

Penetration testing communication systems *nowadays*

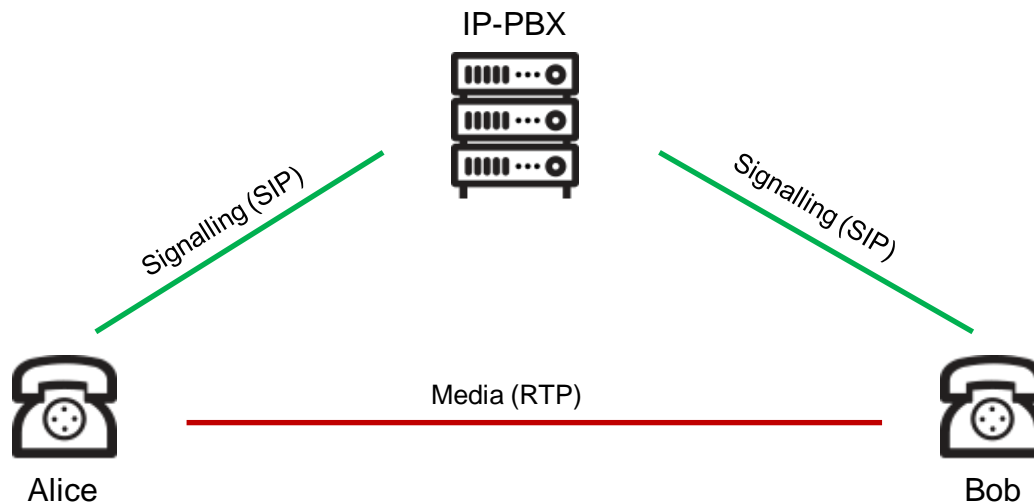


Who am I

- Moritz Abrell
- IT Security Consultant – SySS GmbH
- OSCP
- Many years of professional experience in Voice over IP and Unified Communication Technologies
- Interested in information technology especially IT security – since his early days



When we hear about VoIP ...



VoIP and Unified Communication nowadays



PBX

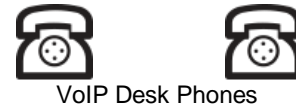
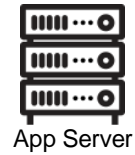


VoIP Desk Phones

VoIP and Unified Communication nowadays



VoIP and Unified Communication nowadays



VoIP and Unified Communication nowadays



App Server



PBX



Active Directory

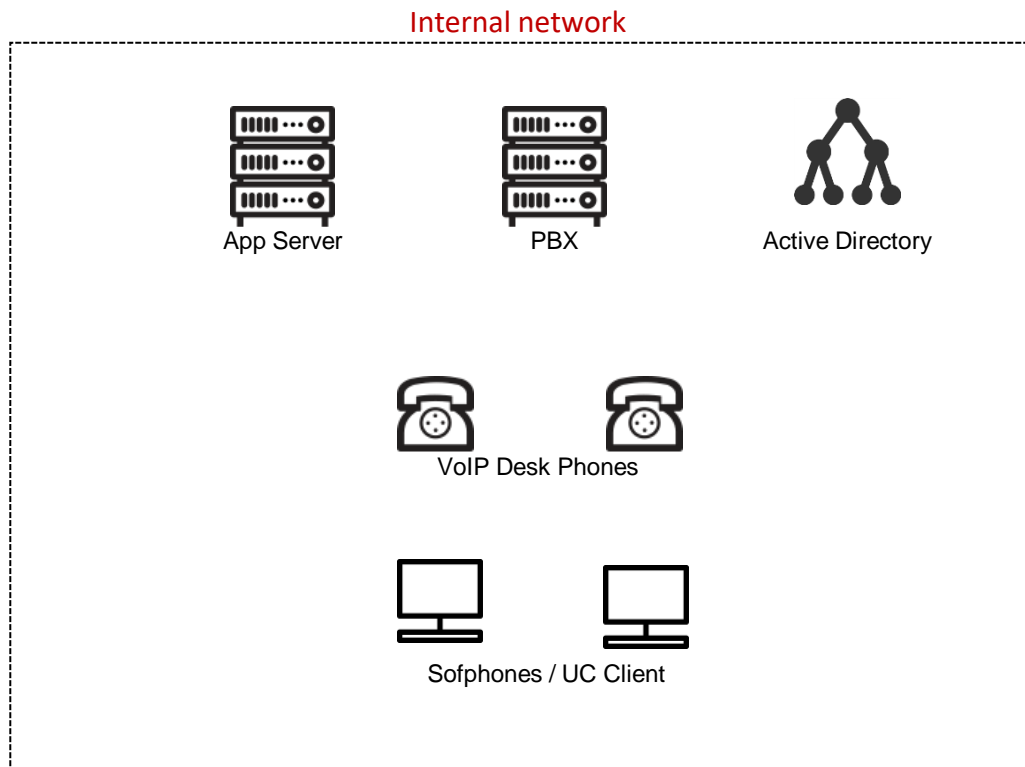


VoIP Desk Phones

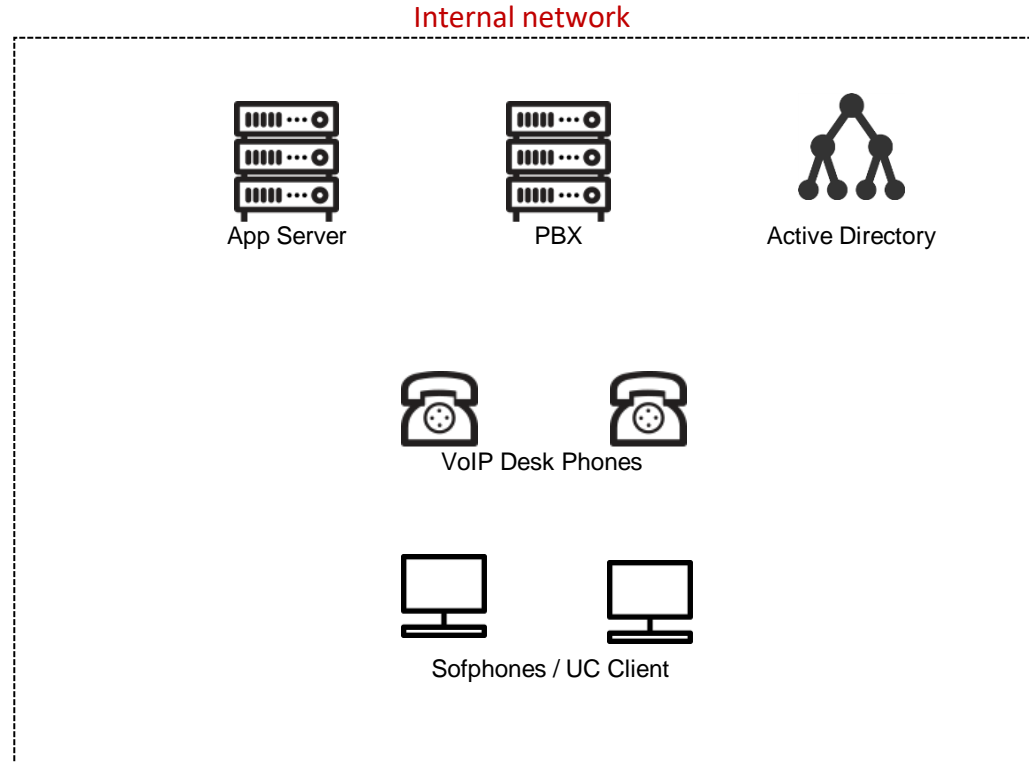


Sofphones / UC Client

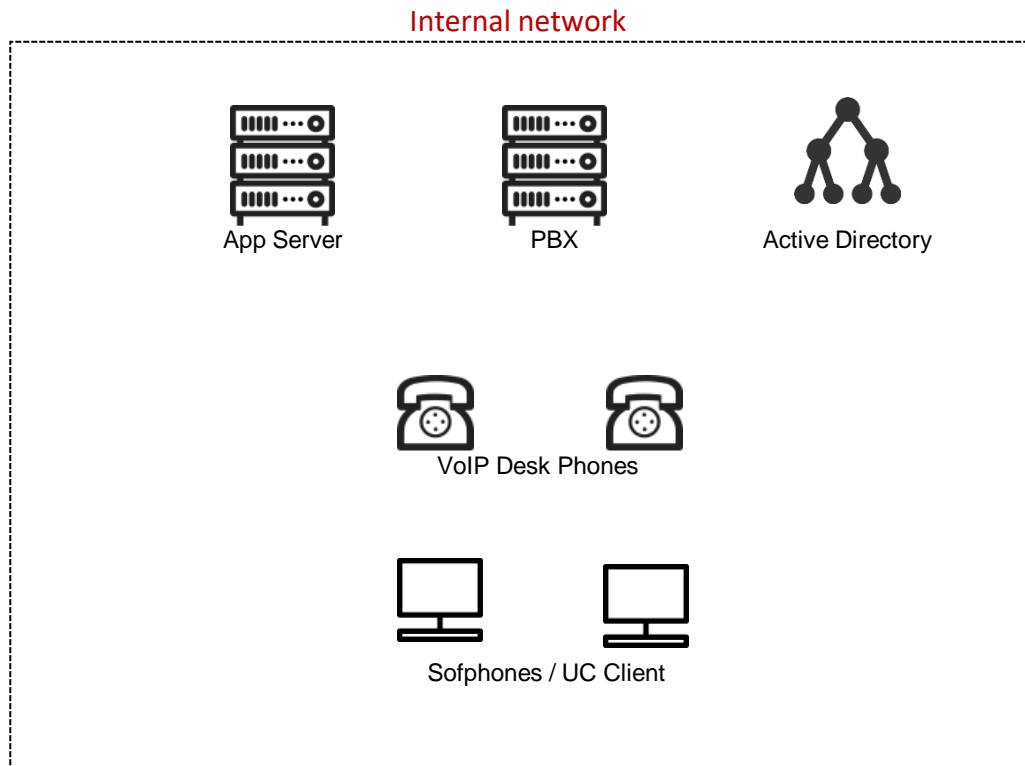
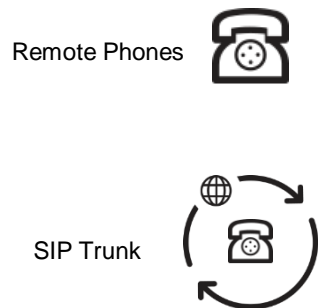
VoIP and Unified Communication nowadays



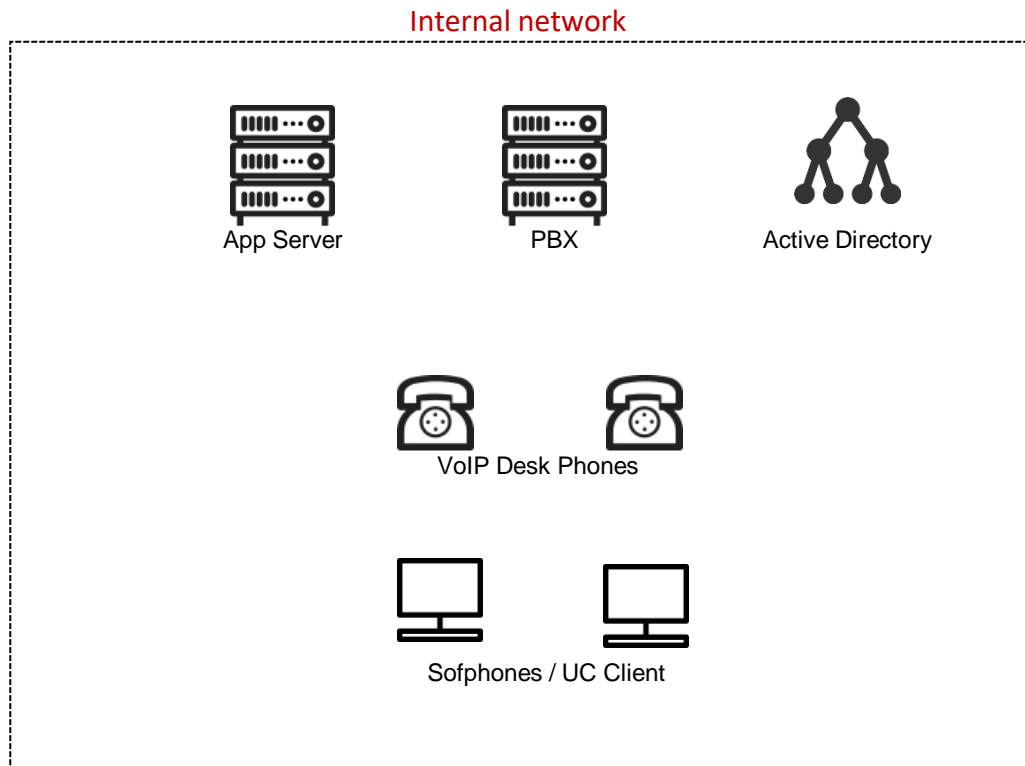
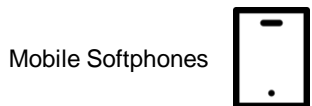
VoIP and Unified Communication nowadays



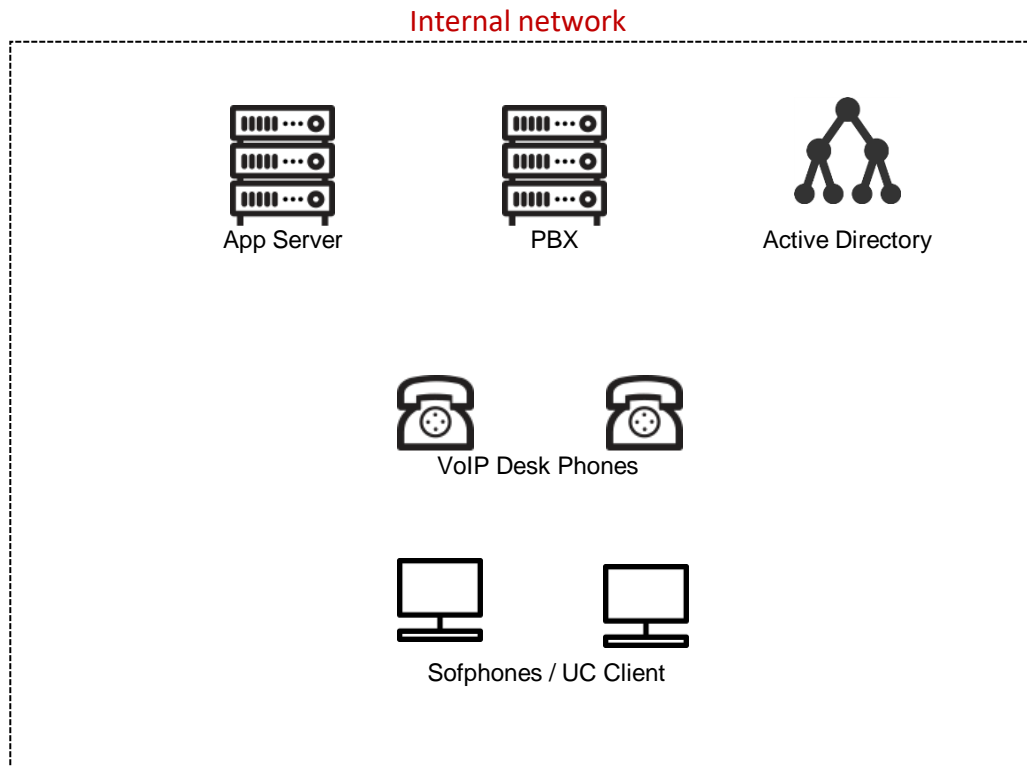
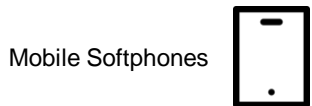
VoIP and Unified Communication nowadays



