Unified Communications by innovaphone
Technical Workshop

innovaphone

PURE IP COMMUNICATIONS

Agenda

- **Simplified Licenses**
- **WebRTC**
- **Opus**
- **Conferencing**
- **myPBX Single Sign On**
- **myPBX Toolbox**
- **All IP**
- **Anywhere Workplace**
- **Reverse Proxy**
- **TURN**
- **New Hardware**

Simplified Port Licenses

Until now:

- The first registration on an object (regardless what type) takes one license

Now:

- The first registration on an User, Executive, Gateway or Trunk object takes one license

=> Eliminates „unexpected“ license requirements, such as:

- Registration on a Waiting Queue for setting CFx
- Slave registrations on a Master- PBX
- Registration of a Master-PBX on a „License only“ Master

Agenda

- Simplified Licenses
- **WebRTC**
- Opus
- Conferencing
- myPBX Single Sign On
- myPBX Toolbox
- All IP
- Anywhere Workplace
- Reverse Proxy
- TURN
- New Hardware

myPBX

Major areas of improvement

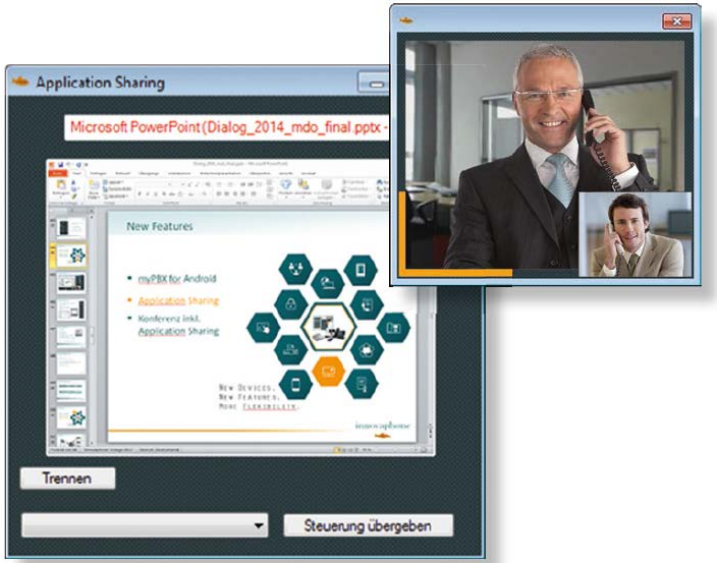
- Support of WebRTC completed
  - WebRTC myPBX with Video
  - WebRTC myPBX with Application Sharing
  - Opus Audio Codec
  - VP8 Video Codec
  - ICE/TURN

- Netlogon

- Conferences
  - Video Support

myPBX WebRTC Application Sharing

- Application Sharing without „myPBX Launcher“
  Not longer only for Windows



- WebRTC Application Sharing users cannot share their own screen
- But they can control shared content

innovaphone

WebRTC Video - Codecs

- WebRTC compatible browsers will support VP8 und H.264
- Both codec have similar quality
- VP8 will supported by myPBX Launcher

→ Good Video-compatibility between WebRTC and innovaphone endpoints

- Video-Bandwidth ca. 300kbps (VP8 and H.264)
- Currently no Videoconference with Chrome
- Chrome intents to implement H.264

WebRTC Audio - Codecs

- WebRTC compatible browser supports G.711 and Opus
  (*mandatory to implement, MTI*)
- innovaphone Audio-Endpoint-Support for Opus:
  - All „new“ Gateways (xx11, IP29)
  - IP111
  - IP112
  - myPBX for Android
  - (in Future) myPBX for iOS
  - 2 variants: Opus-NB und Opus-WB

→ Good Audio-compatibility between WebRTC and innovaphone endpoints

WebRTC Application Sharing - Codec

Codec

- Proprietary Data-transfer by using WebRTC datachannel
- No compatibility with 3rd Party devices
- Bandwidth variable, limited to 500kbps

WebRTC - Configuration

Configuration

- STUN and TURN configuration from the PBX (IP4/STUN) and sent to the browser
- WebRTC *Device* in *User* Object

WebRTC licensing

- New in V12r1
- Licence per „Channel“ (a.k.a. per „Call“)
- PBX License („floatable“ from License-Master)
- Number of Licenses must be assigned to a PBX-> PBX/Config/Max WebRTC calls (i.e. “this PBX may do x WebRTC in parallel”) -> PBX/Config/Max WebRTC calls
- Additional Video and/or Application-Sharing-License if needed (or UC-Lic)
- Port License

Agenda

- Simplified Licenses
- WebRTC
- **Opus**
- Conferencing
- myPBX Single Sign On
- myPBX Toolbox
- All IP
- Anywhere Workplace
- Reverse Proxy
- TURN
- New Hardware

Opus

- Bandwidth specification from 6 to 510 kbit/s
- We use fixed bandwidths
  - 11 kbit/s payload at 8kHz (Opus-NB), Quality like G.711
  - 19 kbit/s payload at 16kHz (Opus-WB), Quality like G.722
- According to *Listening Tests,* Opus NB is even better than G.711 – with only 11 kbit/s
- Support in IP111/112 and all new Gateways
  Fallback to G.711 for all other devices (at WebRTC)

Agenda

- Simplified Licenses
- WebRTC
- Opus
- **Conferencing**
- myPBX Single Sign On
- myPBX Toolbox
- All IP
- Anywhere Workplace
- Reverse Proxy
- TURN
- New Hardware

Conferencing - Audio

Audio

- Like in V11rx
- Opus-NB Support on new Hardware (important for WebRTC)

Conferencing - Video

Video

- New in v12r1
- Efficient MCU, no media blending
- Voice Activity Detection and switchover to talker
- No media blending necessary, but Video Decoding for switchover
  → only H.264 support for Video-Conferencing
- Old Conference Interfaces support less Video Users than Audio Users

  (i.e. IP6010 max. 30 Users, depending on CPU)

Conferencing

- Controlled by *Conference* Object in PBX
- Encryption possible (also DTLS/WebRTC)
- Audio in a conference is always 8KHz, independent of the used codec
- Special Integration of 3rd Party MCUs for Video (v11rx) will not longer supported

Agenda

- Simplified Licenses
- WebRTC
- Opus
- Conferencing
- **myPBX Single Sign On**
- myPBX Toolbox
- All IP
- Anywhere Workplace
- Reverse Proxy
- TURN
- New Hardware

myPBX Single Sign On

- Windows Password can be used for myPBX login
- NETLOGON Protocol is used for SSO
  - Only with Active Directory
  - AD-Account for the PBX
  - Account configuration is made in the PBX
  - Login only for myPBX possible (not for Phones, Hot-Desking)
  - Supports only one AD-Domain
  - PBX doesn‘t saves the Windows PW
- Now, Single Sign On with Windows credentials is possible for myPBX (new) and Admin UI (Kerberos, like before)
- The password must be entered, no real Single Sign On

myPBX Single Sign On

Requirements

- Same Username in PBX and Windows (Replication)
- DNS
- Network connection between PBX and DC (Firewall)
- NTLM must be activated in the AD Domain

Restrictions

- Only one Domain
- Only NTLMv1
- NTLM is not very secure, but HTTPS can be used for myPBX

Agenda

- Simplified Licenses
- WebRTC
- Opus
- Conferencing
- myPBX Single Sign On
- **myPBX Toolbox**
- All IP
- Anywhere Workplace
- Reverse Proxy
- TURN
- New Hardware

myPBX Toolbox

- JavaScript Widgets (Library)
- Easy Integration of myPBX Functionalities in any Websites
  - i.e. Call-Me Button
  - Media-Endpoint based on WebRTC
  - Support for Video and Application Sharing!
  - Presence Information available!
  - Full myPBX functionality is coming soon
- Integration of external Users
- Protocol between Browser and PBX is JSON/Websocket

myPBX Toolbox - Example

Call-me Button on innovaphone Homepage

Features in 12r1

- Outgoing WebRTC calls with Audio, Video and Application Sharing.
- Presence Monitoring

