# Teams Integration for STARFACE: Patton SBC

## Inhalt




Für die Umsetzung der Teams Integration empfehlen wir Ihnen, ausgewählte **Integrationspartner** auszuwählen, die über das entsprechende Know-How im Bereich Teams, STARFACE und Patton verfügen.

Von Fluxpunkt wurde die folgenden "Leuchtturmpartner" ausgewählt, um andere STARFACE-Partner und Endkunden bei der Integration zu unterstützen:

- EDV-BV GmbH
- GDS GmbH
- Kronshage IT
- Luithle & Luithle GmbH
- Netzwerkkontor GmbH & Co. KG
- SMEA IT Services GmbH
- STARFACE GmbH
- swissnet telecommunication ag

Alphabetische Reihenfolge ohne Wertung

Weitere Informationen und Handbücher von Patton

## Vorwort

Das vorliegende Dokument richtet sich an Integrationspartner, die einen Patton SmartNode für die Anbindung der STARFACE an Microsoft Teams einsetzen und für den Kunden betreiben oder bereitstellen möchten.

Beispielhaft werden folgende Annahmen getroffen:

1. STARFACE IP-Adresse: 10.108.2.100
2. STARFACE FQDN: starface.meinefirma.de
3. Benutzerdaten:

| | Rufnummer Extern | Rufnummer Intern | Telefon Benutzername | Telefon Kennwort |
|---|---|---|---|---|
| Benutzer 1 | +497123222 | 222 | user.01 | meingeheimessippasswort01 |
| Benutzer 2 | +497123223 | 223 | user.02 | meingeheimessippasswort02 |
| Benutzer 3 | +497123224 | 224 | user.03 | meingeheimessippasswort03 |

4. SBC Externes Interface FQDN/Protokoll/Port: 123.123.123.123 sbc.meinefirma.de/TLS/5062 (eth01)
5. SBC Internes Interface FQDN/Protokoll/Port: 192.168.1.1/UDP+TCP/5060 (eth00)

Die konkrete Konfiguration des Patton SmartNode SBC ist stark projektabhängig. Die vorliegende Dokumentation dient daher nur als Sammlung relevanter Konfigurationsbestandteile, die von einem Integrationspartner auf die konkrete Kundenumgebung angepasst werden müssen. Fluxpunkt erbringt **keine** Unterstützungsleistungen gegenüber Endkunden oder STARFACE-Partnern, die nicht ausgewählter Integrationspartner sind.

Basis der vorliegenden Konfigurationsbestandteile ist die von Patton mit Microsoft durchgeführte Zertifizierung von SBCs für Microsoft Teams mit Firmware Trinity 3.18.1 (Stand November 2020).

## Technische Voraussetzungen & Vorbereitende Maßnahmen

Für die Umsetzung der Anbindung einer STARFACE an Microsoft Teams mit Hilfe eines Patton SmartNodes sind folgende Voraussetzungen bzw. Anforderungen zu erfüllen:

- Patton SmartNode SBC (oder IAD oder Gateway) mit **Trinity-Firmware 3.18.1 oder neuer;** bevorzugt SN5500, SN5600 oder Virtual SmartNode mit Teams-Lizenzen.
- **Öffentliche IP-Adresse** für den SBC (DNAT-/Portforwarding-Szenarien werden nicht untersützt).

  In Patton **Trinity Firmwareversion 3.19 und höher** (ab Februar 2021) werden DNAT-/Portforwarding-Szenarien unterstützt! Der SBC benötigt damit keine eigene öffentliche IP-Adresse mehr, sondern kann über Portforwardings erreichbar gemacht werden.

