

STARFACE VPN-SSH-Tunnel

Überblick

- Mit Windows-Zugangsdaten an der STARFACE-Cloud anmelden
- Aus der STARFACE-Cloud auf lokale Datenbanken und Dienste zugreifen
- STARFACE-Monitoring oder Telefonie-Datenbanken für lokale Anwendungen freigeben
- STARFACE-Cloud-Backups auf lokalen SMB-Freigaben speichern

Beim Betrieb Ihrer STARFACE in der Cloud gibt es spezielle Herausforderungen, insbesondere beim Zugriff auf lokale Dienste (z.B. Kundendatenbanken) und beim Zugriff auf Dienste der Telefonanlage, die in einem Cloud-Szenario normalerweise nicht zugänglich wären. Hier kommen SSH-Tunnel ins Spiel.

SSH-Tunnel, auch bekannt als Secure Shell-Tunnel, ist eine leistungsfähige Technologie, die eine verschlüsselte Verbindung zwischen zwei Netzwerken ermöglicht. Dies eröffnet eine Vielzahl von Anwendungsfällen und Vorteilen, wenn es um die STARFACE-Telefonanlage geht.

Erstens ermöglichen SSH-Tunnel den sicheren Zugriff auf lokale Dienste, wie z.B. den Domänencontroller für Windows-Anmeldungen oder eine Datenbank mit Kundendaten, selbst wenn die STARFACE-Telefonanlage in der Cloud betrieben wird. Dies kann besonders nützlich sein, wenn Sie Kundendaten für Funktionen wie Namensauflösung benötigen. Zweitens können Kunden über SSH-Tunnel auf Dienste der Telefonanlage wie Datenbanken und Monitoring zugreifen, die sonst nicht von außen erreichbar wären.

Durch die Nutzung von SSH-Tunneln mit STARFACE lassen sich also Herausforderungen in Bezug auf den Zugriff auf lokale Dienste und Dienste der Telefonanlage erfolgreich lösen. Mit dieser Technologie können Sie die Flexibilität und die Vorteile der Cloud nutzen, ohne auf den Komfort und die Sicherheit des lokalen Zugriffs verzichten zu müssen.

Dieser Artikel soll Ihnen nicht nur einen Überblick über die Vorteile von SSH-Tunneln bei der Nutzung von STARFACE geben, sondern auch Anregungen und Ideen liefern, wie Sie diese Technologie in Ihrem eigenen Geschäfts- oder Kommunikationsszenario einsetzen können.

Anwendungsfälle & Einsetzbare Module

SSH-Tunnel lassen sich mit den folgenden Fluxpunkt Modulen anlegen und konfigurieren:

- **Active Directory Synchronisation** (ab v23.5.30)
Anwendungsfall: Zugriff auf das lokale Active Directory oder einen lokalen LDAP-Server für die Benutzeranmeldung
- **Call Recording** (ab v23.5.25)
Anwendungsfall: Aufzeichnung auf lokale SMB-Freigabe, Protokollierung in lokale SQL-Datenbank
- **Insight Analytics** (ab v23.6.16)
Anwendungsfall: Export von Auswertungen in lokale SQL-Datenbank
- **Monitoring**
Anwendungsfall: Freigabe der Monitoring-Ports für lokale Anwendungen (z.B. Prometheus, Check_MK)
- **Multiline TAPI Configuration**
Anwendungsfall: Freigabe des Asterisk Management Interface (AMI) für lokale TAPI-Anwendungen
- **Reverse Lookup PRO** (ab v23.5.25)
Anwendungsfall: Rufnummernauflösung aus lokalen Datenquellen
- **User Template PRO** (ab v23.5.25)
Anwendungsfall: Zugriff auf interne STARFACE-Schnittstellen zu Management- und Überwachungszwecken (Datenbank, Openfire, Prometheus, Autoprovisionierung, etc.).

