cloud ready

So machen Sie Ihr Netzwerk cloud ready

Allgemein
Informieren Sie Ihre zuständige IT über den geplanten Anfangstermin und klären Sie bitte im Vorfeld ab, ob Konfigurationsmaßnahmen am Router oder Ihrer Firewall notwendig sind.

Grundsätzlich benötigt jedes Endgerät eine eigene IP-Adresse, die entweder manuell am entsprechenden Endgerät oder über einen DHCP-Server vergeben werden kann. Falls Sie einen DHCP-Server einsetzen achten Sie bitte darauf genügend IP-Adressen zur Vergabe verfügbar zu haben.

Firewall /Router– Settings
- UDP 123 für NTP (Standard NTP)
- UDP 53 für DNS requests
- UDP 6060 für SIP (nicht der Standard Port 5060)
- TCP 443 erste Kontaktaufnahme zu Cisco (Standard HTTPS)
- TCP 4443 Provisioning bei Universe (Auch kein Standard Port)
- UDP Dynamisch für RTP da gibt es keine festen Ports daher am besten hier das ganze Netz 193.203.210.0/23 freigeben da stehen alle Universe Server.

Es ist nicht notwendig Port-Forwardings einzurichten. In den auf den Folgeseiten genannten Portbereichen dürfen auch keine Port-Forwardings eingerichtet werden!

Basierend auf der Annahme, dass eventuelle Firewalls Stateful sind und Antworten in offenen TCP und UDP Sessions akzeptiert werden, achten Sie auf die folgenden Punkte:
- Ein vorhandenes SIP ALG ist in jedem Fall zu deaktivieren, ebenso ein Store&Forward.
- Setzen Sie ein Intrusion Detection oder Prevention System (IDS/IPS) ein, stellen Sie sicher, dass es sich nicht negativ auf die Telefonie auswirkt. Ggf. müssen die Einstellungen entsprechend angepasst oder das System deaktiviert werden.
- Zudem empfehlen wir einen evtl. vorhandenen Schutz gegen ICMP Redirect, Route Injection und DoS.
- Bei Einsatz von Network Address Translation (NAT) ist ein UDP-NAT Timeout von mehr als 130 Sekunden zwingend.
- Aktivierung eines evtl. vorhandenen „Consistant-NAT“ Modus (dies ist speziell bei SonicWall zwingend nötig!)