- **FQDN** bzw. vollqualifizierter Domänenname **für den SBC** (z.B. sbc01.meinefirma.de) mit Verweis **im DNS** auf dessen öffentliche IP-Adresse.
- **X.509 Zertifikat für den SBC** von einer öffentlichen, vertrauenswürdigen Stammzertifizierungsstelle sowie Zugriff auf den zugehörigen privaten Schlüssel. Das Zertifikat muß auf den FQDN des SBC ausgestellt sein.
- Der Patton SmartNode SBC muß eine **korrekte Datums-/Uhrzeitkonfiguration** besitzen und sich bestenfalls per **NTP** mit einer präzisen Zeitquelle synchronisieren.
- **Folgende Informationen** werden zusätzlich für die Konfiguration benötigt:
  - STARFACE IP-Adresse
  - Liste aller STARFACE-Benutzer, die die Teams-Anbindung verwenden sollen, inklusive ihrer Telefonnummern (intern/extern) und den SIP-Kontodaten (Benutzername und Kennwort).

Selbstverständlich müssen der SBC und die anzubindende STARFACE per SIP und RTP unbeschränkt miteinander kommunizieren können.

## Lizenzierung

Die Patton SmartNode SBC müssen über Lizenzen mit der gewünschten Anzahl SIP-Sessions (gleichzeitige Gespräche) sowie SRTP-Channels (Anzahl verschlüsselter Kanäle) ausgerüstet werden. Da die Kommunikation mit Microsoft zwingend Verschlüsselung voraussetzt, müssen für die zu erwartende Anzahl gleichzeitiger Gespräche sowohl SIP-Sessions, wie auch SRTP-Channels in gleichem Maße lizenziert werden.

Die Modelle der Serie SmartNode SN5500 lassen sich so auf bis zu 200 gleichzeitige Gespräche aufrüsten.
Das Modell SmartNode SN5600 ist für bis zu 1.000 parallele Gespräche ausgelegt.
Der virtualisierte SmartNode kennt keine Beschränkungen – diese sind von der Leistungsfähigkeit der virtuellen Hardware abhängig.

Die von Patton ausgestellte Lizenzdatei sieht hierbei wie folgt aus und kann direkt per Copy&Paste auf der Kommandozeile des Geräts eingegeben werden:

**CLI: Eingabe auf der Kommandozeile per SSH/Telnet**

```
# SIP Sessions [sip-sessions], license serial number: 44879, system serial number: 00aabb0f2439
# Additional SIP Sessions: 20 [extra-sessions=20]
install license YdDBmT/IKgN3CZyBjNDJ6S1m+0yyXlneLhjVeNnWyl3SC

# SRTP Channels [srtp-channels], license serial number: 44880, system serial number: 00aabbcc2439
# Additional SRTP Channels: 20 [extra-channels=20]
install license Gure82bMZFNNe229ee+rEWaV2eVfOe2PJfIFzt60uKwEe
```

Ob die Lizenzen erfolgreich eingespielt wurden, kann anschließend über die Eingabe von *show system licenses* überprüft werden:

```
0F2439(cfg)#show system licenses

Local Licenses
==============

The following licenses are available on the local device:
Serial Number: 00A0BA0F2439

--------------------------------------------------------------------------------
                     Source:                    Available:      Usage:
License Name         Blt-In +  Inst. + Leased =     Total   =   Alloc +   Free
--------------------------------------------------------------------------------
sip-sessions              4       20       57          81                  81
srtp-channels             8       20                  28                  28
voice-channels            4                            4                   4
--------------------------------------------------------------------------------
iprouter                  Y                            Y
sip-registrar             Y                            Y
sip-tls-srtp              Y                            Y
transcoding               Y                            Y
--------------------------------------------------------------------------------
```

## TLS Profile

Für die Kommunikation mit Microsoft über Direct Routing ist Verschlüsselung obligatorisch. Zunächst muss der SBC mit einem X.509-Zertifikat und dem zugehörigen Private Key ausgestattet werden, um sich gegenüber Microsoft auszuweisen. Die folgenden Zeilen sind auf der Kommandozeile des Geräts einzugeben, um das Zertifikat, den Private Key und die Zertifikate der Intermediate CAs zu importieren (jeweils im PEM-Format):

⚠ Nach Eingabe des jeweiligen Import-Befehls (Zeilen 1, 13 und 21) werden die Zertifikate im PEM-Format per Copy&Paste eingefügt und mit einer Leerzeile abgeschlossen.

Die Darstellung der Zertifikate und des Private-Keys auf der linken Seite sind Beispiele und dienen der Veranschaulichung.

