Fortinet Overview
Fortinet VoIP Security

Rainer Baeder

08-10-2010

November 3, 2010

Fortinet Overview

Market-Leading Provider of End-to-End IT Security Solutions

Company Stats

- Founded in 2000
- Silicon Valley-based, strong global presence with 32+ offices worldwide
- $212M+ in revenues (2008)
- Seasoned and proven executive management team
- 1,250+ employees / 750+ engineers
- 550,000+ FortiGate devices shipped worldwide

Innovative, Best-in-Class Technologies and Products

- Six ICSA certifications (Firewall, AV, IPS, IPSec VPN, SSL VPN, Anti-Spam)
- Strong IP portfolio – 20+ patents; 80+ pending
- Government Certifications (FIPS-2, Common Criteria EAL4+, NIST)
- Consistent Antivirus Validation *– (Virus Bulletin 100 approved; 2005, 2006, 2007, 2008)*

Still not relevant to you ??

Gartner

Publication Date: 13 January 2004

Cyberwarfare: VoIP and Convergence Increase Vulnerability
David L. Fraley

By 2005, the United States and other nations will have the ability to conduct cyberwarfare. The increasing use of Voice over IP and the converging of voice/data networks is facilitating it.

The aspects of cyberwarfare have been considered for years. Future cyberattacks could constitute an entire war or an attack type as part of a larger campaign. Cyberwarfare, like any military operation, has two components — offensive and defensive operations.

The U.S. military complex continues work on Presidential Directive 16, including developing the rules and tools. The United States is not the only government thinking about cyberattacks. In the second quarter of 1995, Major General Wang Pufeng of The Chinese Army published a paper, "The Challenge of Information Warfare." In this paper, Pufeng writes that the information era will touch off a revolution in military affairs.

Phony Phone Calls Distract Consumers from Genuine Theft

TDoS - *FBI and Partners Warn Public*

- NEWARK, NJ—Have you recently received a large number of strange and unexplained calls on your mobile or landline telephones? The FBI is warning consumers about a new scheme that uses telecommunications denial-of-service attacks as a diversion to what is really happening: the looting of bank and online trading accounts.
- **The Scheme**
  - The scheme is known as telephony denial-of–service (TDOS) and according to several telecommunications companies working with the FBI, there has been a recent surge of these attacks in the past few weeks. The perpetrators are **suspected of using automated dialing programs and multiple accounts to overwhelm the land and cell phone lines of their victims with thousands of calls. When the calls are answered, the victim may hear anything from dead air (nothing on the other end), an innocuous recorded message, an advertisement, or even a telephone sex menu.** The calls are typically short in duration but so numerous that victims have had to have their numbers changed to make the calls stop…….

http://newark.fbi.gov/pressrel/pressrel10/nk051110.htm

Cloud Attacking

- Amazon EC2 - Amazon Elastic Compute Cloud
  - Complaints of **rampant SIP Brute Force Attacks coming from servers with Amazon EC2 IP Addresses** cause many admins to simply drop all Amazon EC2 traffic. Generally, SIP brute force attacks attempt to register various peer names to a system and/or attempt to guess passwords of known/guesses peers or endpoints.
  - The complaints mentioned this weekend show an excessive amount of traffic; with **some providers claiming 6GB of traffic dedicated to such attacks**. Since we ourselves received an attack from an Amazon hosted server, we also reported and complained to the Amazon NOC/Abuse depts

The SIP messages

```
REGISTER sip:[...] SIP/2.0
Via: SIP/2.0/UDP 10.242.91.15:5182; branch=z9hG4bK-2528031440;rport
Content-Length: 0
From: "2011" <sip:2011@[...]>
Accept: application/sdp
User-Agent: friendly-scanner
To: "2011" <sip:2011@[...]>
Contact: sip:123@1.1.1.1
CSeq: 1 REGISTER
Call-ID: 3361196543
Max-Forwards: 70

["AF_INET", 5182, "ec2-174-129-137-135.compute-1.amazonaws.com", "174.129.137.135"]
```

```
REGISTER sip:[...] SIP/2.0
Via: SIP/2.0/UDP 10.242.91.15:5209;branch=z9hG4bK-[illegible]78605574;rport
Content-Length: 0
From: "2011" <sip:2011@[...]>
Accept: application/sdp
User-Agent: friendly-scanner
To: "2011" <sip:2011@[...]>
Contact: sip:123@1.1.1.1
CSeq: 1 REGISTER
Call-ID: 1992838843
Max-Forwards: 70

["AF_INET", 5209, "ec2-174-129-137-135.compute-1.amazonaws.com", "174.129.137.135"]
```

