IP Telephony & Sicurezza: La soluzione esiste

Uno dei principali fattori di spinta nell'evoluzione del Networking di questi anni è la cosiddetta Convergenza, ovvero la visione di una singola piattaforma di comunicazione aperta per il trasporto di voce, video e dati, che abiliti e semplifichi le interazioni tra singoli utenti ed organizzazioni indipendentemente dagli strumenti utilizzati o dal luogo in cui ci si trovi. Una visione di alto livello con allettanti implicazioni quali:

- abilitazione di servizi innovativi, a beneficio di nuovi livelli di produttività e flessibilità delle organizzazioni
- consolidamento delle infrastrutture di comunicazione
- riduzione dei costi operativi di gestione e manutenzione

Un fondamentale elemento costitutivo di questo scenario è certamente rappresentato dalla Telefonia su IP, o *IP Telephony*. Il principio di funzionamento dell'*IP Telephony* consiste nel digitalizzare in tempo reale il contenuto delle conversazioni telefoniche trasformandolo in un flusso di pacchetti dati che insieme ai relativi messaggi di segnalazione viene appunto instradato e gestito sulla stessa infrastruttura di rete IP utilizzata per il trasporto dei dati. Una soluzione già oggi adottata da molte organizzazioni, visto che IDC stima un mercato della telefonia IP che in Europa entro la fine di quest'anno varrà oltre 1 miliardo di Euro. Ma è altrettando interessante il fatto che per quest'area del comparto ICT è prevista una consistente crescita di oltre il 70% all'anno anche nei prossimi anni, allorchè un numero sempre maggiore di aziende ed organizzazioni coglierà i vantaggi e la riduzione dei costi operativi associati a questa tecnologia; tra cui:

- riduzione dell'investimento altrimenti necessario per realizzare due reti fisicamente e tecnologicamente distinte, una per la voce e una per i dati;
- minori costi associati alla maggior semplicità di gestione per le modifiche delle utenze e l'espansione di nuove sedi o nuovi utenti;
- economie di scala nella gestione centralizzata delle chiamate, anche di sedi remote
- riduzione dei costi e dei tempi legati all'introduzione di nuovi servizi e applicazioni, su una piattaforma IP nativamente predisposta, invece che sistemi PBX proprietari.

In effetti qualunque organizzazione si trovi oggi a sostituire il proprio centralino tradizionale non può prescindere dal prendere quantomeno in considerazione questa tecnologia, e secondo il Gartner Group nell'arco dei prossimi 3 anni si assisterà al cross-over della Telefonia IP rispetto alla telefonia tradizionale in termini di basi installate.

Se dunque i benefici applicativi di questa nuova tecnologia di comunicazione sono più che evidenti, è importante acquisire altrettanta consapevolezza delle implicazioni di Sicurezza legate all'introduzione della Telefonia IP nelle reti aziendali. Parte di queste implicazioni sono inevitabilmente ereditate dalle reti dati a cui un sistema *IP Telephony* si appoggia; vediamone alcune e quelle che sono le tecniche di contenimento dei problemi di sicurezza.

La ***disponibilità*** è la prima considerazione da fare, dato che la convergenza di voce e dati fa sì che sulla stessa infrastruttura siano condensate due reti storicamente disgiunte. Ad oggi le reti dati possono avere eccellenti livelli di ridondanza e disponibilità, anche a beneficio delle applicazioni di Telefonia IP. In effetti, se implementate correttamente, le soluzioni *IP Telephony* sono di per sè più affidabili di quelle centralizzate tradizionali (PBX): l'utilizzo di cluster di più *call manager*, o di funzionalità di backup insite nella rete (SRST - *Survivable Remote Site Telephony*) opportunamente ridondata, consentono un'affidabilità architetturale superiore all'affidabilità di apparato cui si è abituati per le soluzioni di telefonia classica. Se dunque le due reti convergono **fisicamente** sulla stessa infrastruttura, **logicamente** queste restano separate, anzi, la ***separazione*** virtuale fra le due realtà è una considerazione molto importante. Con tecnologie di Virtual LAN (VLAN) e separazione di livello 2 si ha la possibilità di attestare sulla stessa infrastruttura le due applicazioni con politiche di traffico e di sicurezza differenti, come è necessario dato il diverso tipo di traffico