**CLI: Eingabe auf der Kommandozeile per SSH/Telnet**

```
0F2439#import pki:certificate/MYCERTIFICATE
Paste the contents of the file (enter an empty line when done):
-----BEGIN CERTIFICATE-----
MIIGZjCCBU6gAwIBAgIQDfw+rcYnGBfoqe36UQFQPzANBgkqhkiG9w0BAQsFADBH
QswCQYDVQQGEDJVUzEWMBQGA1UEChMNR2VvVHJ1c3QgSW5jLjEgMB4GN1UEVxMX
UmF aWRTU0wgU0hBMjU2IENBIC0gRzIwHhcNMTYxMjI1MDAwMDAwWhcNMjAwMTA1
.....................................................................
bD8l3HKHS/7u2lOzu/Ja0C5u6CSXdmPeq9Zof77vempXQHx0BwI+b5bzOAza28p5
KBbWfi+fdh6kJz2ydXUXWGbGZuBykeu1F+M65FchP7/b7EIpKgtFJJyS3EvYH1iY
1wuJqHHBIOB+3Q==
-----END CERTIFICATE-----

0F2439#import pki:private-key/myprivate.key
Paste the contents of the file (enter an empty line when done):
-----BEGIN RSA PRIVATE KEY-----
/iqCw7vgv+SuzqcCIBtmZ0iH1XAC8fs5RfoM5yeAfv/kOpjGMNg+3hB0f8MVAHcA
.....................................................................
AiEA+DtGLCgvVangxIyhXbWRbxGGEY4wmNCi7x5ib7yYGBACIQCRQlmlL2SHRlED
-----END RSA PRIVATE KEY-----

0F2439#import pki:certificate/CA
Paste the contents of the file (enter an empty line when done):
-----BEGIN CERTIFICATE-----
MChjKSAyMDA4IEdlb1RydXN0IEluYy4gLSBGb3IgYXV0aG9yaXplZCB1c2Ugb25s
.....................................................................
a2qiimBpwFd9svIxDJhlMuwIWs7GmOkhlz8seSkD9faUK1Mx85NoV+HXTzrRYaFg
-----END CERTIFICATE-----
```

- Zeile 1: Import des eigenen X.509 Zertifikats. Der Name MYCERTIFICATE kann frei gewählt werden und wird im Folgenden für die Referenzierung dieses Zertifikats verwendet. Das Zertifikat selbst (beginnend mit -----*BEGIN CERTIFICATE*----- wird per Copy&Paste eingefügt. Das Zertifikat endet auf -----*END CERTIFICATE*----- und muß durch eine Leerzeile abgeschlossen werden.
- Zeile 13: Import des privaten Schlüssels, der zum öffentlichen Schlüssel des X.509-Zertifikats gehört.
- Zeile 21: Import einer Intermediate CA, um die "Chain-of-Trust" von einer vertrauenswürdigen Root-CA bis hin zum eigenen Zertifikat zu bilden.

Die Parameter für die verschlüsselte Kommunikation werden in einem TLS Profile konfiguriert.

**TLS Profile: Parameter für die verschlüsselte Kommunikation mit Microsoft Phone System**

```
profile tls pf_tls_default
  no protocol tls-v1.0
  no protocol tls-v1.1
  compression
  authentication incoming
  authentication outgoing
  private-key pki:private-key/myprivate.key
  own-certificate 1 pki:certificate/MYCERTIFICATE
  own-certificate 2 pki:certificate/CA
  diffie-hellman-parameters pki:diffie-hellman-parameters/DEFAULT-4096
  require certificate-type server
```

- Zeile 2-3: Durch Deaktivierung der Protokolle TLS 1.0/1.1 wird TLS 1.2 erzwungen.
- Zeile 7: Verweis auf den privaten Schlüssel
- Zeile 8: Verweis auf das eigene X.509 Zertifikat, mit dem sich der SBC ausweist.
- Zeile 9: Verweis auf das/die zuvor importierte(n) Intermediate CA(s).