Schritt-für-Schritt-Anleitung

Der Tunnel wird in jedem Fall von der STARFACE aus aufgebaut, so dass es *nicht* notwendig ist, den SSH-Port der STARFACE erreichbar zu machen. Im lokalen Kundennetzwerk muß ein OpenSSH-Server für die STARFACE erreichbar gemacht werden.

1

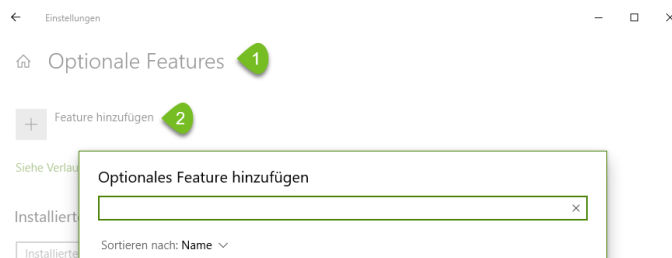
Installation OpenSSH-Server

Unter Windows (ab Windows 10 und Server 2019) können Sie OpenSSH-Server über die **Einstellungen** installieren. Wählen Sie dort **Apps > Apps und Features > Optionale Features** aus. Klicken Sie auf **Feature hinzufügen**.

Detaillinformationen zur Installation mittels PowerShell und dem Starten/Stoppen von OpenSSH als Windows-Dienst finden Sie unter: https://learn.microsoft.com/de-de/windows-server/administration/openssh/openssh_install_firstuse

Der Zugriff per SSH ist nach erfolgreicher Installation über die Windows-Konten des Betriebssystems möglich. Für umfassendere Authentifizierungsmöglichkeiten konsultieren Sie bitte die Dokumentation von OpenSSH.

Tipps: Mit dem Kommando `netstat -aon` auf der Windows Kommandozeile können Sie herausfinden, ob der OpenSSH-Server oder vielleicht ein anderer Dienst an den gewünschten TCP-Port gebunden ist. Unter `C:\ProgramData\ssh\sshd_config` findet sich die Konfigurationsdatei des OpenSSH-Servers, in der ein abweichender TCP-Port konfiguriert werden kann.



Zugriff für Remote-Hosts (über den OpenSSH-Server auf STARFACE-Dienste)

Damit der von einem OpenSSH-Server bereitgestellte Tunnelendpunkt zu einem STARFACE-Dienst auch für Remote-PCs funktioniert, sind folgende Voraussetzungen zu erfüllen:

- Firewall des OpenSSH-Hosts (und Firewalls zwischen PC und OpenSSH-Server) muß dem Remote-PC den Zugriff auf den Tunnelendpunkt-Port gestatten.
- In der `sshd_config` des OpenSSH-Servers müssen die folgenden Optionen aktiviert werden:
 - `AllowTcpForwarding yes`
 - `PermitTunnel yes`
 - `GatewayPorts yes`

2

Firewalleinstellungen / Port-Forwarding

Damit eine STARFACE-Cloud-Anlage einen SSH-Tunnel zu Ihrem SSH-Server aufbauen kann, muß dieser entweder über eine statische öffentliche IP-Adresse oder einen Hostnamen erreichbar sein. Im Regelfall wird auf dem Internet-Gateway/Router/Firewall ein beliebiger freier TCP-Port auf den zuvor ausgewählten Server-Port des OpenSSH-Servers weitergeleitet.

In dieser Anleitung wird exemplarisch der TCP-Port 8822 auf dem Internetgateway verwendet und auf TCP-Port 22 des OpenSSH-Servers im lokalen internen Netzwerk weitergeleitet.