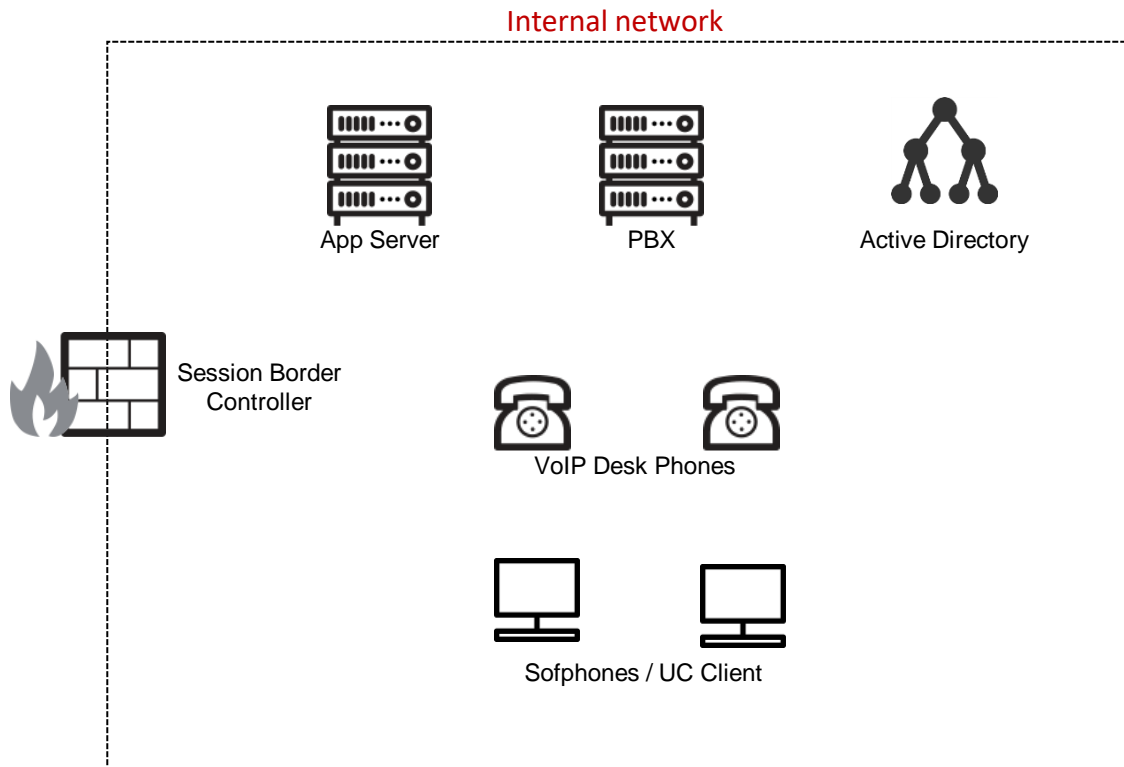
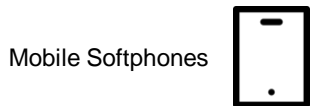
VoIP and Unified Communication nowadays



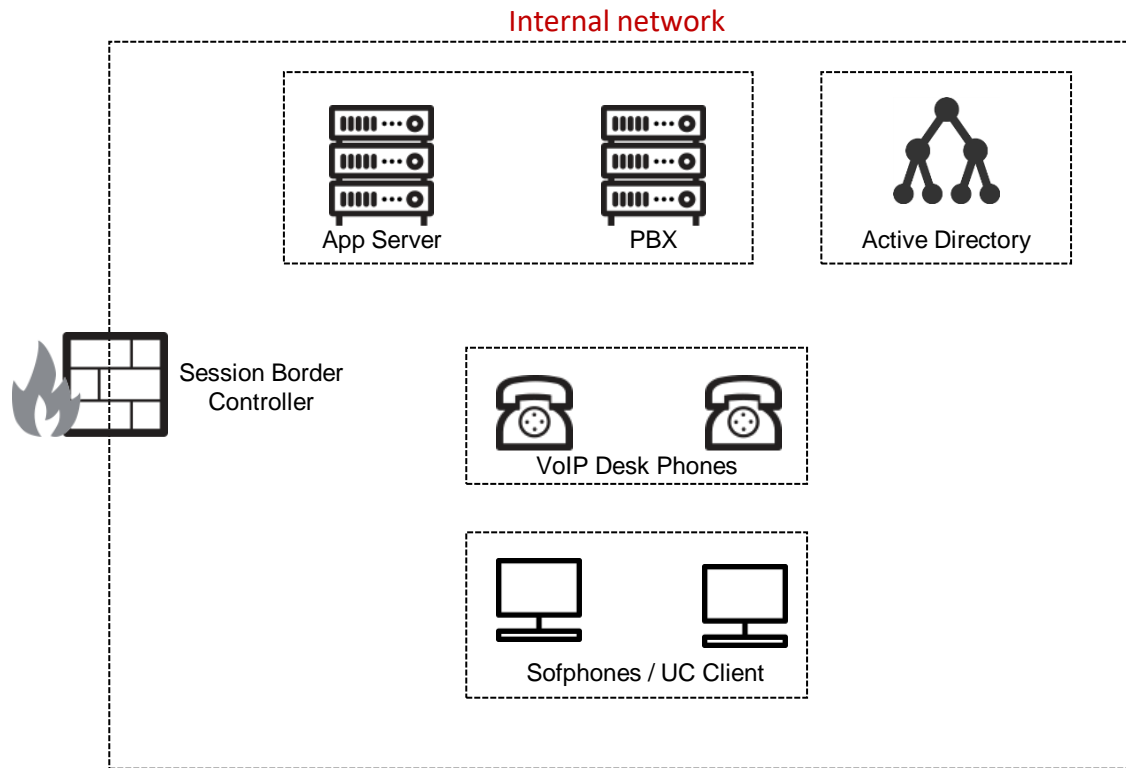
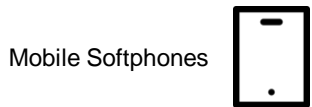
VoIP and Unified Communication nowadays



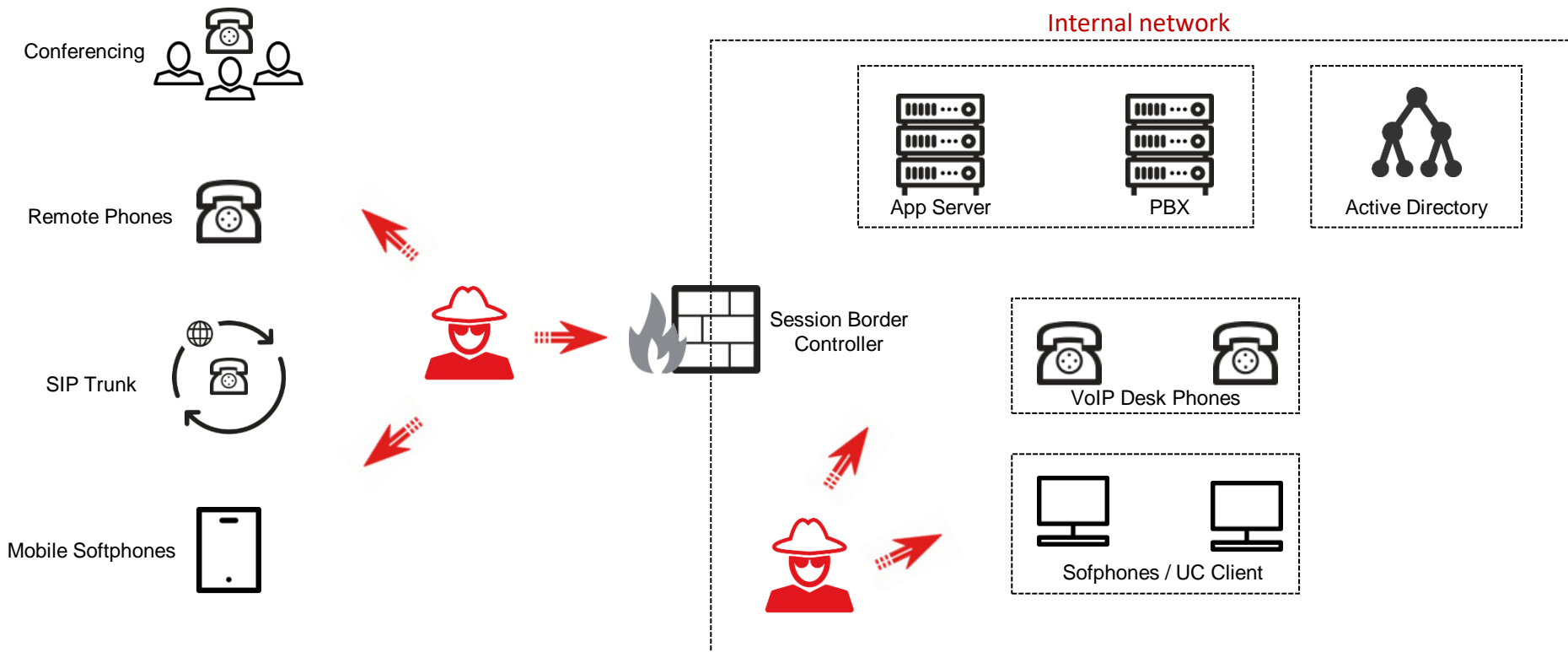
VoIP and Unified Communication nowadays



VoIP and Unified Communication nowadays



Agenda

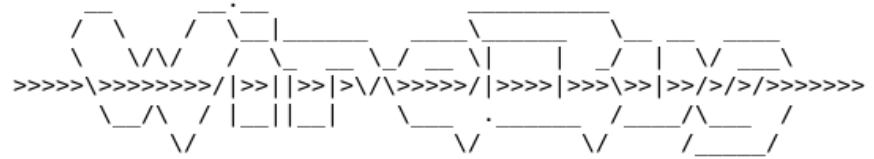


The problem with the tools ...

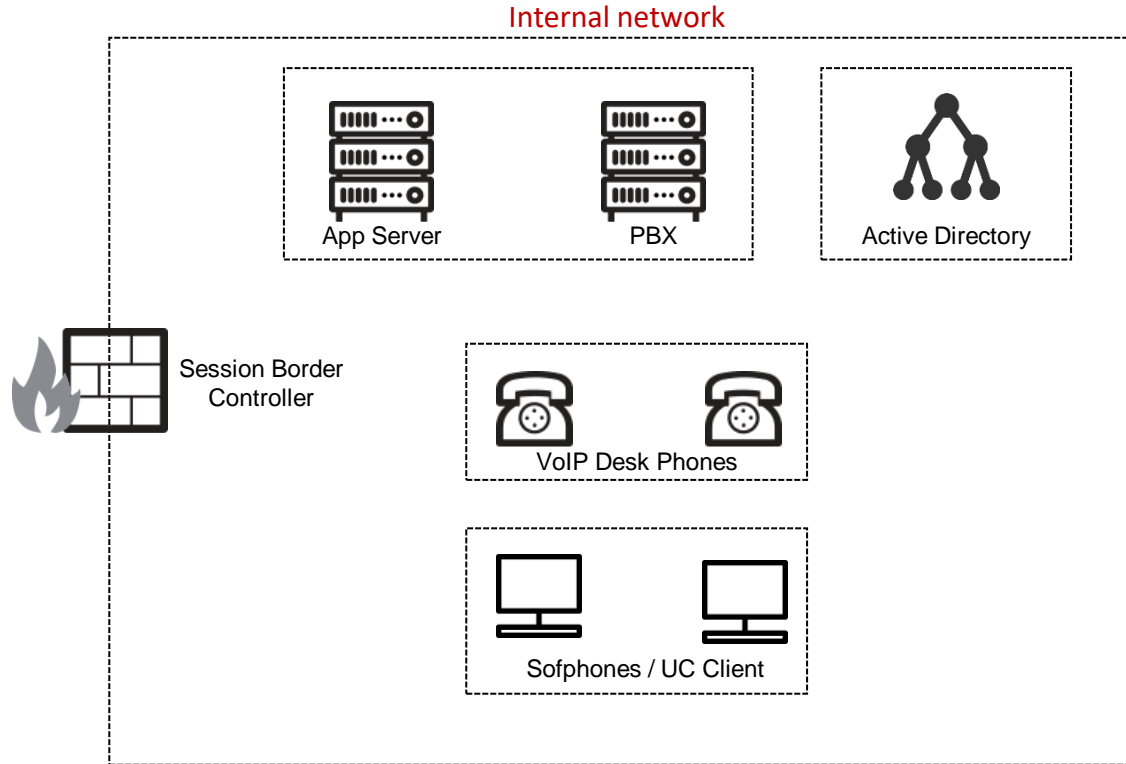
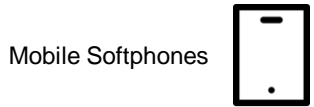
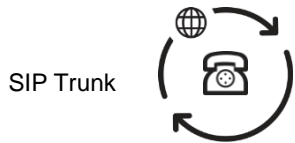
- there are not many tools for VoIP security analysis
- partial outdated
- too static
- manufacturer dependent