## VoIP Profile

Das VoIP-Profile bestimmt die Parameter, mit denen die Audiokommunikation zwischen SBC und Teams respektive SBC und STARFACE abläuft.

**VoIP Profile für die Kommunikation mit Microsoft Phone System / Teams**

```
profile voip pf_voip_microsoft
  codec 1 g711alaw64k rx-length 20 tx-length 20 silence-suppression voice-update-frames
  srtp key-lifetime 31
  media-processing forced
  srtp transmission forced
  rtp rtcp-multiplexing
```

- Zeile 2: Es wird der Audio-Codec G.711alaw gegenüber dem Microsoft SBC angeboten. Weitere Codecs werden nicht konfiguriert, damit keine Codec-Transkodierung notwendig wird (hierfür werden Hardware DSPs in Patton SmartNodes benötigt, die in begrenzter Anzahl in physikalische Geräten vorhanden sind; virtualisierte SmartNodes werden Software DSPs mit Transkodierung zu einem späteren Zeitpunkt unterstützen; vgl. Patton Roadmap).
  Microsoft verlangt von Teams-zertifizierten Geräten die Erzeugung von Komfortrauschen, weshalb Stille im Audiodatenstrom erkannt und durch Rauschen ersetzt werden soll ("silence-suppression").
- Zeile 3: Zur Verbesserung der Sicherheit wird nach $2^{31}$ Paketen der für die Verschlüsselung verwendete SRTP-Schlüssel ausgetauscht. Diese Konfigurationsoption steht ausschließlich auf physikalischen SBCs zur Verfügung und wird auf virtualisierten SmartNodes eine Fehlermeldung erzeugen, die jedoch ignoriert werden kann.
- Zeile 4: Erzwingt die Verwendung von DSP Ressourcen, die für die Verschlüsselung benötigt werden.
  Diese Konfigurationsoption steht ausschließlich auf physikalischen SBCs zur Verfügung und wird auf virtualisierten SmartNodes eine Fehlermeldung erzeugen, die jedoch ignoriert werden kann.
- Zeile 5: SRTP-Verschlüsselung ist zwingend zwischen Microsoft und SBC.
- Zeile 6: RTP und RTCP Multiplexing nach RFC5761 (Verwendung der selben Portnummern; Anforderung von Microsoft).

**VoIP Profile für die Kommunikation mit STARFACE**

```
profile voip pf_voip_starface
  codec 1 g711alaw64k rx-length 20 tx-length 20 silence-suppression voice-update-frames
  media-processing forced
  rtp rtcp-multiplexing
```

- Zeile 2: Es wird der Audio-Codec G.711alaw gegenüber der STARFACE angeboten. Weitere Codecs werden nicht konfiguriert, damit keine Codec-Transkodierung notwendig wird.
- Zeile 3: Erzwingt die Verwendung von DSP Ressourcen, die für die Verschlüsselung benötigt werden.
  Diese Konfigurationsoption steht ausschließlich auf physikalischen SBCs zur Verfügung und wird auf virtualisierten SmartNodes eine Fehlermeldung erzeugen, die jedoch ignoriert werden kann.

## Mapping Tabellen

Die folgenden Abschnitte müssen im **context cs SWITCH** der Patton-Konfiguration eingetragen werden

Der SBC muß zwischen STARFACE und Microsoft Phone System die angerufene Rufnummer bzw. deren URI-Repräsentation in die jeweils erwarteten Formate bzw. Ziele übersetzen. Eine Rufnummer auf Teams-Seite muß in einen SIP-Account-Namen auf STARFACE-Seite konvertiert werden und umgekehrt:

Die jeweiligen Werte für die SIP-Account-Namen und Telefonnummern müssen auf den konkreten Anwendungsfall angepasst werden.
Die IP-Adresse der calling-uri muß der IP-Adresse der STARFACE entsprechen!