3

Konfiguration von SSH-Tunneln

Die Konfiguration eines (oder mehrerer) Tunneln, in den oben aufgeführten Fluxpunkt Modulen für STARFACE, läuft immer gleich ab. Es können beliebig viele Tunnel zu unterschiedlichen Zielen angelegt werden. Ein Tunnel, der in einem Modul angelegt wurde, ist zwar in anderen Modulen sichtbar (als nützliche Information zur Vermeidung von Portkonflikten), aber nur im Ursprungsmodul änderbar. Dadurch wird sichergestellt, dass ein Tunnel, der für die Funktion eines Moduls erforderlich ist, nicht versehentlich bei der Konfiguration eines anderen Moduls verändert oder gelöscht wird. Je nach Modul kann es zudem Einschränkungen der Port-Mappings und Tunnel-Richtungen geben, die die Umsetzung der vorgesehenen Anwendungsfälle erleichtern sollen.

Die folgende Abbildung zeigt eine Tunnelkonfiguration für vier verschiedene Port-Weiterleitungen – jeweils zwei eingehende und zwei ausgehende – für den Zugriff externer Hosts auf STARFACE-Dienste und den Zugriff der STARFACE auf zwei Domänencontroller zu Benutzeranmeldung:

SSH-Tunnelkonfiguration

Alle Bezeichnungen (*remote, lokal, entfernt, etc.*) beziehen sich auf die Perspektive der STARFACE. Der *SSH-Server* kann Ziel oder Zwischenziel (Router) sein und muß einen OpenSSH-Server ausführen.

SSH-Server: * connector.intern.fluxpunkt.de SSH-Port: 8822

Benutzername: * connector-admin Kennwort: *

Fingerprint: ① 19:5b:3f:4f:1c:e6:eb:59:ee:a4:e8:9a:25:59:fe:db

Name / Kommentar: User Template PRO (debug)

⚠ Die markierten Port-Mappings erlauben es weiteren, als den unmittelbar beteiligten Hosts, durch den Tunnel zu kommunizieren.

Verbindung erfolgreich getestet Abbrechen Speichern

TCP-Port-Mappings (Dienste):

Lokaler Port	Richtung	Remote-Port	Remote-Host
1389	→	389	dc1
2389	→	389	dc2
9100	←	9100	
9999	←	9999	

Dienste-Vorlagen

Port 389 des Domänencontrollers dc1 über den SSH-Tunnel auf localhost:1389 erreichbar machen

dc2:389 über den SSH-Tunnel auf localhost:2389 erreichbar machen

Den Prometheus-Server über den SSH-Tunnel auf beliebige Hosts erreichbar machen

Vordefinierte Port-Mappings

Einige Beispiele für ungültige Konfigurationen:

SSH-Server: * connector.intern.fluxpunkt.de SSH-Port: 22

Host nicht erreichbar. Prüfen Sie Hostname und Port

Benutzername: * admin Kennwort: *

Benutzername/Kennwort ungültig

Fingerprint: ① 20:5b:3f:4f:1c:e6:eb:59:ee:a4:e8:9a:25:59:fe:db

Fingerprint des Servers: 19:5b:3f:4f:1c:e6:eb:59:ee:a4:e8:9a:25:59:fe:db

SSH-Server: * connector.fluxpunkt.de SSH-Port: 22

Unbekannter Host

Die Angaben zum SSH-Server betreffen den zuvor installierten OpenSSH-Server. Die Erreichbarkeit des Servers unter dem angegebenen Port sowie Zugangsdaten und Fingerprint werden während der Eingabe geprüft.

Die Angabe des Server-Fingerprint (einem Hash des öffentlichen Schlüssels des Servers zu Identifikationszwecken) ist optional. Beim ersten erfolgreichen Verbindungsversuch wird das Feld automatisch ausgefüllt.

Sobald die Felder *SSH-Server*, *Benutzername* und *Kennwort* ausgefüllt wurden, beginnt im Hintergrund die Verbindungsprüfung. Im Erfolgsfall wird der Server-Fingerprint ausgefüllt und in der Fußzeile *Verbindung erfolgreich getestet* ausgegeben.