IPS – Intrusion Prevent and Detection

- Fortinet's IPS is SIP aware
  - SIP decode is available
- Allows attack prevention and detection with a signature database.
- Signature updates available from Fortinet's FortiGuard service with a very short response time.
- Customer signatures allow service personell to write their own prevention or detection rules
  - Could be used for the quickest reaction to a sudden security threat
- SIP aware IPS customer signature example from a customer:
  - *F-SBID(--name "SIP.Proxy.Require.Header.Buffer.Overflow"; --protocol udp; --service SIP; --flow from_client; --pattern "OPTIONS|20|sip|3a|"; --no_case; --context uri; --within 12,context; --pattern "Proxy-Require|3a 20|"; --no_case; --distance 8; --within 500; --context header; --pattern !"|0a|"; --within_abs 500;)*
  - *This signature blocks OPTION messages with a "Proxy-Require" field.*

VoIP Blacklist Project

- 2010-09-20 10:08:06 NOTICE[14155] chan_sip.c: Registration from '"3147172873"<sip:3147172873@208.51.xxx.xxx>' failed for '206.71.179.32' - Username/auth name mismatch
- 2010-09-20 10:08:06 NOTICE[14155] chan_sip.c: Registration from '"thomas"<sip:thomas@208.51.xxx.xxx>' failed for '206.71.179.32' - Username/auth name mismatch
- 2010-09-20 10:08:06 NOTICE[14155] chan_sip.c: Registration from '"arsenal"<sip:arsenal@208.51.xxx.xxx>' failed for '206.71.179.32' - Username/auth name mismatch
- 2010-09-20 10:08:06 NOTICE[14155] chan_sip.c: Registration from '"monkey"<sip:monkey@208.51.xxx.xxx>' failed for '206.71.179.32' - Username/auth name mismatch
- 2010-09-20 10:08:06 NOTICE[14155] chan_sip.c: Registration from '"charlie"<sip:charlie@208.51.xxx.xxx>' failed for '206.71.179.32' - Username/auth name mismatch
- .....

- **and a couple 100 thousand more like this**

News on www.heise.de

23.09.2008 11:16 « Vorige | Nächste »

Erste größere Attacke gegen deutsche VoIP-Nutzer

vorlesen

Erstmals waren deutsche Voice-over-IP-Nutzer (VoIP) von einer Attacke betroffen. Zwischen dem 4. und 10. September gingen bei den Betroffenen zu nachtschlafender Zeit Anrufe von der Rufnummer 5199362832664 ein, teilweise im Stundentakt. Einige Betroffene wandten sich daraufhin an die örtliche Polizei oder stellte gar Strafanzeige. Eine Nachfrage von heise online bei VoIP-Providern ergab, dass die Anrufe in deren Netzen erst einmal nicht registriert worden waren. Der Angriff war offenbar direkt auf die VoIP-Hardware der Kunden gelenkt worden, um vermutlich einen kostenpflichtigen Rückruf der Opfer zu provozieren. Bei fehlerhaften Konfigurationen von Asterisk-Anlagen soll es allerdings zu automatischen Rückrufen gekommen sein.

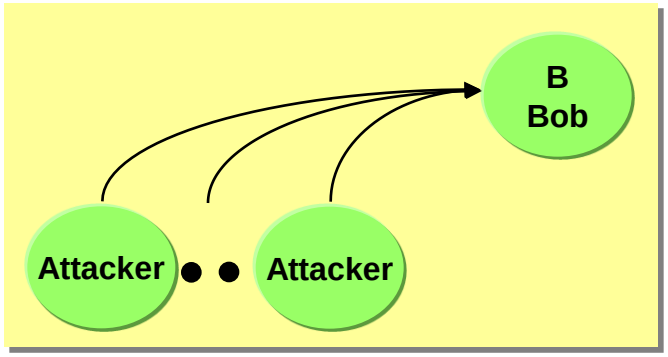
Die Belästigung von Kunden durch die Rufnummer ist bekannt, kann aber durch Freenet nicht behoben werden", antwortete der Provider hilfesuchenden Kunden. Der Anzahl der Postings von Freenet-Kunden nach zu schließen, waren diese besonders betroffen. Der Support des Hamburger Providers riet, sich an die Bundesnetzagentur zu wenden, um eine Sperrung der besagten Rufnummer zu erwirken. Die Sperrung im Router oder beim Kundencenter habe dagegen keine Auswirkung. Sperrungen in den Routern der Kunden selbst erbrachten offenbar aber unterschiedliche Ergebnisse, manche hatten anschließend Ruhe. Freenet versuchte, die Kunden in einer Hinsicht zu beruhigen: Das Unternehmen gehe davon aus, dass die Anrufe bislang keinerlei Kosten verursacht hätten.