**Übersetzung von Teams-Telefonnummern in STARFACE Account-Namen**

```
mapping-table calling-uri to calling-e164 mt_teams2starface-a-e164
  map sip:(.%) to \1
  map tel:(.%) to \1

mapping-table calling-e164 to calling-uri mt_teams2starface-a-uri
  map \+497123222 to sip:user.01@10.108.2.100
  map \+497123223 to sip:user.02@10.108.2.100
  map \+497123224 to sip:user.03@10.108.2.100

mapping-table called-e164 to called-e164 mt_teams2starface-b-internalCalls
  map (00)?49(...?)$ to \2
```

- Zeile 1-3: Das Mapping *calling-uri to calling-e164 mt_teams2starface-a-e164* entnimmt der SIP-URI die Anruferrufnummer und setzt diese als Anruferrufnummer im Feld calling-e164.
- Zeile 5: Das Mapping *calling-e164 to calling-uri mt_teams2starface-a-uri* konvertiert eine konkrete anrufende Telefonnummer zu einer anrufenden SIP-URI.
- Zeile 6-8: Konkrete Telefonnummern werden eine SIP-URI (des jeweiligen STARFACE SIP-Accounts) übersetzt, so dass der Anruf von der STARFACE dem richtigen Endgeräteaccount zugeordnet werden kann. Die IP-Adresse der SIP-URI muß der IP-Adresse der STARFACE entsprechen, da die STARFACE eingehende Anrufe von Teams ansonsten nicht dem richtigen Endgeräte-SIP-Account zuordnen kann.
- Zeile 10-12: Das Mapping *called-e164 to called-e164 mt_teams2starface-b-internalCalls* wandelt von Teams signalisierte zwei- oder dreistellige Zielrufnummern (die von Teams um die Landesvorwahl ergänzt wurden in zwei- oder dreistellige Zielrufnummern ohne Landesvorwahl um. Dadurch lassen sich interne Teilnehmer der STARFACE mit zwei- oder dreistelligen internen Rufnummern erreichen.

**Übersetzung von STARFACE SIP-Account-Namen in Teams-Telefonnummern**

```
mapping-table called-uri to called-e164 mt_starface2teams-b-e164
  map sip:(.+)@(.+) to +4971234567890
  map sip:user.01@.+ to +497123222
  map sip:user.02@.+ to +497123223
  map sip:user.03@.+ to +497123224
```

- Zeile 1: Das Mapping *called-uri to called-e164* konvertiert eine konkrete angerufene SIP-URI zu einer angerufenen Telefonnummer.
- Zeile 2: Beispiel für ein Fallback-Mapping eines beliebigen SIP-Accounts zu einer bestimmten Rufnummer (z.B. für einen Abwurfplatz).
- Zeile 3-5: Konkrete SIP-Accounts werden anhand des Account-Namens in eine Telefonnummer übersetzt, so dass der Anruf dem richtigen Teams-User zugeordnet werden kann.

Zur einfacheren Erweiterbarkeit werden alle notwendigen Anpassungen in die oben angegebenen einzelne Mapping-Tables gegliedert und durch eine Complex-Function für eine konkrete Anrufrichtung zusammengefasst:

**Sammlung der Anpassungen für die jeweilige Gesprächsrichtung**

```
complex-function cf_teams2starface
  execute 1 mt_teams2starface-a-e164
  execute 2 mt_teams2starface-a-uri
  execute 3 mt_teams2starface-b-internalCalls

complex-function cf_starface2teams
  execute 1 mt_starface2teams-b-e164
```

Complex-Functions sind Ansammlungen von Mapping-Funktionen, die der angegebenen Reihe nach ausgeführt werden und Anpassungen der SIP-Parameter vornehmen.

## Routing Tabellen

Routingtabellen definieren, zwischen welchen Schnittstellen (Interfaces) Anrufvermittlung stattfindet. Die Vermittlung von Anrufen kann von verschiedenen Parametern abhängig gemacht werden und es können Regelwerke (Complex-Functions oder Mappingtabellen) auf den vermittelten Anruf angewendet werden.

