setera | UNIFIED COMMUNICATIONS

# IMPOSTAZIONI FIREWALL/ROUTER

Se volete utilizzare **Setera OneCloud** all'interno di una rete protetta da Firewall sarà necessario apportare alcune regole in modo che il centralino Setera OneCloud riesca a comunicare correttamente con i dispositivi all'interno della rete.

1. Nelle impostazioni del Firewall, l'intervallo di IP **185.255.33.208/28** deve essere inserito come **consentito** (whitelist). In questo modo si garantisce che sia aperto al traffico in entrata e in uscita, in modo che i servizi di Setera OneCloud possano funzionare correttamente.
2. Nelle impostazioni del Firewall, i seguenti elementi devono essere **disabilitati**:
    a. SIP-inspection
    b. All-SIP-aware
    c. SIP-ALG
    d. SIP-algorithm
    e. RTP-session timer.
3. Per ottenere una qualità di chiamata ottimale, è consigliato impostare una **VLAN** per il traffico voce dedicata con **QoS** per tutto il traffico SIP (se lo switch aziendale lo supporta).
4. Impostazioni firewall per ricevimento notifiche push su Applicazioni per smartphone.
    a. Guida per Smartphone Android **clicca qui**
    b. Guida per Smartphone iOS **clicca qui**

## TRAFFICO IN USCITA

| Dest. IP(s) | Dest. Port(s) | Transport | Protocol | Rule | Comment |
|---|---|---|---|---|---|
| 185.255.33.208/28 | 443 | TCP | HTTPS | ALLOW | Service management |
| 185.255.33.208/28 | 5061 | TCP | SIP | ALLOW | The SIP-inspection in the firewall has to be disabled |
| 185.255.33.208/28 | 1024 - 65535 | UDP | RTP / SRTP | ALLOW | Media/Speech |
| 89.18.235.149/32 | 80/443 | TCP | HTTP(S) | ALLOW | SIP phone firmware |
| rcs.aastra.com | 80/443 | TCP | HTTP(S) | ALLOW | Mitel phone settings distribution |
| 52.28.89.237 | 443 | TCP | HTTPS | ALLOW | Snom phone settings distribution |
| ump.avsystem.cloud | 10301/10302 | TCP | HTTP(S) | ALLOW | TR-069 Device Management |
| Any | 53 | TCP/UDP | DNS | ALLOW | |
| Any | 123 | UDP | NTP | ALLOW | |