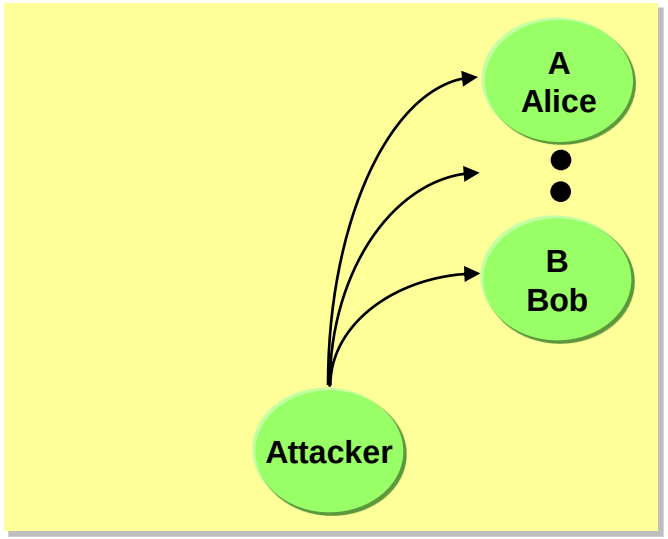
Der VoIP-Provider Sipgate widersprach der Darstellung, dass es sich bei dem Angriff um eine SPIT-Attacke gehandelt habe, denn die Netze der VoIP-Provider seien "nicht involviert" gewesen. "Betroffen war oder sind vor allem alte VoIP-Geräte", erläuterte ein Sipgate-Sprecher. Der angebliche "Anrufer" habe ein Programm genutzt, das INVITE-Pakete generiert und wahllos an verschiedene IP-Ranges sendet. Die Pakete gingen direkt über den Breitbandanschluss zur VoIP-Hardware der Kunden und umgingen dabei auch etwaige Schutzmechanismen der Providernetze. Neuere VoIP-Hardware erlaube aber auch den Schutz der lokalen Anschlüsse, versicherte der Sipgate-Sprecher. Der VoIP-Anbieter QSC versicherte, es habe keine Beschwerden von Kunden gegeben, da der VoIP-Verkehr über die eigenen Server laufen müsse und gefiltert werde.

Dass Spam via Internet-Telefonie (SPIT) zu einen Problem in VoIP-Netzen werden kann, ist seit Längerem bekannt. Allerdings gab es bislang noch nicht allzu viele Angriffe. Die NEC Laboratories, die sich seit mehreren Jahren mit derartigen Angriffen und deren Abwehr (PDF-Dokument) beschäftigen, haben nach eigenen Angaben in den vergangenen Jahren weltweit 108 Angriffe auf VoIP-Systeme registriert. Der September-Angriff sei nach den Analysen der Forscher aber der erste rein VoIP-bezogene Angriff in Deutschland.

http://www.heise.de/newsticker/Erste-groessere-Attacke-gegen-deutsche-VoIP-Nutzer--/meldung/116335

SPIT (SPAM over Internet Telephony)





- **Penetration with Ads or other UC (Unsolicited Communication)**
- **SPAM is well known to everybody using email**
- **Up to 80% of all emails are SPAM**
  - **Depending on how long you use the mail account already**
- **Why should it be different with VoIP**
- **Today mainly unknown ...**
- **With the SPAM knowledge of the FortiMail Fortinet is best positioned to extend the VoIP Security with upcoming major threats of SPIT**