**Routingtabellen für die Weiterleitung von Anrufen zwischen STARFACE und Microsoft Phone System / Teams**

```
routing-table called-e164 rt_from_teams
  route default dest-interface if_sip_starface cf_teams2starface

routing-table called-e164 rt_from_starface
  route default dest-service hg_microsoft-teams cf_starface2teams
```

- Zeile 1-2: Die Routingtabelle *rt_from_teams* sendet alle Anrufe von Teams zum Interface *if_sip_starface* (dieses wird im folgenden Abschnitt beschrieben) und wendet die Complex-Function *cf_teams2starface* mit den darin enthaltenen Mappings an.
- Zeile 4-5: Die Routingtabelle *rt_from_starface* sendet alle Anrufe der STARFACE zur Hunting-Group *hg_microsoft-teams* (die der Reihe nach drei verschiedene georedundante Microsoft-Peers anspricht) und wendet die Complex-Function *cf_starface2teams* mit den darin enthaltenen Mappings an.

## Interfaces und SIP-Gateways

**Schnittstelle zu Microsoft Phone System / Teams**

```
interface sip if_sip_microsoft-directrouting-primary
  bind context sip-gateway gw_sip_wan_5062
  route call dest-table rt_from_teams
  remote sip.pstnhub.microsoft.com 5061
  local sbc.meinefirma.de 5062
  hold-method direction-attribute inactive
  no call-transfer accept
  privacy
  address-translation outgoing-call contact-header user-part fix sbc.meinefirma.de
  use profile voip pf_voip_microsoft
  srtp renegotiate-on-connect
  penalty-box sip-option-trigger interval 60 timeout 60 force tls
  session-timer 3600
  trust remote
  trust 52.114.0.0/16

interface sip if_sip_microsoft-directrouting-secondary
  bind context sip-gateway gw_sip_wan_5062
  route call dest-table rt_from_teams
  remote sip2.pstnhub.microsoft.com 5061
  local sbc.meinefirma.de 5062
  hold-method direction-attribute inactive
  no call-transfer accept
  privacy
  address-translation outgoing-call contact-header user-part fix sbc.meinefirma.de
  use profile voip pf_voip_microsoft
  srtp renegotiate-on-connect
  penalty-box sip-option-trigger interval 60 timeout 60 force tls
  session-timer 3600
  trust remote
  trust 52.114.0.0/16

interface sip if_sip_microsoft-directrouting-tertiary
  bind context sip-gateway gw_sip_wan_5062
  route call dest-table rt_from_teams
  remote sip3.pstnhub.microsoft.com 5061
  local sbc.meinefirma.de 5062
  hold-method direction-attribute inactive
```

```
  no call-transfer accept
  privacy
  address-translation outgoing-call contact-header user-part fix sbc.meinefirma.de
  use profile voip pf_voip_microsoft
  srtp renegotiate-on-connect
  penalty-box sip-option-trigger interval 60 timeout 60 force tls
  session-timer 3600
  trust remote
  trust 52.114.0.0/16

service hunt-group hg_microsoft-directrouting
  timeout 3
  drop-cause normal-unspecified
  drop-cause no-circuit-channel-available
  drop-cause network-out-of-order
  drop-cause temporary-failure
  drop-cause switching-equipment-congestion
  drop-cause access-info-discarded
  drop-cause circuit-channel-not-available
  drop-cause resources-unavailable
  route call 1 dest-interface if_sip_microsoft-directrouting-primary
  route call 2 dest-interface if_sip_microsoft-directrouting-secondary
  route call 3 dest-interface if_sip_microsoft-directrouting-tertiary

location-service ls_microsoft
  domain 1 microsoft.com
  domain 2 sip-du-a-eu.pstnhub.microsoft.com
  domain 3 sip-du-a-us.pstnhub.microsoft.com
  domain 4 sip-du-a-as.pstnhub.microsoft.com
  domain 5 pstnhub.microsoft.com
  domain 6 sip.pstnhub.microsoft.com
  domain 7 sip2.pstnhub.microsoft.com
  domain 8 sip3.pstnhub.microsoft.com

  identity-group DEFAULT
        user phone

    authentication inbound
      authenticate none

    registration outbound
      register none

    call outbound
      transport-protocol force tls

    call inbound
```

