

**SIEMENS**

# Voice and UC Security

## Some key areas of attention

Francois Lagrange  
CISSP  
francois.lagrange@siemens-enterprise.com

Siemens Enterprise Communications



Copyright © Siemens Enterprise Communications 2009. All rights reserved.

## Agenda

**SIEMENS**

Issues  
A Security Approach

Session Border Controllers

802.1x



Copyright © 2008. All rights reserved.  
Siemens Enterprise Communications

SIEMENS

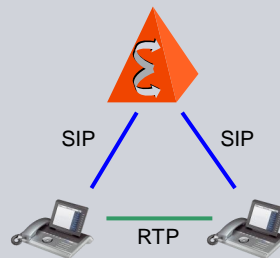
# Issues

## A Security Approach

SIEMENS

### The Issues

- Complex standards hamper seamless interoperability
  - 128 RFCs mentioning “SIP” in their title...
  - The SIP RFC itself: 269 pp.
- Triangular protocols and traffic flows
  - Not typical in traditional networking
  - Both tightly linked together
- Currently intra-company VoIP, but soon anywhere-to-anywhere
  - No inbound or outbound, no inside or outside
- Security issues are beyond the ports, within the protocols



## Principles of VoIP Security

Following the National Institute of Standards and Technology (NIST) security guidelines

- **Perimeter hardening**, like physical measures, is just a first step
- Security must be **layered**, which provides in-depth defense
- Each network element must have **integrated security capability** and not rely solely on the perimeter defenses
- **Multiple security technologies** must be deployed, both internally and externally
- No network link or component is **trustable**

## Our Approach to VoIP Security

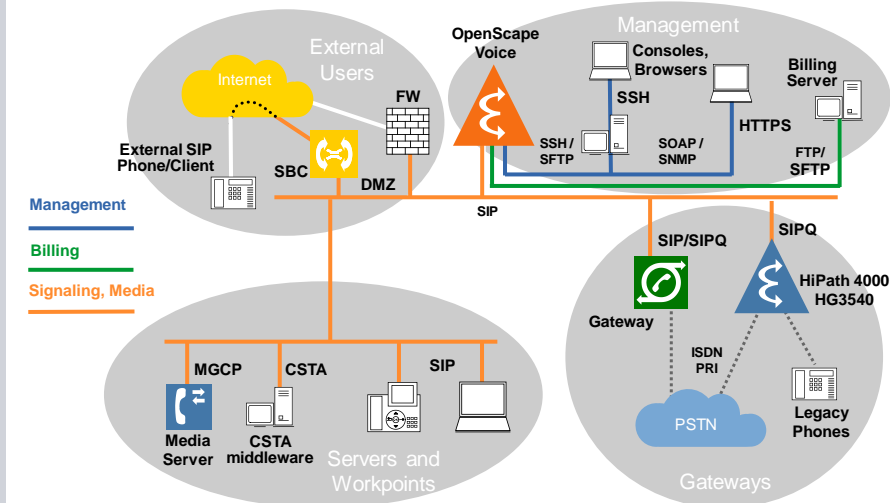
### Layered

- OpenScape Voice Server (iptables, logging, admin roles...)
- Network Design (VLANs, 802.1x...)
- Additional and Specific Solutions (SBC, SIP inspection...)

### Open

- Fully Standards based Solution  
(strictly RFC compliant for best interoperability)
- The Solution must not Dictate a Specific Security Approach  
(we can recommend, our solution makes it all possible, but customer must choose the level of security that fits them well)

## Traffic Separation (VLANs) and Filtering



## DNS, DHCP, NTP, FTP, RADIUS and LDAP are critical

### The often forgotten core network services !

- Doubling of IP addresses
  - Doubling of all demands on DNS, DHCP and in part NTP, RADIUS
  - Possible reorganization or renumbering of IP addresses and host names
- Consider resilient DNS, DHCP, ... services
- Consider better IP Address Management and possible impact on Windows Active Directory

## Signaling and Media Security – How ?

**Signaling security** – with TLS

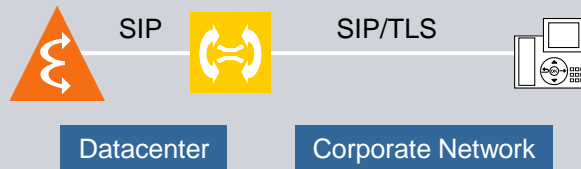
**Media security** – with SRTP

- Confidentiality, authentication and integrity are added to TLS and RTP

→ **Is it needed?**

Obvious benefits of security vs cost, performance, complexity...