che viaggia sulle due. Da una parte il traffico dati, a cui va dato un certo livello di priorità anche in dipendenza delle specifiche applicazioni, e dall'altra il traffico voce, che invece deve viaggiare a massima priorità trattandosi di un'applicazione ***real-time***, in cui parametri trasmissivi come la ***latenza*** e il ***jitter*** sono assolutamente critici**.** Si vuole, inoltre, che il traffico voce, che nella quasi totalità delle implementazioni viaggia in chiaro, resti virtualmente separato dal segmento dove viaggiano normali dati e dove l'utenza è attestata, minimizzando così la possibilità di intercettazioni telefoniche portate a termine con analizzatori di protocollo o ***sniffers***. Ad oggi, l'utilizzo di VLAN offre un ottimo livello di sicurezza nella separazione dei dati, grazie alle ormai mature tecnologie di livello 2 per la separazione e la prevenzione di attacchi. Si hanno quindi tutte le possibilità per prevenire efficacemente tutti quei problemi derivanti da attacchi mirati a violare la separazione virtuale fra i due mondi, che come illustrato in un altro articolo (vedi "*VoIP: una interessante novita' con molte problematiche di sicurezza"*) si potrebbero concretizzare in ***Furto di QoS, eavesdropping,*** sfruttamento di ***Covert Channels*** e disservizi nella segnalazione, che possono portare dalla indebita redirezione delle chiamate fino a parziale e totale disservizio.

Un'altra considerazione riguarda la ***confidenzialità*** del traffico voce. Si è già detto come la voce, dopo essere stata campionata venga inviata *over IP* in chiaro. Questo apre le porte della intercettazione telefonica a chiunque abbia accesso sulla rete ad un flusso di dati voce, grazie all'ampia disponibilità di *sniffers* del traffico. Si è anche già detto come la separazione virtuale fra segmento voce e dati possa aiutare a minimizzare questo rischio, ma ovviamente un'altra opzione disponibile è la cifratura del traffico voce. Questo introduce tempi di latenza che vanno opportunamente considerati in fase di progetto, ed anche la garanzia della ***Qualità del Servizio (QoS)*** va conseguentemente riconsiderata. La *QoS* non è naturalmente un requisito cui è sufficiente trovare rispondenza a livello di singolo dispositivo, quanto piuttosto lungo l'intero percorso che un flusso di traffico Voce su IP si trova a seguire, affinchè alle due estremità di una sessione possa essere effettivamente garantita la necessaria qualità. È proprio questo requisito di supporto *End-to-End* di tutte le funzionalità e meccanismi di gestione del traffico voce su IP di un'infrastruttura di rete che entra pesantemente in gioco anche quando di una realizzazione *IP Telephony* si prendono in considerazione gli aspetti di Sicurezza. E' infatti importante poter continuare a garantire tutto questo anche laddove il traffico voce venga cifrato. Ciò è fattibile attraverso opportuni meccanismi grazie ai quali, sebbene il relativo flusso di pacchetti sia cifrato all'interno di un tunnel IPSec, al traffico voce continui ad essere garantita priorità di instradamento rispetto ad altri flussi di pacchetti. La soluzione Cisco Systems ***Voice and Video over VPN (V^{3}PN)*** indirizza esattamente questa esigenza, estendendo la convenienza della telefonia IP e la sicurezza delle VPN IPSec anche–per esempio– a lavoratori remoti che dispongono di normale connettività xDSL.

