



FAQ
Brandvägg

Innehållsförteckning

1.Introduktion	3
2.Protokoll	3
2.1 FTP	
2.2 DNS	
2.3 HTTP	
2.4 HTTPS	
2.5 TFTP	
2.6 SNTP/NTP	
2.7 SIP	
2.8 RTP	
2.9 RTCP	
3.Nät	5
3.1 Nya nät	
4.Brandvägg och NAT	5
4.1 Vad är NAT	
4.2 SIP och NAT	
4.3 Gör en portmappning för varje anknytning i brandväggen	
4.4 Sätt ner registreringsintervallet på din terminal	
4.4 Aktivera NAT-keepalive	
5.Provisionering	6
6.Rekommendationer	6
6.1 Quality of Service	
6.2 Brandvägg	
6.3 Trafikbegränsningar	
6.4 Portmappningar	
6.5 VLAN	
6.6 WLAN	
6.7 IP-adressering	
7.Fyra sätt att bygga ditt nätverk med IP-telefoni	8
7.1 En brandvägg med SIP-Stöd	
7.2 Fysiskt separerade nätverk	
7.3 Virtuellt separerade nätverk	
7.4 Brandvägg UTAN SIP-stöd	
8.Vanliga frågor	10

1 Introduktion

Denna guide syftar till att ge en koncis överblick av de krav, kommunikationsprotokoll, rutiner och best-practices som används i samband med Tele10 IP-telefonitjänster. Även om strävan är att guiden ska vara så utförlig och korrekt som möjligt, är det svårt att på ett begränsat utrymme täcka in samtliga aspekter av tjänsterna. Guiden riktar sig till nätverkstekniker utan tidigare erfarenheter kring IP-telefoni, men med goda kunskaper i allmänna nätverkstekniker, därmed förutsätts förkunskaper inom områdena IP, NAT, DNS, UDP, TCP, QoS och routing. En del beskrivningar utelämnar detaljer till förmån för överskådligheten, t.ex. visar inte IP-kommunikationsexemplen samtliga paket i samband med respektive procedur utan bara de mest relevanta för att åskådliggöra proceduren. I en företagsbrandvägg som används för många olika tjänster, utgör de krav som telefonin ställer på brandväggen bara en del av helhetsbilden i de krav och specifikationer en brandvägg behöver uppfylla för att fungera tillfredsställande. Vi tar tacksamt emot synpunkter på hur dokumentet kan förbättras ytterligare!

2 Protokoll

Nedan återfinns de protokoll som används av utrustning som levereras av Tele10, samt en beskrivning av deras funktion. Olika terminaltyper använder olika protokoll, t.ex. föredras HTTPS för hämtning av mjukvara framför t.ex. TFTP och HTTP, men i de fallen då terminalen inte stödjer HTTPS används något av de andra. Tele10 rekommenderar inte att man blockerar trafik till och från terminaler baserat på portar och/eller protokoll, utan snarare väljer att lita på samtlig trafik till och från Tele10 nät, beskrivet i kapitlet 3 Nät. Tele10 förbinder sig inte heller att för all framtid använda enbart protokollen nedan, varför en begränsning av tillåten trafik genom brandväggar baserat på nedanstående riskerar att påverka levererade tjänster i det fallet specifikationen nedan ändras. Notera att portarna som anges i samtliga fall är mottagarportar, som regel snarare än undantag använder utrustningen slumpvis valda avsändarportar.

2.1 FTP

File Transfer Protocol, RFC959, TCP port 21 och 20. Används för att hämta terminalkonfiguration och mjukvara.

2.2 DNS

Domain Name Server, RFC1035, TCP/UDP port 53. DNS funktionalitet är en del av ett fungerande IP-nät och de terminaler som levereras av Tele10 fungerar inte om de inte har tillgång till en fungerande DNS. Vilken DNS-adress som används, och huruvida denna är placerad i kundens lokala nät eller i en leverantörs nät, skiljer sig från fall till annat.

I det fallet då DNS:en finns placerad utanför brandväggen, måste brandväggen tillåta terminalerna att göra uppslag mot denna.

