UNIFY Harmonize your enterprise

HiPath 3000 V9
OpenScape Office V3

Tutorial
SIP Attack Protection -
Diagnostic and SIP Provider configuration

Version 1.0

2011-12-08

SIP Attack Protection - Diagnostic and SIP Provider Configuration Hints

In the past the systems were faced with different attacks from the Internet, thus the interfaces had to be equipped with a protection mechanism against such attacks. A hardened SIP stack has been implemented for OpenScape Office V3.2 and HiPath 3000 V9. Those measures require special attention to SIP provider configuration. SIP providers which use unknown IP addresses or ports will not work any longer.

How does OpenScape Office / HiPath 3000 help to protect against SIP attacks?

1) If configuring a new SIP endpoint, the system activates authentication by default and protects the access by a random password.
   -> registration hijacking is prevented
2) A SIP filter allows message reception from trusted peers only.
   Trusted peers are
   - registered endpoints
   - configured trunking partners
   - configured ITSP's

   -> all unauthorized peers are blocked
3) Message floods are detected and originating peers are blocked.
   -> avoid denial of service
4) Eventlogs for attack attempts / missing authentication are provided.
   -> get diagnostic information

If you cannot connect to the system or detect failures in call establishment and/or registration this might be caused by a wrong configuration which may end up in treating a certain endpoint /provider as "not trusted".
The following Events/Traces will give you helpful information in such cases.

Helpful diagnostics for determining problems caused by SIP-Attack protection

1. *Authentication was switched OFF*

```
EventLogEntry from ERH [ldh:192.168.138.90] ….:
EventType: Major
EventCode: MSG_ERH_SECURITY_DENIAL
EventText: fGetERHSIPSubConfigValues: Warning! SIP Authentication is deactivated for subscriber=3561
```

Recommeded measures:

- Switch authentication on again
- Check, if there is unauthorized administration access to the system, if this was not done intentionally

2. *Possible Attack from outside detected (REGISTER with spoofed address)*

```
EventLogEntry from ERH [ldh:192.168.138.90] ….:
EventType: Warning
EventCode: MSG_ERH_SECURITY_DENIAL
EventText: !!Possible-Attack: SIP_PContactInfo-IpAddress does not match with sender
contact=192.168.138.200,sender=89.227.45.11
```

Recommended measures:

- Check firewall settings for your LAN, disable port forwarding for SIP.

3. *Message flood leads to Peer blocking*

```
EventLogEntry from SIP_SA [ldh:192.168.138.90] ….:
EventType: Major
EventCode: SIP_INVALID_PARAMETER_VALUE
EventText: NetworkReceptionSvc: SIP message flood  PeerAddr=89.227.45.11:5060 blocked
```

Recommended measures:

- Check firewall settings for your LAN, disable port forwarding for SIP.
- Eliminate source, if attack is internal.

4. *SIP Attack from untrusted Peer*

Messages are blocked from a “not trusted” peer. If you suspect SIP attacks or have SIP connections, which do not work please **activate the trace component SIP_SA with level 3**. Trace entries, containing the peer address and SIP message, will be printed in the tracelog file.