Resta ancora da considerare la vulnerabilità applicativa dei server su cui si basa l'intera gestione dell'applicazione di telefonia IP. Il controllo della chiamata viene infatti processato da un'applicazione che in molte implementazioni risiede su un sistema operativo *general purpose*. Di quest'ultimo, ovviamente, l'applicazione di *call control* rischia diereditare le vulnerabilità. Oggi le soluzioni più avanzate prevedono la possibilità di utilizzare su questo genere di server uno strato software con funzionalità tipiche di *host intrusion detection* (H-IDS), personal firewall e antivirus, in modo da costruire uno scudo virtuale a garanzia della stabilità, integrità e disponibilità di server così critici. Il server di gestione delle chiamate viene così *"blindato"* e configurato per eseguire solo le operazioni strettamente legate all'applicazione specifica di gestione del sistema di telefonia IP. Grazie a tecnologie di *intrusion protection* di ultima generazione basate su analisi euristico-comportamentali e prevenzione di azioni potenzialmente pericolose a livello del sistema operativo, senza bisogno di alcun aggiornamentoè così possibile minimizzare i pericoli potenzialmente derivanti dall'utilizzo per applicazioni critiche come la telefonia IP di sistemi operativi generici, che potrebbero altrimenti risultare vulnerabili a worm, virus e attacchi di tipo *Denial-of-Service* (DoS).

Anche il filtraggio del traffico voce al momento in cui attraversa un firewall è un aspetto molto importante, e considerato critico e difficoltoso fino a poco tempo fa. In realtà con l'ultima

generazione di firewall grazie alla loro potenza ed elevata intelligenza di sistema, l'accoppiata VoIP/Firewall è oggi meno critica. Un firewall molto diffuso sul mercato come il Cisco PIX è già oggi ad esempio in grado di trattare e filtrare il traffico voce alla stregua di ogni altro tipo di traffico, introducendo tempi di latenza trascurabili. Per le ragioni su esposte quest'ultimo aspetto risulta poi di particolare importanza nel qualificare un firewall rispetto ai suoi livelli di integrazione nativa con una soluzione di telefonia IP.

Altre considerazioni riguardanti i sistemi di telefonia IP e le loro implicazioni di sicurezza possono poi essere ricondotte a più generali *best practices* per il miglior contenimento di rischi su di una rete IP, trattandosi ovviamente di indicazioni e pratiche di utilizzo che finiscono per andare a beneficio della soluzione *IP Telephony*, oltre che della rete su cui questa si basa.

Un discorso a parte merita il trittico IP Telephony, Wireless e Sicurezza. Se il mix si presenta quanto mai appetibile, ricadono in esso considerazioni di sicurezza giá valide per le wireless LAN. Su questi tipi di terminale, per contenere al massimo i ben noti limiti di sicurezza dello standard wireless e' bene implementare accorgimenti e tecnologie come la configurazione automatica della separazione dei segmenti voce/dati (***automatic IEEE 802.1q configuration***), estensioni ***802.1x*** per l'autenticazione del terminale stesso, cifratura ***WEP 40/128bit*** gia a bordo ed una opzionale password di blocco dell'apparecchio. Il terminale ***VoIP Wireless*** 7920 prodotto da Cisco Systems incorpora queste funzionalita' atte a minimizzare i rischi dell'unione di IP Telephony e WLAN.
In effetti tutto quanto fin qui considerato concorre proprio a definire un quadro complessivo in cui è quantomai indispensabile che l'approccio alla sicurezza delle implementazioni *IP Telephony* faccia riferimento alle più aggiornate ed autorevoli *best practice* relative al progetto di reti IP convergenti intrinsecamente sicure. In sintesi, questi i **criteri** a cui in generale si riferiscono queste linee guida:

- protezione globale -non dei singoli dispositivi o sistemi-, combinando diverse funzionalità e componenti di Sicurezza che agendo su fronti diversi e complementari garantiscano i desiderati livelli di protezione, controllo e gestione del rischio;
- stretta integrazione, supporto ed interoperabilità *end-to-end* delle funzionalità *IP Telephony* tra le componenti di Sicurezza e la stessa infrastruttura di rete IP;
- architetture di Sicurezza multilivello, in modo da prevenire la compromissione dell'intera infrastruttura nell'evenienza in cui un singolo sistema venga compromesso.