Hacking VoIP for Scrippy Kids

Example of detailled hacking is described

Enumerating SIP Devices on a Network

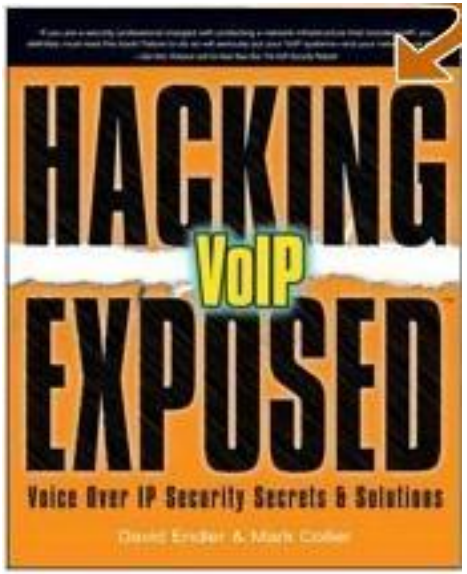
Here's how to enumerate SIP devices on a network, step by step:

1. Download Nmap from *http://insecure.org/nmap/*.
2. Enter nmap on the command line (Windows) or shell (Unix) to retrieve the syntax of the tool.
3. Enter the following nmap command on the command line/shell to enumerate SIP User Agents and other intermediate devices.
   nmap.exe -sU -p 5060 IP Address Range
4. Or, for a class B network address range on a 172.16.0.0 network, enter:
   nmap.exe -sU -p 5060 172.16.0.0/16
5. Each IP address that shows open for the STATE (as shown in Figure 2-2) is probably a SIP device. As you can see in Figure 2-2, the addresses 172.16.1.109 and 172.16.1.244 are probably SIP devices.

etc

C:\Documents and Settings\rbaider\My Documents\Books\Aufräumen\Hac_VoIP.chm

Hacking VoIP for Scrippy Kids



Example of detailled hacking is described

Attack – UDP Flooding Attacks

Popularity:	8
Simplicity:	9
Impact:	8
Risk Rating:	8

Protocol (UDP) flooding is a preferred type of bandwidth flooding attack because UDP source addresses can be easily spoofed by the attacker. Spoofing often allows an attacker the ability to manipulate trust relationships within an organization to bypass firewalls and other filter devices (for example, by crafting a DoS stream to appear as a DNS response over UDP port 53).

Almost all SIP-capable devices support UDP, which makes it an effective choice of attack transport. Many VoIP devices and operating systems can be crippled if a raw UDP packet flood is aimed at the listening SIP port (5060) or even at random ports.

Companion Web Site Check out our website at http://www.hackingvoip.com for our udpflood tool. There are a variety of other UDP flooding tools freely available for download from the following sites to test the susceptibility of your applications and network:
http://www.foundstone.com/resources/freetooldownload.htm?file=udpfl ood.zip
http://packetstormsecurity.org/exploits/DoS/

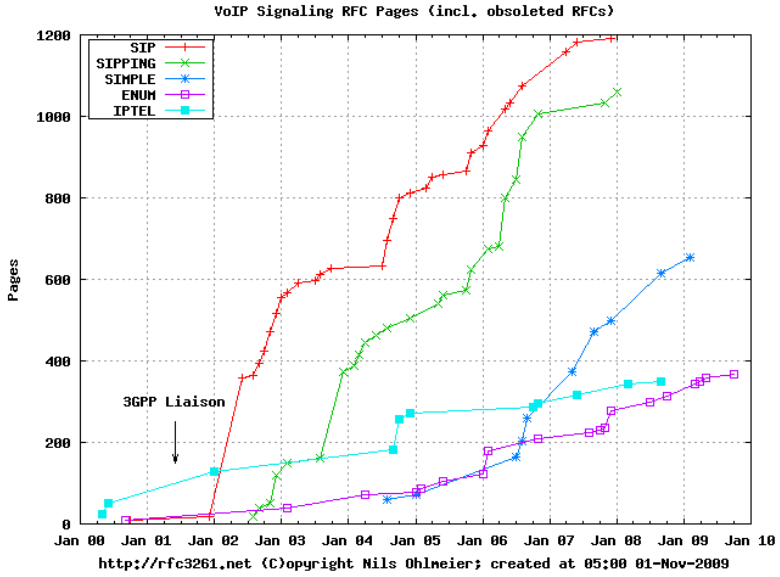
C:\Documents and Settings\rbaider\My Documents\Books\Aufräumen\McGraw.Hill.Hacking.Exposed.VoIP.Voice.Over.IP.Security.Secrets.&.Solutions.chm

