

04.07.2022

STARFACE SIP Trusted IP Helper Modul

Dieses Modul dient dazu, fehlschlagende eingehende Anrufe zu verhindern, die von der STARFACE abgelehnt werden.

Designed wurde das Modul aufgrund der bekannten Probleme mit der Telekom im Zusammenhang mit fehlschlagenden eingehenden Anrufen. Es kann aber auch für andere Provider eingesetzt werden.

Um zu verstehen, was das Modul genau macht, muss das Problem verstanden werden, welches damit gelöst werden soll.

Frage / Fehlerbeschreibung:

Seit etwa einem Jahr tritt vermehrt das Problem auf, dass Telekomanschlüsse nicht mehr eingehend erreichbar sind. Der Anrufer erhält in diesem Fall eine Ansage vom Provider, dass die Rufnummer nicht vergeben sei.

Dies geschieht dann so lange weiter, bis die STARFACE neu gestartet wird.

Identifikation:

Im PBX.log (Log des Asterisk) der STARFACE ist dann folgender Fehler erkennbar:

```
chan_sip.c: Call from '' (217.0.21.65:5060) to extension '<Zielrufnummer>' rejected because extension not found in context 'default'.
```

Die Meldung "extension not found in context 'default'" kann mehrere Gründe haben.

In diesem konkreten Fall wird diese Meldung ausgegeben, da die Quell-IP des SIP-Invites der STARFACE nicht bekannt ist.

Der auf der STARFACE verwendete Asterisk erlaubt aus Sicherheitsgründen nur Anrufe von bekannten Quellen. Diese werden in der Datei sip.conf im Verzeichnis /etc/asterisk gespeichert.

Hier sind dann Einträge für die an der STARFACE angebotenen Endgeräte und Providerleitungen zu finden.

Die sip.conf wird hierbei regelmäßig aktualisiert. Hierfür führt die STARFACE alle 24 Stunden eine DNS-Auflösung auf die im Providerprofil hinterlegten SIP-Hosts aller Leitungen durch und speichert die hier erhaltenen IP-Adressen in der sip.conf.

Diese IPs dürfen dann auf dem Asterisk anrufe starten.

Nun besteht allerdings das Problem, dass die Telekom immer wieder Umstellungen an deren SIP-Hosts durchzuführen scheint, wodurch manchmal bei der DNS-Auflösung nicht alle Hosts der Telekom zurückgegeben werden.

Dies führt dazu, dass die Telekom anschließend SIP-Invites von IPs sendet, die nicht in der sip.conf enthalten sind und dementsprechend vom Asterisk abgeblockt werden.

Im DNS.log der STARFACE ist dies wiederum gut nachvollziehbar.

Schaut man sich hier die letzte DNS-Auflösung vor dem ersten Fehlerfall an, fällt hier immer auf, dass die Quell-IP des Anrufs fehlt.

Im Beispielfehlerfall ist im PBX.log gut zu erkennen, dass der Anruf von der 217.0.21.65 abgelehnt wird:

```
chan_sip.c: Call from '' (217.0.21.65:5060) to extension '<Zielrufnummer>' rejected because extension not found in context 'default'.
```

Im DNS.log fehlt diese IP wiederum bei der letzten DNS-Auflösung:

```
[DnsResolver] ----- RESOLVING DNS SERVICE ( Name:tel.t-online.de Secured:false TCP:false Dns Server: ) -----  
-----  
[DnsResolver] | A dnsService (d-epp-110.edns.t-ipnet.de): Entry{ h='217.0.28.33', p=-1, w=-1, d=A, n='' }  
[DnsResolver] | A dnsService (b-epp-110.edns.t-ipnet.de): Entry{ h='217.0.21.129', p=-1, w=-1, d=A, n='' }  
[DnsResolver] | A dnsService (h2-epp-110.edns.t-ipnet.de): Entry{ h='217.0.29.33', p=-1, w=-1, d=A, n='' }  
[DnsResolver] | -- Found DNS Entries: --  
[DnsResolver] | [Entry{ h='217.0.28.33', p=20, w=0, d=A, n='' }, Entry{ h='217.0.21.129', p=10, w=0, d=A, n='' },  
Entry{ h='217.0.29.33', p=30, w=0, d=A, n='' }]  
[DnsResolver] | -- After sorting: --  
[DnsResolver] | [Entry{ h='217.0.21.129', p=10, w=0, d=A, n='' }, Entry{ h='217.0.28.33', p=20, w=0, d=A, n='' },  
Entry{ h='217.0.29.33', p=30, w=0, d=A, n='' }]  
[DnsResolver] | -- After removed double entries: --  
[DnsResolver] | [Entry{ h='217.0.21.129', p=10, w=0, d=A, n='' }, Entry{ h='217.0.28.33', p=20, w=0, d=A, n='' },  
Entry{ h='217.0.29.33', p=30, w=0, d=A, n='' }]
```

Hierbei handelt es sich um ein vom Provider (in diesem Fall die Deutsche Telekom) ausgelöstes Problem, welches alle Asterisk basierten Telefonanlagen betrifft, nicht nur die STARFACE!

Lösung durch das STARFACE SIP Trusted IP Helper Modul:

Das Modul umgeht dieses Problem, indem dieses die sip.conf des Asterisk pflegt.

Hierfür überwacht Das Modul in einem konfigurierbaren Zeitintervall die pbx.log und sucht nach der oben genannten „extension not found“-Meldung.

Anschließend wird die darin enthaltene IP-Adresse mit dem im Modul angegebenen freigegebenen Subnetzraum verglichen und bei einem passenden Logeintrag in der Whitelist des Moduls gespeichert.

In einem ebenfalls konfigurierbaren Zeitintervall überprüft das Modul wiederum die sip.conf und ergänzt diese um alle IPs der Modulwhitelist, die in der sip.conf fehlen.