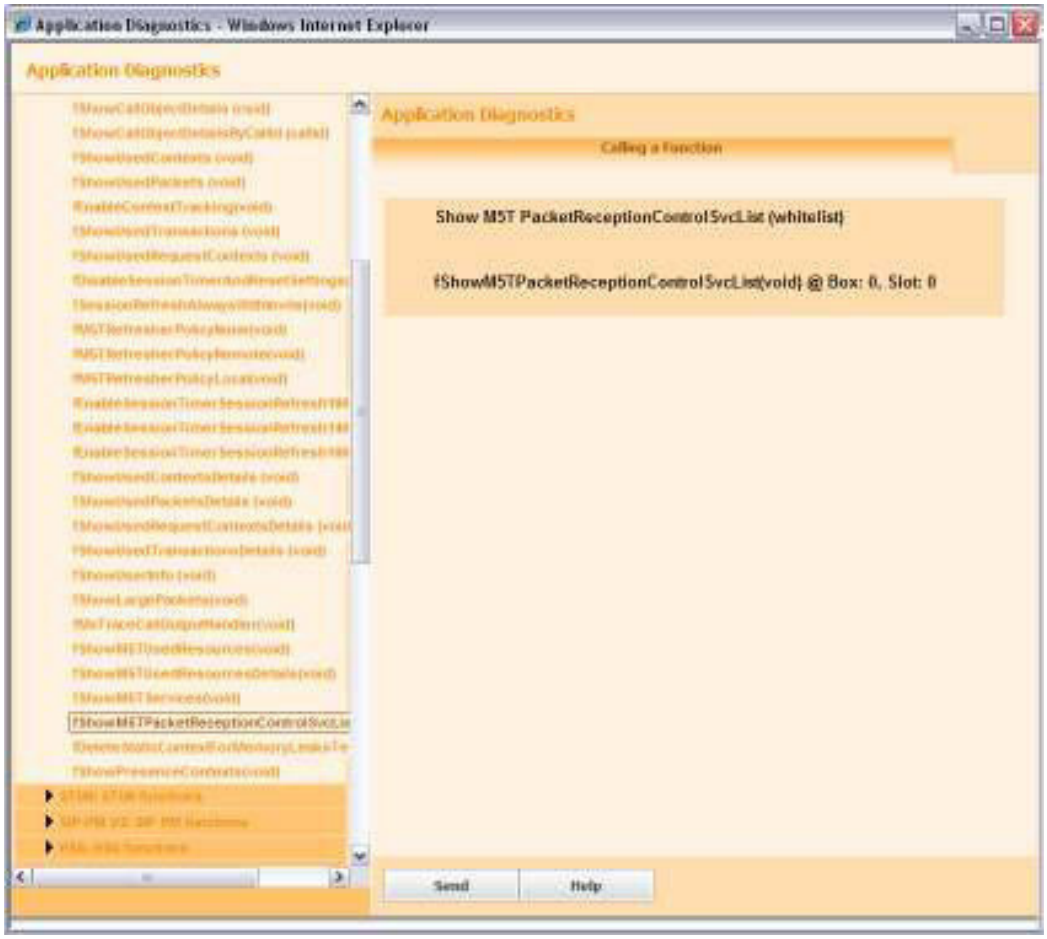
```
(SIP_SA [ldh:192.168.138.72] 0x3023 "11/24/2011 15:40:57.611601" CSipEngine.cpp 6764)
PacketReceptionControlMgr:EvUnapprovedPeerPacketReceived  PeerAddr=192.168.138.70:43597  method=OPTIONS
```

Recommended measures:

- Check firewall settings for your LAN, disable port forwarding for SIP.
- If a wanted connection is blocked, follow the configuration hints below

.

A diagnostic function is available to print the list of trusted peers at Expert mode > Maintenance > Application diagnostics > Mainboard > SSA:SSA functions