Tele10 rekommenderar starkt att man i de fallen då kunds utrustning/terminaler konfigureras manuellt, använder sig av domännamn snarare än IP-adresser. Det går inte att garantera tillgängligheten av specifika tjänster på specifika IP-adresser, däremot kommer tjänsterna via funktionsnamn (så som sip14.Tele10.se) alltid finnas tillgängliga. Konkret innebär det att Tele10 inte ger några garantier att funktionen sip14 alltid kommer att återfinnas på dess nuvarande IP 80.83.208.7, däremot kommer den alltid att finnas tillgänglig på sip14.Tele10.se som i sin tur upplöser mot IP-adressen som funktionen finns på för tillfället.

2.3 HTTP

Hyper Text Transfer Protocol, RFC2616, TCP port 80. Används för att hämta terminalkonfiguration och mjukvara. Det krävs normalt ingen specifik konfiguration för att HTTP ska fungera tillfredställande då detta är ett av de vanligast använda protokollen på Internet.

2.4 HTTPS

Hyper Text Transfer Protocol over Secure Socket Layer, RFC2818, TCP port 443. Används för att hämta terminalkonfiguration och mjukvara.

2.5 TFTP

Trivial File Transfer Protocol, RFC1350, UDP port 69 samt dynamiskt allokerade portar för data överföring. Används för att hämta terminalkonfiguration och mjukvara. Notera att ett uttryckligt stöd för just TFTP ofta är nödvändigt för att TFTP-klient bakom en brandvägg ska fungera, detta då dataöverföringsportarna förhandlas under sessionens gång och kräver att brandväggen dynamiskt allokerar dessa.

2.6 SNTP/NTP

(Simple) Network Time Protocol, RFC1305/RFC1361, UDP port 123. Används för att sätta tid/klocka i terminalen.

2.7 SIP

Session Initiation Protocol, RFC3261, UDP port 5060. SIP används som kontrollprotokoll mellan SIP-proxyn ("växeln") och terminalen ("telefonen"). SIP används för att skicka de "kommandon" mellan SIP-proxyn och terminalen som används för samtalskontroll.

2.8 RTP

Real Time Transfer Protocol, RFC1889, UDP port 1024-65535 (Tele10 använder UDP port 10 000-20 000) Ljudströmmen mellan terminalen och telefonen under ett samtal strömmar som RTP. Vilken port som används slumpas fram i samband med att ett samtal initieras. Samtliga av Tele10 levererade terminaler använder symmetrisk RTP vilket innebär att mottagar- och avsändarport för RTP-strömmen är samma för både inkommande och utgående ljudström. Detta medför att ljudströmmen som går från terminalen till proxyn öppnar sessionen i brandväggen för att även tillåta inkommande talström över samma session. Konkret gör det att man i de fallen då man inte explicit begränsar vilken trafik man tillåter initieras från insidan, implicit tillåter RTP-trafiken från utsidan och in.

2.9 RTCP

Real Time Control Protocol, RFC3550, UDP port 1024-65535. En del terminaler genererar RTCP-paket som används i kommunikationen mellan RTP-ändpunkter för att förmedla lokal statistik och samtalsdata såsom information om jitter och eventuella paketförluster. Denna väljs som RTP-porten+1, dvs. om RTP-strömmen går över porten 12480, kommer RTCP att använda UDP port 12481.

3 Nät

Om kunden vill begränsa vilka tjänster som tillåts passera den eventuella brandvägg som sitter framför terminalerna, rekommenderas att man tillåter samtlig trafik, initierad från insidan till samtliga nedanstående nät, utan att vidare begränsa vilka protokoll/portar som tillåts. Detta då protokollen som beskrivs ovan kan komma att förändras med tiden, medan nätadresser tenderar vara mer permanenta.

3.1 Nya nät

Alla nya tjänster (såsom SIP-proxies) som driftsatts efter januari 2008, tilldelas IP-adresser i detta nätet: 80.83.208.0/20

De SIP-proxies som har ett nummer 13 eller högre (dvs. sip13.tele10.se och upp), återfinns i detta nät. Vidare håller samtliga tjänster från ovanstående, äldre nät, gradvis på att flyttas över till Tele10 egna adresser i detta nät.

