Übersicht der Portnutzung der STARFACE

Das Netzwerk, in dem sich die STARFACE befindet bzw. dessen Sicherheitseinstellungen, muss die folgende Portnutzung der STARFACE berücksichtigen, wenn die zugrunde liegenden Funktionen genutzt werden sollen. Dies gilt insbesondere bei der Nutzung von Port-Forwarding, den Einstellungen einer Firewall oder der Nutzung von NAT.

Die Verantwortung für die Absicherung des Netzwerkes obliegt grundsätzlich dem Partner bzw. dem Netzwerkadministrator. Dieser muss entscheiden, welche der folgenden Ports, URLs und IP-Adressen für die individuelle Konfiguration freigegeben werden bzw. erreichbar sein müssen. Es können keine individuellen Empfehlungen zur Absicherung eines Netzwerkes ausgesprochen werden. Eine grundsätzliche Empfehlung ist jedoch, wann immer möglich, für den Zugriff auf die STARFACE bzw. das Netzwerk ein VPN zur zusätzlichen Absicherung einzurichten.

Sollte es zu Problemen mit der Sprachqualität kommen, gibt es dafür einen eigenen Fehlerleitfaden (siehe auch Fehlerleitfaden - Echo bzw. schlechte Qualität bei aktiven Gesprächen).

Port	Protokoll	Beschreibung
53	UDP und TCP	DNS
80	TCP	Zugriff auf die Weboberfläche der STARFACE und das REST Interface der STARFACE via http
123	UDP	Setzen/Abgleichen der Systemzeit über einen externen NTP-Server
389	LDAP	Unverschlüsselter Zugriff auf ein externes Adressbuch (siehe auch LDAP-Anbindung eines Adressbuches konfigurieren)
443	TCP	Zugriff auf die Weboberfläche der STARFACE via https
636	LDAP	Zugriff mit TLS auf ein externes Adressbuch (siehe auch LDAP-Anbindung eines Adressbuches konfigurieren)
443	TCP	Zugriff auf grundlegende Funktionen in den STARFACE Desktop Apps und in den STARFACE Mobile Apps. Wird der Standardport im Webserver geändert müssen auch die Firewallfreigaben angepasst werden.
1902	UDP	Benutzerauthentifizierung über Active Directory
3090	TCP und UDP	Aufbau und Nutzung des Anlagenverbunds
5060	UDP	Nutzung durch SIP (z.B. Gesprächsaufbau)
5060	TCP	Nutzung durch SIP (z.B. Gesprächsaufbau)
5061	TCP	TLS-Verschlüsselung in den STARFACE Desktop Apps und bei verschlüsselten Verbindungen zu einigen SIP-Providern
5222	TCP	Anmeldung der STARFACE Desktop Apps und der STARFACE Mobile Apps am XMPP-Server der STARFACE
10.000 bis 20.000	UDP	eingehende RTP-Audiodaten
1.025 bis 65.535	UDP	ausgehende RTP-Audiodaten
50080	TCP	Autoprovisioning (alle 3 Arten) und Telefonmenüs (unverschlüsselt)
50081	TCP	Autoprovisioning (alle 3 Arten) für Openstage und Snom (mit TLS)

Die Nutzung von TLS 1.0 und TLS 1.1 ist für die folgenden Ports nicht möglich, alle höheren Versionen von TLS werden unterstützt:

- 443
- 5061
- 5222

Zugriffe auf Serveradressen

Die folgenden Serveradressen müssen von der STARFACE aus erreichbar sein:

Adresse	Port	Protokoll	Beschreibung
license.starface.de	80	HTTP	Zugriff auf den Lizenzserver der STARFACE betreffend Abgleich der Lizenzen
license.starface.de	443	HTTPS	Zugriff auf den Lizenzserver der STARFACE betreffend Abgleich der Lizenzen
license.starface.de	8383	HTTPS	Zugriff auf den Lizenzserver der STARFACE betreffend Abgleich der Lizenzen
update.starface.de	80	HTTP	Zugriff auf Updates der STARFACE
update.starface.de	443	HTTPS	Zugriff auf Updates der STARFACE

starface-cdn.de	80	HTTP	Zugriff auf Updates und die Firmwares der STARFACE
starface-cdn.de	443	HTTPS	Zugriff auf Updates der STARFACE
www.starface-cdn.de	80	HTTP	Zugriff auf Updates der STARFACE
www.starface-cdn.de	443	HTTPS	Zugriff auf Updates der STARFACE
siptrunk.de	443	HTTPS	Zugriff auf das Providerportal

Zugriff für die STARFACE Mobile Apps

Der folgende DNS Eintrag muss via Port 443 für die STARFACE und die Mobile Apps erreichbar sein, damit die Funktionalität der STARFACE Mobile Apps gewährleistet ist:

- push-cluster.starface.de (ab der Version 7.0.0.19)
- push.starface.de (bis zur Version 7.0.0.8)

Zugriff auf STARFACE Connect

Die folgende Subdomain muss von der STARFACE aus erreichbar sein, wenn eine STARFACE Connect Leitung genutzt werden soll:

cluster.starface-connect.com

Sollte dies nicht möglich sein, können auch die folgenden IP-Adressen in der Firewall eingetragen werden:

- 37.120.180.58
- 37.120.180.6
- 37.120.181.198
- 37.120.181.229
- 46.38.248.81
- 46.38.248.53
- 85.184.250.15
- 185.145.168.32
- 185.145.168.63
- 185.145.168.86
- 185.145.168.116
- 212.79.205.28
- 185.145.169.250
- 212.79.202.172
- 212.79.204.144
- 212.79.206.208
- 45.143.185.126
- 212.79.200.42
- 212.79.203.47
- 45.143.185.251
- 212.79.220.34
- 212.79.220.35
- 212.79.220.36

Hinweis: Es wird von der Eintragung einzelner IP-Adressen in der Firewall abgeraten, da die genutzten IP-Adressen immer wieder erweitert und /oder verändert werden können.

Zugriff auf STARFACE NEON

Die Systemvorrausetzungen für den Zugriff auf STARFACE NEON sind in einem anderen Teil der Dokumentation aufgeführt (Link zur Dokumentation von STARFACE NEON).

Telefone des Herstellers Yealink an der STARFACE Cloud

Sollen Telefone des Herstellers Yealink an eine STARFACE Cloud angebunden werden über das Partnerportal der Firma Starface (siehe auch Erklärung zu der STARFACE Provisionierung), müssen die Yealink Telefone die folgenden Hosts erreichen können

- dm.yealink.com
- api-dm.yealink.com
- rps.yealink.com
- rpscloud.yealink.com
- pscloud.yealink.com

Dabei müssen die folgenden Ports freigegeben sein für die oben aufgeführten Hosts:

- 80
- 443
- 8443
- 8445

- 8446
- 9989