WireBug

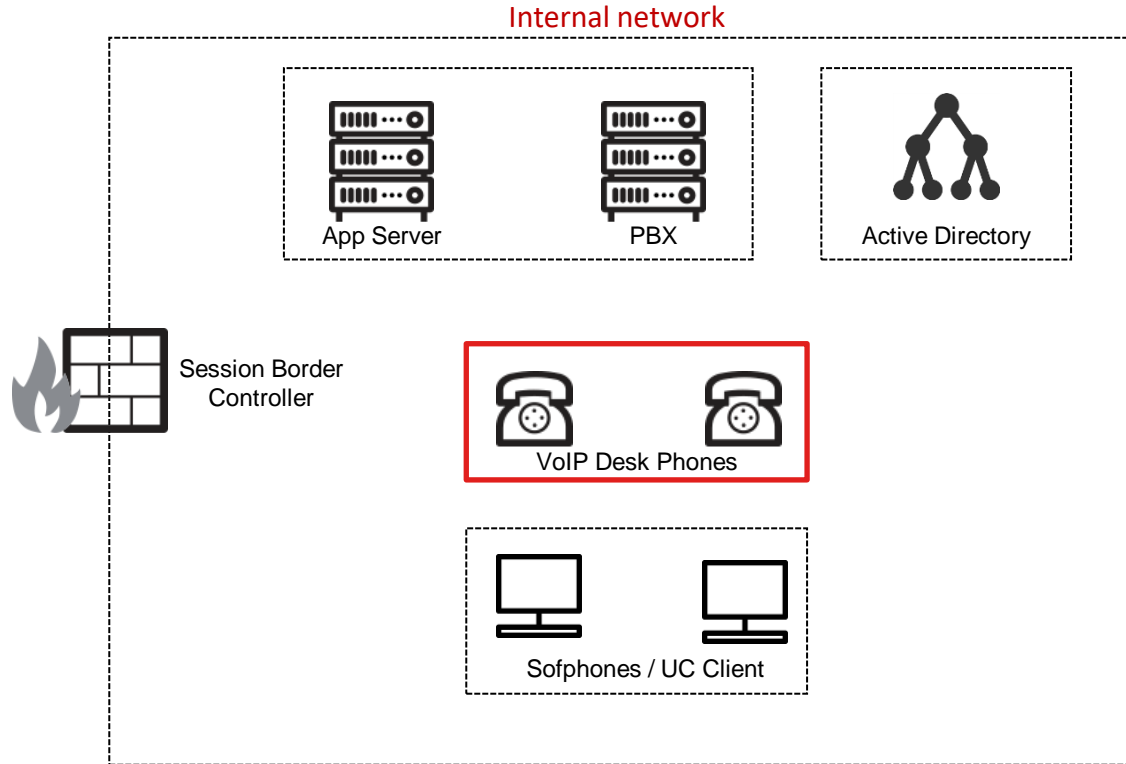
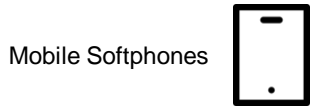
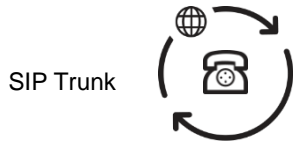
- open source
- Python
- manufacturer independent
- customizable
- Wizard for handy usage
- every tool can be used independently



<https://github.com/SySS-Research/WireBug>



Network separation



Network separation

→ Network Access Control

→ 802.1x and MAC based Authentication

→ <https://www.defcon.org/images/defcon-19/dc-19-presentations/Duckwall/DEFCON-19-Duckwall-Bridge-Too-Far.pdf>

→ <https://github.com/SySS-Research/Lauschgeraet>

Network separation

→ Network Access Control

→ 802.1x and MAC based Authentication

→ <https://www.defcon.org/images/defcon-19/dc-19-presentations/Duckwall/DEFCON-19-Duckwall-Bridge-Too-Far.pdf>

→ <https://github.com/SySS-Research/Lauschgeraet>

→ Link Layer Discovery Protocol – MEDIA (LLDP-MED)

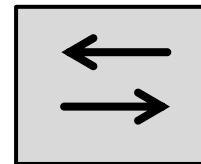
→ Layer 2 Protocol (OSI Model)

→ protocol to exchange information between physical neighbors

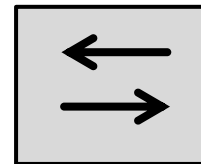
→ no authentication

→ MEDIA: VLAN-IDs, Call-Server IP address, DiffServ

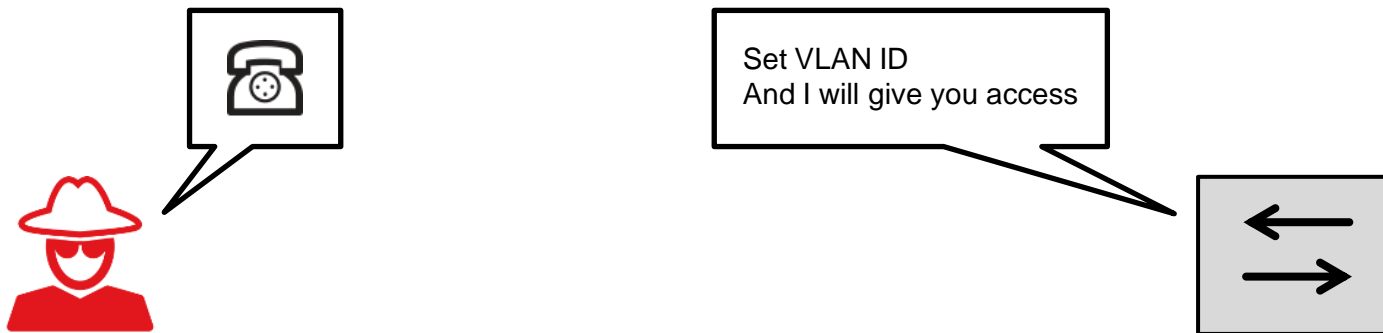
Network separation

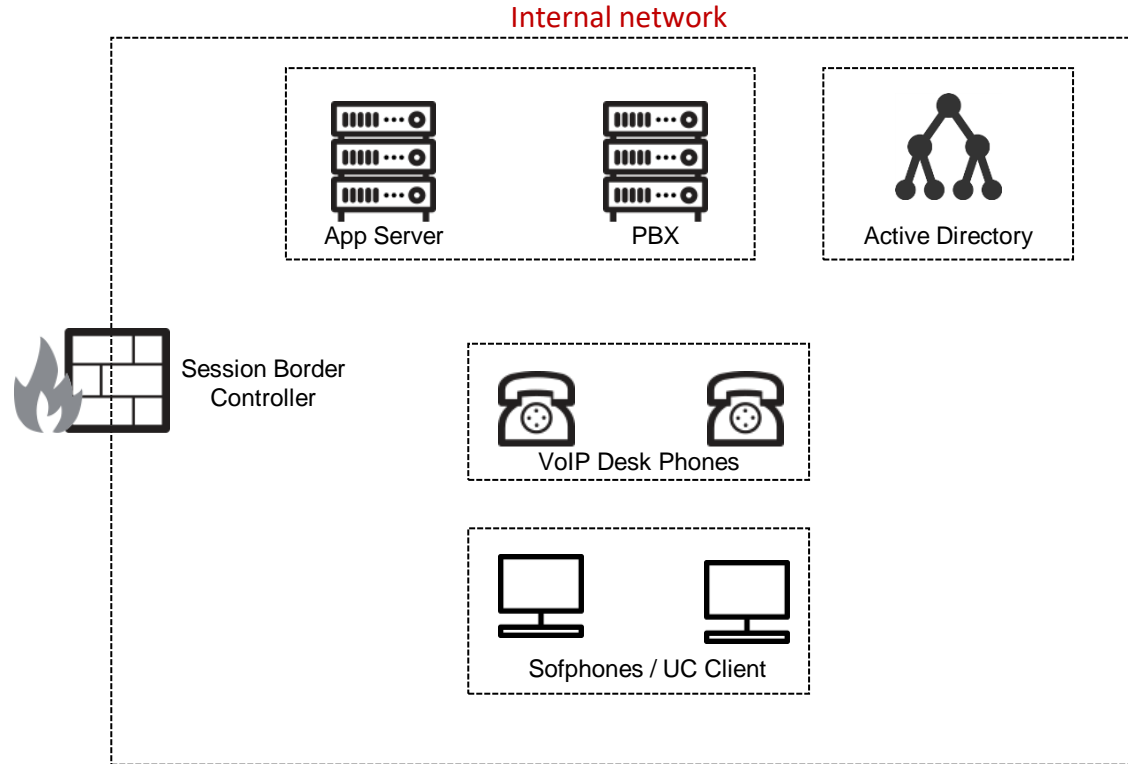
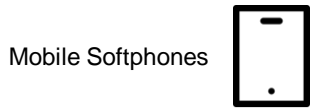


Network separation

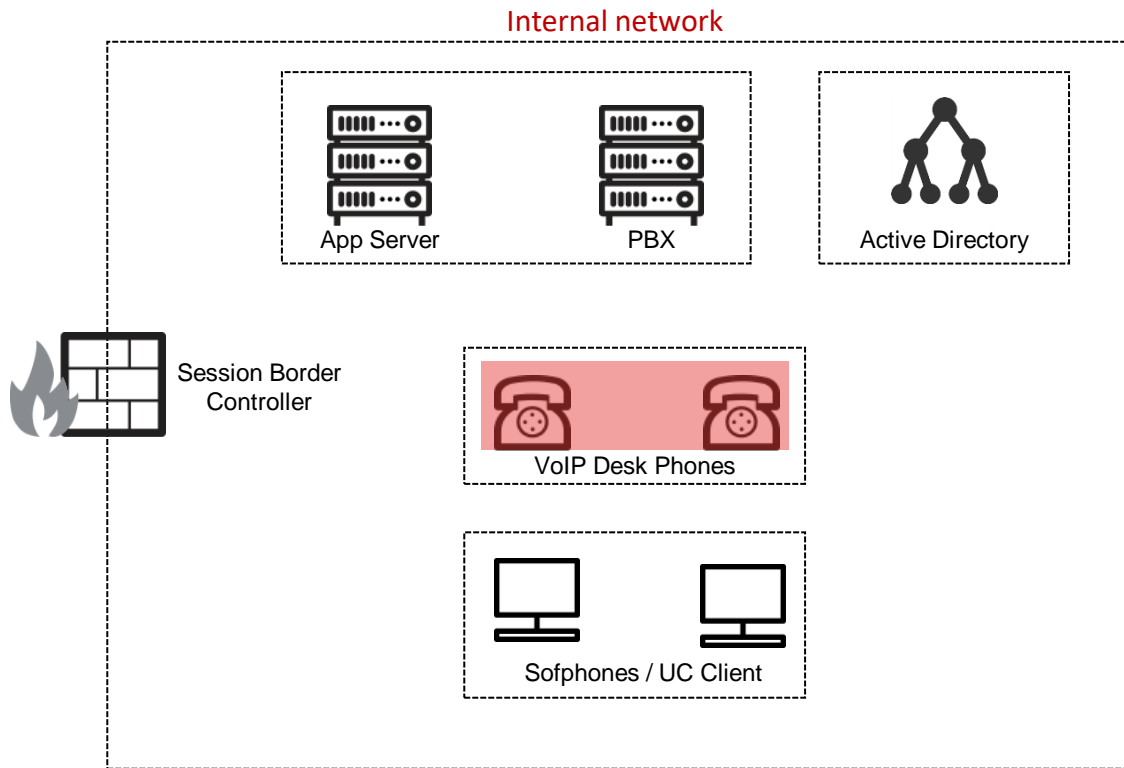
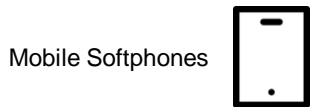


Network separation





Desk Phones



Eavesdropping calls



→ today SIP and RTP is encrypted

Eavesdropping calls



→ today SIP and RTP is encrypted

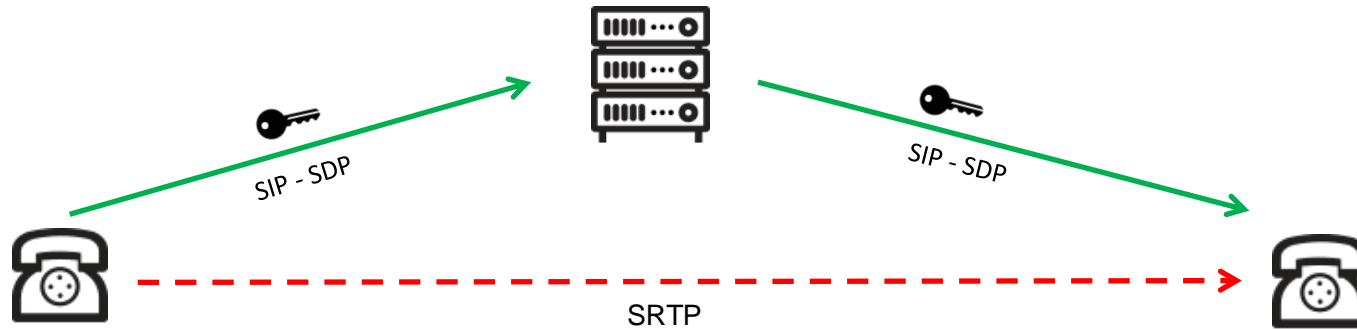
→ SIP over TLS

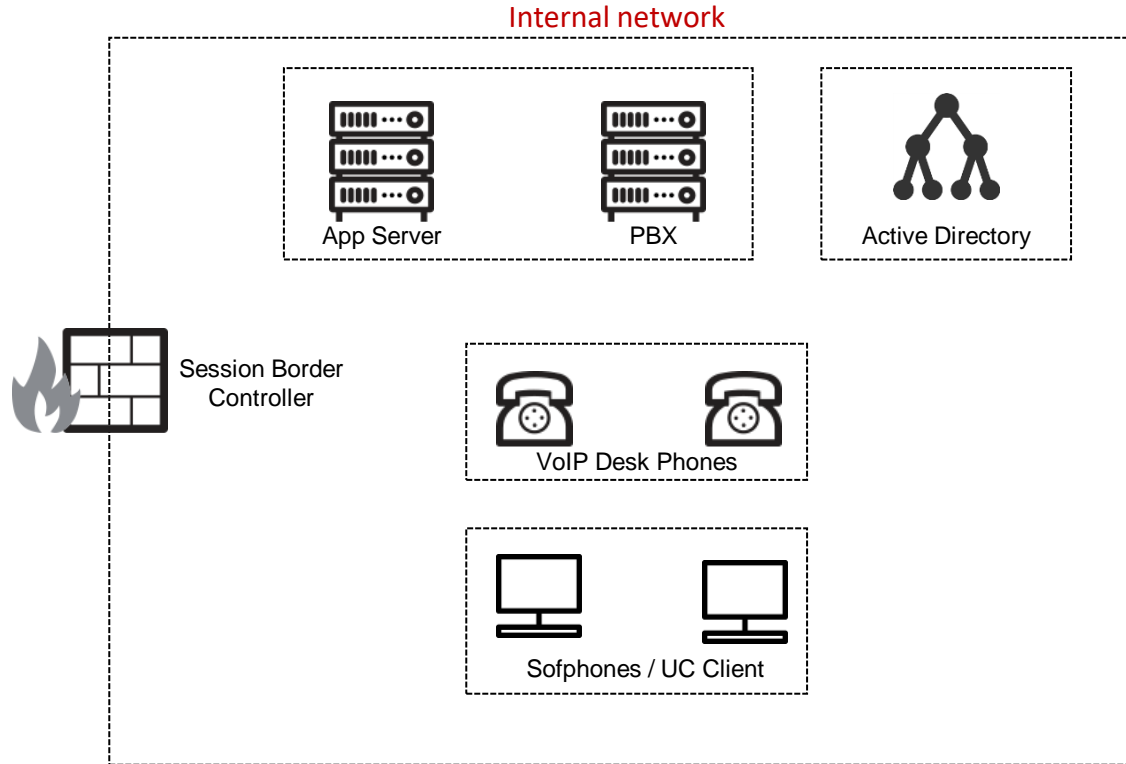
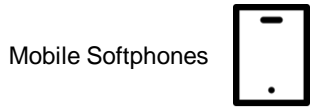
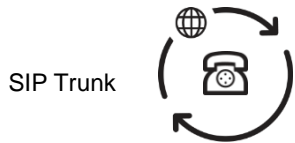
Eavesdropping calls

