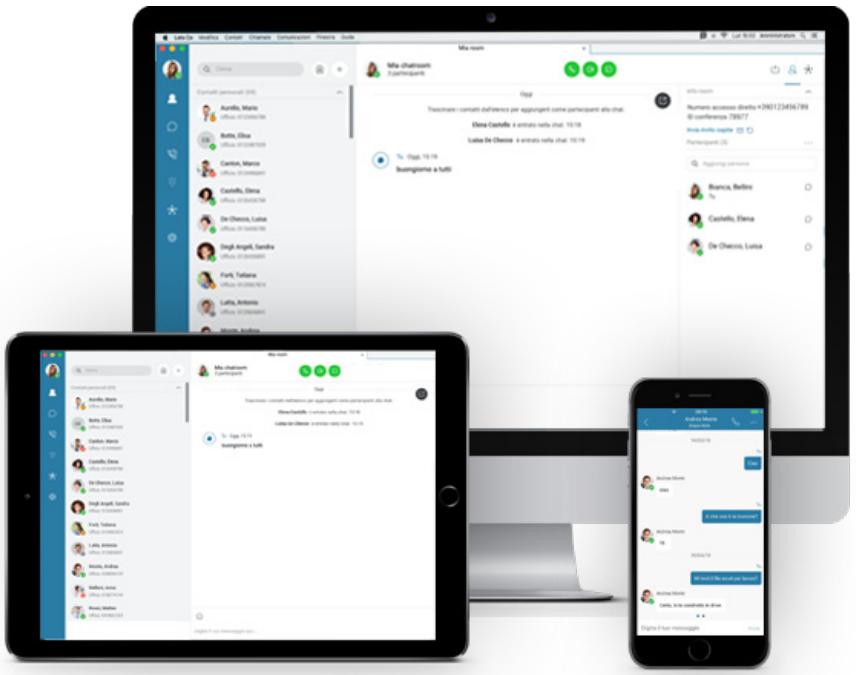
Let'sCo

Communication and Collaboration



REQUISITI MINIMI DI RETE

SOMMARIO

Premessa

Let's Co è la soluzione di Collaboration e Communication erogata in Cloud mediante differenti infrastrutture informatiche dislocate su diverse sedi nel mondo. Il servizio è costituito da più componenti, tra cui applicazioni vocali, video, desktop e mobili, applicazioni web e strumenti di controllo e monitoraggio della qualità del servizio.

Questi componenti richiedono la comunicazione tra i dispositivi nella rete locale del cliente (LAN) verso l'infrastruttura Let's Co; tali comunicazioni avvengono attraverso connessioni internet pubbliche (WAN) o mediante connessioni di rete private (MPLS).

Affinché queste comunicazioni funzionino correttamente, le connessioni delle reti interne ed esterne del cliente devono rispettare dei requisiti minimi e i dispositivi di protezione installati presso la sede del clienti, come i firewall, non devono bloccare gli indirizzi IP e le porte dei servizi TCP / UDP utilizzati dal servizio Let's Co.

Le seguenti sezioni di questo documento forniscono informazioni necessarie per dimensionare correttamente le connessioni e configurare correttamente il firewall cliente per consentire tutte le comunicazioni tra i dispositivi e le applicazioni cliente verso i servizi Let's Co.

Vista la natura tecnica delle argomentazioni trattate nel presente documento consigliamo di affidare il presente documento al referente dei sistemi informatici aziendali o all'azienda esterna incaricata. Il presente documento unitamente all'offerta commerciale è da considerarsi parte integrante delle condizioni generali e viene richiamato al punto 14 e 16 delle condizioni generali stesse.

ATTENZIONE: La mancata o errata configurazione dei dispositivi di rete può causare anomalie nel funzionamento di Let's Co e incidere nella qualità del servizio.

ATTENZIONE: Si raccomanda l'utilizzo di un sistema firewall opportunamente configurato che sia in grado di proteggere la rete aziendali e i dispositivi collegati a Let's Co scongiurando cosi problematiche di sicurezza e frodi.