4 Brandvägg och NAT

4.1 Vad är NAT

NAT (Network Address Translation) är en teknik som används av i stort sett alla routrar och brandväggar avsedda för både hem- och företagsbruk. I de flesta Internetabonnemang för privatpersoner ingår endast en IP-adress, vilket blir ett problem om man vill ansluta mer än en apparat mot Internet. All utrustning som du ansluter mot Internet behöver en unik IP-adress för att kunna kommunicera med omvärlden. I fallet då man använder en NAT-brandvägg delar denna (oftast) ut unika, icke-publika IP-adresser till utrustningen på insidan. Brandväggen själv tar då den enda publika IP-adressen och visar denna utåt. Vilka IP-adresser som ska användas i icke-publika nät finns specificerat i RFC1918, dessa varken kan eller får routas på Internet.

4.2 SIP och NAT

Det är vanligt att SIP och NAT inte fungerar som tänkt då brandväggens sessionstimer stänger sessionen som skapades i samband med registreringen efter en tid (normalt två-tre minuter) som normalt är mycket kortare än SIP-klientens omregistreringsintervall (normalt 60 minuter). Detta gör att inringande samtal till en terminal bakom en brandvägg droppas i brandväggen eftersom det vid det inringande tillfället inte längre finns någon aktiv session som matchar porten växelns försöker nå terminalen på.

4.3 Gör en portmappning för varje anknytning i brandväggen

Terminalen använder sig som standard av port 5060 för att skicka och ta emot SIP-meddelanden. Om du har fler terminaler behöver de vars en unik port, först terminalen på 5060, andra på 5061 osv.

4.4 Sätt ner registreringsintervallet på din terminal

Om terminalen registrerar sig med ett intervall som är tillräckligt kort för att hålla brandväggens sessionstimer aktiv, kommer inkommande samtal att fungera trots att ingen specifik portmappning är gjord. Denna lösning är snarare att betrakta som en "workaround" och rekommenderas inte eftersom den ofta inte ger en helt tillförlitlig tjänst, framförallt då flera SIP-klienter förekommer bakom en och samma brandvägg. Kortaste registreringsintervall som idag tillåts av Tele10 är 120 sekunder, men kommer i framtiden förmodligen bli längre vilket gör att denna lösning knappast är framtidssäkrad.

4.5 Aktivera NAT-keepalive

Denna funktion finns aktiverad i utrustning som levereras av Tele10. SIP-klienter med stöd för denna funktion skickar med jämna intervall (Tele10 använder 90 sekunder) ett tomt SIP-paket med samma avsändar/mottagar-port/IP som de "riktiga" SIP-paketerna. På så sätt belastas både SIP-proxy, SIP-klient och bandbredd avsevärt mindre då mängden data och beräkningar som krävs för varje paket är mindre än i exemplet ovan med kortare registreringsintervall, effekten är dock densamma.

5 Provisionering

Samtliga SIP-klienter som levereras av Tele10 hämtar sin konfiguration från Tele10s servrar med jämna intervall (normalt en gång i timmen och vid omstart). Detta sätt att underhålla en terminals konfiguration och mjukvara kallas provisionering. Detta innebär att inställningar som görs lokalt t.ex. i en terminals webbkonfigurationsgränssnitt eller menysystem, normalt fungerar fram till att terminalen uppdaterar sin konfiguration från Tele10 eller startas om.

6 Rekommendationer

6.1 Quality of Service

Om man vill använda sig av trafikprioritering är Tele10s rekommendation att prioritera samtlig UDP-trafik till Tele10s nättrymd (se kap. 3 Nät). QoS kan i många fall vara svårt att konfigurera och verifiera att man har en konfiguration som fungerar önskvärt. Ju enklare prioriteringsmodell man tillämpar, desto enklare är det att konstatera huruvida den fungerar som tänkt eller inte. Felaktigt konfigurerade QoS-parametrar ställer ofta till mer skada än nytta och det rekommenderas därför att man först utvärderar telefonin utan att ha konfigurerat QoS i brandväggen och i det fallet då kvaliteten inte är tillfredsställande, konfigurerar QoS.

