Merkblatt Plug & Play

A. Allgemeines

Allgemeines

Bitte beachten Sie folgende Punkte bzgl. Ihres Netzwerks, um das Plug & Play zu ermöglichen:

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. Der DHCP-Server darf keine Option 66 propagieren. Eine ggf. existierende DHCP-Conflict-Database ist optional für die Telefone zu deaktivieren.

Einstellungen für Switches

- Generell empfehlen wir den Einsatz vom Spanning Tree Protocol (vgl. Wikipedia) auf Ihren Switchen. Bei aktiviertem Spanning Tree sollte jedoch darauf geachtet werden, dass die Ports, an denen Sie Telefone oder ähnliche Endgeräte anschließen, passend konfiguriert sind. Je nach Switch-Hersteller und Firmware ist die empfohlene Option als „PortFast“ oder „Edge Mode“ bekannt. Die Option sorgt dafür, dass ein angestecktes Gerät sofort eine Verbindung bekommt und nicht wie bei Spanning Tree üblich zunächst für 30 Sekunden o.ä. blockiert wird. Ein lastabhängiges Spanning-Tree auf Cisco-Switchen (PVST+ Mode) ist in jedem Fall zu deaktivieren!
- Deaktivierung von Proxy-ARP Mechanismen, wir empfehlen darüber hinaus einen Schutz gegen MAC-Spoofing.

Einstellungen für den Router / Firewall

- 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 65 Sekunden zwingend. Wir empfehlen für die obigen Protokolle ein Setting zwischen 125 und 130 Sekunden.
    - Aktivierung eines evtl. vorhandenen „Consistant-NAT“ Modus (dies ist speziell bei SonicWall zwingend nötig!)

- Wir empfehlen unseren Kunden unser Netz (109.68.96.0/21) bei Ihren Email-Providern zu whitelisten, da eventuell sonst keine Emails ankommen könnten.
- Sobald für einen Kunden Verschlüsselung aktiviert wird, werden alle zur Verschlüsselung zertifizierten Geräte automatisch auf diese umgestellt. Es ist nicht möglich, einzelne Geräte dieses Typs selektiv zur Verschlüsselung freizugeben oder diese davon auszunehmen. Bei der Abrechnung werden immer nur die zur Verschlüsselung fähigen Geräte betrachtet.

B. Firewall Einstellungen

Firewall Einstellungen

Genutzte Ports

Für die Kommunikation mit der Telefonanlage müssen die Endgeräte in der Lage sein, über folgende Ports ausgehend zu kommunizieren:

Protokoll	Zielport	Zweck	Ziele
TCP	80, 83, 443, 18443	Provisionierung	alle Netze
UDP	123	NTP	alle Netze
UDP	53	DNS	DNS Server des Kunden
UDP	alle Ports	SIP, RTP, T-38, FMC, etc.	109.68.96.0/21
TCP	alle Ports	SIP/TLS, SIP, FMC	109.68.96.0/21

C. Router

Viele Router haben sich in der Praxis bei korrekter Konfiguration bewährt, daher wird kein spezieller Router empfohlen.

Tipps für eine korrekte Routerkonfiguration:

- Ein UDP-NAT Timeout zwischen 120 und 130 Sekunden.
- Deaktivierung eines evtl. vorhandenen SIP-ALG
- Aktivierung des „consistent nat“-Features (sofern vorhanden – Bsp: Sonicwall)
- Deaktivierung von Store&Forward für die Verbindungen von / zu der Telefonanlage.

Router

Aufgrund einer teils sehr hohen Komplexität können wir

für Router / Firewalls von SonicWall keinen Support auf die

Funktionalität der Telefonanlage bieten!

Wir raten dringend dazu auf der Firewall SIP ALG (SIP Helper)

zu deaktivieren!