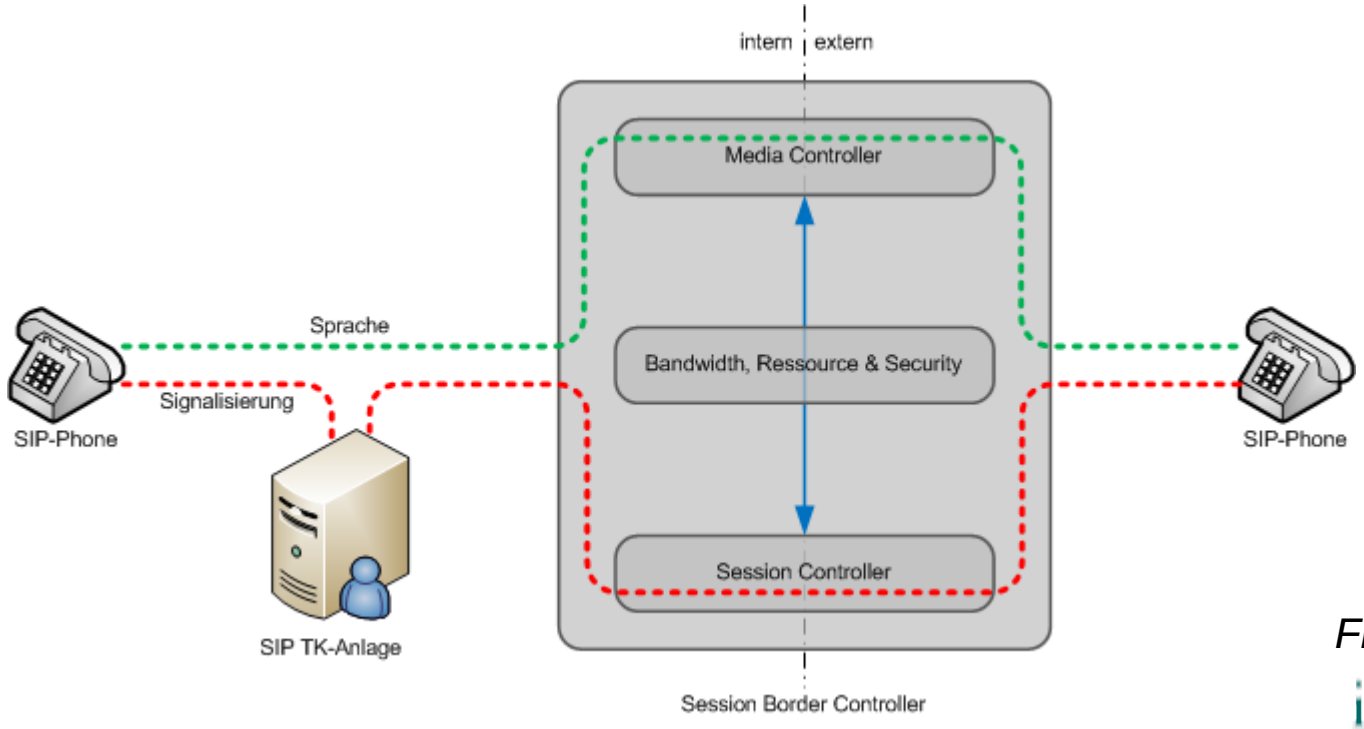
innovaphone

Agenda

- Simplified Licenses
- WebRTC
- Opus
- Conferencing
- myPBX Single Sign On
- myPBX Toolbox
- **All IP**
- Anywhere Workplace
- Reverse Proxy
- TURN
- New Hardware

All IP

- All IP will replace the existing ISDN Trunk Lines by SIP Trunks
- We already support this! But customers are confused by wrong public information like „An SBC is mandatory“ in Wikipedia. The required SBC functionality was always present in our Gateways.



From Wikipedia

innovaphone

All IP

Current Problems

- Discussion about Session Border Controller for All IP
- There is no real unique definition about SBC
- Customers are mixing different items like „remote access“ and „SIP Trunks“
- It‘s not possible to place an argument like „Session Border Controller are not needed“

All IP

Solution in v12

- We provide an overall Security Concept for SIP Trunks and Remote Access
- Depending on the requirements, we can provide a „dedicated Box“ (i.e. for DMZ) or an „all-in-one Box“
- Session Border Controller functionality is included

  → An innovaphone box can run as SBC now

- There is no more reason to use 3rd Party SBCs (except for special scenarios where a special Vendor certificate is postulated – like Lync)

All IP

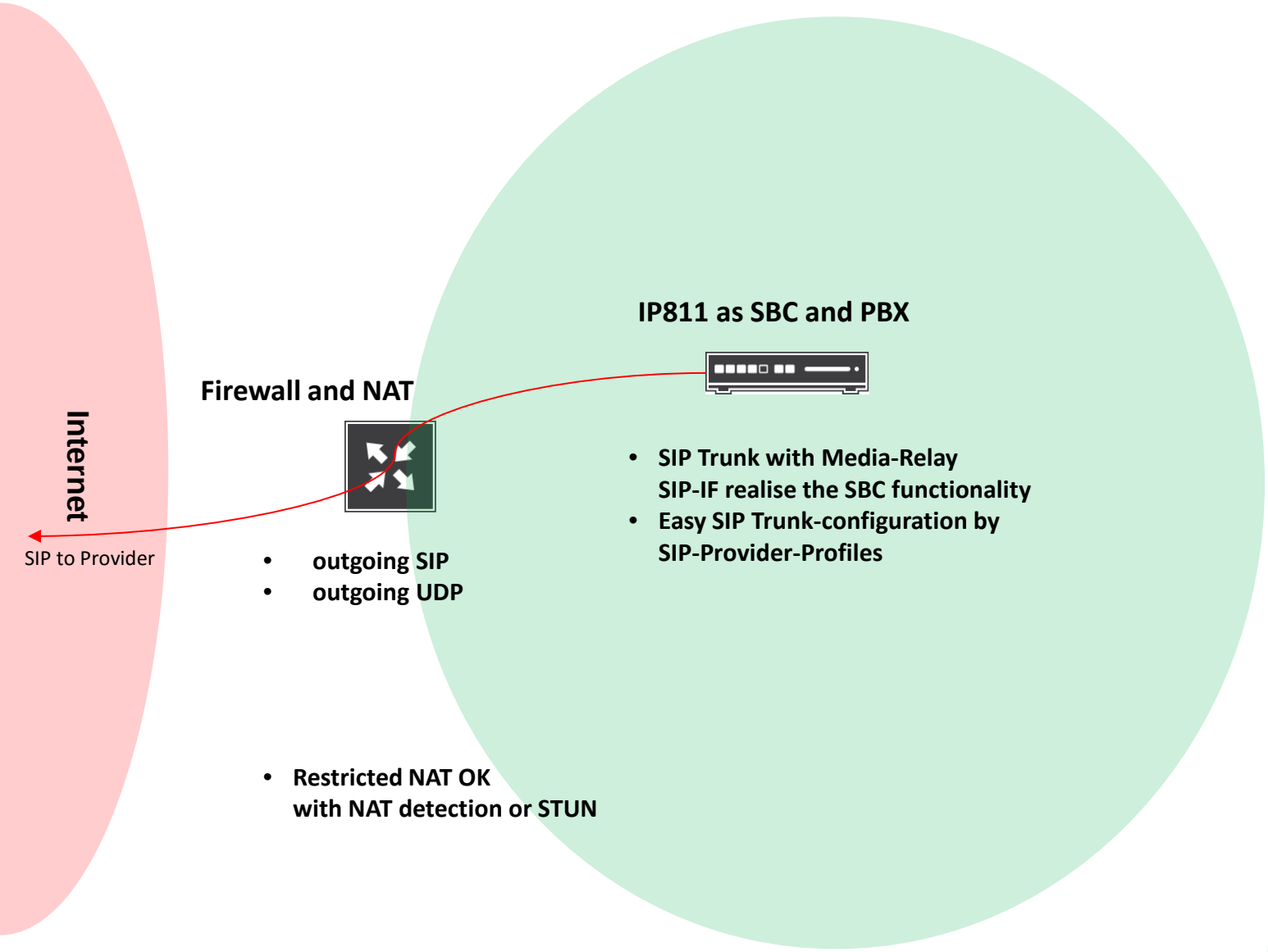
Do we support everything what a conventional SBC supports?