6.2 Brandvägg

I stort sett vilken brandvägg som helst går att konfigurera för att fungera väl tillsammans med IP-telefoni. Tele10 rekommenderar Ciscos ASA5500-serie med firmware versioner 8.0(3) eller senare. För ytterligare information se guide för Cisco ASA5505. Tele10 erbjuder inte någon support på denna eller någon annan brandvägg. Utöver den allmänna konfigurationen som krävs, såsom IP adressuppgifter, konfiguration av ev. DHCP-server, behövs inga ytterligare inställningar för att SIP-trafik ska fungera. Brandväggen spårar SIP-registreringarna och håller på så sätt ett register över vilka inkommande samtal och övriga SIP-dialoger som tillåts. Brandväggar som saknar denna eller motsvarande typ av funktionalitet behöver konfigureras med statiska portmappningar för varje SIP-klient i LAN:et.

6.3 Trafikbegränsningar

I det fallet då man t.ex. av säkerhetsskäl vill begränsa vilken trafik man tillåter till- och från SIP-klienter på ett LAN rekommenderar Tele10 att man enbart baserar begränsningarna på IP-adresser och inte på protokoll och/eller portar. Eftersom de protokoll/portar som används i kommunikationen mellan SIP-klienter och SIP-proxies kan komma att förändras med tiden, riskerar man att påverka funktionaliteten negativt i de fall då man baserar tillåtna trafiktyper på de protokoll/portar som nyttjas just nu. Det ger dessutom en mer omfattande konfiguration, som är svårare att överblicka, och därmed medför en större risk för fel som en följd av detta.

6.4 Portmappningar

För att göra en portmappning i en brandvägg för en SIP-klient på LAN:et krävs följande information

- SIP-klientens IP adress
- SIP-klientens avsändar-port
- Eventuellt även SIP-klientens MAC-adress

Det generella tillvägagångssättet följer nedan.

- 1 I DHCP-serverns konfiguration, associera SIP-klientens MAC-adress till en specifik IP-adress, detta säkerställer att SIP-klienten får samma IP-adress även då DHCP-servern t.ex. startas om.
- 2 I brandväggen, skapa en portmappning för SIP-klientens IP-adress och avsändarport, det är denna som ser till att hålla en statisk session för att brandväggen ska kunna skicka inkommande trafik till SIP-klienten rätt.
- 3 Kontrollera att SIP-klienten kommer ut från rätt port i brandväggen. För att portmappningen i föregående steg ska vara till någon nytta är det den som måste vara avsändarport för telefonens registrering.

Tele10 kan inte hjälpa dig med att lägga upp portmappningar, titta i din brandväggs manual och läs mer på t.ex. <http://www.portforward.com> för information om hur det fungerar med din specifika modell av brandvägg.

6.5 VLAN

I de allra flesta fall krävs inte att man separerar telefontrafiken i ett eget VLAN. Dock kan det i vissa fall t.ex. beroende på att man vill underlätta överskådlighet och "accountability" i nätet, vara en bra idé.

6.6 WLAN

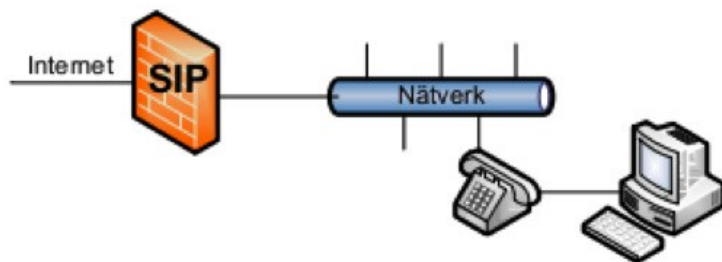
De parametrar som påverkar talkvaliteten och tillförlitligheten i IP-telefonitjänsten i högst utsträckning är jitter och paketförluster, båda dessa parametrar påverkas påtagligt negativt då data överförs trådlöst. Tele10 avråder från att man använder trådlös överföring av telefontrafiken då det är lokala, på förhand omöjliga att bedöma, parametrar som avgör i vilken utsträckning paketförluster och jitter introduceras över den trådlösa förbindelsen.

