM and AT&T	Firewall monitoring; end-to-end infrastructure management	Team up IPT and security engineers	Integrate security with voice and data infra-structure; large IPT security practice
SecureLogix	Key partnership with Avaya; supports others	Provides security management tools for the perimeter	Dedicated team for telecom security services	Security product is adjunct to data firewalls for voice; uses partners for service
Sprint	Cisco and Nortel Networks	Fully managed premise-based IPT security services	Large security team with CISSP, CCSP certifications	Secure, flexible NW solutions, integrated wireline and wireless solutions
VeriSign	Supports Avaya, Nortel Networks, and Cisco	Views IPT as integral part of end-to-end solution	Security is overlay to consulting team	Integrate services with security as one component; acquired Guardent in 2004

Source: Forrester Research, Inc.

Conclusioni

- **Sfide imposte da VoIP e corrispondenti “best practies”**
  - Controllo Accessi
    - VLAN separate per dispositivi VoIP
  - Autenticazione
    - Utilizzo di certificati X.509 e firma digitale
  - Disponibilità
    - Utilizzo di Firewall Statefull tra la rete Voce e quella Dati
  - Integrità
    - Utilizzo di Host & Network IDS
  - Privacy
    - Servizi di disabilitazione dell’ID del chiamante
    - Servizi di Magistratura per indagini