Small Wikipedia vs. innovaphone-speak translator:

- *Security Offloading*
  This are functions like internal encryption but not to the ISP – This we do on our SIP interfaces
- *Media Pinholing*
  Voice Payload must be send through NAT Router/Firewall. ICE/STUN/TURN protocols can be used for that, this is implemented on our SIP interfaces
- *Transcoding*
  This is a codec adaption between intern and extern. This is not implemented because of additional delay in Jitter Buffer – and loosing of Voice Quality
- *Protocol Translation*
  Adaption of internal and external VoIP protocols. This is realized by Interop Flags in SIP Interfaces
- *Header Manipulation*
  Adaption of Phone Numbers etc. This we do with the Interface Maps and routes in the Gateway
- *Media Anchoring*
  Forwarding of Media Streams to the correct endpoints. This is the Media Relay Feature in our gateways

- Except for transcoding (which we intentionally don't do), we do it all!!

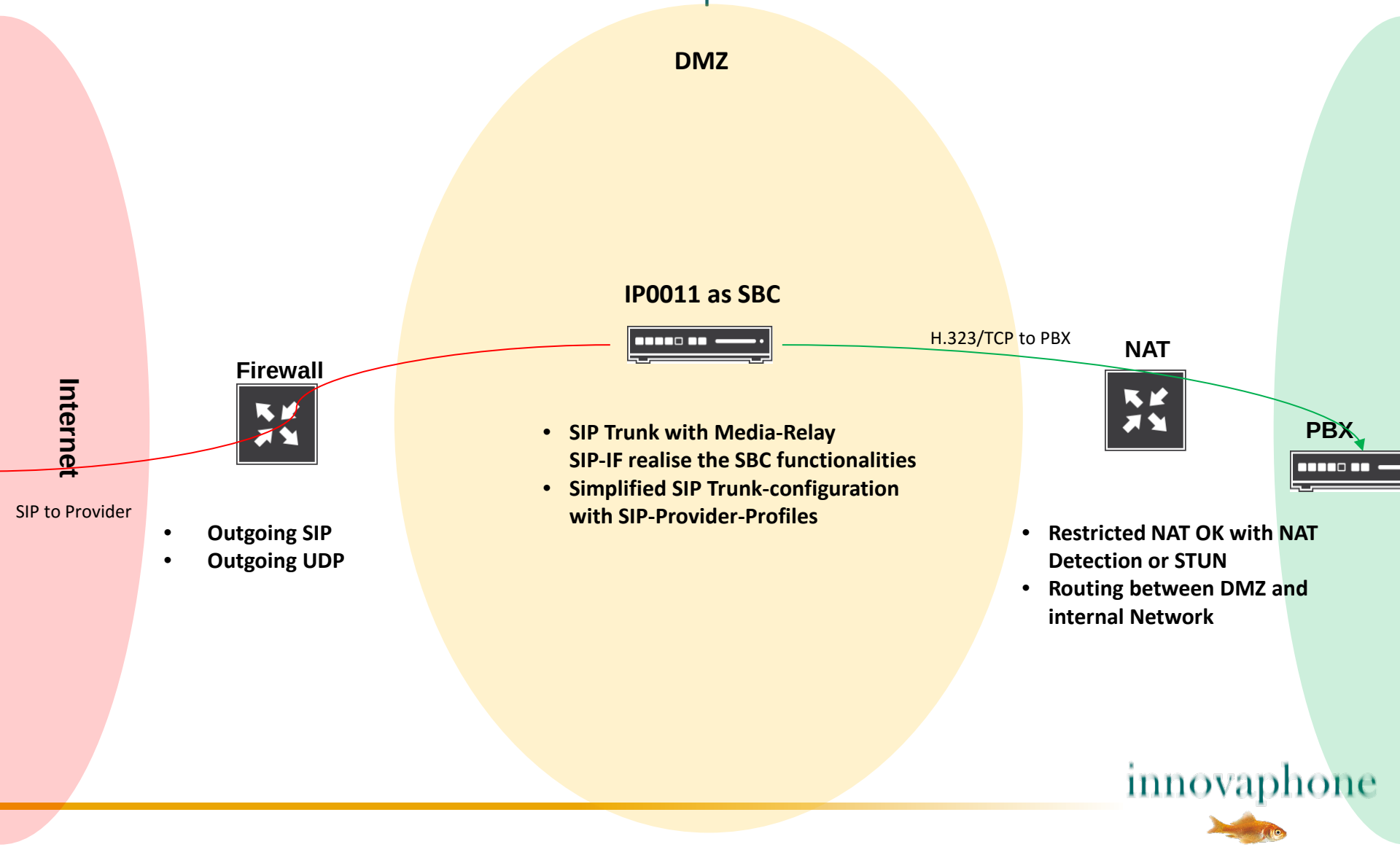
Simple All IP Scenario



innovaphone

Enhanced All IP Scenario

Business scenarios are often more complex

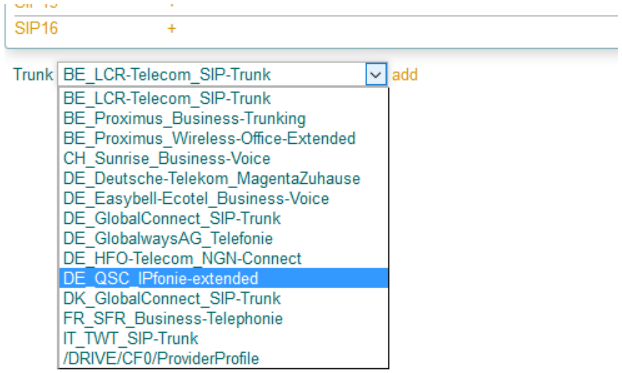


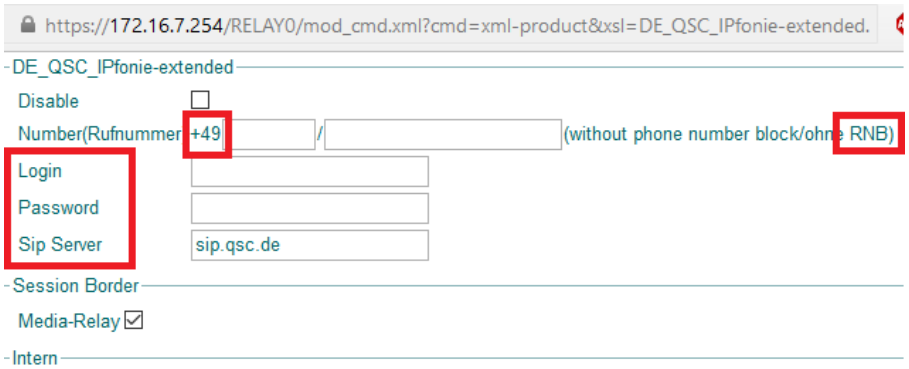
innovaphone

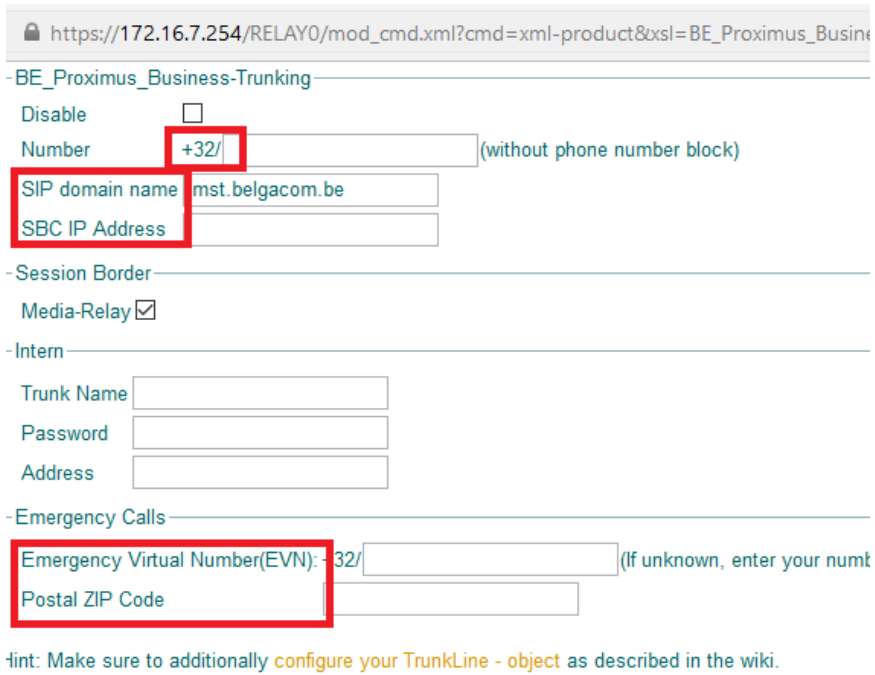
All IP News

SIP Provider Profiles

- List will be permanently enhanced
- Provider-specific Configuration and Layout







innovaphone

All IP SIP Provider Tests

- innovaphone performs the SIP Provider Tests
- All tested provider will be taken into nightly test cycle
  → guarantees ongoing compatibility
- New Test-requirements to the Provider
  - innovaphone is testing
  - SIP Trunk must be reachable on premise in Sindelfingen
  - Permanent Account
  - Painless conditions if possible (no monthly accounting, etc.)