REQUISITI TECNICI

La progettazione e la configurazione della rete del cliente sono caratterizzate da molte variabili, che possono influenzare le prestazioni e la qualità del servizio VoIP (Voice over IP). Affinché il servizio VOIP Let's Co funzioni nella maggior parte degli ambienti di rete dei clienti, ci sono una serie di requisiti minimi che tale rete deve soddisfare per garantire il funzionamento del servizio come previsto. Questi requisiti si applicano sia ai telefoni SIP che agli adattatori analogici (ATA), da qui in avanti generalmente definiti come dispositivi VOIP.
Di seguito, il riepilogo dei requisiti minimi richiesti:

- ✓ La rete LAN del cliente deve contenere un server DHCP capace di fornire all'avvio un indirizzo IP ai dispositivi VOIP.
- ✓ La rete LAN del cliente deve contenere un server DNS o deve poter fornire un inoltro DNS per la risoluzione degli URL utilizzati dai dispositivi VOIP per comunicare con piattaforme di servizio esterne.
- ✓ Il server DNS deve essere in grado di risolvere sia i record SRV sia i record A.
- ✓ Il firewall del cliente deve consentire il traffico HTTP (porta TCP 80) e HTTPS (porta TCP 443) ai dispositivi VOIP per comunicare con server esterni di configurazione.
- ✓ Il firewall del cliente deve permettere il traffico SIP e RTP affinché i dispositivi VOIP possano effettuare e ricevere chiamate.
- ✓ Il router del cliente deve impostare il tempo di persistenza del NAT a un valore maggiore o uguale a 45 secondi.
- ✓ Il router/firewall del cliente non deve manipolare i pacchetti SIP o RTP a livello di applicazione. Se qualsiasi dispositivo CPE può funzionare come gateway di accesso a livello SIP (ALG), la funzionalità ALG deve essere disabilitata.
- ✓ Il router del cliente deve supportare DSCP (Differentiated Service Code Point) e garantire che i pacchetti con maggiore priorità abbiano la precedenza su tutti gli altri pacchetti in uscita.
- ✓ Il router del cliente deve essere configurato per contrassegnare con priorità alta tutti i pacchetti SIP e RTP dalle piattaforme di controllo delle chiamate Let's Co così da garantire che questi abbiano la massima priorità su tutti gli altri pacchetti in entrata. Le piattaforme di monitoraggio delle chiamate Let's Co possono essere identificate in modo univoco da un insieme di indirizzi IP specifici. I pacchetti SIP e RTP possono essere individuati dalle porte indicate nella sezione Firewall di questo documento.
- ✓ La larghezza di banda Internet del cliente deve essere proporzionata in modo da consentire la quantità minima di larghezza di banda dati richiesta oltre al numero totale di chiamate vocali simultanee richieste dall'ufficio.
- ✓ Le dimensioni della rete locale (LAN) del cliente devono essere proporzionata in modo da consentire la massima quantità di larghezza di banda dati richiesta oltre al numero totale di chiamate vocali simultanee richieste dall'ufficio.

Server DHCP

Il protocollo DHCP (Dynamic Host Configuration Protocol) è un protocollo utilizzato dai dispositivi collegati in rete per ottenere vari parametri necessari per far sì che i dispositivi operino in una rete IP. I parametri DHCP forniti dal server DHCP del sito e necessari per il corretto funzionamento del servizio Let's Co sono l'indirizzo IP, la Subnet mask, il gateway predefinito e il server DNS.

I server DHCP sono generalmente integrati nel router del cliente, ma possono essere un server autonomo dedicato esclusivamente alla funzione DHCP. Per la maggior parte delle applicazioni a banda larga, il server DHCP sarà integrato nel router a banda larga fornito dal service provider. In questo caso, la configurazione del server DHCP (incluso il fatto che sia attivato o disattivato) può essere controllata accedendo al router a banda larga.

Tutti i dispositivi VOIP Let's Co sono configurati di default per ottenere informazioni sull'indirizzo IP e sul server DNS da un server DHCP locale. Quando un dispositivo VOIP viene avviato, tenta di individuare il server DHCP locale e di ottenere queste informazioni. Se la rete del cliente non contiene un server DHCP o non fornisce le informazioni richieste, il dispositivo VOIP non si avvierà correttamente e sarà inutilizzabile.

Alcuni server DHCP forniscono “opzioni” come parte della risposta alla richiesta di un client. Per quanto riguarda le applicazioni SIP, l'opzione 66 viene comunemente utilizzata per fornire al client, in questo caso un dispositivo VOIP, l'indirizzo del server di configurazione che deve contattare per ottenere la sua configurazione. Nel caso del servizio Let's Co, questa opzione non è richiesta. Tutti i dispositivi VOIP Let's Co sono codificati per puntare all'indirizzo di uno specifico server di configurazione e se un'opzione 66 viene ricevuta dal dispositivo VOIP in risposta a una richiesta DHCP, il dispositivo VOIP la ignorerà.