→ **Session Border Controllers**



## Session Border Controllers

## Firewalls and SIP (*just as an example*)

- “I guess, we also had some issues w/ Check Point due to misconfiguration. The firewall has blocked calls with more than n-digit party numbers and also rejected second call legs (e.g. pickup groups, call forwarding,...)”
- “[...] is using the Check Point as well and we know that there can be issues due to wrong configurations on it. We had the experiences that OK messages were killed by the Check Point when we made a load test with the OScV. During the load test we have registered up to phones per second and have initiated a SIP call immediately.”
- “The firewalls are managed by the customer so we don't even know if there are wrong settings in their configuration or if it is related to software bugs or hardware problems. We just like to know if there are other customers using this combination or if they are really the only one.”
- “We tested this during an evaluation by a customer. If some phones and OScV is in one segment of the Check Point and the other phones are on an other segment, you need to configure Check Point as described in the attachment.”

→ Why the interoperability doesn't always work...

## Limitations of traditional Firewalls The issues

Most **Firewalls** are device or end-point agnostic:

- Anyone can communicate with the DMZ servers
- Typically protect **trusted** side from the **un-trusted**
- SIP/UDP doesn't really have a “connection” other than a session/dialog, which is the SIP layer
- They can not look back into the protocol or device history

## Limitations of traditional Firewalls

### Typical problems

SIEMENS

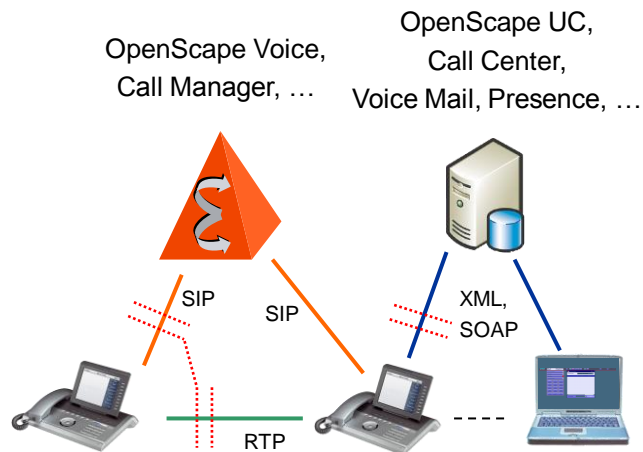
Some firewalls claim some SIP-awareness but they...

- cannot understand SIP-specific attacks
- cannot open/close RTP media ports based on SIP signaling ('RTP pin-holing')
- cannot always handle NAT, and do not understand redirection, call forwarding, voice-mail flows, conferences
- cannot handle TLS and SRTP encrypted call flows

... or sometimes they do, partially...

## Voice and UC Traffic Flows

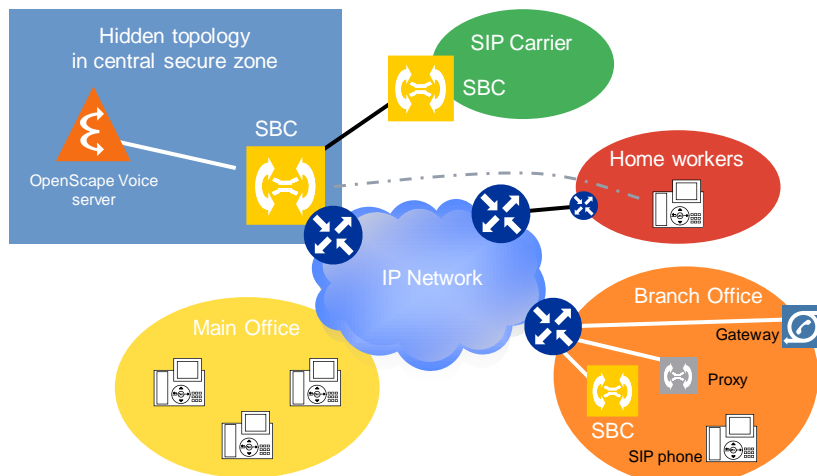
SIEMENS



Session Border Controllers (SBC)

