FIREWALL INSTRUCTIONS

Setup of the company's firewall/router for Touchpoint Plus Softphone and/or Desktop.

1. In the Firewall settings, **IP range** should be entered as **allowed.**
   This will ensure that it is open to both incoming and outgoing traffic, so the services in Touchpoint Plus can work correctly.

2. In the Firewall settings, the following should be **disabled:**
   a. SIP-inspection
   b. All-SIP-aware
   c. SIP-ALG
   d. SIP-algorithm
   e. RTP-session timer.

3. To obtain optimum call quality, a separate dedicated voice VLAN should be set up with QoS for all SIP traffic (if the company's switch supports this).

4. For companies with MPLS networks:
   Here, call quality can be further optimised by using a **local internet breakout** at the individual locations. This is illustrated in the drawing on the next page.

Table of IP range settings

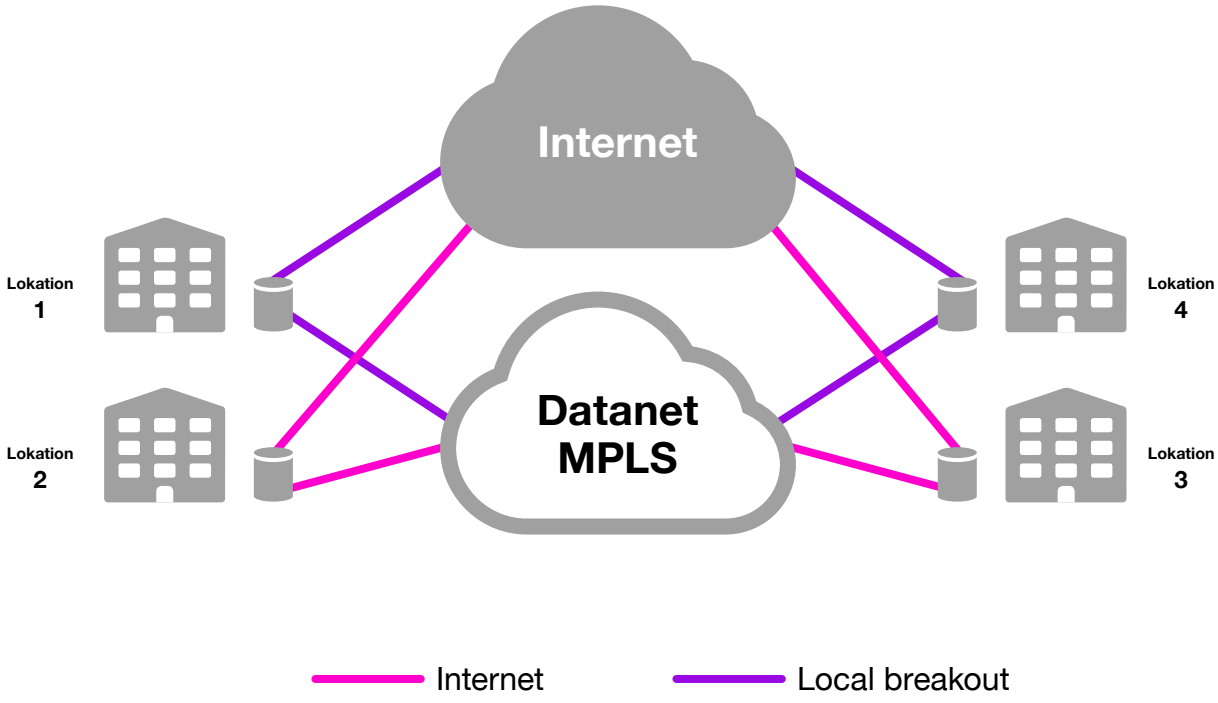
Outgoing traffic					
Dest IP(s)	**Dest port**	**Application**	**Protocol**	**Rule**	**Comment**
194.255.208.128/26	443	HTTPS	TCP	ALLOW	
194.255.208.128/26	5060-5061	SIP	TCP/UDP	ALLOW	The SIP-inspection in the firewall has to be disabled.
194.255.208.128/26	49152-65534	RTP/RTCP	UDP	ALLOW	Media- (voice) trafic
194.255.209.128/26	514	SYSLOG	UDP	ALLOW	
Any	53	DNS	TCP/UDP	ALLOW	
Any	123	NTP	UDP	ALLOW	

Ingoing trafic					
Dest IP(s)	**Dest port**	**Application**	**Protocol**	**Rule**	**Comment**
194.255.209.128/26	443	HTTPS	TCP	ALLOW	

LOCAL INTERNET BREAKOUT

MPLS netværk
Illustration of MPLS network with **local internet breakout.**

A central internet breakout can also be used, but QoS is then recommended in the MPLS network between the locations.



Telia
Mere at sige ja til