Server DNS

Il DNS (Domain Name System) è un servizio Internet che traduce i nomi di dominio in indirizzi IP. Fornisce un metodo per denominare i dispositivi di rete con parole, che sono più facili da ricordare rispetto ad un indirizzo IP numerico. Inoltre, alcuni tipi di record DNS sono in grado di associare una singola parola a un elenco di indirizzi IP. Tutti i dispositivi VOIP Let's Co richiedono il DNS per tradurre i nomi di dominio in indirizzi IP.

Durante il processo di avvio, il nome del dominio del server di configurazione del dispositivo VOIP viene tradotto in modo che il dispositivo VOIP possa individuare e ricevere le informazioni di configurazione dal server di configurazione corretto.

Inoltre, una volta che il telefono ha completato il processo di avvio, il nome del dominio dei server per il controllo delle chiamate viene tradotto in modo che il dispositivo VOIP possa individuare e comunicare con questi server. Se un server DNS non è disponibile per fornire la traduzione del nome, il dispositivo VOIP non si avvierà correttamente e sarà inutilizzabile.

Esistono diversi tipi di record DNS. Il servizio Let's Co utilizza record “A” (indirizzo) e “SRV” (servizio). I record “SRV” vengono utilizzati per fornire un meccanismo di ridondanza per le piattaforme di controllo delle chiamate. Affinché Let's Co funzioni correttamente, i due record devono essere supportati sulla rete del cliente.

Server NTP

Il Network Time Protocol, in sigla NTP, è un protocollo per sincronizzare gli orologi dei computer e dei dispositivi VOIP all'interno di una rete a commutazione di pacchetto, quindi con tempi di latenza variabili ed inaffidabili. L'NTP è un protocollo client-server appartenente al livello applicativo ed è in ascolto sulla porta UDP 123.

Let's Co gestisce le sorgenti NTP durante la configurazione automatica del telefono VOIP, questi ultimi non saranno in grado di completare il loro ciclo (iniziale o costante) di aggiornamento della configurazione senza una risorsa NTP.

FUNZIONALITÀ E APPLICAZIONI DI ROUTING

Network Address Translation

Il NAT (Network Address Translation) è una funzione comune dei router che consente a molteplici indirizzi IP privati su una rete LAN di essere tradotti in un unico indirizzo IP pubblico sulla rete WAN. La ragione principale dell'esistenza della funzionalità NAT è la conservazione degli indirizzi IP pubblici. Non ci sono abbastanza indirizzi IP all'interno del protocollo IPv4 per consentire a ogni computer connesso a Internet di avere un indirizzo IP pubblico univoco. Inoltre, la funzionalità NAT fornisce ai dispositivi un livello di sicurezza aggiuntiva tramite gli indirizzi IP privati, poiché tali dispositivi spesso non sono indirizzabili pubblicamente.

Anche se necessaria, la funzionalità NAT crea problemi per il traffico VOIP. Il NAT comunemente traduce solo le informazioni IP da private a pubbliche a livello TCP/IP. Tuttavia, non traduce alcuna informazione sull'indirizzo IP a livello di application layer. Ciò significa che tutte le informazioni sull'indirizzo IP nel payload dell'application layer dei pacchetti VOIP non vengono tradotte. Dato che questi indirizzi sono privati, non sono instradabili in un dominio pubblico e sono effettivamente irraggiungibili. Nel caso del SIP, l'indirizzo IP e la porta, che il dispositivo VOIP comunica per stabilire la connessione, sono presenti nel payload del SDP allegato ai messaggi SIP. Se queste informazioni non vengono tradotte, dall'altra estremità della linea non saranno in grado di comunicare con il dispositivo VOIP. Questo, di solito, crea un fenomeno comunemente noto come RTP a senso unico, ovvero il percorso vocale è disponibile solo in una direzione.