Howto: innovaphone SIP Provider Tests

All IP – Media Relay

- We recommend Media Relay in the SBC
  - Most SIP Provider do not support ICE/DTLS (so WebRTC does not work)
  - Mobility functions difficult (as RTP DTMF bypasses PBX)

- Media Relay is default in new SIP Profiles

All IP – Media Relay

- Media Relay on SBC needs performance
  - In larger environments, it‘s recommended to use a separate box as SBC

- SBC Media Relay performance
  (extern RTP, intern SRTP, max. at 100% CPU load):
  - IP811, IP0011, IP1130, IP3011 – 200 Channels
  - IP411, IP311 – 125 Channels

  - IP810, IP6010, IP1060, IP3010 – 170 Channels
  - IP6000 – 35 Channels
  - IP800 – 10 Channels
  - IP302, IP305 – 12 Channels

Agenda

- Simplified Licenses
- WebRTC
- Opus
- Conferencing
- myPBX Single Sign On
- myPBX Toolbox
- All IP
- **Anywhere Workplace**
- Reverse Proxy
- TURN
- New Hardware

Anywhere Workplace

- Is that everything for All IP?
- Customers have
  - Home Offices
  - Branches without VPN
  - Mobile Devices (myPBX Mobile)

- The *All IP* Scenario must be enhanced by *Anywhere Workplace*

Anywhere Workplace

Do you remember to *Session Border* Objects?

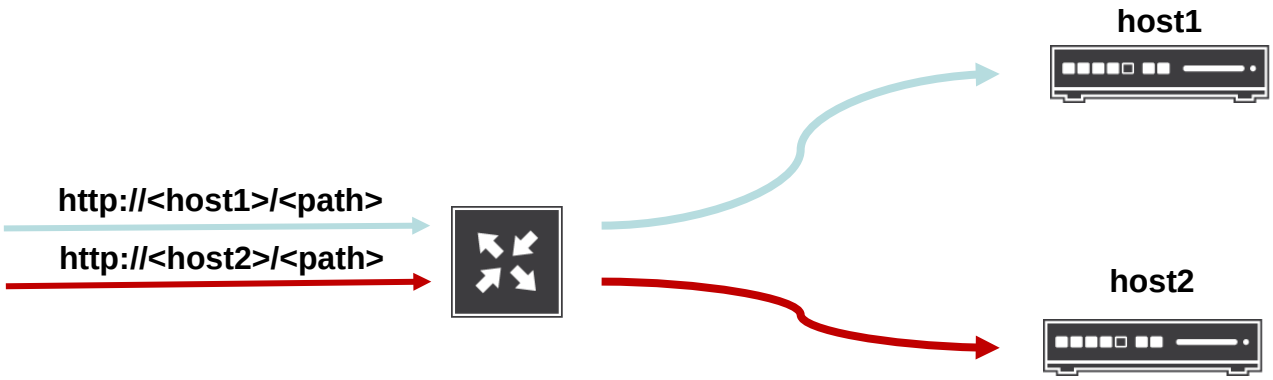
- Complex configuration
- Only acts for incoming registrations
  Missing solutions for
  - LDAP
  - HTTP

Session Border Objects replaced by the Reverse Proxy in v12

Agenda

- Simplified Licenses
- WebRTC
- Opus
- Conferencing
- myPBX Single Sign On
- myPBX Toolbox
- All IP
- Anywhere Workplace
- **Reverse Proxy**
- TURN
- New Hardware

Reverse Proxy – basic functionality



- Similar function to NAT Port Forwarding, incoming TCP/TLS connections will be forwarded to a defined target
- Connections will be terminated in the RP. The RP creates a new session to the other site.
  - i.e. HTTPS/HTTP possible
- Not only the IP-port defines the target, but also the application content of the payload

Reverse Proxy – H.323

- H.323/TCP, H.323/TLS
  - Forwarding based on *Gatekeeper ID* (domain) for registrations
  - Forwarding based on domain for calls with a <name>@<domain> target
    This makes sure calls w/o registration work for H.323 federation
  - Optional certificate validation for TLS
- No support for classic H.323/RAS-UDP
- Connection between RP and PBX can be trusted, as RP does certificate validation
- TCP/TCP, TCP/TLS, TLS/TCP and TLS/TLS possible

Reverse Proxy – SIP

- SIP/TCP, SIP/TLS
  - Forwarding based on domain Parts in the *From: Header* in REGISTER
  - Forwarding based on domain for INVITE with a <name>@<domain> target
    This makes sure calls w/o registration work for SIP federation

- SIP is usually not used in innovaphone Scenarios (except for federation)

Reverse Proxy - HTTP

- HTTP, HTTPS
  - Forwarding based on *Hostname Header*
  - Optional URL/PATH filtering

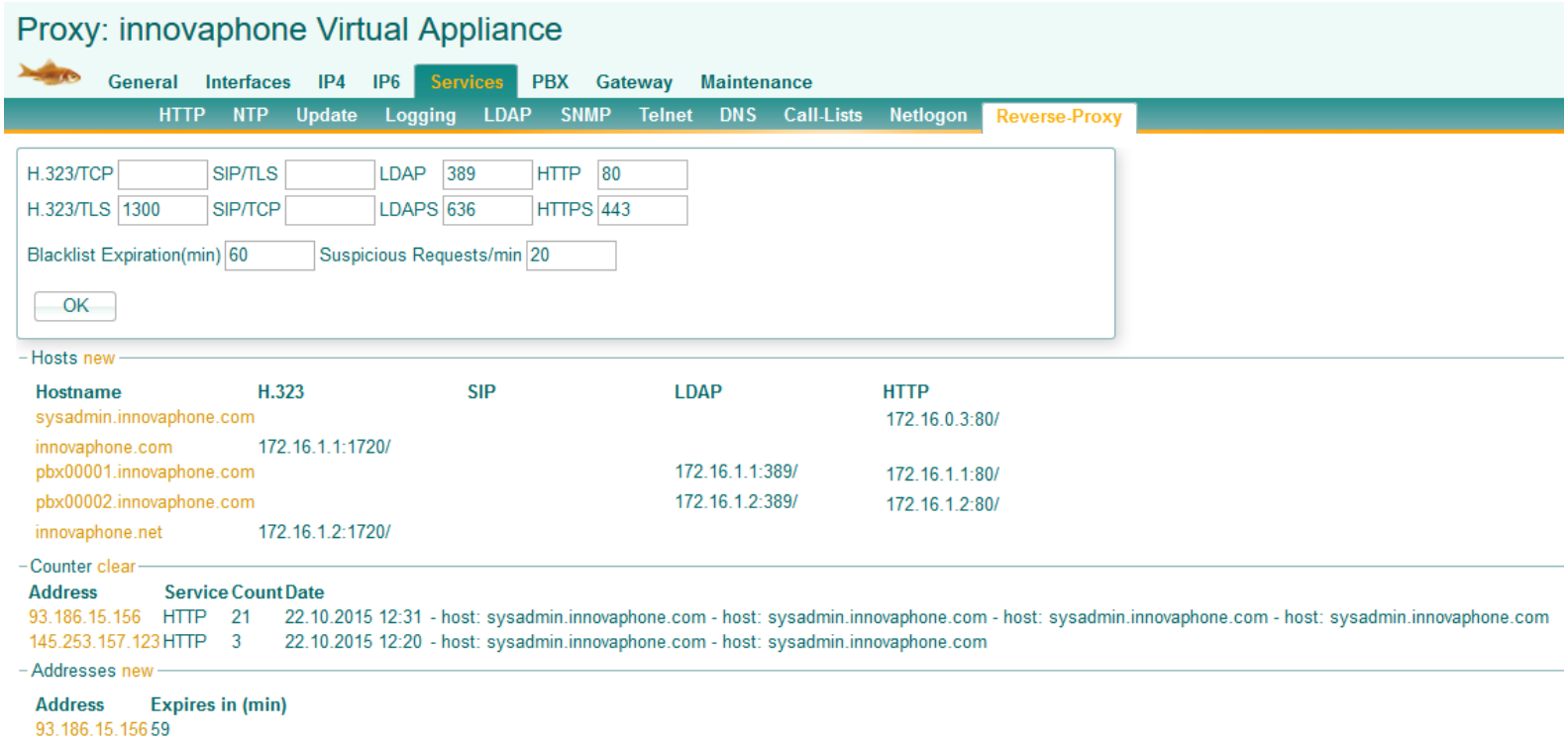
- Allows limited service access e.g.
  - myPBX only
  - No Admin UI
  - No SOAP