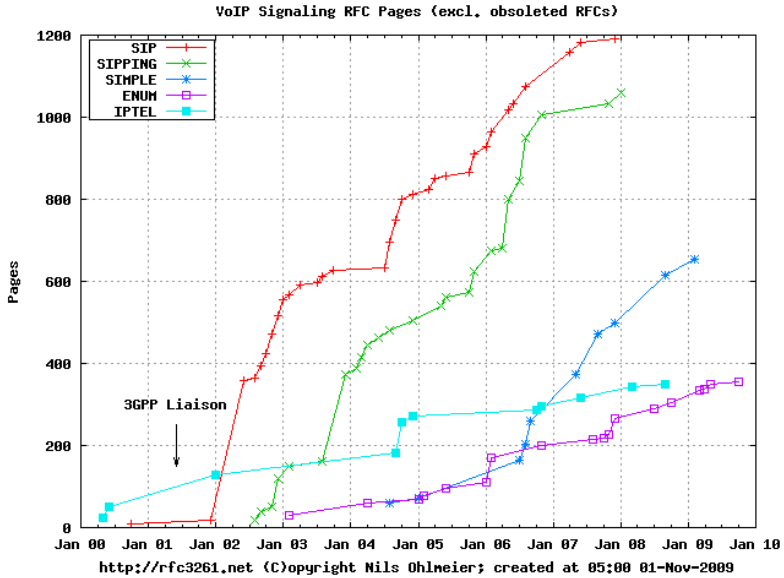
Malware on Mobile Phones

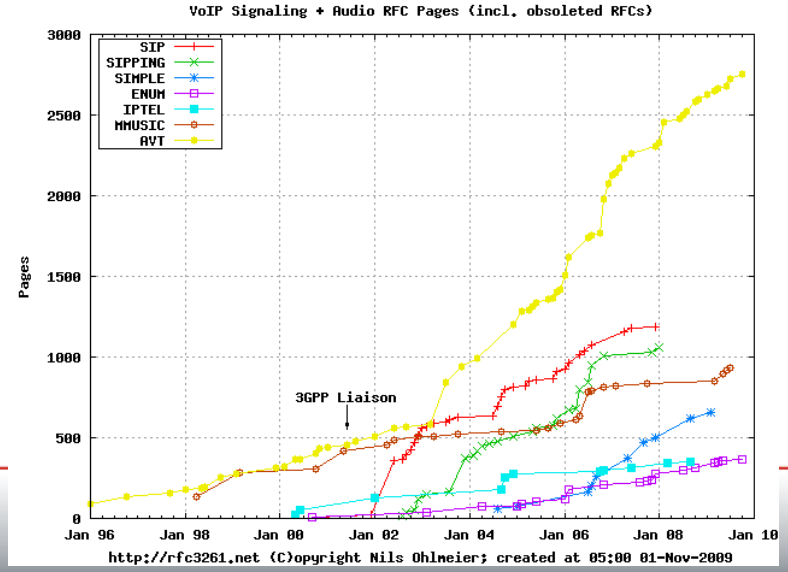
- How does Malware get on Mobile Phones ??