TCP-Port-Mappings (Dienste)

Die Konfiguration erfolgt aus Perspektive der STARFACE. Alle Angaben, wie z.B. *remote, lokal, entfernt, etc.* beziehen sich auf diese Betrachtung.

Über die Taste **Dienste-Vorlagen** (Abb. rechts) finden Sie eine vordefinierte Auswahl an Weiterleitungskonfigurationen für verschiedene Dienste. Die Auswahl einer Vorlage fügt die entsprechenden Regelwerke in die Liste der Port-Mappings ein. Per **Mouse-Over**-Funktion auf den Port-Mapping-Feldern wird die Bedeutung der aktuellen Konfiguration ausführlich erläutert.

Ein Port-Mapping definiert, wer wie auf welche Dienste zugreifen darf. Die Symbole der Kopfzeile, sowie die darunter befindlichen Felder haben folgende Bedeutung:

STARFACE	Verschlüsselter Tunnel	SSH-Server	Optionale Weiterleitung	Optionaler Ziel-Server
Lokaler Port	Richtung	Remote-Port	Richtung	Hostname/IP

Die Felder *Lokaler Port* und *Remote-Port* werden während der Eingabe validiert. Je nach Weiterleitungsart/Richtung können z.B. nur Ports ≥ 1024 konfiguriert werden. Es wird außerdem geprüft, ob verschiedene Port-Mappings kollidierende Port-Angaben enthalten. Es ist z.B. nicht möglich, einen (1) lokalen Port auf verschiedene Remote-Ports abzubilden. Es können jedoch verschiedene Remote-Ports auf einen lokalen Port verweisen oder verschiedene lokale Ports auf einen Remote-Port.

Die Verwendung von Portnummern kleiner 1024 erfordert zudem erhöhte Rechte (Windows-Administrator- oder -System bzw. Linux-Root). Wird ein solcher Port angegeben, wird das entsprechende Feld mit einer Warnung und einem Hinweis versehen.

Ob es dem SSH-Server möglich ist, an einen gewählten Remote-Port zu binden, hängt vom SSH-Serversystem, den Rechten des SSH-Server-Dienstes und anderen darauf laufenden Diensten ab. Eine Vorabprüfung ist deshalb nicht möglich. Beim späteren Aktivieren des Tunnels wird jedoch jedes Mapping aktiv geprüft und entsprechende Fehler angezeigt.

Weiter- leitungsart	Bedeutung	Optional
	Nur der SSH-Server selbst darf über seinen Remote-Port auf den lokalen STARFACE-Port zugreifen.	UCI/XMPP5222 OpenFire Administration9090 Prometheus9100, 9999 Check_MK / Nagios6556
	Nur die STARFACE selbst darf über ihren lokalen Port auf den Remote-Port des SSH-Servers (oder eines Ziel-Servers) zugreifen.	→ Ziel-Host Eingabemaske für eine optionale Weiterleitung zu einem Ziel-Host
	Die STARFACE und mit ihr verbundene Hosts dürfen über den lokalen STARFACE-Port auf den Remote-Port des SSH-Servers (oder eines Ziel-Servers) zugreifen. Da die STARFACE in dieser Konfiguration als Gateway für andere Systeme dient, die über den SSH-Tunnel auf den Ziel-Server/SSH-Server zugreifen können, wird die entsprechende Port-Mapping-Zeile besonders hervorgehoben. Ein zusätzlicher Hinweis wird in der Fußzeile des Dialogfensters eingeblendet.	→ Ziel-Host Eingabemaske für eine optionale Weiterleitung zu einem Ziel-Host
	Der SSH-Server und mit diesem verbundene Hosts dürfen über den Remote-Port auf den lokalen STARFACE Port zugreifen. Da der SSH-Server in dieser Konfiguration als Gateway für andere Systeme dient, die über den SSH-Tunnel auf die STARFACE zugreifen können, wird die entsprechende Port-Mapping-Zeile besonders hervorgehoben. Ein zusätzlicher Hinweis wird in der Fußzeile des Dialogfensters eingeblendet.	←    (Optischer Hinweis auf die Zugriffsmöglichkeit Dritter)