- today SIP and RTP is encrypted
- SIP over TLS
- SRTP-SDES

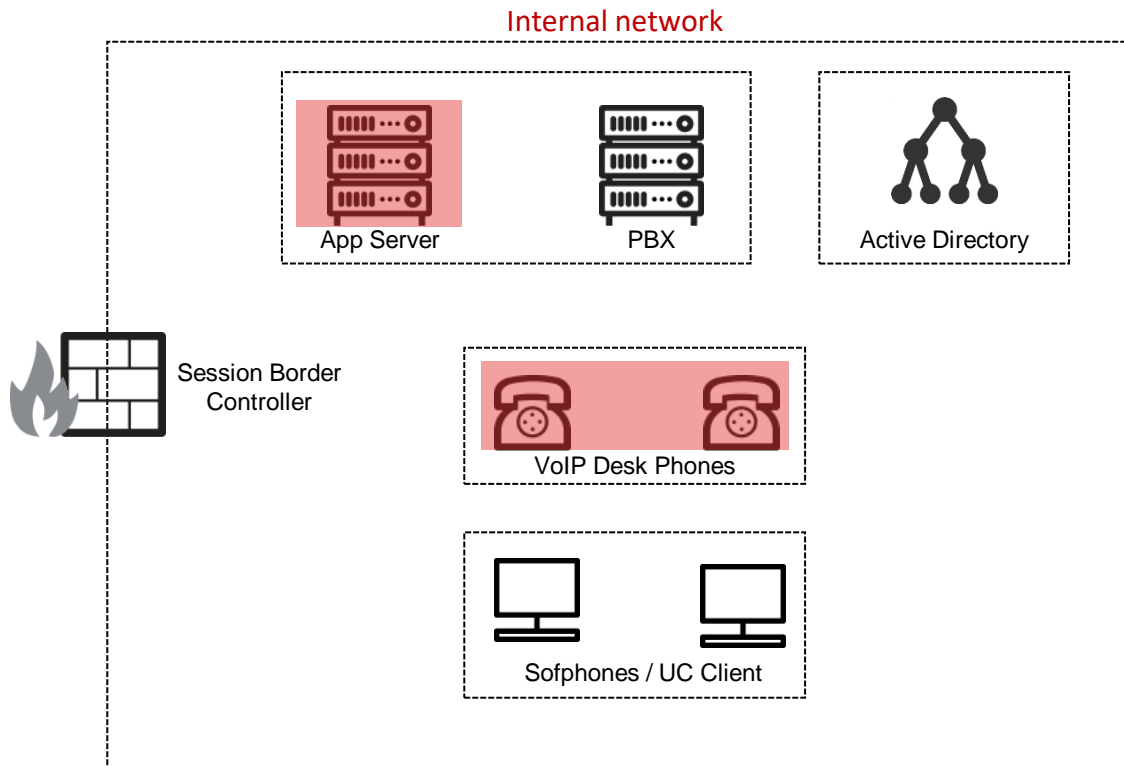
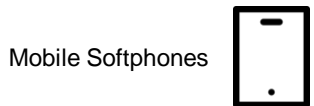
Eavesdropping calls

- today SIP and RTP is encrypted
- SIP over TLS
- SRTP-SDES





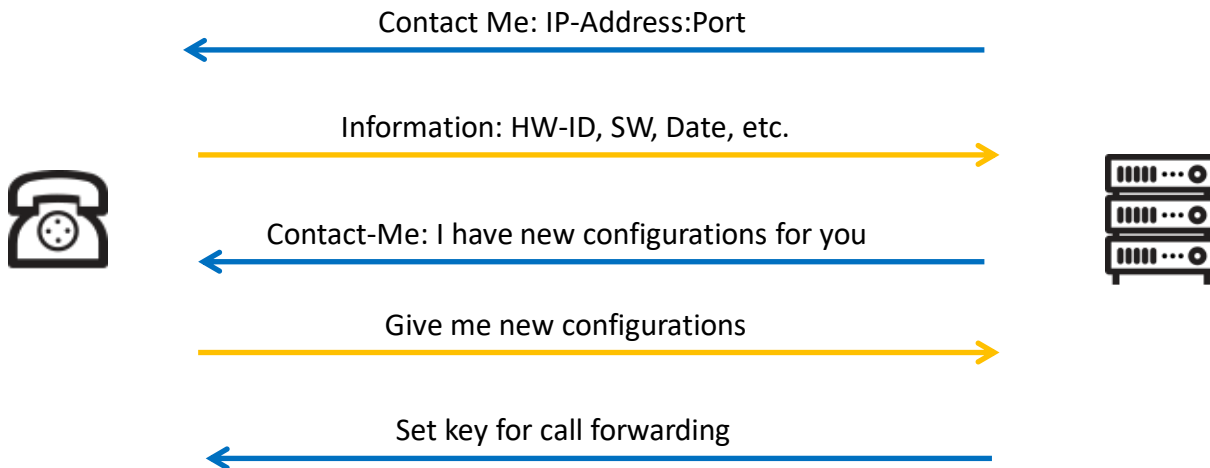
Provisioning



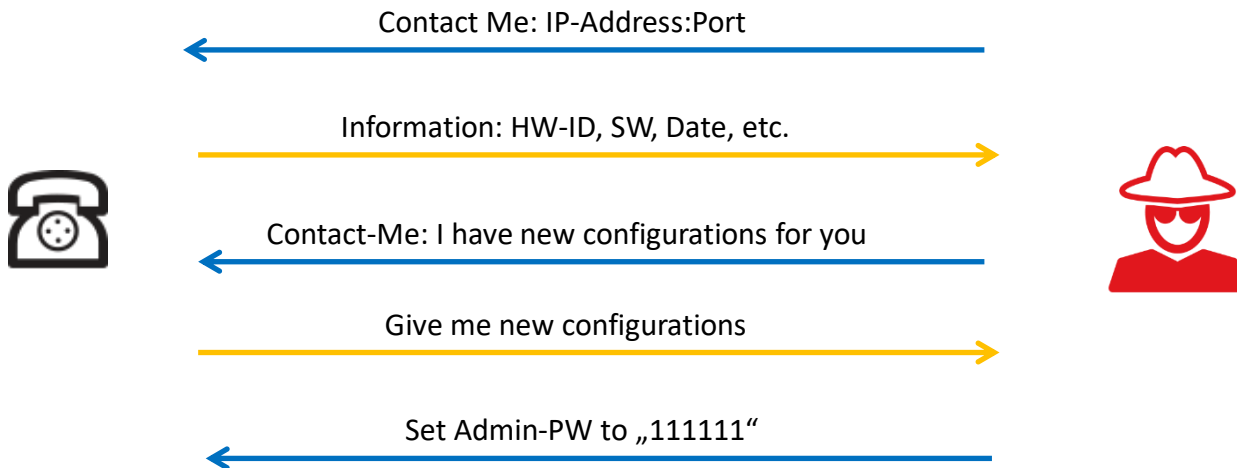
Provisioning | As an admin you want ...

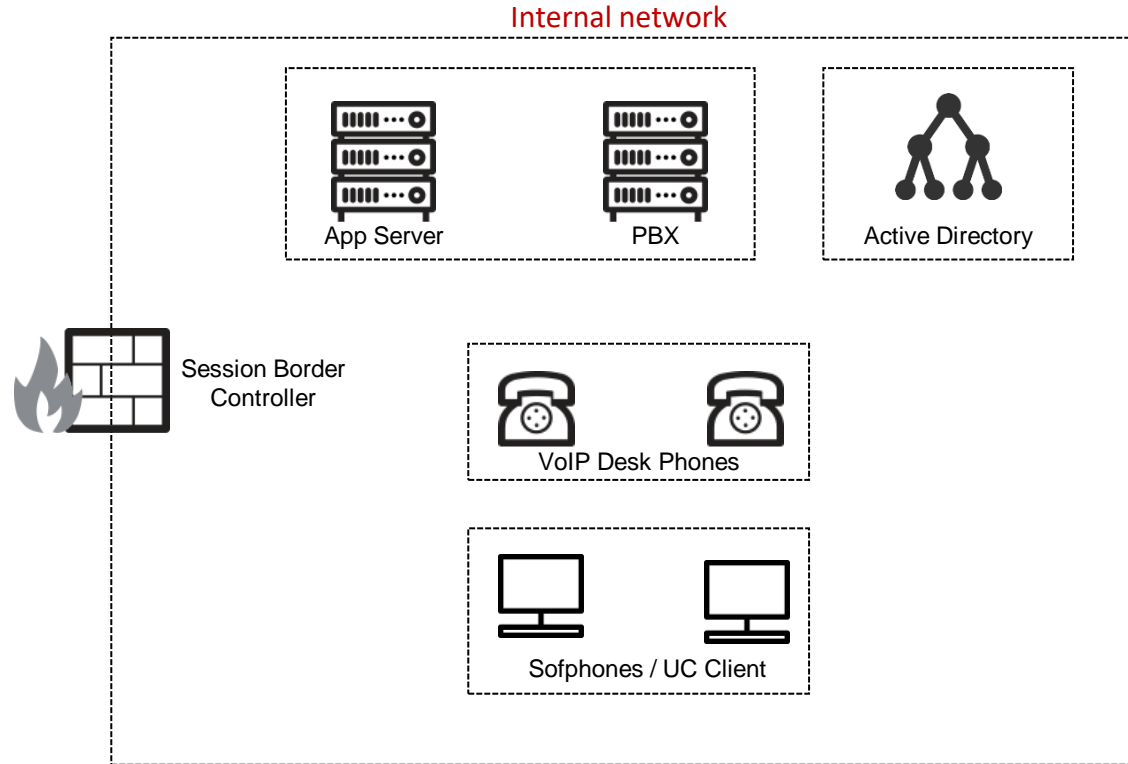
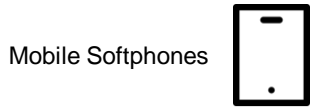
- as little effort as possible
- automatic provisioning and deployment of new phones
- central administration

Provisioning | Example OpenScape Business

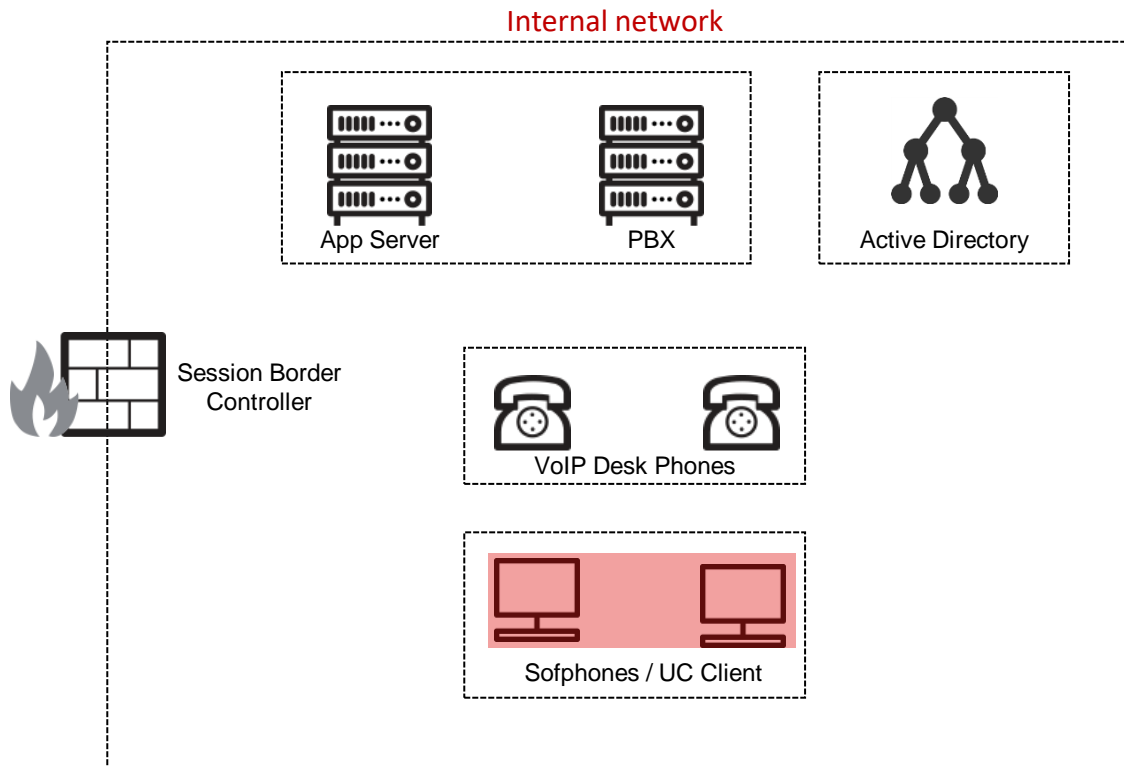
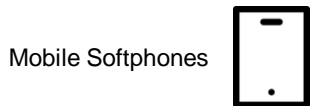