L'attuazione di queste linee guida per la securizzazione di sistemi di telefonia IP porta quindi alla definizione di tre **componenti chiave** di un progetto:

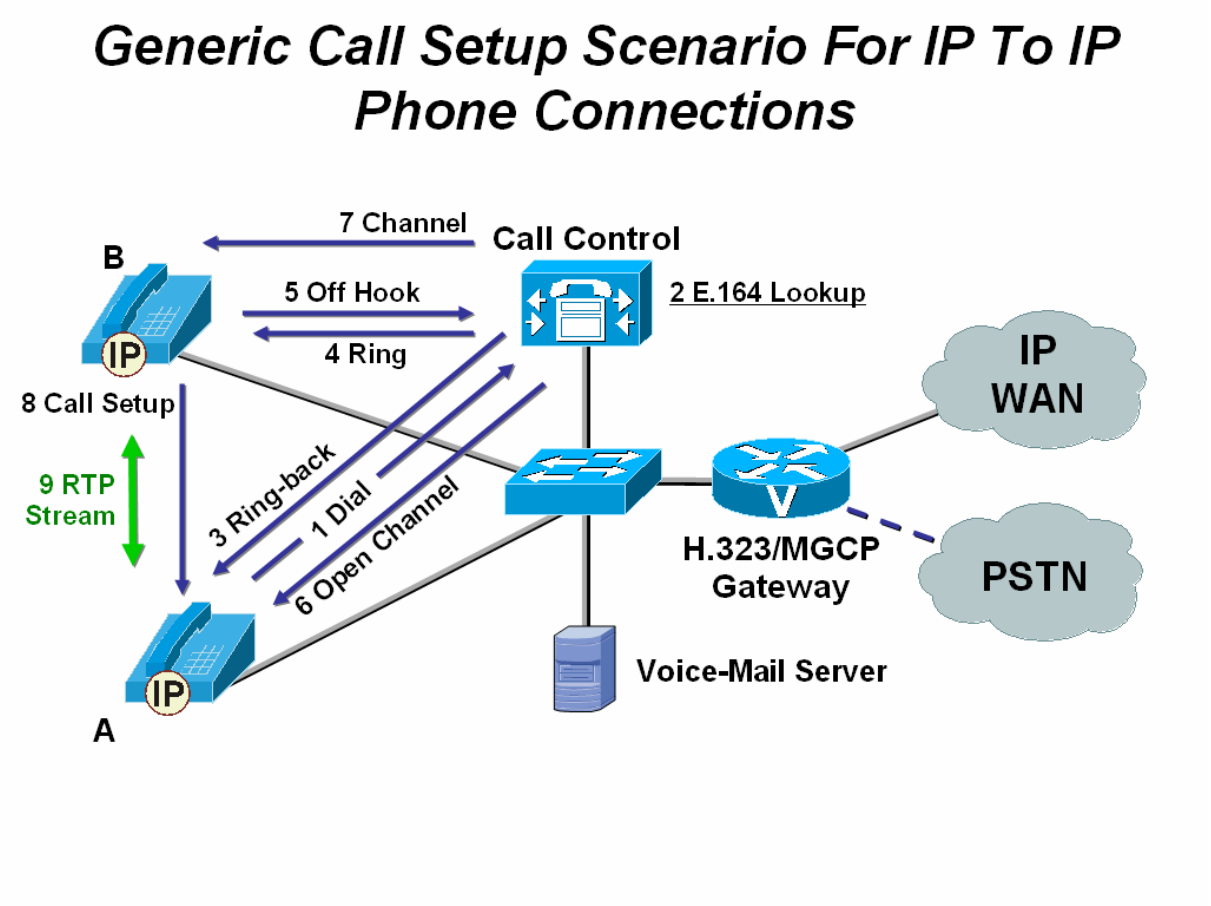
1. Elementi di sicurezza perimetrale, per la segregazione di opportune sezioni di rete tramite la quale sia possibile controllare che solo i legittimi dispositivi e applicazioni abbiano accesso a risorse particolarmente critiche, come un *call manager*;
2. Elementi per la risevatezza delle comunicazioni e della sicurezza delle connessioni, tramite meccanismi di autenticazione e opportuna segmentazione del traffico dati rispetto al traffico voce in ambito locale (LAN), e l'impiego di VPN - *Virtual Private Network* con supporto della *Quality of Service* per il traffico voce in ambito geografico (WAN).
3. Elementi di Intrusion Protection -sia sugli specifici segmenti di rete interessati, sia sui server critici su cui risiedono le applicazioni Voce-, a cui è affidata l'analisi in tempo reale del contenuto e del contesto dei singoli pacchetti per controllare tentativi di intrusione o attività sospette.