Reverse Proxy - LDAP

- LDAP, LDAPS
  - Forwarding based on the domain found in the authentication name in the *BIND Request* (like in <domain>\<user>)

- LDAP sessions must be authenticated to the directory service

Reverse Proxy - Configuration



- *Blacklist Expiration* set for automatic entries to the blacklist
- Configurable Threshold (*Suspicious Requests/min*)
- Top 10 suspicious addresses, showing requested service and host
- Black/White list parameters can be configured manually (with or without blacklist expiration)
- Event is generated when an entry is added to the blacklist

innovaphone

Reverse Proxy - Features

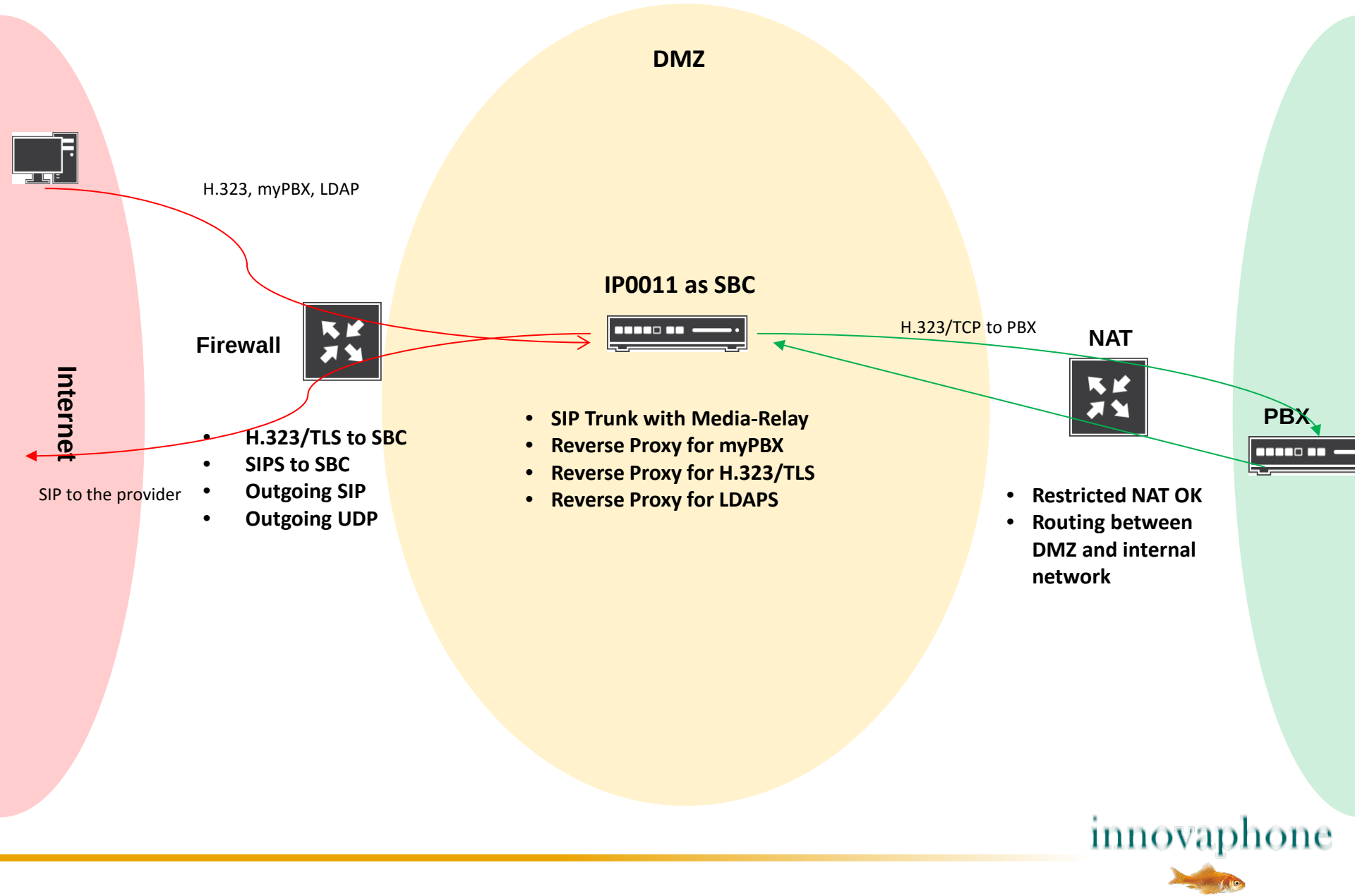
- TCP/TLS may be different between far and local end
- Service ports can be configured for non-standard ports
- Attacks (*suspicious requests*) are detected based on unsuccessful connects
- Display of *suspicious requests* counters
- Attackers IP address is added to the blacklist automatically
- Display of the blacklist. Administrator can remove address from blacklist or add it to whitelist explicitly
- Optional limitation to specific networks
- No IPv6 support (yet)

Reverse Proxy - Scenarios

- Cloud Installation
  - One public, one private IP address (DMZ)
  - Centralized point of access for the registration of endpoints incl. certificate validation, H.323/TLS or SIP/TLS
  - HTTP(S) access to customer PBX limited to myPBX service
  - LDAP(S) access to directory service

- Remote PBX access (Anywhere Workplace)
  - Can be installed with in the PBX or in the customers local network
  - Limit PBX access to configured protocols
  - Limit allowed HTTP/S URLs (e.g. limit to myPBX access)
  - For installations w/o DMZ, the RP can be run on the PBX
  - Can be accessed through NAT router with simple port forwards to the RP

All IP + Anywhere Workplace Scenario



innovaphone

All IP + Anywhere Workplace scenario (simplified)

H.323, myPBX, LDAP
incoming

IP811 as SBC and PBX

Firewall and NAT

Internet

SIP to the provider

- **SIP Trunk with Media-Relay**
- **Reverse Proxy for myPBX**
- **Reverse Proxy for H.323/TLS**
- **Reverse Proxy for LDAPS**

- **H.323/TLS to SBC**
- **SIPS to SBC**
- **Outgoing SIP**
- **Outgoing UDP**

- **Restricted NAT OK**

NAT Router has port-forwarding to PBX, reverse proxy on PBX implements all intended limitations

innovaphone

Agenda

- Simplified Licenses
- WebRTC
- Opus
- Conferencing
- myPBX Single Sign On
- myPBX Toolbox
- All IP
- Anywhere Workplace
- Reverse Proxy
- **TURN**
- New Hardware

What's wrong with STUN/ICE?