Un altro problema con la funzionalità NAT è che i dispositivi privati non sono raggiungibili pubblicamente a meno che non venga creata una traduzione, comunemente indicata come bind, tra l'indirizzo IP privato e l'indirizzo IP pubblico. Questo avviene ogni volta che un dispositivo privato tenta di comunicare con un dispositivo pubblico. L'atto di richiedere la comunicazione fa sì che il NAT crei un collegamento temporaneo tra l'indirizzo IP privato che richiede la comunicazione e l'IP pubblico con il quale sta tentando di comunicare. La durata del binding è controllata da un timer che scade e fa sì che il binding venga rimosso se c'è un periodo di inattività pari alla lunghezza del timer. Mentre il binding è attivo, la comunicazione da pubblico a privato è possibile, ma una volta che il binding diventa inattivo, il dispositivo privato non è più raggiungibile pubblicamente. Solitamente questo timer dura tra i 30 e i 60 secondi. Inoltre, i binding possono essere spesso configurati in modalità statica sul NAT. Questa funzionalità viene indicata come port forwarding. In questa modalità, il NAT viene configurato con un binding permanente tra un indirizzo pubblico e privato.

Con il servizio Let's Co, si affrontano le sfide derivate dalla presenza del NAT. Una tecnica chiamata NAT Traversal viene utilizzata per superare i problemi creati dal NAT. Parte della piattaforma di controllo delle chiamate Let's Co è responsabile del mantenimento della comunicazione costante con tutti i dispositivi VOIP.

Questa comunicazione costante garantisce che il timer del NAT non scada mai, rendendo il collegamento dinamico di fatto permanente. Senza questo, un dispositivo VOIP in una rete privata non sarebbe in grado di ricevere chiamate. Inoltre, la piattaforma di controllo delle chiamate Let's Co utilizza una tecnica chiamata Media Relay per risolvere il fatto che il NAT non manipola le informazioni sull'application layer. Questa funzionalità consente alla piattaforma di controllo delle chiamate di rilevare l'indirizzo IP pubblico e la porta del flusso RTP una volta che il dispositivo VOIP invia il suo primo pacchetto RTP. La piattaforma di controllo delle chiamate esegue questa funzione su entrambe le estremità di una chiamata e le collega, trasmettendo efficacemente il traffico da un dispositivo ad un altro.
Si segnale, infine, che in presenza di un doppio NAT il servizio Let's Co potrebbe presentare malfunzionamenti. In tal caso, per risolvere il problema, occorrerà rimuovere uno dei due NAT.

Application Layer Gateway

L'ALG (Application Layer Gateway) è un metodo per manipolare le informazioni su indirizzo IP e porta usata sull'application layer. E' simile alla funzionalità NAT in quanto converte l'IP privato e le informazioni sulla porta, create da un dispositivo VOIP su una rete privata, in un IP pubblico e in informazioni sulla porta dalla parte del WAN del router che esegue la funzione ALG. Se eseguita correttamente, questa funzionalità annulla la necessità di usufruire della funzionalità di Media Relay poiché tutte le informazioni a livello di application layer sono instradabili pubblicamente.
Anche se questa funzionalità ha lo scopo di migliorare il traffico VOIP, non tutti i dispositivi ALG eseguono correttamente la conversione dei pacchetti sull'application layer. In molti casi, parti del pacchetto vengono modificate quando non dovrebbero e ciò causa problemi di funzionamento tra il dispositivo VOIP e la piattaforma di controllo delle chiamate. Se ciò accade, ALG fa sì che il dispositivo SIP non funzioni correttamente.
Con il servizio Let's Co, si consiglia di disattivare tutte le funzionalità di "Sip Aware" ovvero SIP ALG tra il dispositivo VOIP e la piattaforma di controllo delle chiamate. In questo modo, si elimina la possibilità che l'ALG traduca erroneamente pacchetti, azione che potrebbe rendere inutilizzabile il servizio. Tuttavia, in alcuni casi, questa funzionalità potrebbe non essere configurabile. Per soddisfare questa necessità, il servizio Let's Co utilizza porte non comuni per il traffico SIP e RTP. Le porte dalla 8933 alla 8943 vengono utilizzate al posto della 5060, che è comunemente usata per il SIP. Dato che la maggior parte degli ALG presumono l'uso della porta 5060 per il SIP, l'utilizzo della porta dalla 8933 alla 8943 farà sì che l'ALG ignori completamente il pacchetto e non esegua alcuna manipolazione. Inoltre, lo stesso processo vale per RTP. Sebbene non specificamente definito da uno standard, l'intervallo di porte più comunemente utilizzato per RTP è 16384-16482. Per evitare l'interazione con l'ALG, il prodotto Let's Co utilizza le porte RTP 19560-65535.