- Zeile 1: Primärer Microsoft Phone System/Direct Routing Peer.
- Zeile 2: Das Interface wird an das Gateway *gw_sip_wan_5062* gebunden.
- Zeile 3: Anrufe von Microsoft Phone System werden an die Routingtabelle *rt_from_teams* übergeben und dort in Richtung STARFACE geroutet.
- Zeile 4: FQDN und Portnummer des Microsoft Peers
- Zeile 5: Lokale Identität und Portnummer des SBCs
- Zeile 9: Im SIP-Contact-Header für ausgehende Anrufe den FQDN des SBCs setzen.
- Zeile 10: Zuvor konfiguriertes VoIP-Profil verwenden
- Zeile 12: In Intervallen von 60 Sekunden ein SIP-Options-Paket an Microsoft senden (zwingend)
- Zeile 17, 33: Sekundärer und Tertiärer Microsoft Phone System/Direct Routing Peer. Identische Konfiguration wie beim primären Peer; lediglich abweichende Remote-Adresse.
- Zeile 49: Hunting Group, die der Reihe nach die einzelnen Microsoft Peers anspricht (Hochverfügbarkeit); Timeout von 3 Sekunden, falls ein Peer nicht antwortet
- Zeile 63: Location Service, der Pakete von Microsoft von den angegebenen Domänen akzeptiert, "user=phone" der SIP-URI hinzufügt und als Transportprotokoll TLS erzwingt.

**Schnittstelle zur STARFACE**

```
interface sip if_sip_starface
  bind context sip-gateway gw_sip_lan_5060
  route call dest-table rt_from_starface
  remote starface.meinefirma.de
  hold-method direction-attribute sendonly
  early-disconnect
  no call-transfer accept
  no call-transfer emit
  address-complete-indication accept set
  address-translation incoming-call calling-e164 from-header
  address-translation incoming-call calling-uri from-header
  address-translation incoming-call calling-name from-header
  use profile voip pf_voip_starface
  trust remote

authentication-service as_starface-sipaccounts
  username user.01 password meingeheimessippasswort01
  username user.02 password meingeheimessippasswort02
  username user.03 password meingeheimessippasswort03

location-service ls_starface
  domain 1 starface.meinefirma.de

  identity-group teams

    authentication outbound
      authenticate 1 authentication-service as_starface-sipaccounts

    authentication inbound
          authenticate none

    registration outbound
          registrar starface.meinefirma.de
          lifetime 180
      register auto

    call outbound

    call inbound

        identity user.01 inherits teams
        identity user.02 inherits teams
        identity user.03 inherits teams
```

**SIP-Gateways**

```
context sip-gateway gw_sip_lan_5060
  bind location-service ls_starface

  interface if_gw_sip_lan_5060
    transport-protocol udp+tcp 5060
    no transport-protocol tls
    bind ipaddress ROUTER if_eth00 if_eth00

context sip-gateway gw_sip_lan_5060
  no answer-untrusted-hosts
  no shutdown

context sip-gateway gw_sip_wan_5062
  use profile tls pf_tls_default
  bind location-service ls_microsoft

  interface if_gw_sip_wan_5062
    no transport-protocol udp+tcp
    transport-protocol tls 5062
    bind ipaddress ROUTER if_eth01 if_eth01
    spoofed contact-header manual sbc01.fluxpunkt.de port 5062
    spoofed via-header manual sbc01.fluxpunkt.de port 5062

context sip-gateway gw_sip_wan_5062
  no answer-untrusted-hosts
  connection-reuse
  no shutdown
```

## IP-Router und physikalische Netzwerkport-Konfiguration

**IP Router Konfiguration**

```
context ip ROUTER

  interface if_eth00
        ipaddress if_eth00 192.168.1.1/24
    tcp adjust-mss rx mtu
    tcp adjust-mss tx mtu

  interface if_eth01
    ipaddress if_eth01 123.123.123.123/28
    tcp adjust-mss rx mtu
    tcp adjust-mss tx mtu
```

**Physikalische Portkonfiguration**

```
port ethernet 0 0
  bind interface ROUTER if_eth00
  no shutdown

port ethernet 0 1
  bind interface ROUTER if_eth01
  no shutdown
```