6.7 IP-adressering

Tele10 rekommenderar att man i samtliga fall använder en DHCP-server för IP-adressering av klienter i det lokala nätverket. I det fallet då man på grund av t.ex. portmappningar enligt ovan, önskar fasta adresser i den bemärkelsen att samma terminal under alla omständigheter får samma IP-adress, rekommenderas det att man i DHCP-servern associerar IP-adressen med terminalens MAC-adress. I och med detta får terminalen alltid samma IP-adress utan att man behöver konfigurera någon inställning i terminalen. Detta underlättar överskådligheten och minskar drastiskt mängden arbete som krävs i samband med installation.

7 Fyra sätt att bygga ditt nätverk med IP-telefoni

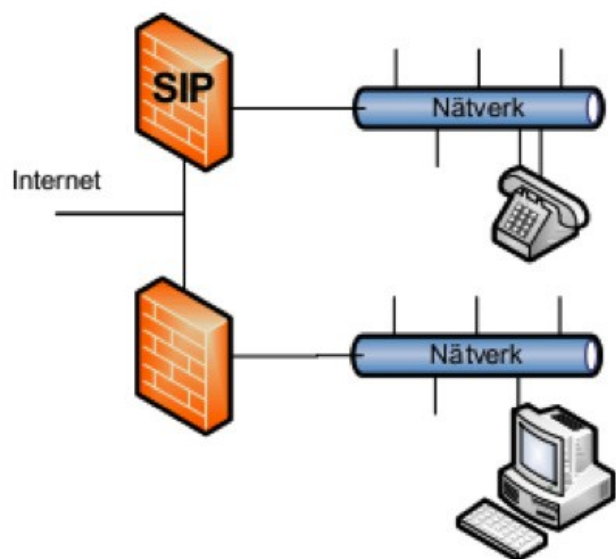
7.1 En brandvägg med SIP-Stöd



En brandvägg med SIP-stöd håller reda på vilka anslutningar som finns registrerade på insidan och skickar därför inkommande samtal till rätt terminal. Hur detta fungerar i praktiken skiljer sig åt mellan olika tillverkare. Det är dessutom många implementationer som inte fungerar som avsett varför det absolut rekommenderas att man inte blint litar på utlovad funktionalitet utan att testa först.

Tele10 rekommenderar i första hand att man bygger sitt nätverk med en brandvägg som stödjer protokollet SIP (Session Initiation Protocol). Detta möjliggör att datorer och telefoner kan dela samma nätverk.

7.2 Fysiskt separerade nätverk

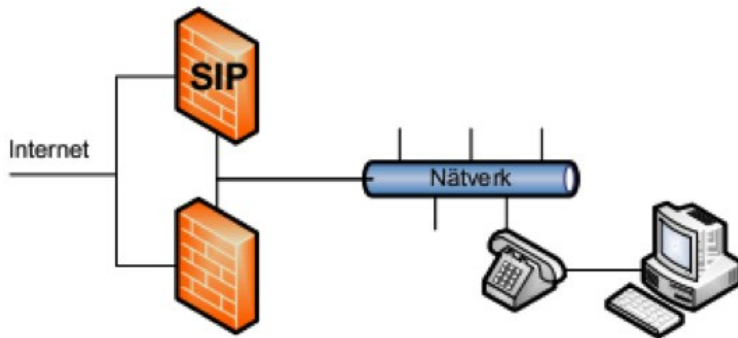


En bra lösning för kunder med en avancerad befintlig brandvägg och gott om Nätverksuttag. Används generellt vid större installationer.

En kvalitetssäker installation som i vissa fall kan vara kostsam. Genom att separera näten säkerställer man både säkerheten i datanätverket samt kvalitén för IP-telefonin.