SIP Session Audit

Per proteggersi da potenziali frodi nel caso di chiamate più lunghe, la piattaforma Let's Co esegue una Session Audit ogni 15 minuti. La Session Audit invierà un messaggio UPDATE o re-INVITE SIP a seconda di cosa può supportare il dispositivo VOIP. Si prevede una risposta con 200 OK. Se non viene ricevuto tale messaggio, l'UPDATE o il re-INVITE saranno riavviati e se non viene ricevuta alcuna risposta, la chiamata sarà ritenuta non valida e verrà terminata.

Qualità del servizio

Il QOS (Quality of Service) si riferisce alla capacità di attribuire differenti priorità a varie applicazioni su una connessione di rete dati per garantire che il traffico con maggior urgenza abbia la precedenza sul resto del traffico.
Una conversazione vocale avviene in tempo reale, pertanto il traffico associato ad una chiamata vocale deve essere elaborato in modo efficiente o si verificano problemi come il clipping o l'audio discontinuo. Al contempo, il normale traffico Internet transita in modalità best-effort. Se i pacchetti vengono scartati o posticipati, solitamente il servizio non subisce interruzioni evidenti. Di conseguenza, il traffico vocale è considerato un traffico con maggiore priorità rispetto al traffico dati.
Il servizio Let's Co utilizza il DSCP (Differentiated Services Code Point), comunemente noto anche come DiffServ, per la marcatura della priorità dei pacchetti. Ogni dispositivo VOIP imposta automaticamente ogni pacchetto che invia come prioritario. Tuttavia, ciò non garantisce che tutte le apparecchiature di rete nel percorso del traffico rispettino le impostazioni e consentano al traffico vocale di avere la priorità sul traffico dati. Per garantire che i pacchetti vocali abbiano la priorità sui pacchetti dati, i router dei clienti e dell'operatore che fornisce il servizio di connettività devono essere configurati correttamente per gestire il DSCP.
Talvolta questa funzionalità viene definita Class of Service (COS) o Coda di Priorità. In entrambi i casi, si consiglia di configurare il router con una coda di priorità rigorosa, in modo che i pacchetti contrassegnati con valori DSCP più alti abbiano una priorità maggiore. Se ciò non viene eseguito correttamente, la qualità della chiamata potrebbe peggiorare notevolmente durante i periodi di traffico intenso.
Inoltre, impostare una priorità alta sui pacchetti inviati dai dispositivi VOIP risolve solo il problema del traffico inviato dal dispositivo VOIP ad altri dispositivi al di fuori della rete del cliente. Non affronta la questione dei pacchetti in entrata verso il dispositivo VOIP. Generalmente questi pacchetti non sono contrassegnati con una priorità maggiore quando vengono ricevuti dal router del cliente, in quanto i valori prioritari non vengono mantenuti su WAN. Di conseguenza, senza una configurazione aggiuntiva a questi pacchetti non verrà attribuita maggiore priorità rispetto al normale traffico dati. Per risolvere questo problema, si consiglia di stabilire regole di priorità per consentire a tutto il traffico SIP e RTP in entrata di avere una priorità maggiore rispetto al resto del traffico. Le porte associate a SIP e RTP sono definite nella sezione Firewall di questo documento. Potrebbe, inoltre, essere necessario assegnare agli indirizzi IP delle piattaforme di controllo delle chiamate Let's Co una priorità maggiore rispetto al resto del traffico. Anche se soggetti a modifiche in allegato al presente documento vengono dettagliati gli indirizzi IP specifici. La prioritizzazione degli indirizzi IP è richiesta per specifiche applicazioni del cliente, perciò gli indirizzi IP univoci che dovranno essere provvigionati potranno essere forniti anche su richiesta al servizio di assistenza tecnica Let's Co.

LARGHEZZA DI BANDA

Banda Internet WAN

La larghezza di banda Internet è la misura della capacità di traffico Internet disponibilità sulla rete di un cliente. Tale quantità è determinata dal servizio fornito dall'Internet Service Provider. La quantità di banda disponibile determinerà l'ammontare di chiamate vocali simultanee e di traffico dati che la connessione Internet supporterà. Se dimensionato correttamente e con le corrette impostazioni QOS nel router del cliente, il servizio Let's Co funzionerà senza errori.
Tuttavia, se sottodimensionato o se il QOS non viene impostato nel modo giusto, la qualità della chiamata percepita potrebbe deteriorarsi notevolmente durante i periodi di traffico di punta. Le seguenti informazioni forniscono dati e linee guida per il corretto dimensionamento del servizio vocale per una determinata larghezza di banda Internet.