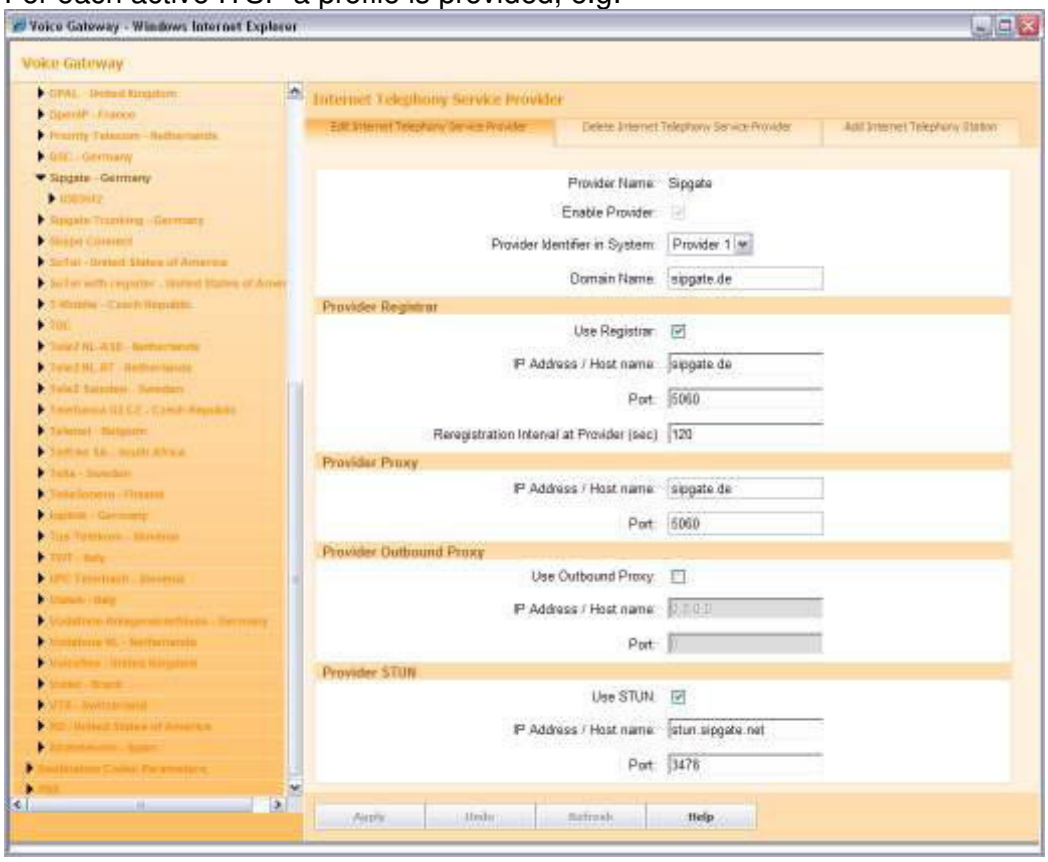


When calling this function by pressing “Send”, a list containing all trusted peers will be printed. If port=0 is listed for an IP-address, all ports are accepted, otherwise the listed port only.

```
ApprovedPeerList  size=6
   PeerList[0]:  172.17.164.161:5060
   PeerList[1]:  172.17.164.162:5060
   PeerList[2]:  172.17.164.157:5060
   PeerList[3]:  172.17.162.152:0
   PeerList[4]:  172.17.164.159:5070
   PeerList[5]:  172.17.160.13:5060
```

Configuration hint for connections with ITSP’s using different Servers in a static configuration

For each active ITSP a profile is provided, e.g:



Provider Registrar and Provider Proxy can be configured either by an IP-Address or Hostname. It is important to know that the system accepts incoming SIP packets only from the peers specified by these entries.

Configuration examples:

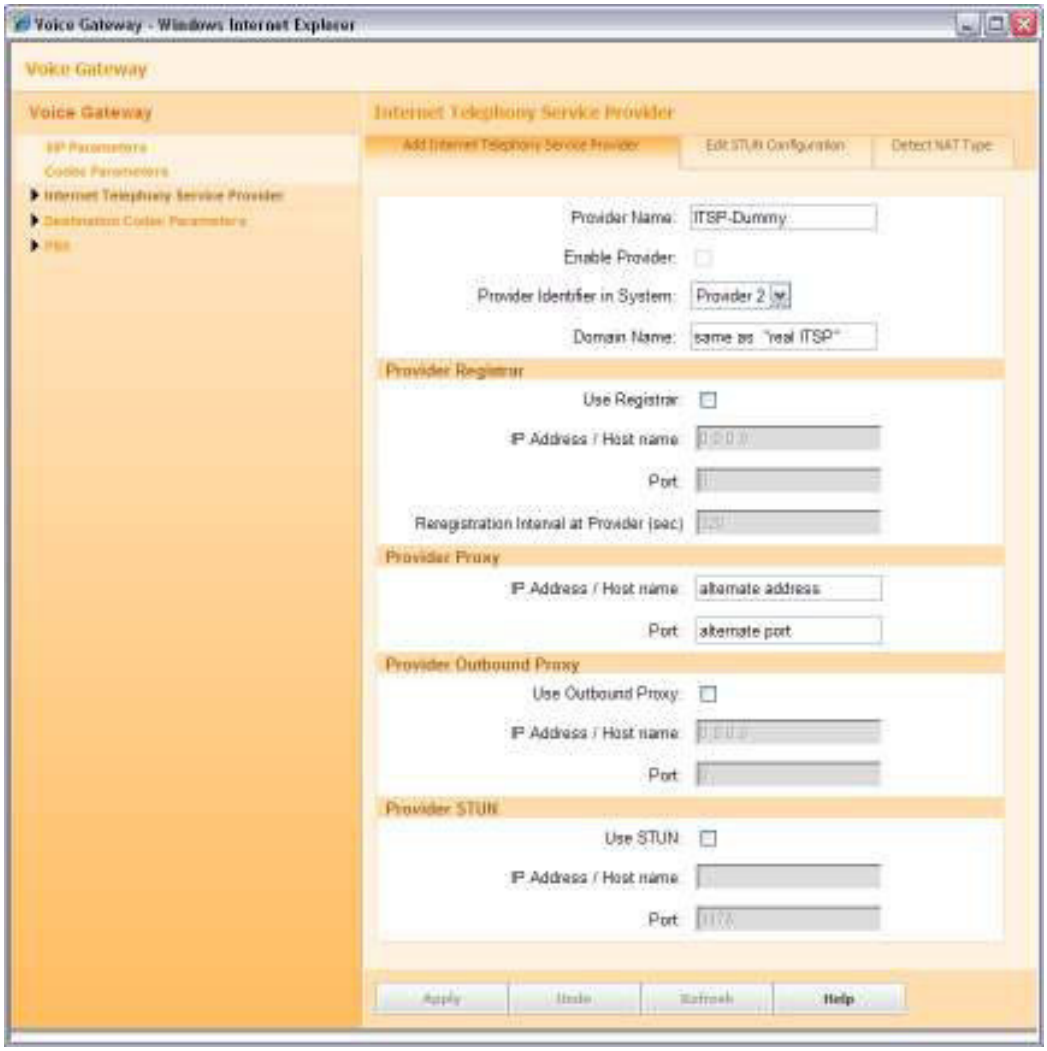
IP-Address / Host name	Port	Packets accepted from
87.237.24.13	5060	87.237.24.13:5060
Sipgate.de	5060	IP Address returned from DNS-A query:5060
vp.thinktel.ca	0	All IP-Addresses returned from DNS-SRV and DNS-A

If a provider operates different servers, it is crucial to use DNS-SRV, so that the system can learn the IP-Addresses where incoming SIP packets must be accepted.

If DNS-SRV is NOT used, such a provider needs a special configuration workaround:

A “dummy provider” has to be created where the different server, which is used by the provider, is configured.

- Enter Provider Name
- Select next unused Provider Identifier
- Switch “Use Registrar” off
- Configure “Provider Proxy” for additional server
- Use same STUN setting as for real ITSP
- Add a “dummy user account” at the tab “Add Internet telephony station”
- Enable the “dummy provider” using the wizard at Setup > Central telephony > Internet telephony



!	If LCR routing entries in dialplan had been changed manually, these changes have to be checked / restored, as they may have been changed by the ITSP

	wizard.

The same workaround is necessary if the provider uses a different port for sending than for receiving messages (e.g. port 5060 is configured, system sends all SIP messages to port 5060, but the provider sends back with src-port 5061).

This workaround is limited to max 3 additional addresses if one real ITSP is used.

About Unify

Unify is one of the world's leading communications software and services firms, providing integrated communications solutions for approximately 75 percent of the Fortune Global 500. Our solutions unify multiple networks, devices and applications into one easy-to-use platform that allows teams to engage in rich and meaningful conversations. The result is a transformation of how the enterprise communicates and collaborates that amplifies collective effort, energizes the business, and enhances business performance. Unify has a strong heritage of product reliability, innovation, open standards and security.

Unify.com

Copyright © Unify Software and Solutions GmbH & Co. KG 2015
Mies-van-der-Rohe-Str. 6, 80807 Munich/Germany
All rights reserved.

The information provided in this document contains merely general descriptions or characteristics of performance which in case of actual use do not always apply as described or which may change as a result of further development of the products. An obligation to provide the respective characteristics shall only exist if expressly agreed in the terms of contract.

Availability and technical specifications are subject to change without notice.

Unify, OpenScape, OpenStage and HiPath are registered trademarks of Unify Software and Solutions GmbH & Co. KG. All other company, brand, product and service names are trademarks or registered trademarks of their respective holders.

UNIFY Harmonize your enterprise