Provisioning | Example OpenScape Business





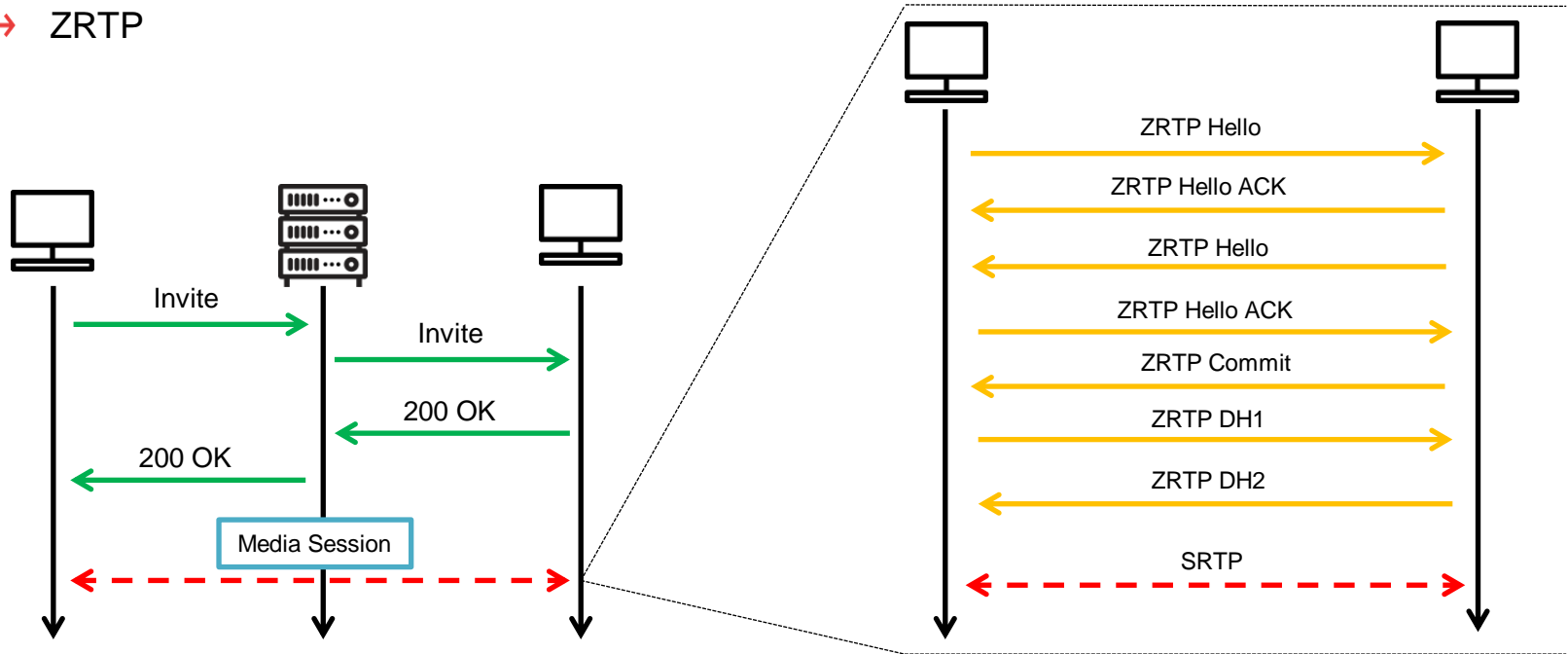
Softphones

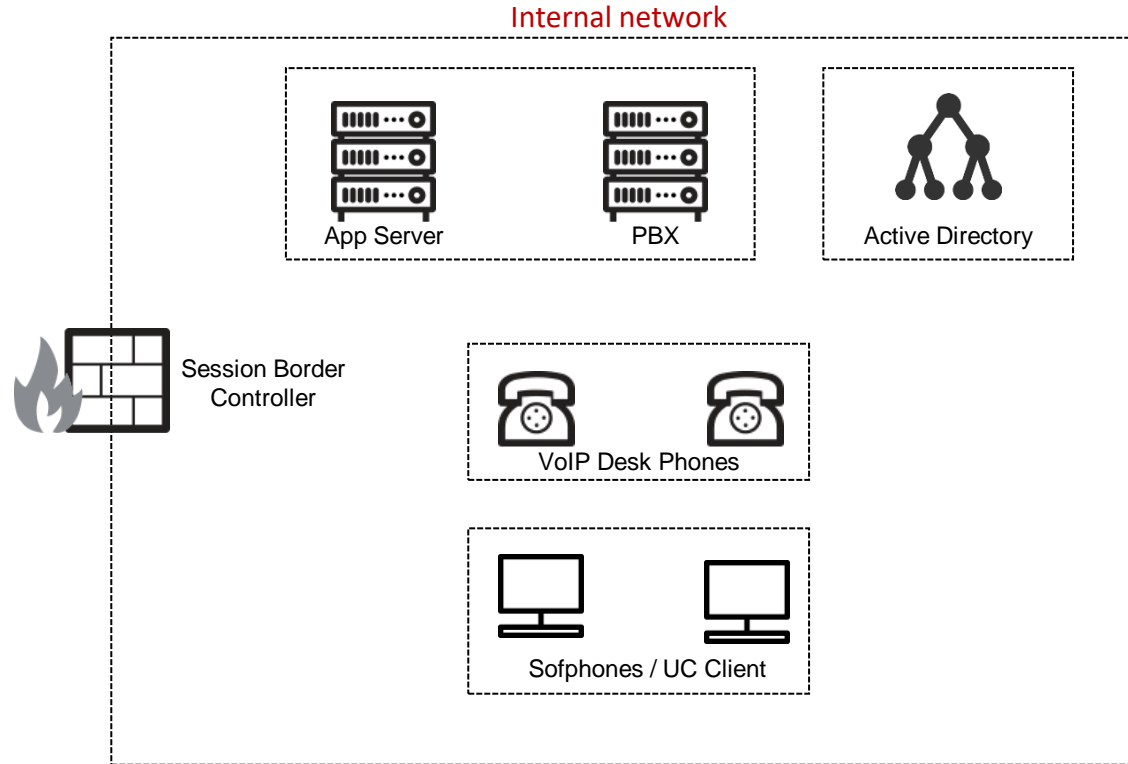
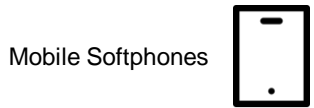


Eavesdropping calls - Softphones

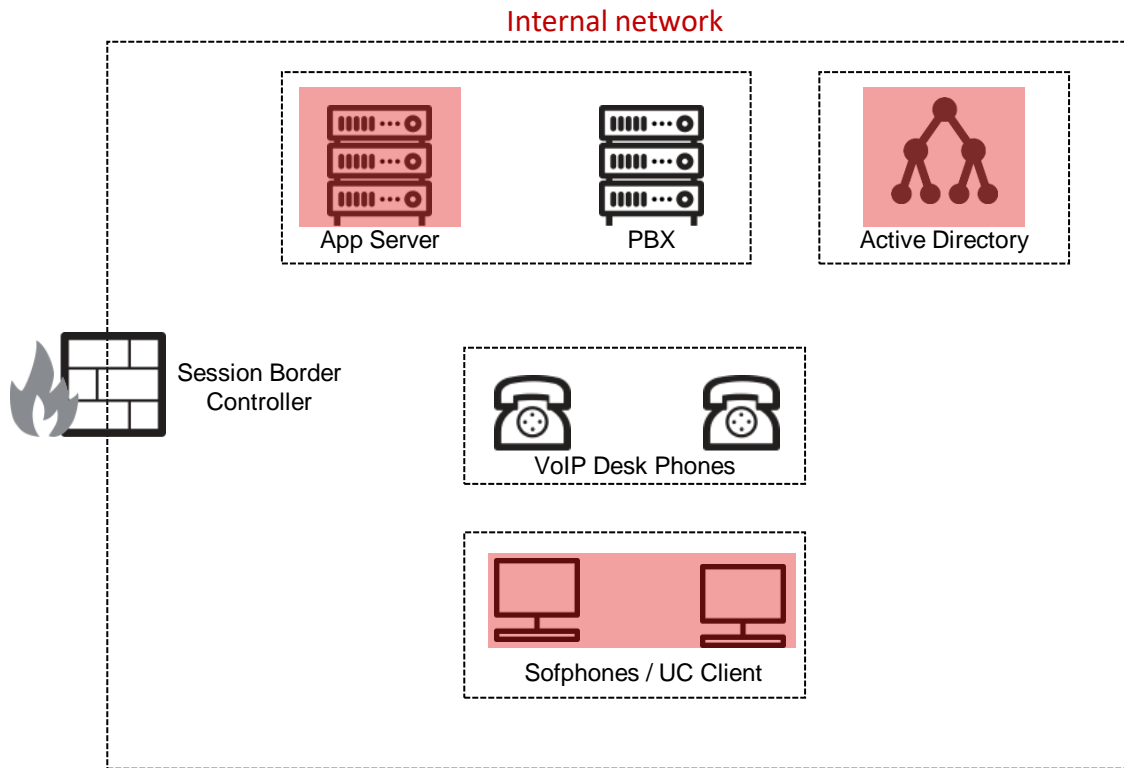
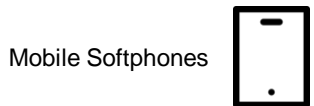
→ SIP over TLS

→ ZRTP

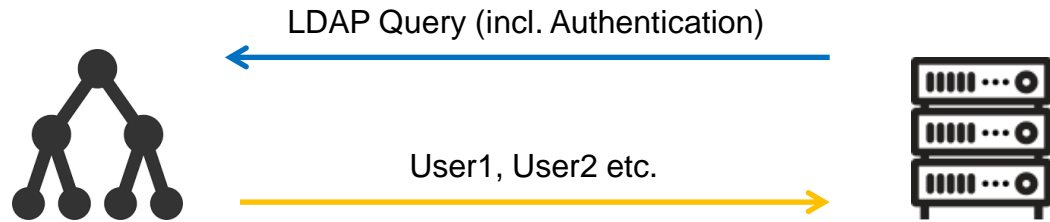




Unified Communication Software



Unified Communication Software



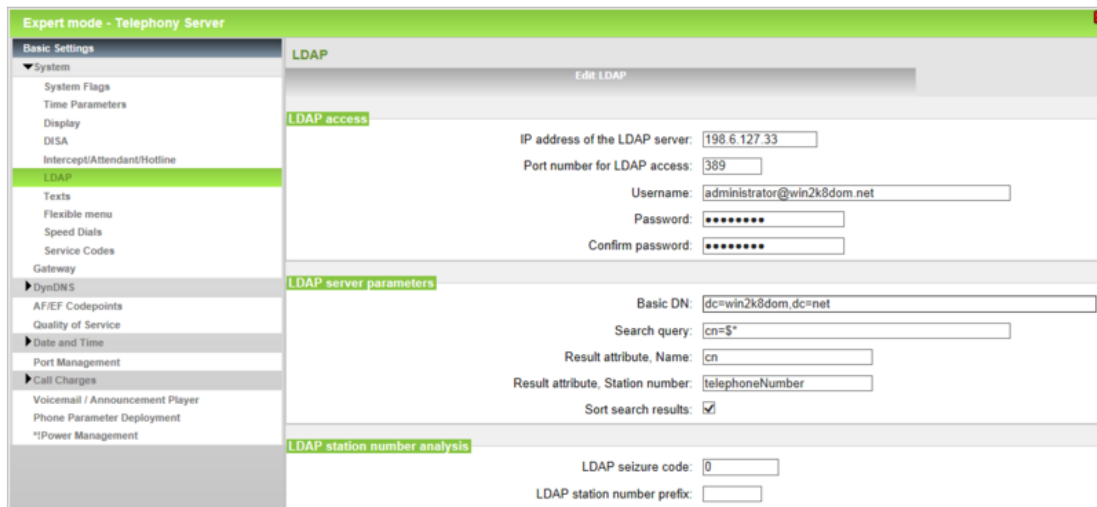
Unified Communication Software

https://wiki.unify.com/wiki/How_to_connect_OpenScope_Business_to_LDAP_Server

Example: System LDAP connection to Active Directory

Within this example the following is assumed:

- IP address of the Active Directory LDAP server: 198.6.127.33
- Username: Administrator@win2k8dom.net
- Password / Confirm password: Password of the Administrator user
- Basic DN: dc=win2k8dom,dc=net



The screenshot shows the 'Expert mode - Telephony Server' configuration window. The left sidebar contains a tree view with 'LDAP' selected under 'Basic Settings'. The main area is titled 'LDAP' and contains several sections:

- LDAP access:** IP address of the LDAP server: 198.6.127.33; Port number for LDAP access: 389; Username: administrator@win2k8dom.net; Password: [masked]; Confirm password: [masked].
- LDAP server parameters:** Basic DN: dc=win2k8dom,dc=net; Search query: cn=\$*; Result attribute, Name: cn; Result attribute, Station number: telephoneNumber; Sort search results: [checked].
- LDAP station number analysis:** LDAP seizure code: 0; LDAP station number prefix: [empty].

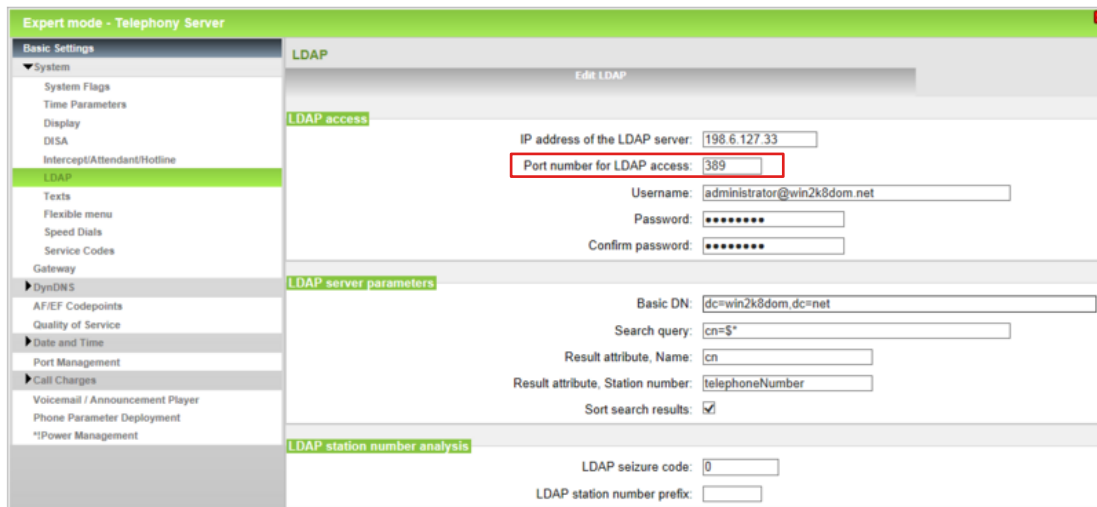
Unified Communication Software

https://wiki.unify.com/wiki/How_to_connect_OpenScape_Business_to_LDAP_Server

Example: System LDAP connection to Active Directory

Within this example the following is assumed:

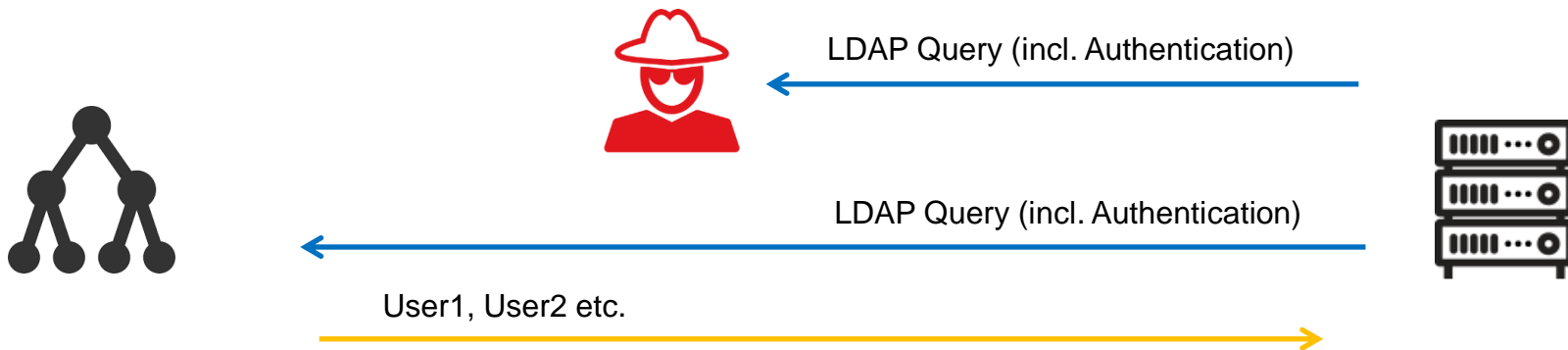
- IP address of the Active Directory LDAP server: 198.6.127.33
- Username: Administrator@win2k8dom.net
- Password / Confirm password: Password of the Administrator user
- Basic DN: dc=win2k8dom,dc=net

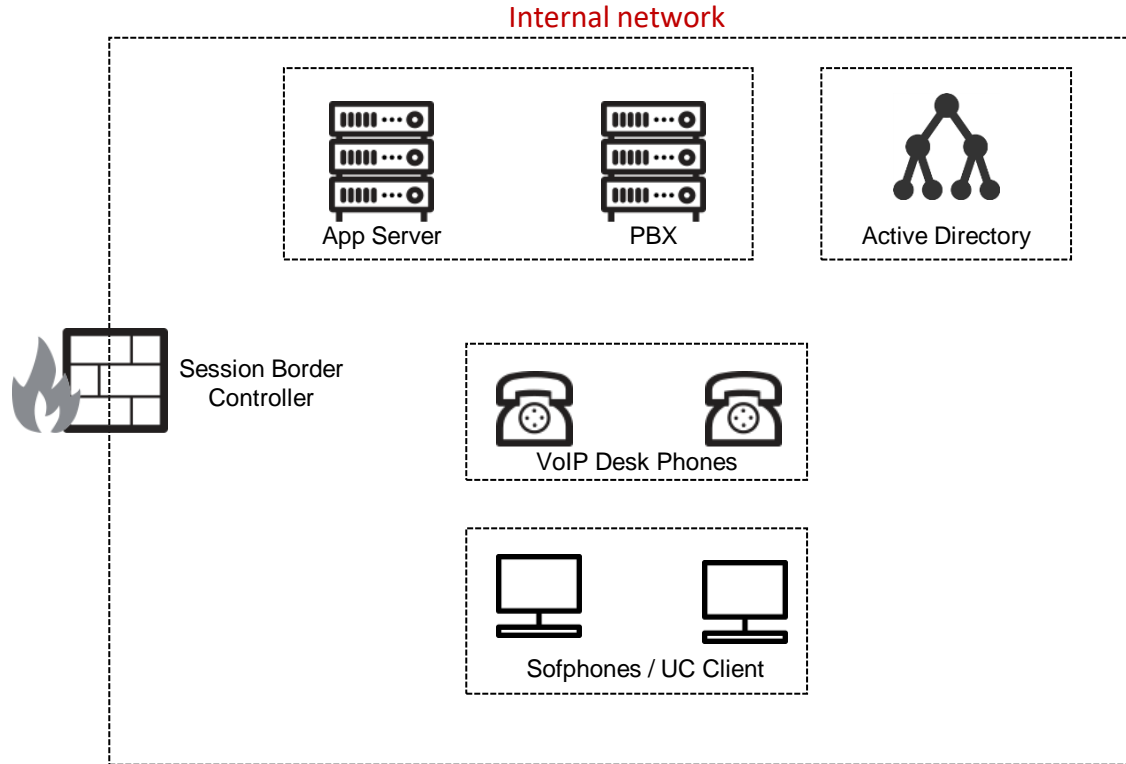
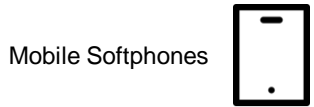
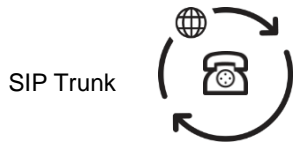


The screenshot shows the 'Expert mode - Telephony Server' configuration window. The left sidebar contains a tree view with categories like System, LDAP, DynDNS, Date and Time, Port Management, and Call Charges. The main area is titled 'LDAP' and contains several sections:

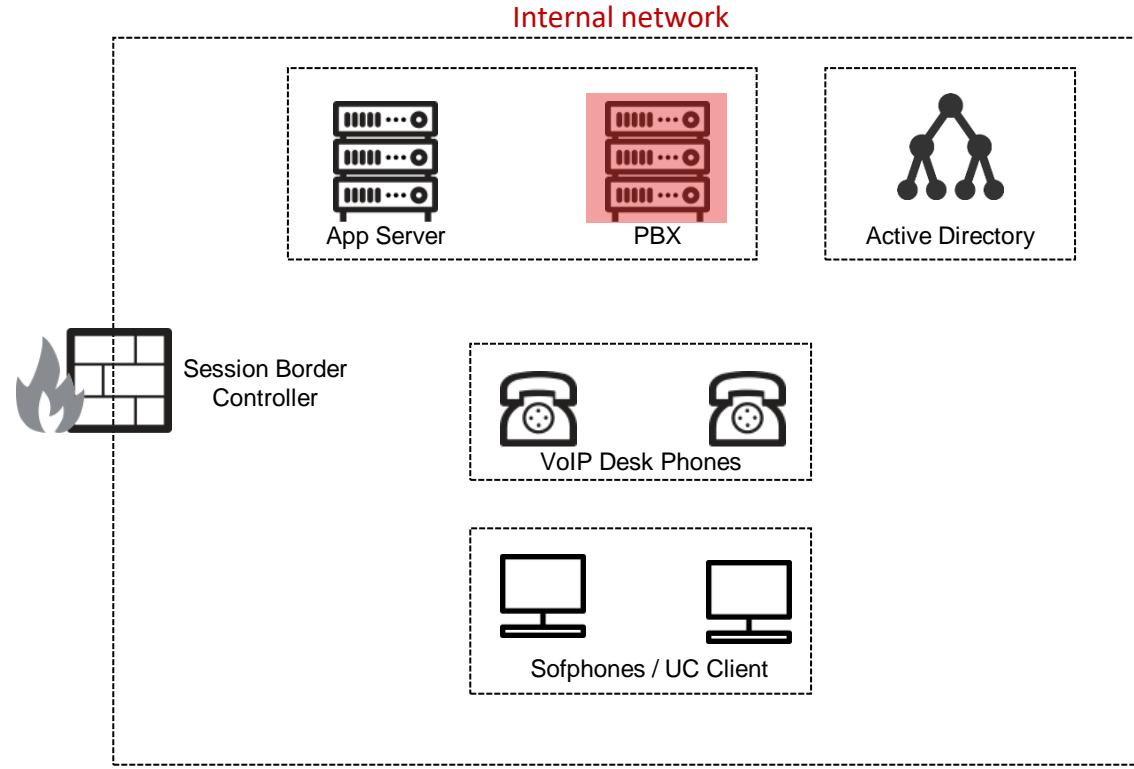
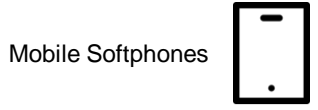
- LDAP access:** Includes fields for 'IP address of the LDAP server' (198.6.127.33) and 'Port number for LDAP access' (389). The port field is highlighted with a red box.
- LDAP server parameters:** Includes fields for 'Username' (administrator@win2k8dom.net), 'Password' (masked with dots), 'Confirm password' (masked with dots), and 'Basic DN' (dc=win2k8dom,dc=net).
- LDAP station number analysis:** Includes fields for 'LDAP seizure code' (0) and 'LDAP station number prefix' (empty).

Unified Communication Software





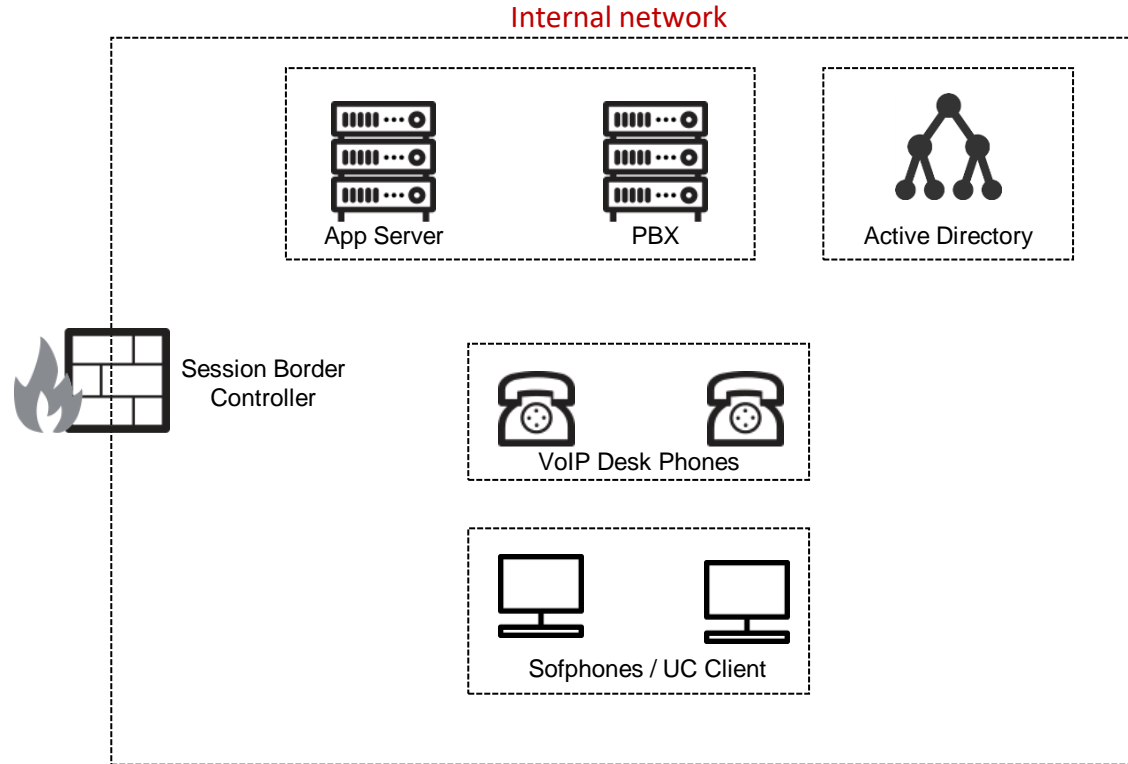
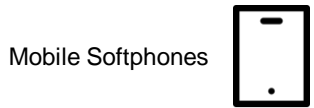
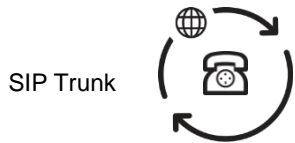
PBX



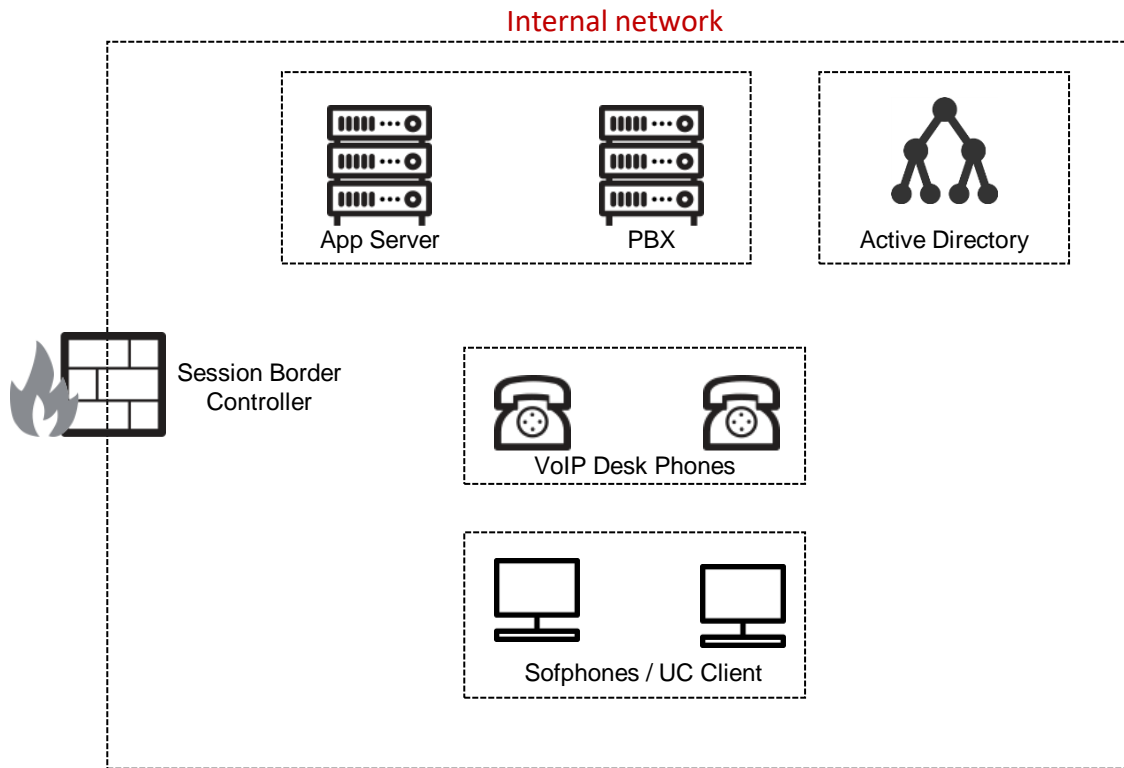
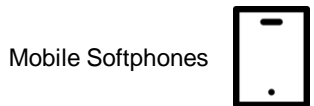
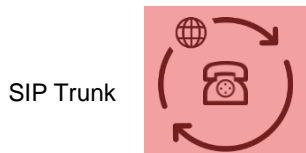
PBX and SIP

- user enumeration
 - Sending a register request to the PBX
 - Get 401 or 407 back in case user exists
 - Get 200 back in case there is no password required