Per determinare il numero di telefoni che possono essere supportati su una determinata larghezza di banda, è necessario innanzitutto calcolare il numero massimo di chiamate simultanee che possono essere supportate.
Tale calcolo deve considerare anche l'effetto degli algoritmi di compressione (Codec), nello specifico per gestire ciascuna chiamata audio la banda Internet utilizzata da Let's Co è di 50 kbps/chiamata con Codec G.729 e 100 kbps/chiamata con Codec G.711, quest'ultimo di norma viene utilizzato per i fax. Per le chiamate video dipende dalla risoluzione scelta, nella tabella in seguito i dati di occupazione per il desktop client.

Codecs	Communicator Video Size	H.264 Profile Level	Video Size	FPS Default	Recommended CPU	Default Maximum Bit Rate (Kbps)	Minimum RAM (GB)	H.263 Resolutions
Any supported codec	Small	1.1	174 x 144	15 through 30	Pentium Dual Core 1.7 GHz	192	1	SQCIF
Any supported codec	Medium	2	352 x 288	15 through 30	Pentium Dual Core 1.7 GHz	384	1	QCIF
Any supported codec	Large	3	640 x 480	15 through 30	Pentium Dual Core 1.7 GHz	512	1	CIF
G.722 for audio, H.264 for video	HD	3.1	1280 x 720	15 through 30	Pentium Quad Core	4096	2	4CIF

I dati della tabella sono indicativi e si riferiscono a una sola direzione, vanno quindi moltiplicati per due. Per le linee asimmetriche come l'ADSL e dati cellulari, bisogna tenere presente che la banda in upload è molto più bassa di quella in download.

Banda della rete locale LAN

La larghezza di banda della LAN è la quantità di traffico che la rete interna di un cliente può supportare. Questo quantitativo è determinato dalla capacità di trasmissione dell'infrastruttura di rete LAN. Nella maggior parte dei casi, l'infrastruttura di rete LAN del cliente è composta da un singolo switch di livello 2. La quantità di banda disponibile determinerà la quantità di chiamate vocali simultanee e il traffico dati che la LAN supporterà. Se dimensionato correttamente, il servizio Let's Co funzionerà correttamente. Tuttavia, se sottodimensionato, la qualità delle chiamate percepita potrebbe deteriorarsi notevolmente durante i periodi di traffico di punta.
È responsabilità del cliente assicurarsi che la propria rete interna sia ridimensionata correttamente per supportare l'aggiunta del VOIP alla propria rete.

FIREWALL E POLITICHE DI SICUREZZA

Firewall e servizi

Un firewall è un dispositivo o una serie di dispositivi in una rete dati configurato per proteggere la rete dal traffico potenzialmente dannoso. Tali dispositivi o tali funzionalità di protezione sono un requisito fondamentale per il buon funzionamento del servizio Let's Co e per proteggere la rete del cliente da attacchi informatici scongiurando anche possibili frodi.

La funzione comune del firewall è quindi consentire o negare il passaggio di specifici tipi di servizi attraverso l'interfaccia di rete pubblica. Un'applicazione di questa funzionalità consiste nel limitare i tipi di servizio a cui gli utenti della rete privata possono accedere o limitare l'accesso pubblico alla rete privata per garantire la sicurezza della rete.

I firewall possono impedire ai dispositivi VOIP di comunicare con i server di configurazione, i server di controllo delle chiamate, i gateway di rete e altri dispositivi VOIP. Affinché il servizio Let's Co funzioni correttamente, i firewall devono consentire i seguenti servizi:

- ✓ HTTP (porta 80) - necessaria per la comunicazione tra i dispositivi VOIP locali e i server di configurazione che detengono le informazioni di configurazione dei dispositivi VOIP.
- ✓ HTTPS (porta 443) - necessaria per la comunicazione tra i dispositivi VOIP locali e i server di configurazione che detengono le informazioni di configurazione dei dispositivi VOIP.
- ✓ SIP (porta 5060) - necessaria per la comunicazione tra i dispositivi VOIP locali e i dispositivi VOIP remoti, incluse le piattaforme di controllo delle chiamate, i gateway di rete e altri dispositivi VOIP.
- ✓ SIP (porta da 8933 a 8943) - necessaria per la comunicazione tra i dispositivi VOIP locali e i dispositivi VOIP remoti, comprese le piattaforme di controllo delle chiamate, i gateway di rete e altri dispositivi VOIP. Nota: questo intervallo di porte non è comunemente associato al traffico SIP. In questo caso, viene utilizzato per evitare scontri con le funzionalità di Application Layer Gateway (ALG) che potrebbero danneggiare il payload dei pacchetti SIP. Per ulteriori informazioni, fare riferimento alla sezione Application Layer Gateway di questo documento.
- ✓ RTP (porte 19560-65535) - necessarie per la comunicazione tra i dispositivi VOIP locali e i dispositivi VOIP remoti, incluse le piattaforme di controllo delle chiamate, i gateway di rete e altri dispositivi VOIP. Nota: le porte 19560-65535 non sono comunemente associate al traffico RTP. In questo caso, vengono utilizzate per evitare scontri con le funzionalità di Application Layer Gateway (ALG) che potrebbero danneggiare il payload dei pacchetti RTP. Per ulteriori informazioni, fare riferimento alla sezione Application Layer Gateway di questo documento. Con questi servizi permessi, i dispositivi VOIP dovrebbero essere in grado di comunicare correttamente con tutte le fonti esterne necessarie.
- ✓ Lo strumento di test della rete ExamiNet, richiedibile al supporto tecnico Let's Co, viene utilizzato per determinare se il servizio Let's Co funzionerà correttamente sulla rete in fase di prova. Affinché questo strumento e il dispositivo PacketSmart funzionino correttamente, il firewall deve consentire ai computer che eseguono il test ExamiNet e al dispositivo PacketSmart di accedere attraverso il firewall stesso a specifici endpoint IP.

SPECIFICHE DI CONFIGURAZIONE DEL FIREWALL DEL CLIENTE

Le impostazioni del firewall necessarie per il corretto funzionamento del servizio Let's Co sono documentate come segue.

Subnet pubbliche

La configurazione del firewall deve garantire la raggiungibilità dell'infrastruttura di Let's Co e nello specifico delle subnet e dei relativi indirizzi IP pubblici, riportati in seguito:

Location	Range IP	Piattaforma
Francoforte, Germania	85.119.56.0/24	Primaria
Londra, Inghilterra	85.119.57.0/24	Secondaria

Riepilogo porte TCP

Affinché ogni servizio funzioni correttamente è necessario configurare le porte TCP nel firewall del cliente verso le Subnet Pubbliche, nella configurazione dalla LAN alla WAN.

Service	Protocol	Start Port	End Port	Application
DNS	UDP	53	53	For resolving configutation server A Records and call control SRV Records
NTP Note1	UDP	123	123	Time Server Sync
HTTP/HTTPS	TCP	80 443 1025 1061 1081 2208 5222 5280 8443 8943 19560 52644 65525 65535	80 443 1025 1061 1081 2208 5222 5281 8443 8943 19560 52645 65525 65535	Configuration Management, Presence, File Transfer, BW Feature Configuration, PS Reporting and Configuration Management, Desktop Sharing, SOCKS-5 (File Exchange), BOSH (IM&P/IM&P Secure), Examinet, Various
SIP	UDP/ TCP	5060 8933 8943 8060	5061 8933 8943 8070	SIP Signaling (Application Guest Client)
RTP	UDP	8500 8600 15000 19560	8598 8699 19000 65535	Media Streams (Audio and Video)
Traceroute	UDP	33434	33534	Network Path Tests

Nota 1: NTP deve essere abilitato per ciascun indirizzo IP in uscita. Durante la configurazione iniziale i dispositivi finali del cliente possono cercare un server NTP impostato di Default dal produttore, tali server NTP non sono collegati al servizio Let's Co. Se il dispositivo non riesce a contattare il server NTP impostato dal produttore si possono verificare dei problemi durante la validazione del certificato HTTPS utilizzato per stabilire la connessione necessaria alla configurazione del dispositivo stesso.

Tutte le porte TCP/UDP indicate dovrebbero essere aperte verso tutte le sottoreti di Let's Co, quindi Le porte e protocolli associati elencati in precedenza devono essere consentiti per le relative sottoreti: 85.119.57.0/24 e 85.119.56.0/24.
Al fine di verificare la raggiungibilità dell'infrastruttura di Let's Co è possibile effettuare dei test mediante dei comandi di ping o trace route agli indirizzi 85.119.56.218 per la subnet pubblica primaria e all'indirizzo 85.119.57.218 per quella secondaria. Mediante tali test è possibile monitorare, anche se in modo non completo, i valori di latenza, jitter e Mos.