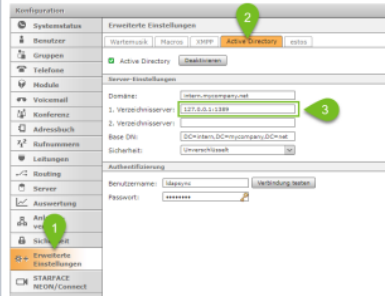
Löschen bestehender Port-Mappings

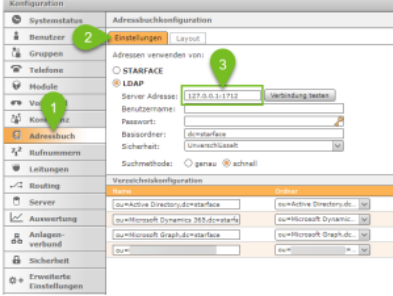
Port-Mappings können durch Auswahl des X-Symbols am rechten Zeilenrand gelöscht werden. Das Symbol wird bei einem Mouse-Over über die Port-Mapping-Zeile eingeblendet.



Die SSH-Tunnel eines Moduls werden deaktiviert, wenn der Tunnel in der Tunnelkonfiguration deaktiviert wird oder die letzte verbleibende Modulkonfiguration eines Moduls deaktiviert oder gelöscht wird. Jedes Modul stellt sicher, dass die durch seine Modulkonfigurationen angelegten Tunnel funktionieren. Hierzu wird alle 20 Sekunden ein kleines Datenpaket über den Tunnel versendet, um diesen netzwerkseitig offen zu halten und zu verifizieren, dass der Tunnel funktional ist. Sollte der Tunnel abbrechen oder nicht funktionieren, wird der Tunnel nach spätestens 20 Sekunden neu aufgebaut. Nach einem STARFACE-Neustart die in den Modulkonfigurationen aktivierten Tunnel automatisch aufgebaut.

BEISPIELKONFIGURATIONEN

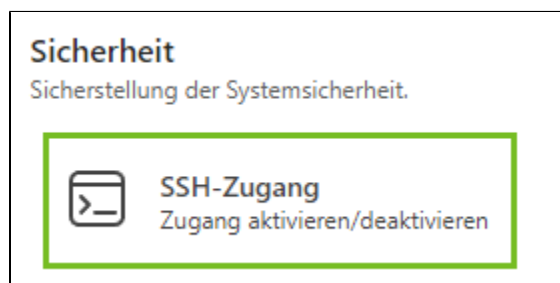
						Per Vorlage	
Zugriff der STARFACE auf ein lokales AD	1389 (beliebiger Port)		389	<Domänencontroller>* (IP oder Hostname)	Auf der STARFACE ist der Domänencontroller anschließend über 127.0.0.1:1389 erreichbar.	LDA P /LDA PS	1 2 3 

Zugriff der STARFACE auf einen lokalen Microsoft SQL-Server	1433 (beliebiger Port)		1433	<SQL-Server>* (IP oder Hostname)	Auf der STARFACE ist der SQL-Server anschließend über 127.0.0.1:1433 erreichbar.	Microsoft SQL-Server	
Zugriff der STARFACE und von Endgeräten auf ein lokales ESTOS MetaDirectory	1712 (beliebiger Port)		1712	<ESTOS MetaDirectory>* (IP oder Hostname)	Auf der STARFACE ist das MetaDirectory anschließend über 127.0.0.1:1712 erreichbar. Für Telefone im STARFACE-Subnetz ist das MetaDirectory über <STARFACE-IP>:1712 erreichbar (sofern dieser Port in der STARFACE Firewall geöffnet wurde).	estos MetaDirectory LDAP	
Zugriff auf das Prometheus-Frontend für eigene Systeme	9100 9999		9100 9999		Aus dem internen Firmennetzwerk (hinter dem SSH-Server) ist Prometheus über <SSH-Server>:9100 bzw. <SSH-Server>:9999 erreichbar.	Prometheus	