- STUN answers the question „who am I?“ (which external IP address do I have, a.k.a. *server-reflexive address*), by initiating a connection to the STUN server and thereby creating a new NAT map on the router
- ICE tries to establish an end-to-end media connection through all involved NAT routers
- However, RTP media exchange fails, when both NAT routers have *symmetric* or *port restricted* NAT and thus do not allow a direct router-to-router communication for RTP (cause in this case, only the STUN server could send data through the opened NAT whole to the endpoint behind the NAT/FW)
- It may also fail if FWs employ a restrictive policy

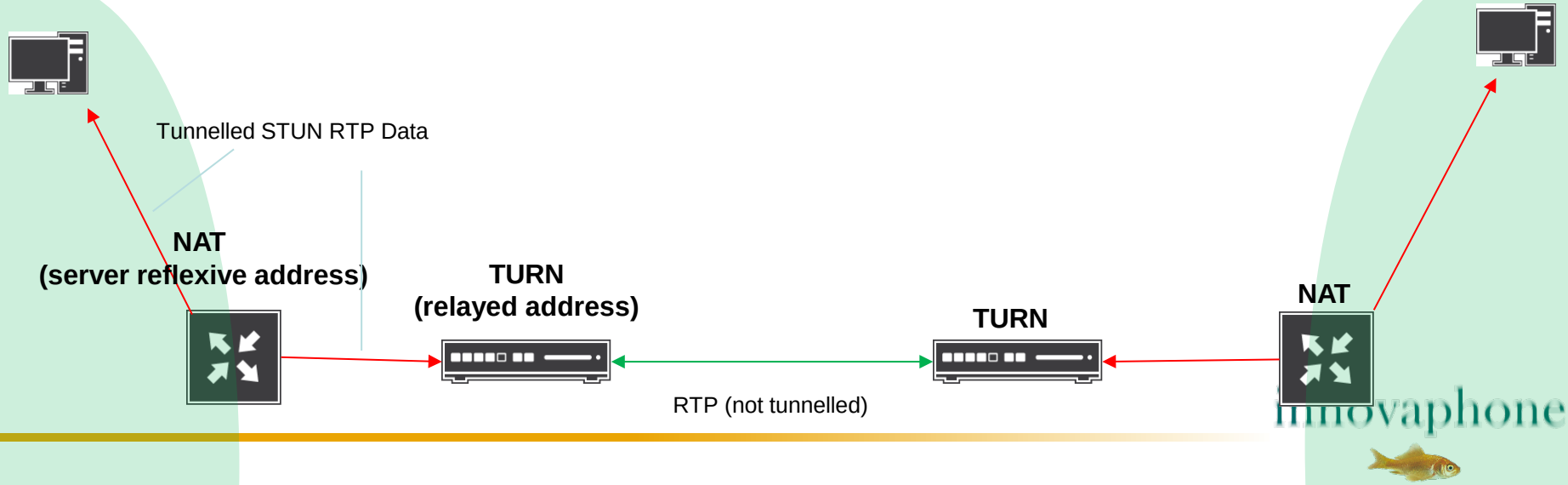
→ typical issue with V11rx

Certain types of NAT-Router/Firewalls create issue
No Media (RTP)!

TURN

To fix this the RTP issue, an entity in the public internet is required which relays media data (RTP) between the 2 NAT routers (i.e. **T**raversal **U**sing **R**elays around **N**AT) → The TURN Server

- Client (phone/PC) moves its own RTP endpoint in to the internet (to the TURN server)
- Client talks STUN protocol only to the TURN server (no plain RTP) (UDP or TCP)
- Original RTP data is tunnelled to the TURN server using STUN (bi-directional)
- Firewall/Router only sees STUN!
- Plain RTP between both TURN Servers only
- RTP becomes a non-Issue ☺



TURN

- Works with all kinds of NAT, including restrictive NAT Router/Firewalls
- TURN should be used only if direct communication is not possible indeed (due required resources, delay)
- This is ensured by ICE, as the *candidates* gathered with STUN (*server reflexive address*) get a higher priority than the candidate received from TURN (*relayed address*)
- Each client has its own TURN server, asymmetric configurations (only one party has TURN) possible

→ TURN can safely be configured always, used only if need be
→ With ICE/TURN RTP media will always work, unless it is explicitly disallowed by a firewall

TURN

But…

- Public TURN servers are rare
  Although any ISP/ITSP should offer one
- Therefore, our customers need to run their own usually

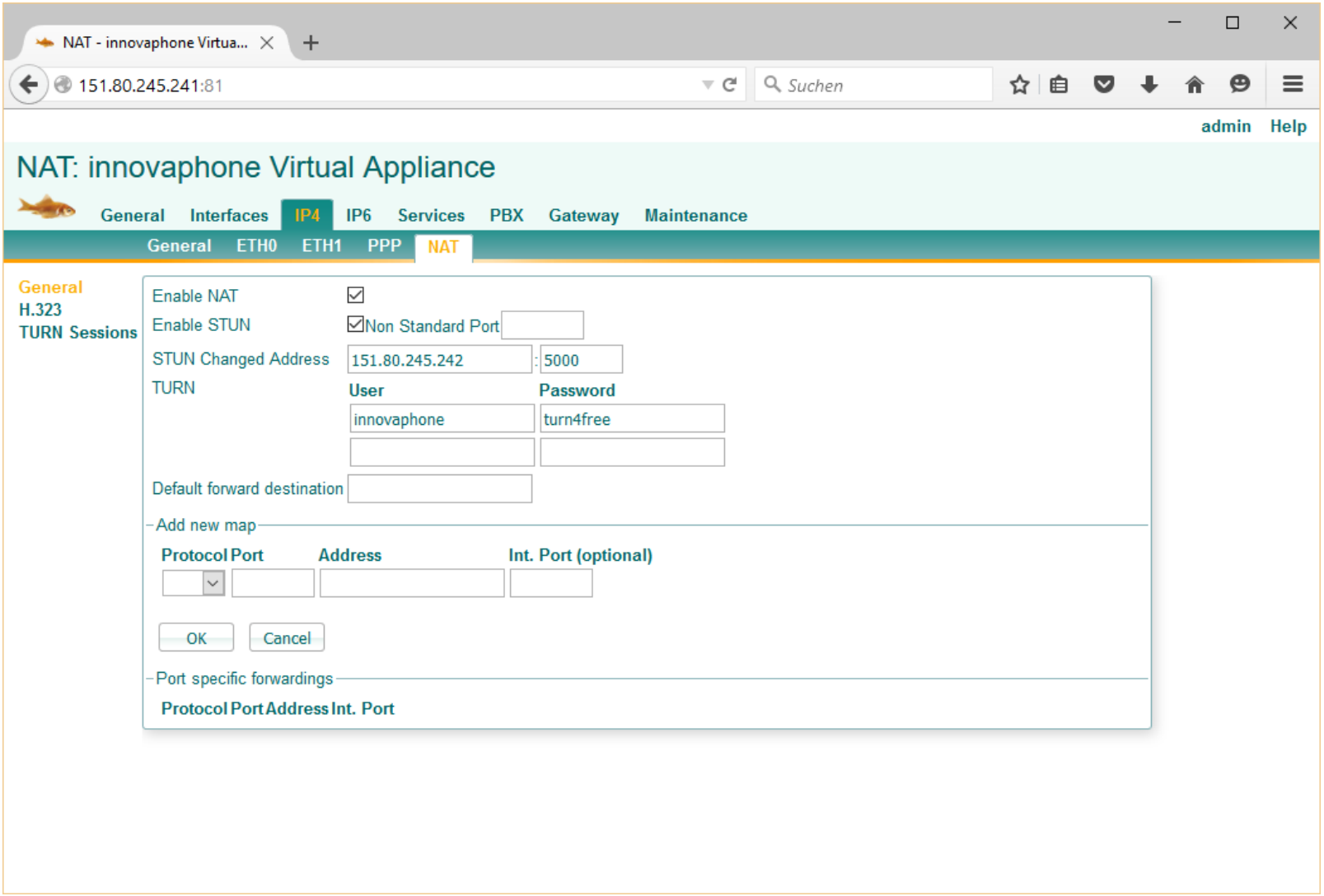
→ TURN server is now available in the innovaphone firmware