- online brute force attack



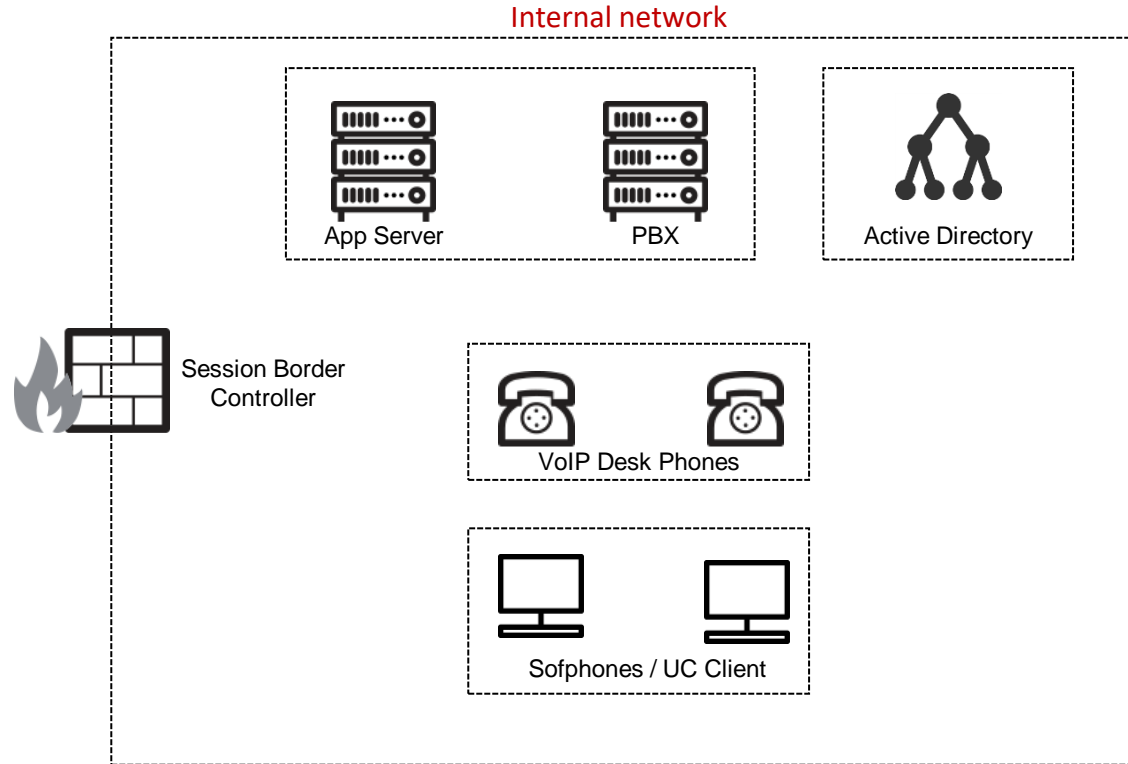
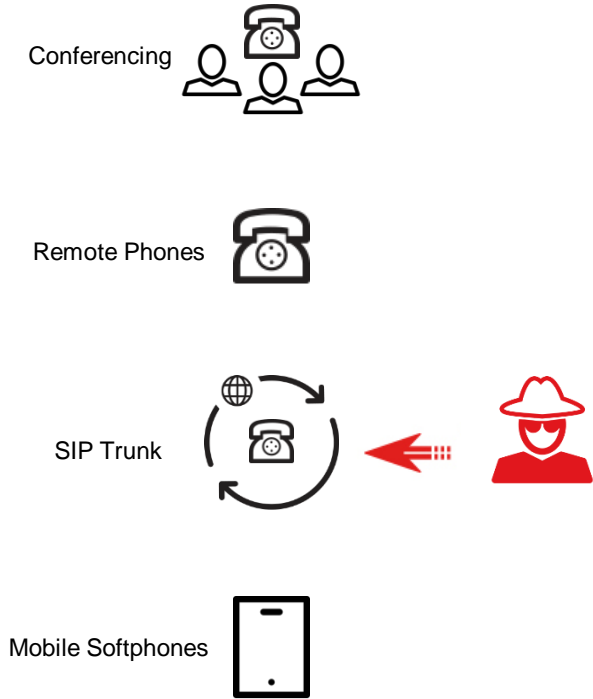
SIP Trunk

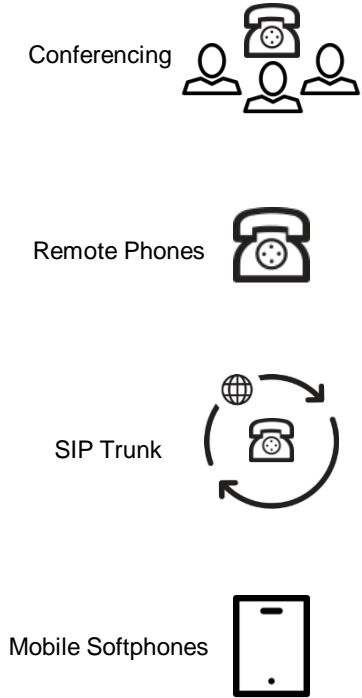


SIP Trunk

- Registration Mode
 - password based authentication
 - Security depends on the password quality

- Static Mode
 - IP based authentication
 - Security depends on network ACLs





Session Border
Controller



Internal network



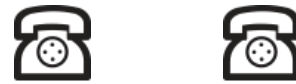
App Server



PBX



Active Directory

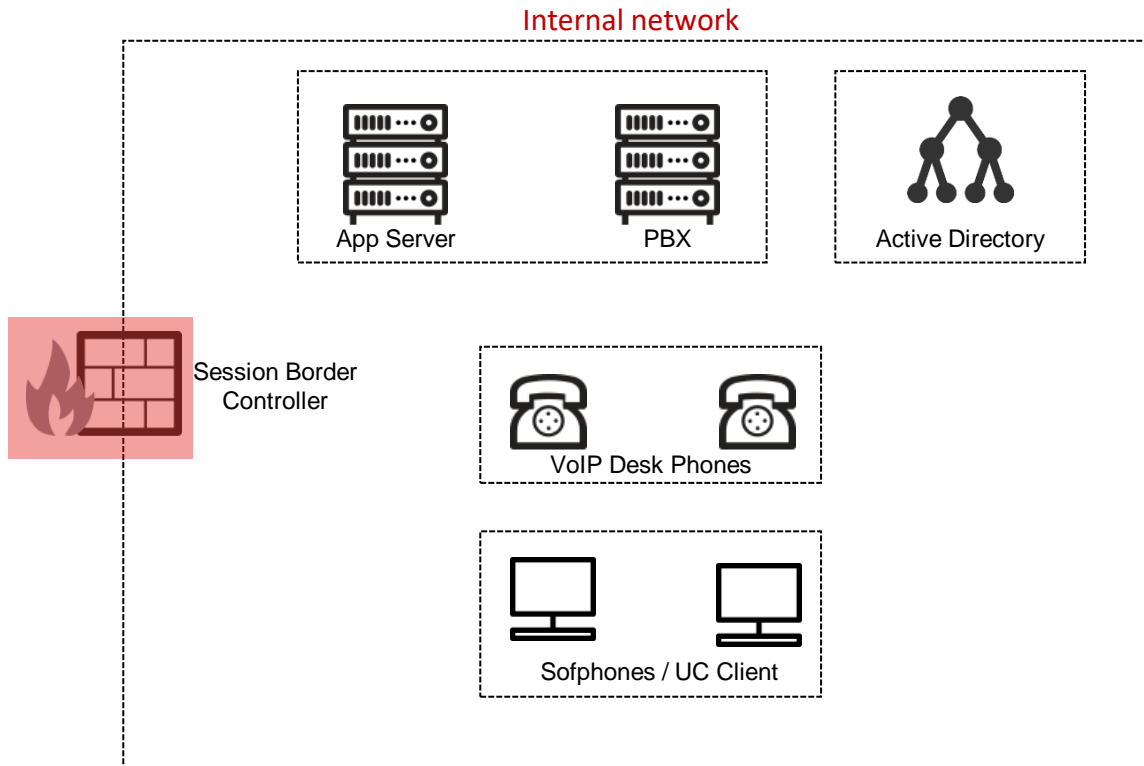


VoIP Desk Phones



Sofphones / UC Client

Mobile Softphones



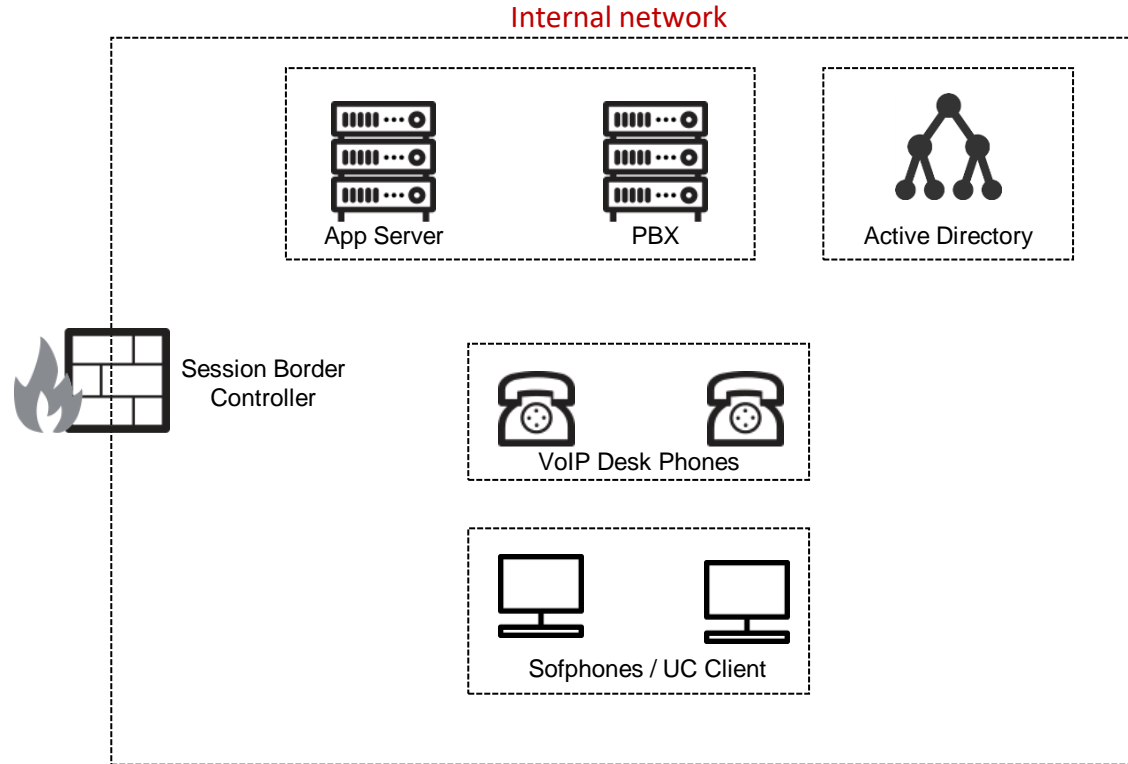
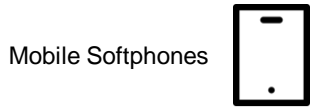
Mobile Softphones

- external access to internal services
- customer statement: „This is not a problem because everything is encrypted and we are using an expensive session border controller to detect and prevent attacks and finally keep our internal network secure.“

Mobile Softphones

[MaliciousSignatureDB]

| Index | Name | Pattern |
|-------|-----------------|---|
| 0 | SIPVicious | Header.User-Agent.content prefix 'friendly-scanner' |
| 1 | SIPScan | Header.User-Agent.content prefix 'sip-scan' |
| 2 | Smapi | Header.User-Agent.content prefix 'smapi' |
| 3 | Sipsak | Header.User-Agent.content prefix 'sipsak' |
| 4 | Sipcli | Header.User-Agent.content prefix 'sipcli' |
| 5 | Sivus | Header.User-Agent.content prefix 'SIVuS' |
| 6 | Gulp | Header.User-Agent.content prefix 'Gulp' |
| 7 | Sipv | Header.User-Agent.content prefix 'sipv' |
| 8 | Sundayddr Worm | Header.User-Agent.content prefix 'sundayddr' |
| 9 | VaxIPUserAgent | Header.User-Agent.content prefix 'VaxIPUserAgent' |
| 10 | VaxSIPUserAgent | Header.User-Agent.content prefix 'VaxSIPUserAgent' |
| 11 | SipArmyKnife | Header.User-Agent.content prefix 'siparmyknife' |



Remote Desk Phones



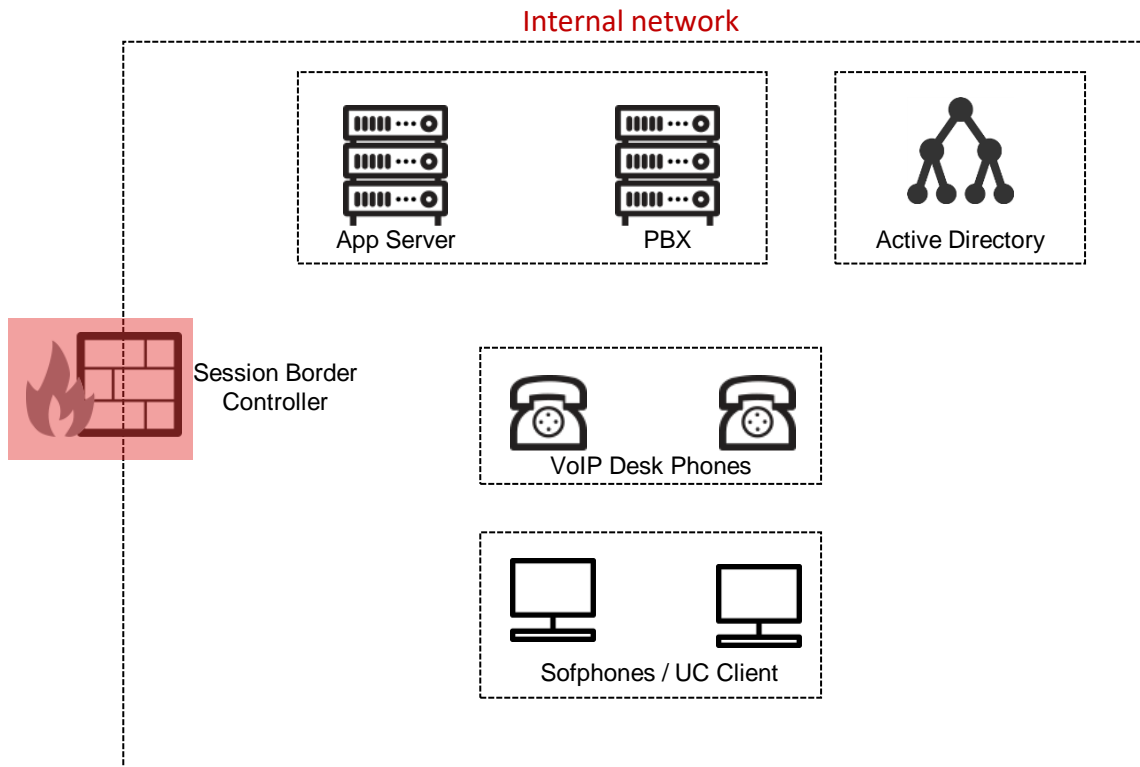
Remote Phones



SIP Trunk



Mobile Softphones



Remote Desk Phones

- external access to internal services
- VPN (IPSec)
- Reverse Proxy

Remote Desk Phones | Reverse Proxy



→ „The RP will validate incoming registrations against their certificate”

