

Anschluss einer VoIP-fähigen Telefonanlage hinter einer Digitalisierungsbox Standard / Premium-MGW

1. Vorbereitung

Nach der Inbetriebnahme durch den Schnellstartassistenten bitte zuerst sicherstellen, dass die Mediagateway Komponente deaktiviert ist.

Menü:

VoIP – Einstellungen, Registerkarte „Optionen“

Teilnehmer		SIP-Konten	Standorte	ISDN-Trunks	Optionen
Basisparameter					
Status des Media Gateways	<input type="checkbox"/>	Aktiviert			
Session Border Controller Modus	Auto				
Anrufrkontrolle für lokale Nummern	<input checked="" type="checkbox"/>	Aktiviert			
Media Stream Termination	<input checked="" type="checkbox"/>	Aktiviert			
Standard-Abwurfnebenstelle					
Wahlpause	5	Sekunden			
SIP-Provider-Einstellungen					
DSCP-Einstellungen für SIP-Daten	DSCP-Binärwert	110000			
SIP Port	5060				
Erweiterte Einstellungen					
OK Abbrechen					

Als weitere Vorbereitung bitte an der Telefonanlage / PBX überprüfen (oder so ändern) und sicherstellen, ob / dass die folgenden DSCP-Werte (lt. 1TR114) verwendet werden:

SIP: binär 110000 / dezimal 48 / hexadezimal 30

RTP: binär 101110 / dezimal 46 / hexadezimal 2e

2. Durchführung des Assistenten „VoIP PBX im LAN“

Rufen Sie jetzt bitte den Assistenten „VoIP PBX im LAN“ auf und nehmen die entsprechenden Eintragungen vor.

Bei der WAN-Schnittstelle tragen Sie Ihren **PPPoE WAN-Partner** ein (nicht die Modem-Schnittstelle) und definieren dann im Feld darunter die Upload Geschwindigkeit dieser Schnittstelle. Dieser Wert dient der Kalkulation darüber, ab wann Pakete aus der Default Queue (Best Effort) „weggeschmissen“ werden müssen zu Gunsten der priorisierten Pakete. Im DSCP-Filter kann der Vorschlag übernommen werden, der Eintrag der IP-Adresse der Telefonanlage PBX komplettiert den Assistenten.

Menü:

Assistenten – VoIP PBX im LAN, -> „Neu“

VoIP PBX im LAN

Geben Sie die Einstellungen der VoIP PBX im LAN ein:	
WAN-Schnittstelle für VoIP-Priorisierung	DTAG Internet Zugang ▼
Maximale Upload-Geschwindigkeit	10000 kbit/s
DSCP-Filter zur Priorisierung	TOS-Binärwert ▼ 10111000
IP-Adresse der VoIP PBX im LAN	<div style="border: 1px solid #ccc; padding: 2px;"> IP Adresse <input style="background-color: #ffffcc;" type="text" value="192.168.2.?"/> 🗑️ </div> <div style="text-align: center; margin-top: 5px;"> Hinzufügen </div>

Der Assistent setzt entsprechende Filter auf den DSCP-Wert im QoS, klassifiziert den gefilterten Traffic als „HP“ und erstellt auf dem WAN-Interface die entsprechende HP-Queue sowie das Traffic Shaping für den maximalen Upload Wert.

Zusätzlich werden im NAT für die angegebene IP-Adresse der Telefonanlage /PBX ausgehende Einträge erzeugt, die ein „Full-Cone-NAT“ ermöglichen. Diese Einträge bitte **nicht** mittels GUI editieren!

3. Komplettierung der QoS-Filter und HP-Queue für SIP-DSCP Wert „110000“

Da die durch den Assistenten angelegten Filter bisher nur den RTP-Traffic abdecken, sollten entsprechende Filter für SIP-Traffic auch angelegt werden und diesen ebenfalls in die Klasse „High Priority“ (HP) einordnen.

Menü:

Netzwerk – QoS, Registerkarte „IPv4/IPv6-Filter“, -> „Neu“

IPv4/IPv6-Filter

QoS-Klassifizierung
QoS-Schnittstellen/Richtlinien

Basisparameter	
Beschreibung	SIP-Traffic
Dienst	any ▼
IPv4-Zieladresse/-netzmaske	Beliebig ▼
IPv6-Zieladresse/-länge	Beliebig ▼
IPv4-Quelladresse/-netzmaske	Beliebig ▼
IPv6-Quelladresse/-länge	Beliebig ▼
DSCP / Traffic Class Filter (Layer 3)	DSCP-Binärwert ▼ 110000
COS-Filter (802.1p/Layer 2)	Nicht beachten ▼