Each innovaphone box (including the SBC/RP) can be used as TURN server

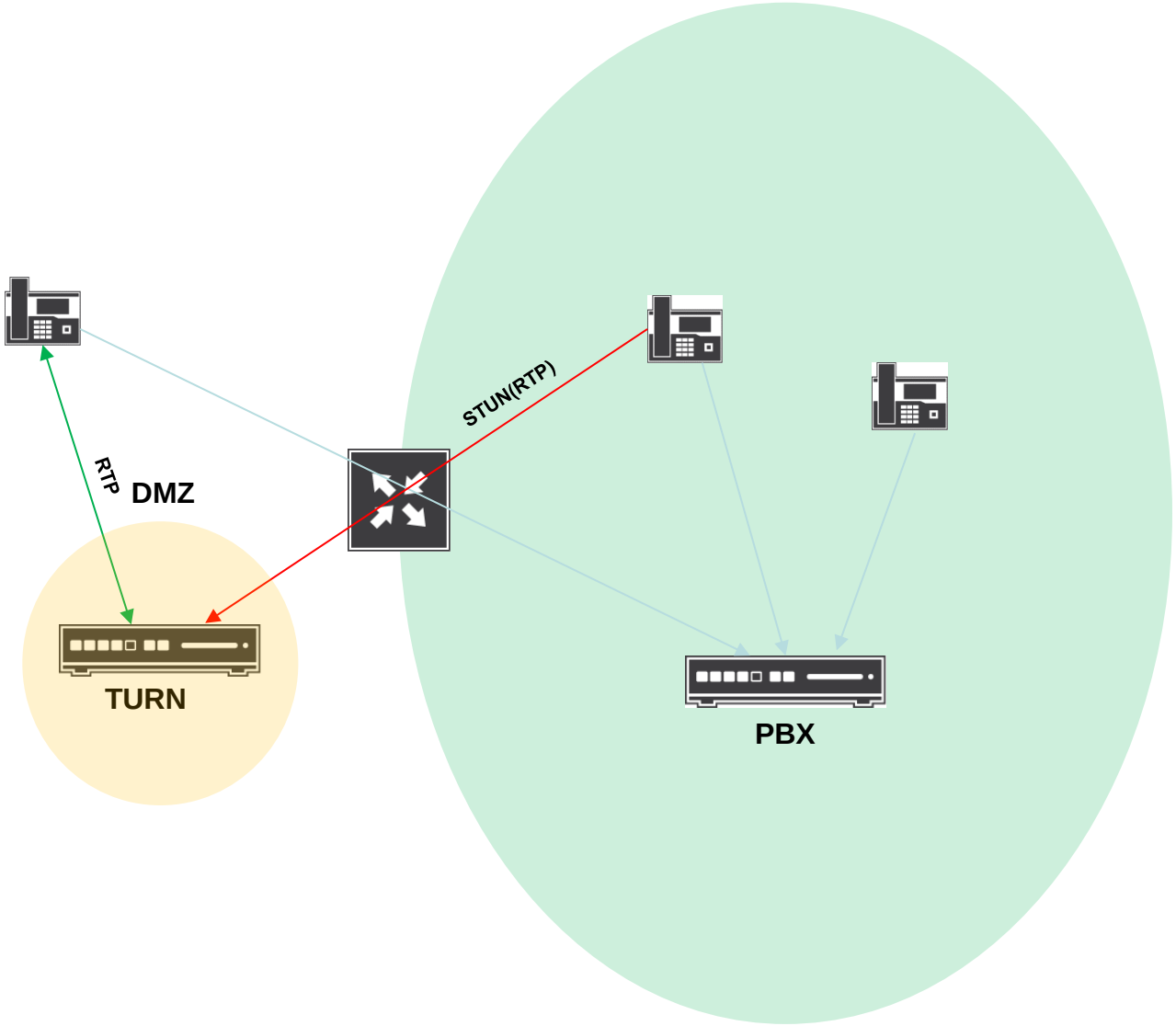
TURN Configuration

- TURN is part of our STUN implementation. STUN needs to be enabled thus
- TURN is configured by specifying a TURN account (user/password)
  - The TURN user/password mechanism is just to avoid misuse – e.g. DoS attack

TURN Configuration



TURN Sample Application – with DMZ

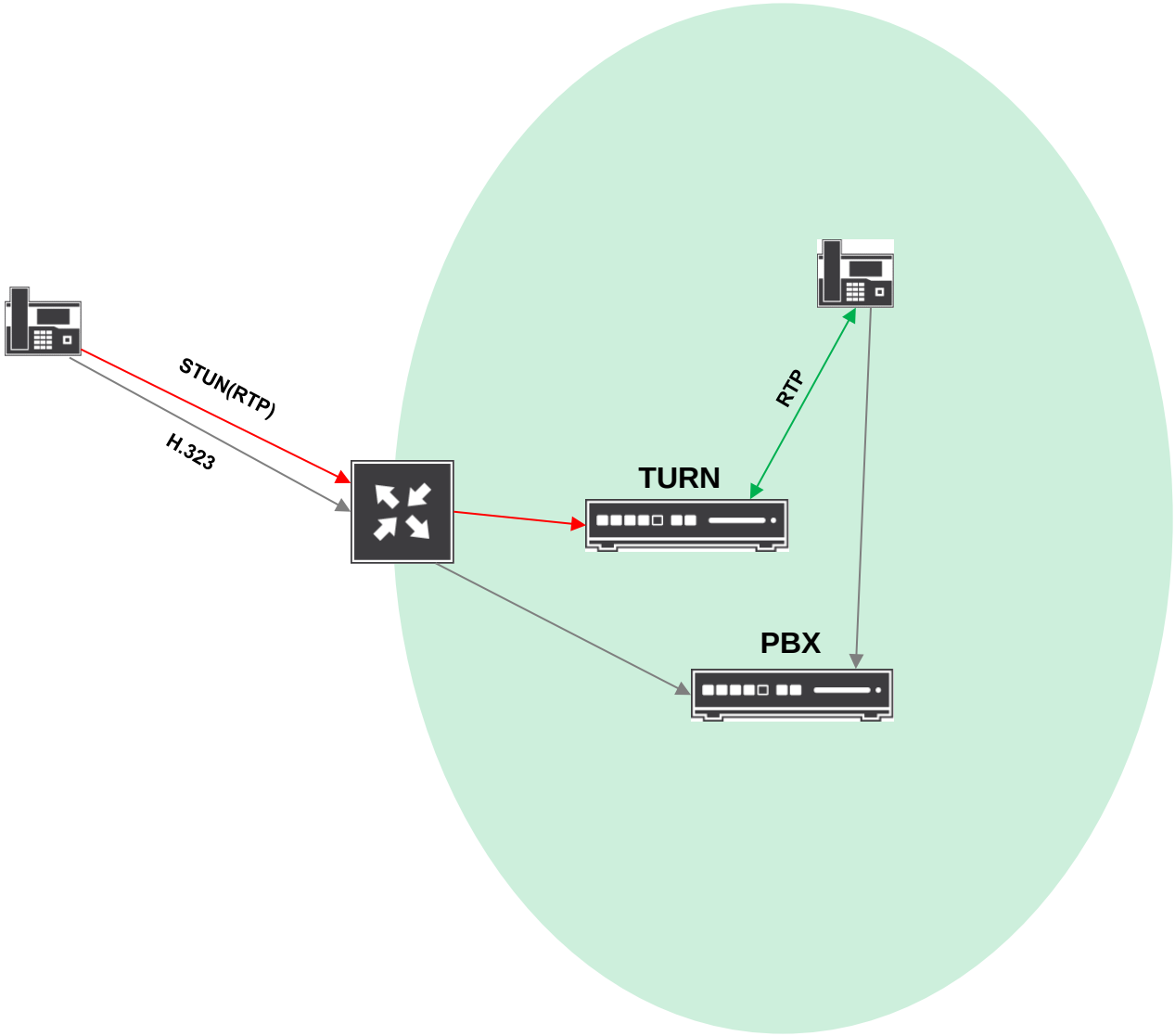


Minimal ports to be opened in the firewall

- **Outgoing single UDP port for STUN**
- **Incoming single TCP port forwarding for H.323/TLS to the PBX**
- **RTP data will be tunnelled through the firewall using STUN**
- **TURN used only if required**

innovaphone

TURN Sample Application – w/o DMZ



Minimal ports to be opened in the firewall. w/o DMZ

- **Single UDP port forwarding for STUN**
- **Single TCP port forwarding for H.323/TLS**
- **RTP tunnelled through the firewall with STUN**
- **TURN server and PBX can run on the same device**
- **TURN used only if required**

Could even be run with DynDNS!

innovaphone

All IP + Anywhere Workplace scenario - security

Threats

- Unauthorized Access
  - *Brute Force* attack to guess passwords
  - SIP dialler
  - Access to the administrational UI

