cloud ready

How to make your network cloud ready

In general

Inform your responsible IT about the planned start date and clarify in advance whether configuration measures are necessary on the router or your firewall.

Basically, each terminal requires its own IP address, which can be assigned either manually on the appropriate terminal or via a DHCP server. If you use a DHCP server, please make sure that you have enough IP addresses available for assignment.

Firewall / Router Settings

- UDP 123 for NTP (Standard NTP)
- UDP 6060 for SIP (not the standard port 5060)
- UDP 53 für DNS requests
- TCP 443 first contact with Cisco (standard HTTPS)
- TCP 4443 Provisioning at Universe (also no standard port)
- UDP Dynamic for RTP because there are no fixed ports therefore best here the whole network 193.203.210.0/23 release there are all Universe server.

It is not necessary to set up port forwardings. In the port areas mentioned on the following pages, no port forwardings may be set up!

Based on the assumption that any firewalls are stateful and accepting responses in open TCP and UDP sessions, pay attention to the following points:

- An existing SIP ALG must be deactivated in any case, as well as a Store & Forward.
- Use an Intrusion Detection or Prevention System (IDS / IPS) to make sure it does not interfere with telephony. Possibly. the settings must be adjusted accordingly or the system must be deactivated.
- In addition, we recommend a possibly existing protection against ICMP Redirect, Route Injection and DoS.
- When using Network Address Translation (NAT), a UDP NAT timeout of more than 130 seconds is mandatory.
- Activation of a possibly existing "Consistent NAT" mode (this is especially necessary with SonicWall!