Das Modul ist dadurch also lernfähig und lernt somit mit der Zeit alle nötigen IPs des Providers, damit die Anrufe nicht mehr geblockt werden.

Die IPs sind auch manuell in der Whitelist eintragbar.

Konfiguration des Moduls:

Modul-Konfiguration: IP-Helper					
<div style="display: flex; border-bottom: 1px solid black;"> <div style="border: 1px solid black; padding: 2px 5px; margin-right: 5px;">Allgemein</div> <div style="border: 1px solid black; padding: 2px 5px; margin-right: 5px; background-color: #f4a460;">Konfiguration</div> <div style="border: 1px solid black; padding: 2px 5px;">Experten-Einstellung</div> </div>					
Konfiguration					
Name der Leitung zu der die Instanz gehört	*1 <input type="text"/>				
Beim Speichern SIP-Reload ausführen	*2 <input type="checkbox"/>				
Regelmässiger SIP.conf Check ausführen	*3 <input checked="" type="checkbox"/>				
E-Mail Alarm, wenn eine neue IP hinzugefügt wurde	*4 <input type="checkbox"/>				
Alarm E-Mail	*5 <input type="text"/>				
Vertraute Subnetze	*6 <div style="border: 1px solid black; padding: 2px;"> <div style="background-color: #f4a460; padding: 2px;">IP/CIDR</div> <div style="border: 1px solid black; padding: 2px;">217.0.0.0/16</div> <div style="text-align: right; padding: 2px;"> X </div> <div style="text-align: right; padding: 2px;"> + </div> </div>				
Die Liste der Vertrauten IP's wird automatisch geführt. Es können auch manuell Einträge hinzugefügt werden.					
Liste der Vertrauten IPs	*7 <table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th style="background-color: #f4a460;">IP</th> <th style="background-color: #f4a460;">Kommentar</th> </tr> </thead> <tbody> <tr> <td style="height: 20px;"></td> <td></td> </tr> </tbody> </table> <div style="text-align: right; padding: 2px;"> + </div>	IP	Kommentar		
IP	Kommentar				

*1 Hier muss der Name der betroffenen Leitung hinterlegt werden. Dies ist wichtig für die korrekte Ergänzung der sip.conf.

*2 Durch diese Checkbox wird beim speichern des Moduls ein SIP-Reload durchgeführt. Dadurch lädt der Asterisk die sip.conf neu.

*3 Mit dieser Checkbox wird die Überwachung der sip.conf aktiviert / deaktiviert.

*4 *5 Mit diesen Optionen kann eine E-Mail-Benachrichtigung eingerichtet werden um festzustellen, wann der Fehlerfall jeweils aufgetreten ist.

*6 Hier wird der Subnetzraum definiert, auf dessen Basis die pbx.log überprüft wird. Die Telekom sendet ihre Invites soweit uns bekannt immer aus dem 217.0.0.0/16 Subnetz. Es können aber auch andere Subnetze eingetragen werden.

*7 Dies ist die Whitelist, in die die im konfigurierten Subnetzraum zugehörigen IP's eingetragen werden, von denen Invites fehlschlagen. Hier sind die IPs inklusive Datum und Uhrzeit des Hinzufügens ersichtlich.

Modul-Konfiguration: IP-Helper			
Allgemein	Konfiguration	Experten-Einstellung	
LogCrawler-Intervall *8			
Zeitintervall:	Minute	Wiederholung jede(n)	30. Minute
Start (dd.mm.jjjj):	1	1	2022
		Zeit (hh:mm):	1 0
SIP.conf Checker *9			
Zeitintervall:	Minute	Wiederholung jede(n)	1. Minute
Start (dd.mm.jjjj):	1	1	2022
		Zeit (hh:mm):	1 0

*8 Hier ist das Zeitintervall konfigurierbar, in dem die PBX.log überprüft wird.

Wird zu diesem Zeitpunkt eine IP gefunden, wird diese automatisch in der sip.conf hinterlegt und ein sip-reload durchgeführt.

Dieser Vorgang benötigt Systemressourcen, weshalb es zu empfehlen ist, das Intervall bei größeren Anlagen zu erhöhen.

Ein kürzeres Intervall bedeutet eine kürzere Ausfallzeit, falls der Fehler auftreten sollte.

*9 Hier wird das Zeitintervall konfiguriert, in dem die sip.conf mit der Modulwhitelist verglichen und ergänzt wird.

Dadurch wird auch nach Systemneustart die sip.conf mit bisher bekannten IP's gefüllt.

Haftungsausschluss

Mit dem STARFACE SIP Trusted IP Helper Modul können grundlegende Sicherheitseinstellungen der STARFACE Telefonanlage aufgehoben werden. Die Möglichkeit, beliebige IPs oder Subnetze für INVITES freizugeben, kann bei falscher oder zu weitreichender Konfiguration eine Sicherheitslücke darstellen.

Die einzig sichere Methode dieses Modul zu benutzen, besteht darin die Whitelist manuell zu pflegen und die eingetragenen IPs regelmäßig zu überprüfen. Wird das Modul so konfiguriert, dass es IPs aus einem vertrauten Subnetz automatisch der Whitelist hinzufügt, ist darauf zu achten, dass das Subnetz klein wie möglich ist.

Die Pflege der Moduleinstellungen obliegt ausschließlich dem Administrator der Telefonanlage.

Für die Aktivierung und Einrichtung des Moduls sowie daraus resultierender Sicherheitslücken haftet ausschließlich der Administrator der Telefonanlage.

Für Schäden jeglicher Art, die aus der Verwendung des STARFACE SIP Trusted IP Helper Moduls resultieren, übernimmt die STARFACE GmbH keine Haftung.