Remote Desk Phones | Reverse Proxy

- *„The RP will validate incoming registrations against their certificate”*
- *“If the certificate is valid (...), the registration is forwarded to the PBX using TLS”*

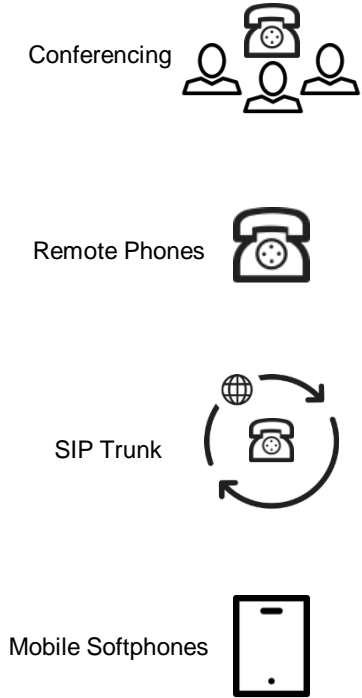
Remote Desk Phones | Reverse Proxy

- *„The RP will validate incoming registrations against their certificate”*
- *“If the certificate is valid (...), the registration is forwarded to the PBX using TLS”*
- *“If the certificate is not valid or the incoming registration was sent with TCP (not TLS) or the Check Certificate check-mark is not set, it is forwarded to the PBX using TCP”*

Remote Desk Phones | Reverse Proxy

- „The RP will validate incoming registrations against their certificate”
- “If the certificate is valid (...), the registration is forwarded to the PBX using TLS”
- “If the certificate is not valid or the incoming registration was sent with TCP (not TLS) or the Check Certificate check-mark is not set, it is forwarded to the PBX using TCP”

<https://wiki.innovaphone.com/index.php?title=Course12:Advanced - Reverse Proxy#Reverse Proxy and Certificates>



Session Border
Controller



Internal network



App Server



PBX



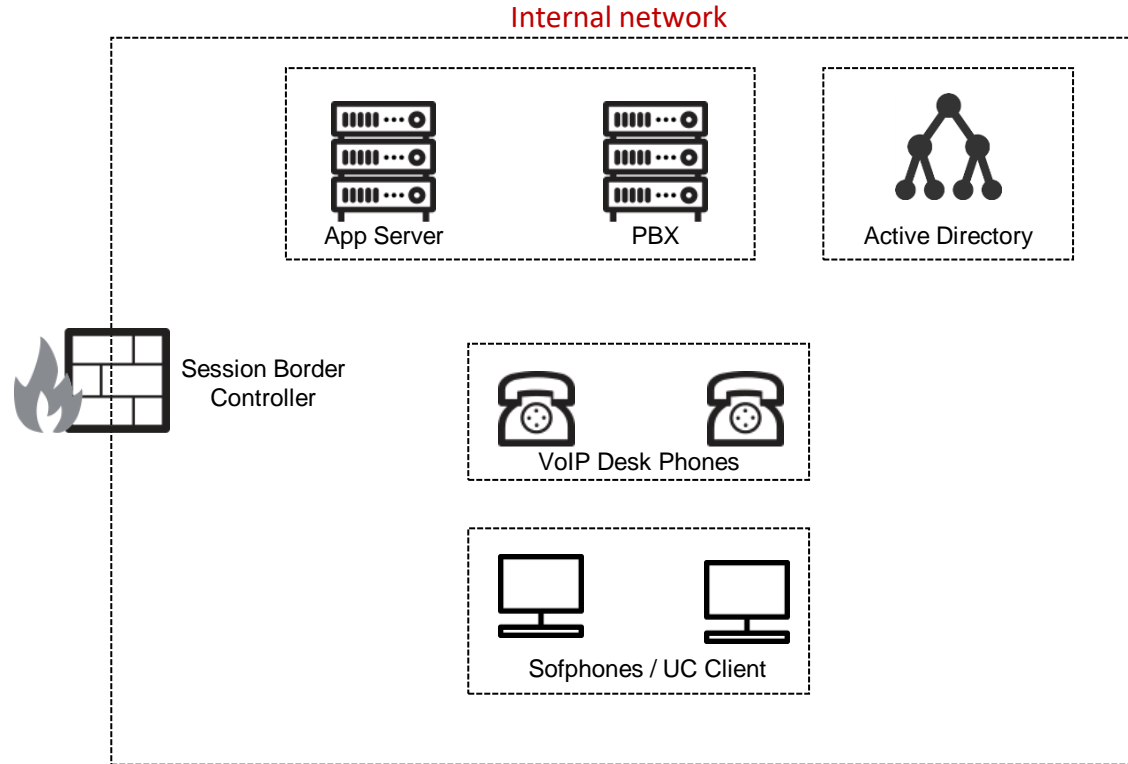
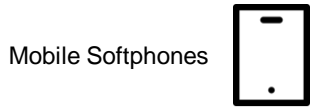
Active Directory



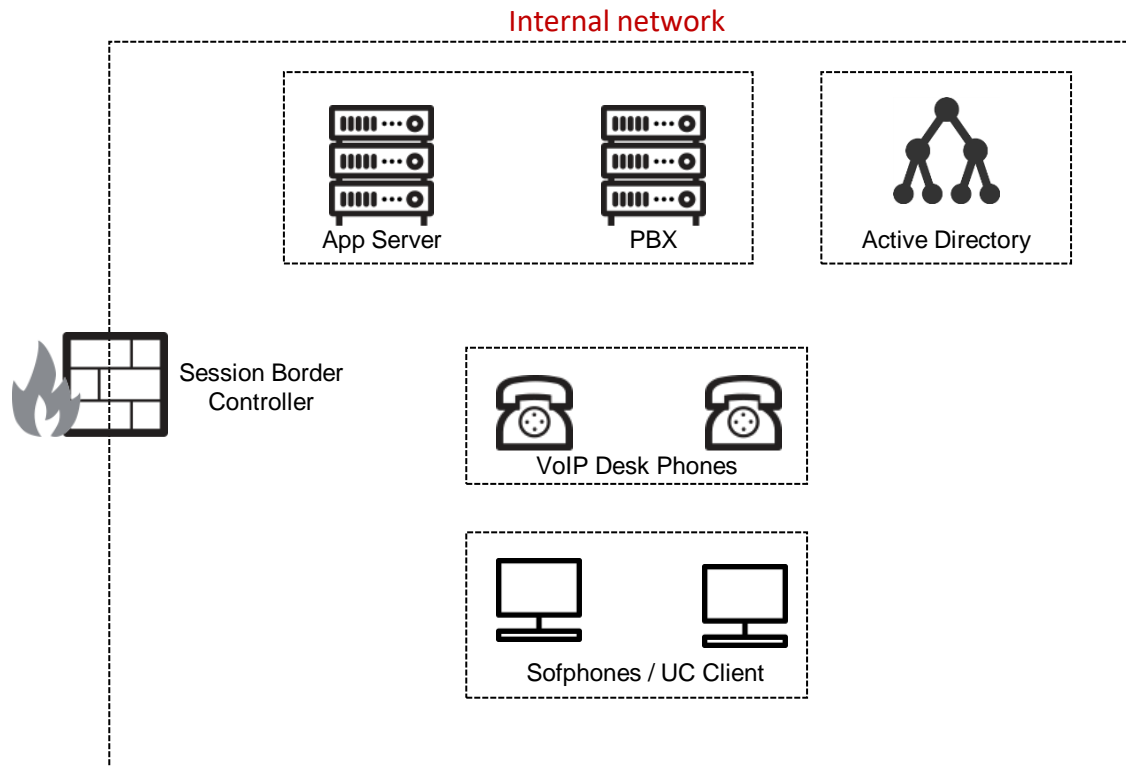
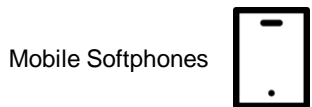
VoIP Desk Phones



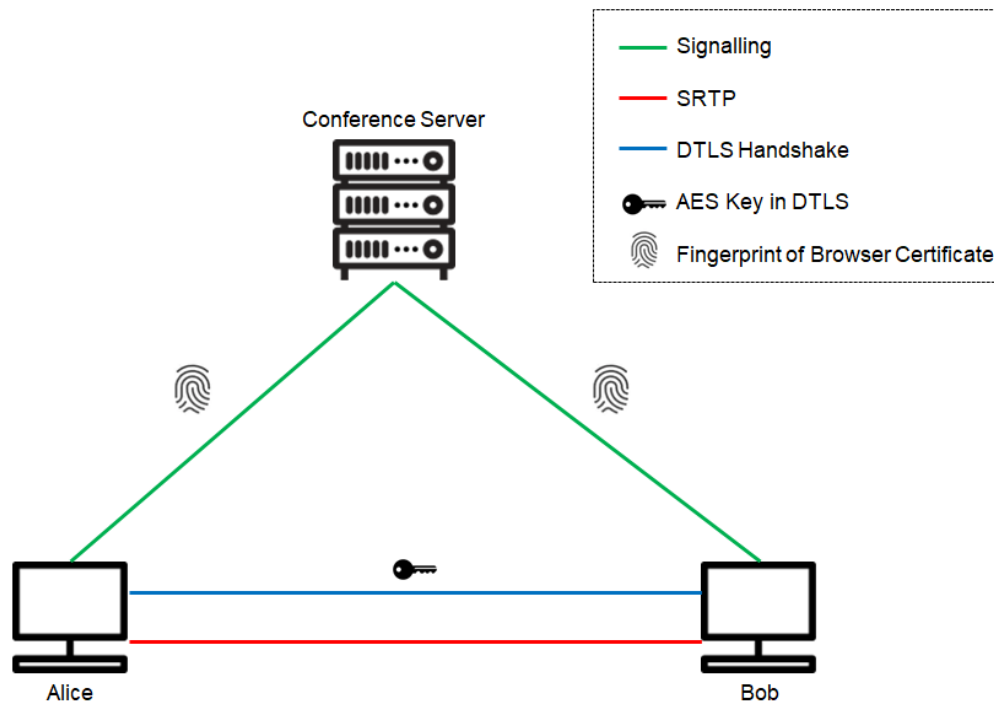
Sofphones / UC Client



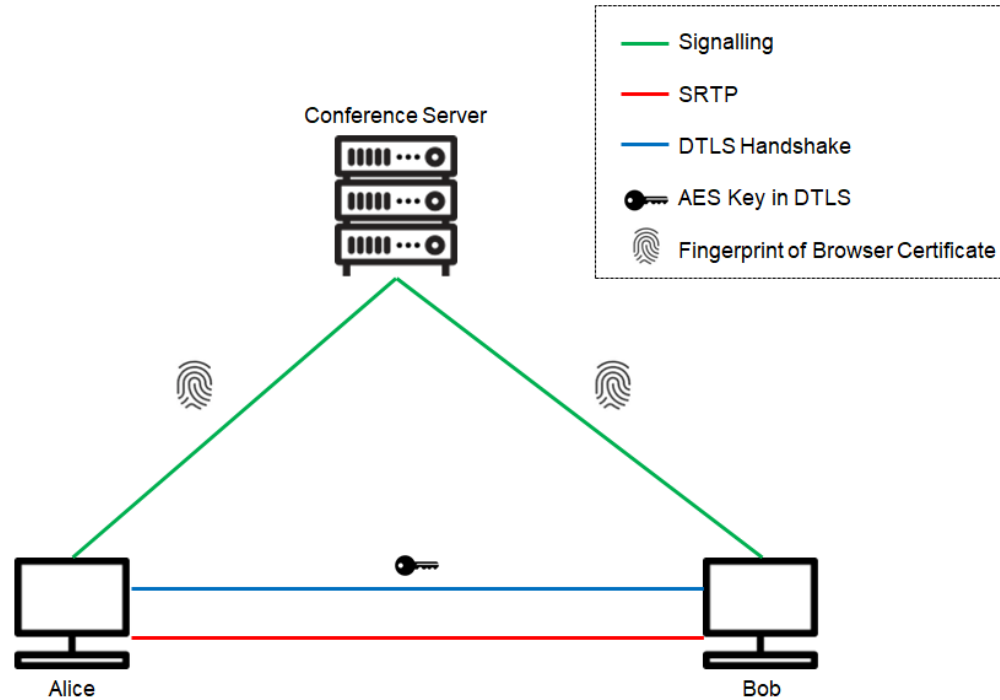
Conferencing



Conferencing | SRTP-DTLS



Conferencing | SRTP-DTLS



https://www.sysS.de/fileadmin/dokumente/Publikationen/2020/2020_07_28_New_Ways_of_Communicating_When_End-to-End-Encryption_Gains_a_New_Meaning.pdf

Conclusion & Recommendation



Conclusion & Recommendation



→ VoIP and UC means not just a few IP phones in your network

Conclusion & Recommendation

- VoIP and UC means not just a few IP-Phones in your network
- Do not trust the „encryption“

Conclusion & Recommendation

- VoIP and UC means not just a few IP-Phones in your network
- Do not trust the „encryption“
- Think twice if you follow manufacturer documentations

Conclusion & Recommendation

- VoIP and UC means not just a few IP-Phones in your network
- Do not trust the „encryption“
- Think twice if you follow manufacturer documentations
- Include VoIP and UC components into your IT security concept.

Conclusion & Recommendation

- VoIP and UC means not just a few IP-Phones in your network
- Do not trust the „encryption“
- Think twice if you follow manufacturer documentations
- Include VoIP and UC components into your IT security concept.
- Do VoIP and UC penetration testing

Conclusion & Recommendation

- VoIP and UC means not just a few IP-Phones in your network
- Do not trust the „encryption“
- Think twice if you follow manufacturer documentations
- Include VoIP and UC components into your IT security concept.
- Do VoIP and UC penetration testing
- *„Smart people defend your networks. Products do not defend your networks“*
- Joe McCray, Hacktivity 2012

Thank you! | Contact me

→ Mail: moritz.abrell@syss.de

→ Homepage: <https://www.syss.de/en>

→ WireBug: <https://github.com/SySS-Research/WireBug>

→ YouTube: <https://www.youtube.com/SySS Pentest TV>

→ Publication about WebRTC and conferencing analysis:

https://www.syss.de/fileadmin/dokumente/Publikationen/2020/2020_07_28_New_Ways_of_Communicating_When_End-to-End-Encryption_Gains_a_New_Meaning.pdf