OK
Abbrechen

Menü:
 Netzwerk – QoS, Registerkarte „QoS-Klassifizierung“, -> „Neu“

IPv4/IPv6-Filter
QoS-Klassifizierung
QoS-Schnittstellen/Richtlinien

Basisparameter	
Klassenplan	VoIP-QoS-Assistent ▾
Filter	SIP-Traffic ▾
Richtung	Ausgehend ▾
High-Priority-Klasse	<input checked="" type="checkbox"/>
DSCP/Traffic-Class-Filter setzen (Layer 3)	Erhalten ▾
Setze COS Wert (802.1p/Layer 2)	Erhalten ▾

OK
Abbrechen

Als Resultat werden nun sowohl SIP- als auch RTP-Traffic in die vom Assistenten bereits angelegte HP-Queue auf dem WAN-Partner eingeordnet und entsprechend priorisiert:

IPv4/IPv6-Filter
QoS-Klassifizierung
QoS-Schnittstellen/Richtlinien

Ansicht 20 pro Seite << >> Filtern in Keiner ▾ gleich ▾ Los							
Klassenplan	Zugewiesene Schnittstelle	Filter	Zugewiesene Klassen-ID	Richtung			
VoIP-QoS-Assistent	DTAG Internet Zugang						
		VoIP-QoS-Assistent	HP	Ausgehend			
		SIP-Traffic	HP	Ausgehend			

Seite: 1, Objekte: 1 - 3

Neu

4. Anpassung der IPv4 Firewall

Durch das Firewall Zonenkonzept der Digitalisierungsbox und den Status der WAN-Schnittstellen als „untrusted“ muss eine zusätzliche Regel den eingehenden Traffic ermöglichen. Ansonsten käme dieser z.B. im Falle von „Early Media“ zwar durch die NAT (siehe Full-Cone-NAT durch den Assistenten), würde aber durch die Firewall geblockt werden.

Zuerst muss die IP-Adresse der Telefonanlage / PBX und „Any_UDP“ als Alias zur Erstellung der Regel definiert werden.

Menü:
 Firewall – Adressen, Registerkarte „Adressliste“, -> „Neu“

Adressliste Gruppen

Basisparameter	
Beschreibung	PBX
IPv4	<input checked="" type="checkbox"/> Aktiviert
Adresstyp	<input checked="" type="radio"/> Adresse/Subnetz <input type="radio"/> Adressbereich
Adresse/Subnetz	192.168.2.? / 255.255.255.255
IPv6	<input type="checkbox"/> Aktiviert

Menü:
 Firewall – Dienste, Registerkarte „Dienstliste“, -> „Neu“

Dienstliste Gruppen

Basisparameter	
Beschreibung	Any_UDP
Protokoll	UDP
Zielportbereich	0 65535
Quellportbereich	0 1 <input checked="" type="checkbox"/> Nicht beachten

Nun kann mit Hilfe dieser Aliase in den Richtlinien eine entsprechende IPv4 Filterregel erstellt werden, die vor dem Default Verhalten eingehenden UDP-Traffic zur IP-Adresse der Telefonanlage / PBX erlaubt.

Menü:
 Firewall – Richtlinien, Registerkarte „IPv4-Filterregel“, -> „Neu“

IPv4-Filterregeln IPv6-Filterregeln Optionen

Basisparameter	
Quelle	WAN_DTAG INTERNET ZUGANG
Ziel	PBX
Dienst	Any_UDP
Aktion	Zugriff

Dieses resultiert dann ausgehend vom Standard in folgenden Regeln:

Ansicht 20 pro Seite << >> Filtern in Keiner gleich Los

Abfolge	Quelle	Ziel	Dienst	Aktion	Priorität	Richtlinie aktiv				
1	WAN_DTAG INTERNET ZUGANG	PBX	Any_UDP	Zugriff	Keine	<input checked="" type="checkbox"/> Aktiviert				

Seite: 1, Objekte: 1 - 1

Standardfilterregeln

Abfolge	Quelle	Ziel	Dienst	Aktion	Priorität	Richtlinie aktiv
n+1	Vertrauenswürdige Schnittstellen	Beliebig	beliebig	Zugriff	Keiner	<input checked="" type="checkbox"/> Aktiviert
n+2	Nicht vertrauenswürdige Schnittstellen	Beliebig	beliebig	Verweigern	Keiner	<input checked="" type="checkbox"/> Aktiviert

Neu OK Abbrechen

Sollten noch weitere Filterregeln definiert sein, achten Sie bitte unbedingt auf die Reihenfolge der Regeln.

In der Stateful Inspection Firewall gilt:

Traffic, den ich vorher verbiete kann ich hinterher nicht mehr erlauben (und umgekehrt)!