Tempi di Timeout delle sessioni TCP e UDP
Si richiede di controllare ed eventualmente modificare i tempi di Timeout delle sessioni TCP e UDP come segue:
- TCP= 45 secondi
- UDP= 300 secondi

La configurazione specifica del firewall dipende dalla marca e dal modello del firewall utilizzato dal cliente; Tuttavia, la maggior parte dei firewall di tipo professionale hanno funzionalità che consentono di creare configurazioni e criteri di servizio che includono o escludono range di indirizzi IP specifici. Se il cliente non conosce la combinazione degli indirizzi IP e dei servizi abilitati e come abilitarli, deve consultare il manuale d'uso del firewall o contattare il servizio di supporto del produttore.

CONFIGURAZIONE DEL TRUNK SIP

Se all'interno del servizio Let's Co viene richiesta l'abilitazione del servizio Trunk SIP è necessario che il gateway (d'ora in poi Customer Premises Equipment) sia configurato correttamente all'interno della rete aziendale. La configurazione del servizio Let's Co Trunk SIP richiede la configurazione del CPE per abilitare i servizi di accesso remoto affinché sia possibile effettuare la manutenzione. A titolo esemplificativo, altri protocolli come Telnet e FTP / TFTP sono comunemente utilizzati per aggiornamenti e backup di configurazione e sono quindi da prendere ovviamente in considerazione.

ATTENZIONE: è estremamente importante per qualsiasi IP PBX o Gateway multimediale accessibile via Internet tramite un indirizzo IP che vengano implementate nella rete del cliente tutte le protezioni necessarie alla CPE.

Tutte le CPE e quindi gli IP PBX e gateway multimediali devono essere protetti da un firewall configurato in modo appropriato per impedire l'accesso al CPE da fonti sconosciute. Qualora le credenziali di accesso vengano consegnate durante l'installazione del CPE l'utente dovrà modificare immediatamente la password di accesso di default.

PREVENZIONI DELLE FRODI

Assicurare la prevenzione delle frodi è una priorità chiave per Let's Co e pertanto le CPE collegate alla LAN del cliente vengono gestite con file di configurazione create con l'intento di prevenire le frodi. Tutte le password di autenticazione

SIP sono complesse e criptate all'interno del signaling per garantire l'impossibilità di essere intercettate. Laddove richiesta una password per un dispositivo configurato manualmente, come un IP PBX o un gateway multimediale, il portale provisioning genererà casualmente credenziali complesse che dovrebbero essere utilizzate all'interno del CPE.

Let's Co gestisce uno strumento complesso di intercettazione delle frodi che analizza attivamente le chiamate nel caso di attività sospette. Il sistema può adottare misure proattive per prevenire le frodi quando le chiamate risultano anormale e bloccate. L'implementazione di questo strumento non deve essere considerata come una rete di sicurezza che consente la configurazione e l'utilizzo di un dispositivo CPE scarsamente protetto. E' pertanto unica responsabilità del cliente finale quella di proteggere l'infrastruttura tecnologica di Let's Co, attuando e configurando correttamente tutti i dispositivi on premises (Switch, Firewall, Router, IP PBX, Access Point). Il responsabile IT o della sicurezza informatica del cliente finale dovrà accertarsi che gli utenti utilizzino correttamente il servizio, procedendo all'utilizzo di password e abilitazioni che rispecchino i requisiti minimi di sicurezza e confinino al massimo il rischio di frodi aziendali.

Nota bene: per sensibilizzare la giusta attenzione in merito alle frodi informatiche, vi segnaliamo che abbiamo pubbliche evidenze di come alcuni Hacker si intromettano in modo fraudolento al sistema di comunicazione (applicazioni, centralino, gateway, etc.), approfittando di una scarsa protezione informatica o di un comportamento poco responsabile da parte dell'utente finale. La finalità dei collegamenti è spesso quella di generare chiamate automatiche a pagamento verso numerazioni premium anche internazionali. In pochi minuti si possono generare frodi per decine di migliaia di euro non risarcibili. Vi invitiamo, quindi, a controllare costantemente il livello di sicurezza informatica aziendale , anche per le apparecchiature di comunicazione, e disabilitare, tramite il pannello di controllo di amministratore, le chiamate premium e quelle internazionali per gli utenti che non ne fanno uso o che non sono autorizzati. il nostro servizio di assistenza tecnica è a vostra disposizione per supportarvi nelle attività di prevenzioni delle frodi.