* Die Angabe eines Zielservers ist nur dann erforderlich, wenn der OpenSSH-Server nicht auf dem Zielsystem läuft. Der OpenSSH-Server leitet den Netzwerkverkehr an den Zielsystem weiter; entsprechende Netzwerkkonnektivität wird vorausgesetzt.

Beispiel: SSH-Zugriff auf STARFACE-Anlagen mit privater IP-Adresse

Falls der Zugriff auf die Linux-Konsole bei einer STARFACE-Anlage deaktiviert oder aufgrund einer Firewall unzugänglich ist und sich die Anlage in einem privaten Subnetz hinter einem NAT-Router befindet, ist für den Zugriff auf die Linux-Konsole ein mehrstufiger Prozess notwendig, den Sie mit Hilfe von [User Template PRO](#) umsetzen können. Wechseln Sie in User Template PRO zunächst auf den Tab **Einstellungen / Lizenz > STARFACE Verwaltung**. Klicken Sie dort, im Bereich Sicherheit, auf den Eintrag **SSH-Zugang**:



Aktivieren des SSH-Dienstes (falls inaktiv)

Falls der SSH-Dienst aus Sicherheitsgründen deaktiviert wurde, denken Sie bitte daran, ihn später wieder zu deaktivieren.

1

SSH-Server SSH-Tunnel

Root-Passwort: Neues Kennwort

SSH-Zugang: ☒ an

Wiederholung

Neues Passwort setzen

Public-Key	Benutzer
Neuen Public-Key hier einfügen (Format: ssh-rsa AAAA... user@hostname)	
AAAAB3NzaC1yc2EAAAADAQABAAQDJJctlgA6llsnRoYf4yP6rc49jW/KExSBz...	fluxpunkt

2

Setzen des Root-Passworts *oder* Eingabe eines SSH-Public-Keys

3

Anlegen eines SSH-Tunnels, der den Zugriff auf den SSH-Port (22/TCP) der STARFACE über einen beliebigen Port des SSH-Servers erlaubt

SSH-Tunnelkonfiguration

Alle Bezeichnungen (*remote, lokal, entfernt, etc.*) beziehen sich auf die Perspektive der STARFACE. Der SSH-Server kann Ziel oder Zwischenziel (Router) sein und muß einen OpenSSH-Server ausführen.

SSH-Server: * SSH-Port: 8822

Benutzername: * Kennwort: *

Fingerprint: ① 19:5b:3f4f:1c:e6:eb:59:ee:a4:e8:9a:25:59:fe

Name / Kommentar: User Template PRO

Ihr SSH-Server

TCP-Port-Mappings (Dienste):

22	←	2222
lokal	←	remote

Weiterleitung eines beliebigen Ports auf Port 22/TCP der STARFACE-Cloud

Dienste-Vorlagen ▾

Abbrechen Speichern

4

Auf Ihrem SSH-Server können Sie nun mittels SSH-Client (z.B. [Putty](#)) über localhost und den ausgewählten Port (hier: 2222) auf Ihre STARFACE-Instanz und dem Benutzer *root* zugreifen und sich mittels SSH-Public-Key oder dem von Ihnen gesetzten Passwort anmelden.

VERWANDTE ARTIKEL

- [STARFACE VPN-SSH-Tunnel](#)
- [Synology NAS als Veeam Gateway](#)
- [Windows: Einem Server-Zertifikat vertrauen](#)
- [Sennheiser DW an Yealink Telefon](#)
- [Jabra Pro 920 an Yealink Telefon](#)