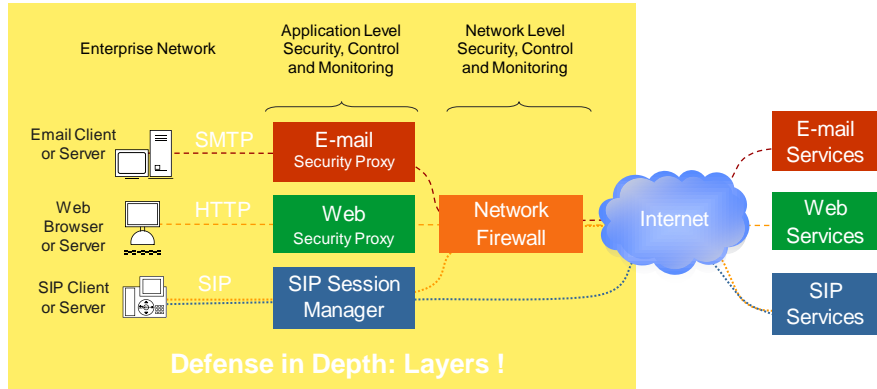
Session	Controller
<ul style="list-style-type: none"> <li>Real-time, interactive communications using SIP, H.323, MGCP, H.248</li> </ul>	<ul style="list-style-type: none"> <li>Security - authentication, authorization, admission, attack protection, signaling and media encryption</li> <li>Service reach maximization - overload protection, interworking, protocol fixing, media stream transcoding</li> <li>SLA assurance – QoS Metrics</li> <li>Revenue &amp; cost optimization</li> <li>Regulatory compliance - lawful intercept</li> </ul>
Border	
<ul style="list-style-type: none"> <li>Service provider - customer /subscriber: peering</li> <li>Data Center edge</li> <li>Subscriber access: enterprise, residential or mobile services</li> <li>Site-to-site access</li> </ul>	

Centralized SBC as an additional layer of protection



The (not so) new Approach to Filtering

Most enterprises already use some defense-in-depth model using application-level security proxies for email and web traffic. Why not for SIP as well ?



Other Products and Solutions



- SBC Market leader
- Carrier and large enterprise
- Purchased Coverage



Unified Border Element

- IOS SBC add-on
- Supported on many Cisco platforms



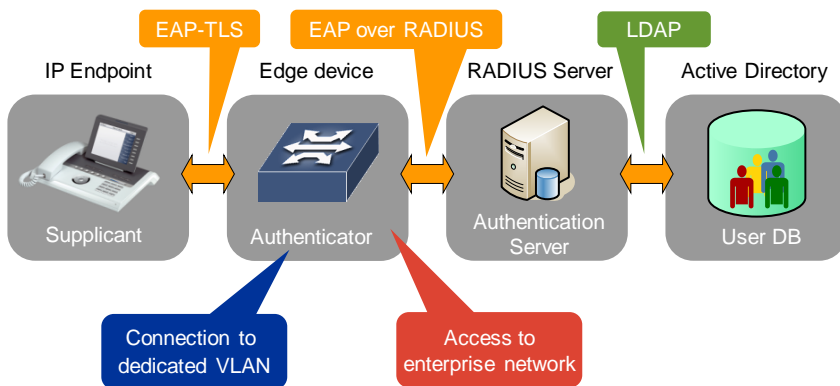
- Very advanced for SIP inspection and header manipulation



- Focuses on UC traffic
- Advanced flow filtering (IM, Facebook, Skype...)

# 802.1x and Port Based Authentication

## 802.1x – Infrastructure and Overview



## 802.1x Port Based Security

- 802.1x is an IEEE security Standard to protect the network edge ('similar' to NAC/NAP)
- Each entity/device should be authenticated by a **central authentication server** (typically: RADIUS)...
- ...**before** it gains access to the network altogether
- Based on Layer 2 mechanism and can use digital certificates, User-Password combination, One-Time-Passwords or MAC-Addresses

## 802.1x – Method of Operation

- The authentication mechanism based on certificates and **EAP-TLS**
- This device specific certificate is checked against the one in the user database (RADIUS)
- Access to the voice VLAN is granted only to authenticated end devices based on VLAN tagging
- Risk mitigation of not authorized entities
- Also to consider: double authentication of PC and phone...

SIEMENS

## Authenticating both the Phone and the PC

- We want both the phone and the PC on the same port...
  - and we want them both on separate VLANs...
  - and they should both be authenticated
- **MDA, Multi Domain Authentication**  
or **MVAP, Multi VLAN Access Port** capable switches
- **Cisco MAB, MAC Authentication Bypass w. Cisco AV-pairs**



Page 23

August 2009

Copyright © 2008. All rights reserved.  
Siemens Enterprise Communications

SIEMENS

Questions? Remarks?

# Thank you!