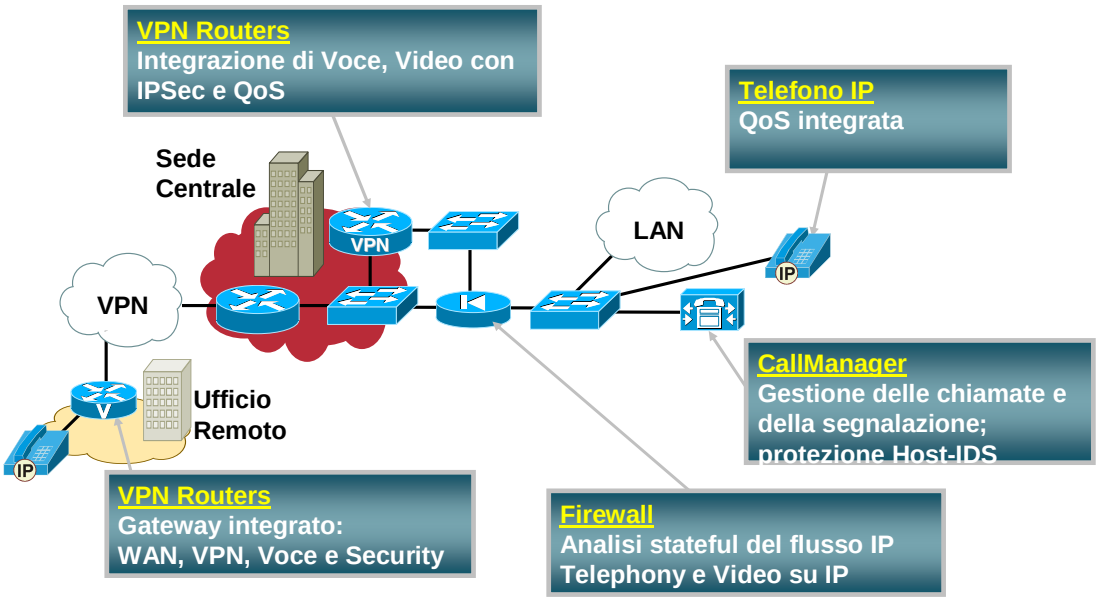
Le considerazioni sin qui esposte portano dunque alla logica conclusione che qualunque strategia premiante per la sicurezza dei sistemi *IP Telephony* non può prescindere da un più ampio approccio al disegno delle moderne reti convergenti su IP. Un approccio in cui Sicurezza, funzionalità di rete e nuove tecnologie sono nativamente integrati.

Referenze:

Cisco SAFE IP Telephony Security in Depth:
http://cisco.com/go/SAFE

Cisco Voice and Video over VPN
http://cisco.com/go/V3PN




VPN Routers
Integrazione di Voce, Video con IPSec e QoS
Telefono IP
QoS integrata
Sede Centrale
VPN
LAN
IP
VPN
Ufficio Remoto
IP
CallManager
Gestione delle chiamate e della segnalazione; protezione Host-IDS
VPN Routers
Gateway integrato: WAN, VPN, Voce e Security
Firewall
Analisi stateful del flusso IP Telephony e Video su IP