- *Denial of Service* attacks
  - Cease PBX service using bulk requests
  - restart of infrastructure elements by sending „unusual“ requests and exploiting bugs

- Takeover of full control
  - Execution of malware by sending „unusual“ requests and exploiting *Buffer Overruns* or similar mechanisms

All IP + Anywhere Workplace scenario - security

Counter measures

- Unauthorized Access
  - Limit access using the reverse proxy
  - *Brute Force* detection in reverse proxy
  - Minimal need for administration on the device in the DMZ (SBC/RP)
  - No critical data required in the DMZ
- *Denial of Service* attacks
  - PBX isolated from the attackers by virtue of the SBC/RP
  - Restart of the infrastructure elements in the DMZ do not affect internal telephony service (at least)
- Takeover of full control
  - Unlikely, as we are not running on any known standard OS
  - Once we are as big (thus as attractive as a target) as Cisco is today: the SBC/RP is open for a small, well defined set of protocols only -> rather easy to protect

All IP + Anywhere Workplace scenario - security

- IP Blacklist
  - IP Addresses are blocked if they are „suspicious“ according to various criteria. Suspicious IP address can also be added to the blacklist manually. Current blacklist entries can be display. Blacklist entries can be removed manually or automatically (timeout)
- IP Whitelist
  - Known-good addresses can be added to a whitelist
- Display of various run time information
  - Display of current RP sessions, statistical data
- Events
  - Generated when entry is added to the blacklist automatically

All IP + Anywhere Workplace scenario - security

So is this all that is required?

Good question ☺ !

Please report any doubts you or your customers may have. We will consider and fix it need be!

Any 3rd party SBC creates more issues than benefits and should b e avoided thus

- Exception: if it is required due to certifications (some SIP trunks, Lync)

All IP + Anywhere Workplace scenario - SBO Migration

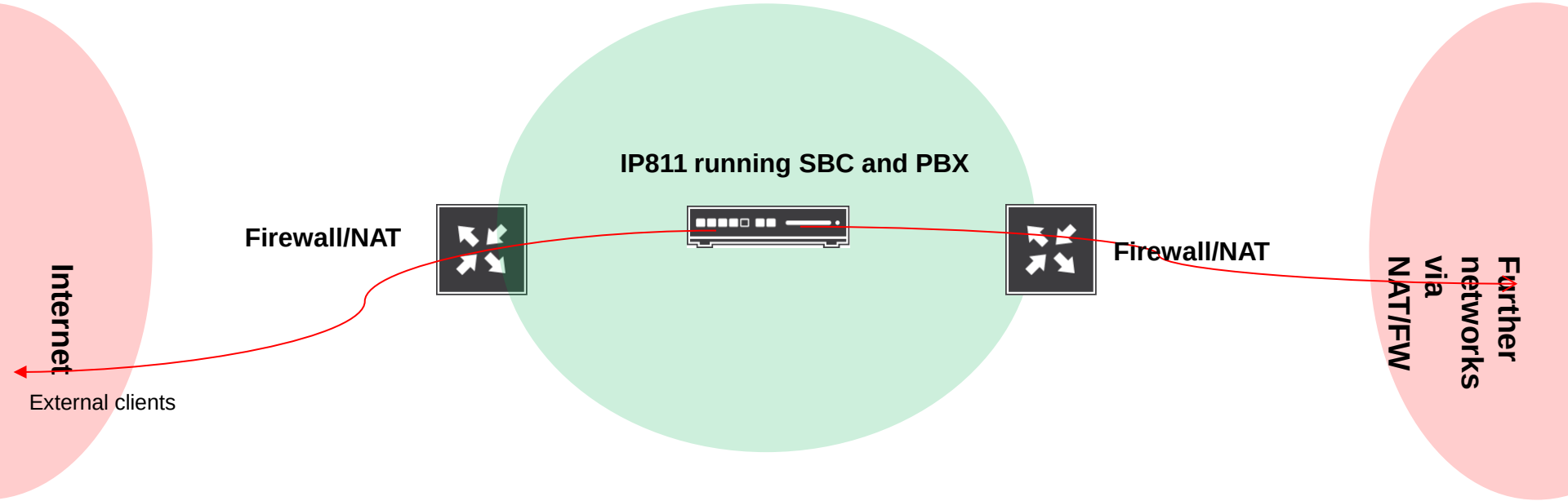
- What about the V11rx *Session Border o*bjects in PBX?
  - Not part of the v12 security design
  - Not being enhanced any further
  - Still there for v11 compatibility
  - Migration to *Reverse Proxy* recommended

- Migration is a rather uncomplicated re-configuration of the *Frontend* PBX

- Severe simplification
  - No duplicate maintenance of the remote users
  - Only PBXs need to be configured in the *Reverse Proxy*

Dual-STUN

- V11rx supports a single STUN towards a single NAT-ed network only
- Some scenarios however require 2 such networks
  - E.g. Voice-, Data- and Internet separated by NAT
  - So far, STUN/ICE did work towards only one of them



From v12r1 we support 2 NAT-ed networks

(but only one TURN server)

innovaphone

Agenda

- Simplified Licenses
- WebRTC
- Opus
- Conferencing
- myPBX Single Sign On
- myPBX Toolbox
- All IP
- Anywhere Workplace
- Reverse Proxy
- TURN
- New Hardware

New Hardware – Key Features

- Opus
- CF replaced by mSATA SSD (e.g. for Linux AP)
- Additional flash memory (NAND, a.k.a. *Flash Disk*), independent of mSATA storage
  - 128 MB (IP311, 411) or 1 GB (IP0011, 811, 3011)
- Better Linux performance (newer CPU, more Linux RAM 768-1536MB vs. 256)
- Linux also available on the All-in-one boxes (IP311/411)
- Internal clock now 5ppm (previously 50ppm)
- Pricing ☺

New Hardware – SSD/Flash Disk

- mSATA SSD (DRIVE/CF1)
  - Need to open housing for installation
  - Not shipped with device, SSD requirements
    - <= 2.500 mW max power consumption
    - min. 3 Gbit/s
    - 3.3V
    - Format JEDEC MO-300
    - max. usable size depending on application (internal WS: FAT32, Linux de facto ∞)
  - DRIVE/CF1 (if no Linux AP running)
  - Needs to be acquired and installed by partner and/or customer
- Internal *Flash Disk* (NAND)
  - For internal web server (DRIVE/CF0) e.g. if Linux AP is using mSATA SSD
  - Limited space (311/411 128MB, otherwise 1 GB)

New Devices: VoIP Gateways – replacements

		IP311
IP305 + IP302	→	IP411
IP810 + IP800	→	IP811
IP3010	→	IP3011
IP1060	→	IP1130 *2
IP0010	→	IP0011
IP28	→	IP29

innovaphone

New Hardware – Gotchas!

- EOL IP28 IP302 IP305 IP800 IP810 IP0010 IP1060 IP3010 (not IP6010)
- Opus runs on DSP (except for the new phones), only NB
  → will not be available in older gateways
- 1060 => 2 * 1130
  - Although this gives you 60 DSP and CONF channels, the max. size of a single conference is limited to 30 (previously 60)
- Single conferences with 31+ channels with IP6010 only
  - However: no Opus
- Why no IP6010 replacement?
  - Could be done. Not yet decided
  - (*IP1160* + *IP0011* or *IP6011*)
- IP0011 has no CONF (no conferences)
- IP3011 has no BRI (sync), no HDLC (PPPoISDN)
- IP811 BRI have no phantom, feeding (for bus-powered ISDN phones ☺)
- Firmware V12 only

innovaphone

FRs

Some FRs which made it into 12r1

- Admin UI / PBX Kerberos + AD replication - Use Kerberos for User PBX logins and for VoIP Registration
  implements part of: AD Login via NetLogon for myPBX
- myPBX / myPBX launcher / Implement single Sign-on solution
  AD Login via NetLogon for myPBX
- Admin UI / Additional HTTP-Server Allowed Stations only for administration access
  implemented by the Reverse Proxy
- iQM *Server as service*
- iQM Monitor Skip empty
- *myPBX / Buddylist / Use entries from buddy list for name res ...*
- *myPBX SSL – Redirect*
- Custom PPI on non-registered interfaces
- Moving function keys

We can’t do all – but we consider all of them!

Thank you!

Questions?