## Configurazione di rete

Nella realizzazione di una videoconferenza su rete IP uno dei primi problemi che ci trova a dover superare è rappresentato dal fatto che il collegamento tra le reti interne delle varie organizzazioni e il mondo Internet è realizzato con Firewall e dispositivi che implementano il NAT (Network Address Translation) che bloccano le chiamate video e voce su IP. In particolare:

- I Firewall bloccano il traffico IP relativo a voce e video interponendo una barriera contro ogni comunicazione non richiesta ("unsolicited") proveniente dall'esterno.
- I dispositivi che implementano il NAT bloccano il traffico IP visto che gli apparati posti all'interno del NAT stesso usano indirizzi IP privati e quindi non indirizzabili al di fuori del loro dominio locale.

I protocolli voice e video IP-base, come H.323, richiedono terminali in grado di stabilire tra loro canali di comunicazione audio-video usando indirizzi IP e porte dati. In questa situazione si presenta un problema: i terminali devono restare in ascolto (listening) per le chiamate entranti in modo da poter stabilire la connessione IP, ma il Firewall è generalmente configurato in modo da non lasciar passare i pacchetti che non siano stati espressamente richiesti. Anche se l'amministratore di rete lasciasse aperta una porta per ricevere la segnalazione della chiamata, la 1720 designata come "well-known TCP port", i protocolli di Video Comunicazione e voice su IP necessitano di ulteriori porte aperte per ricevere i messaggi di controllo e aprire il canale audio e il canale video. Gli identificativi di queste ulteriori porte sono determinati dinamicamente, non a priori, ciò implica che l'amministratore di rete dovrebbe aprire tutte le porte sul Firewall per permettere la Video Comunicazione e le applicazioni voice su IP, disabilitando di fatto il Firewall. Uno scenario così prospettato non troverebbe del tutto applicazione perché elimina le politiche di sicurezza della rete. Anche il NAT crea un ostacolo per le comunicazioni video e voice su IP. Il NAT permette ad una organizzazione di assegnare indirizzi IP privati sulla rete locale, LAN, ma i router che controllano il flusso dati verso Internet possono spedire solamente pacchetti con indirizzi 'routable' o IP pubblici. Un terminale che si trova dietro al NAT, sulla LAN, può iniziare una comunicazione verso ogni altro terminale sulla stessa LAN perché gli indirizzi IP all'interno della LAN sono routable, cioè è possibile avere delle sottoreti all'interno di una organizzazione gestite da un router interno che permette di stabilire una comunicazione audio-video su rami diversi della sottorete. Essendo i loro indirizzi privati, quindi non indirizzabili all'esterno del NAT, i terminali sulla LAN non possono essere raggiunti da chiamate provenienti dall'esterno. Anche se i terminali all'interno del NAT iniziano una chiamata verso un terminale esterno, si presenta ancora un problema. Quando inizia la chiamata, infatti, l'indirizzo IP del terminale chiamante è contenuto nel payload del pacchetto spedito. Il terminale di destinazione riceve i pacchetti di setup della chiamata, li esamina ed inizia a trasmettere audio e video verso il terminale da cui ha ricevuto la chiamata e di cui ottiene l'indirizzo IP esaminando il payload dei pacchetti ricevuti. Se questo indirizzo IP è privato, il router di accesso ad Internet scarterà i pacchetti audio e video inviati dal terminale esterno al NAT verso il terminale interno perché spediti verso indirizzi IP non-routable. La connessione tra i due terminali sembra riuscita, ma in realtà il terminale all'interno del NAT non riceve mai l'audio ed il video del terminale esterno.

**Soluzione per il problema NAT-Firewall**
Esistono molte soluzioni per superare il problema delle comunicazioni IP attraverso il NAT e il Firewall:

- **Apparato di Videoconferenza pubblico**
  la soluzione limite è quella di aggirare completamente questi dispositivi. Poiché i sistemi di videoconferenza hanno solitamente indirizzi IP privati non raggiungibili da router esterni, l'amministratore di rete può definire un NAT statico (una associazione permanente tra un indirizzo IP privato e un indirizzo IP pubblico riservato per la videoconferenza H.323 aperto sulle porte necessarie alla videocomunicazione ) per ogni terminale che necessita di essere raggiunto da connessioni esterne. In questo caso il NAT sostituisce l'indirizzo IP statico, D, nell'intestazione e nel Payload del pacchetto di Setup inviato dal terminale interno verso il terminale esterno. Il terminale di destinazione utilizza l'indirizzo pubblico D presente nel Payload per indirizzare i pacchetti di risposta, questi vengono rispediti verso il terminale chiamante attraverso l'indirizzo IP del NAT. In alternativa, laddove è possibile, si può assegnare all'apparato di videoconferenza un indirizzo IP pubblico, aperto sulle porte necessarie alla comunicazione H323/SIP.
- **Apparati NAT/Firewall H323 Compatibili**
  L'unico apparato che non crea nessuno dei problemi esposti è un apparato NAT/Firewall H.323 compatibile. In questo caso il Firewall non blocca la porta TCP 1720 e permette il passaggio anche sulle altre porte H.323 determinate dinamicamente.
- **Firewall ALG**
  Gli Application Level gateways (ALG) sono Firewall programmati per riconoscere specifici protocolli IP, come H.323. Invece di guardare solo all'informazione contenuta intestazione dei pacchetti per determinare se trasmetterli o bloccarli, gli ALGs analizzano nel dettaglio i dati contenuti nel Payload del pacchetto stesso. Il protocollo H.323 inserisce importanti informazioni di controllo nel Payload dei pacchetti, ad esempio gli identificativi delle porte audio e video sulle quali il terminale si aspetta di ricevere la connessione audio e video dal terminale remoto che sta chiamando. Analizzando quali porte il terminale andrà ad utilizzare, l'ALG apre dinamicamente solo quelle che vengono effettivamente utilizzate dall'applicazione H.323, lasciando chiuse le altre e garantendo così la sicurezza della rete.

**La Soluzione Firewall Traversal di Regione Toscana**
Una ulteriore soluzione al problema della comunicazione in videoconferenza attraverso NAT e Firewall è quella di uscire in connessioni semi-tunneling.
A tal fine Regione Toscana ha acquisito un sistema di Firewall Traversal con il quale, di fatto, si realizza una serie di "VPN H.323" con topologia stellare; i tunnel vengono instaurati da una componente "Client FT" da installare dietro ogni NAT/Firewall di accesso alla rete e terminati su un "Server FT" installato presso la Sede Centrale.
Il Server lavora in coppia con un "Client", da installare su un PC "dedicato" dietro il Firewall di ogni sito remoto.
Il "Server" si occupa di processare la segnalazione ed i flussi Audio/Video tra la rete privata della Sede Centrale ed ogni sito remoto in cui è presente un "Client", gestendo le comunicazioni su una specifica porta del Firewall, che diventa l'unica porta di comunicazione tra le due componenti. Ciò permette all'Amministratore di rete una facile configurazione del Firewall, aprendo una sola porta per la connessione delle sue componenti del "Firewall Traversal" e garantendo quindi la sicurezza della rete.