- Kräver en SIP-brandvägg
- Kräver en Internetaccess med flera IP-adresser
- Kräver 2st nätverksuttag per arbetsplats

7.3 Virtuellt separerade nätverk

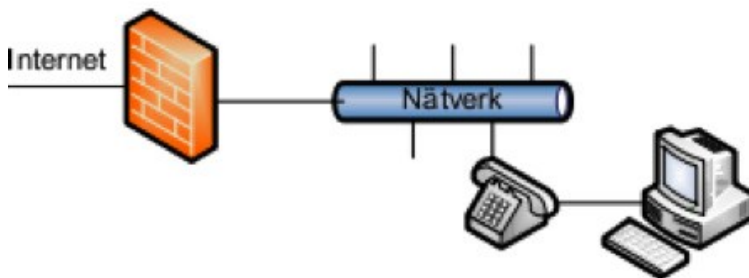


För företag vars befintliga brandvägg inte stödjer SIP och inte har möjlighet att byta brandvägg. Genom att placera två brandväggar i nätverken kan man låta IP-telefonin gå ut genom en SIP-brandvägg (telefonerna använder denna som "standard gateway").

Samtidigt som datortrafiken hanteras som tidigare genom den befintliga brandväggen.

Att styra trafiken till de olika gateways görs lämpligast genom att konfigurera olika DHCP-klasser.

7.4 Brandvägg UTAN SIP-stöd



Framförallt till företag med avancerad brandvägg och Internetaccess med bara en IP-adress.

Företag

1. vars befintliga brandvägg inte stödjer SIP
2. som inte har möjlighet att byta brandvägg
3. som inte kan placera en parallell SIP-brandvägg finns lösningen att behålla tidigare lösning och med hjälp av portmappningar låta SIP trafiken passera.

- Kräver brandvägg med stöd för portmappningar
- Kräver god kunskap om brandväggen

8 Vanliga frågor

Varför kan jag ringa ut men inte in?

Det är vanligt att all trafik som initieras från insidan (LAN-sidan) på brandväggen tillåts passera på väg ut. Utgående samtal kan jämföras med en vanlig WWW-siduppslagning vad avser trafikflödena. Ett inkommande samtal kräver däremot att det finns en session i brandväggen som kan dirigera trafiken till rätt enhet på insidan.

Varför fungerar det ibland?


Din terminal registrerar sig mot sitt routing-home med jämna mellanrum, din brandvägg håller då en session med de associerade portarna/IP-adresserna aktiv under en tid, vanligen kring två-tre minuter. Om du ringer in till din terminal strax efter att den skickat trafik kommer det att finnas en aktiv session som ser till att ditt samtal släpps in till rätt telefon.

Varför fungerar det att ringa in precis efter att jag ringt ut?

En session i NAT-brandväggen hålls aktiv eftersom den nyss öppnats inifrån, se ovan.

Kan Tele10 konfigurera min brandvägg för IP-telefoni?

Nej, eftersom Tele10 inte levererat din brandvägg kan vi inte heller lämna någon support på dess funktion och/eller konfiguration. Det är ditt eget ansvar att se till att din brandvägg fungerar med de tjänster du har för avsikt att nyttja den för.



Vår affärsidé är att erbjuda flexibla och kostnadseffektiva kommunikationstjänster för företag och organisationer, Fast eller mobil telefon. På kontoret, på landet, hemma eller i Peking. Det skall vara enkelt och billigt att vara en del av företagets växel var man än befinner sig.

Med hjälp av den senaste tekniken tar vi fram tjänster som effektiviserar både kostnader och Ert sätt att arbeta.

Tele10 är ett dotterbolag till Rockford Solutions AB.

Företagets medarbetare har funnits i telekombranschen i mer än 15 år.

.....

Vår vision är att förändra marknaden för telefoni och att vara den ledande operatören inom kvalitativa IP-baserade telekommunikationstjänster i Norden.



Tele10 AB

Olof Asklundsgata 8 | SE-421 30 Västra Frölunda

Telefon: 031-7344900

E-post: info@tele10.se

Hemsida: www.tele10.se