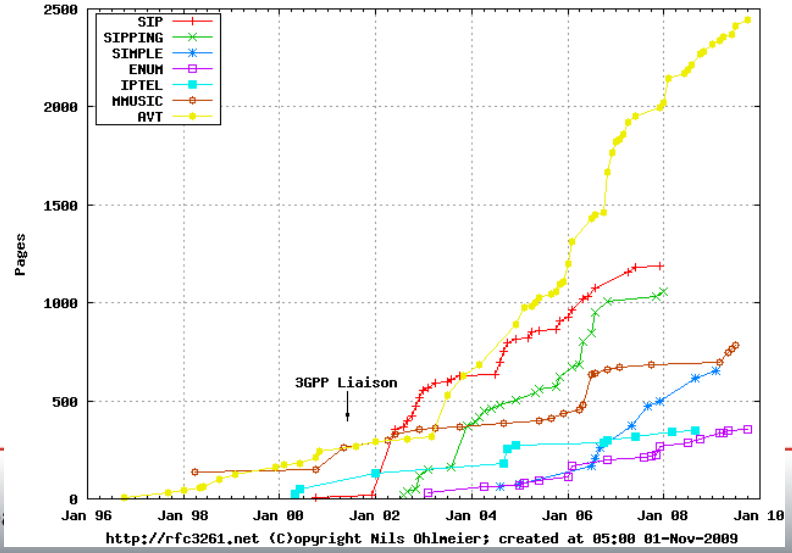
RFC 3261 - the VoIP RFC Watch

The following graphs illustrate the enormus growing rate of RFCs which are related to SIP or VoIP in general. www.rfc3261.net
They are regularly (once a week) updated automatically.
Thanks to Dr. Christian Stredicke who wrote the very first version of the scripts

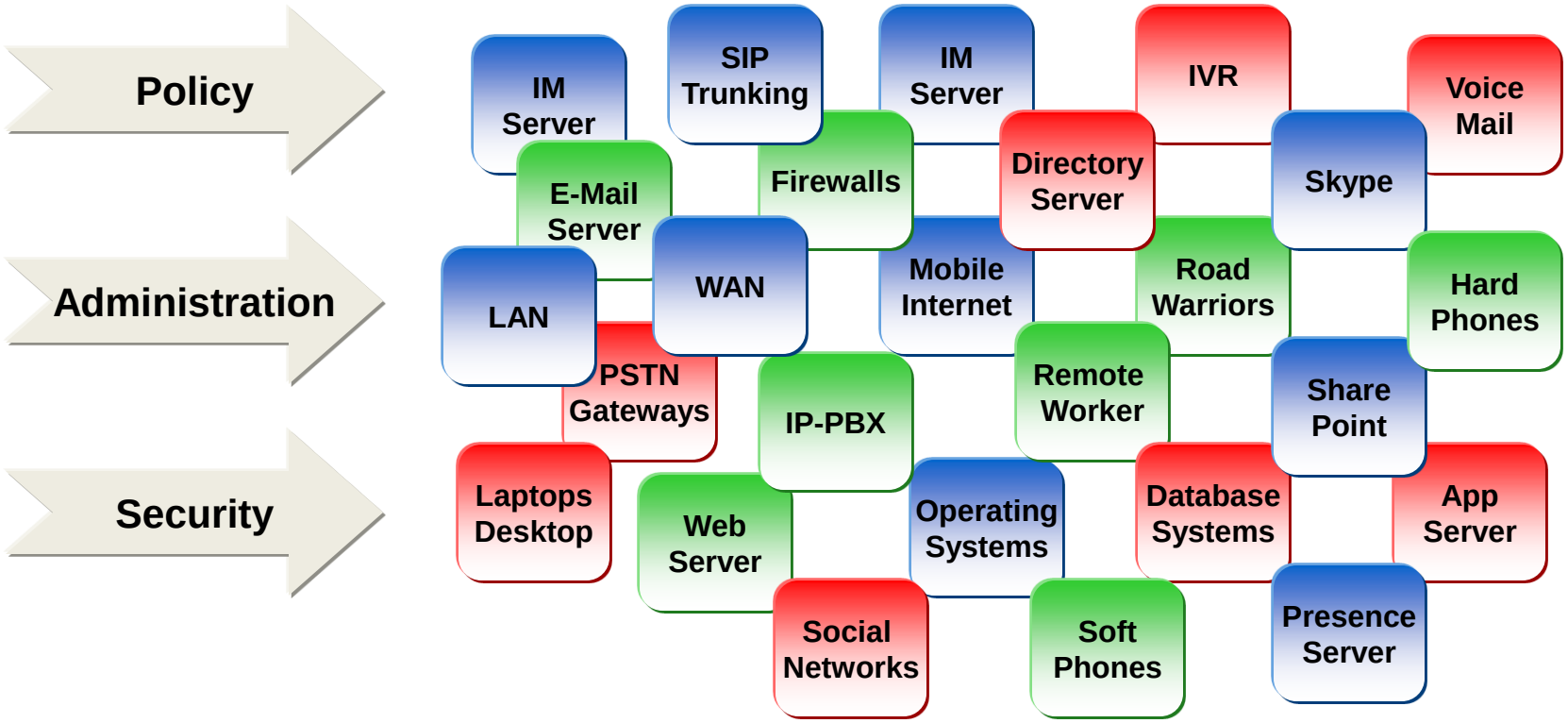








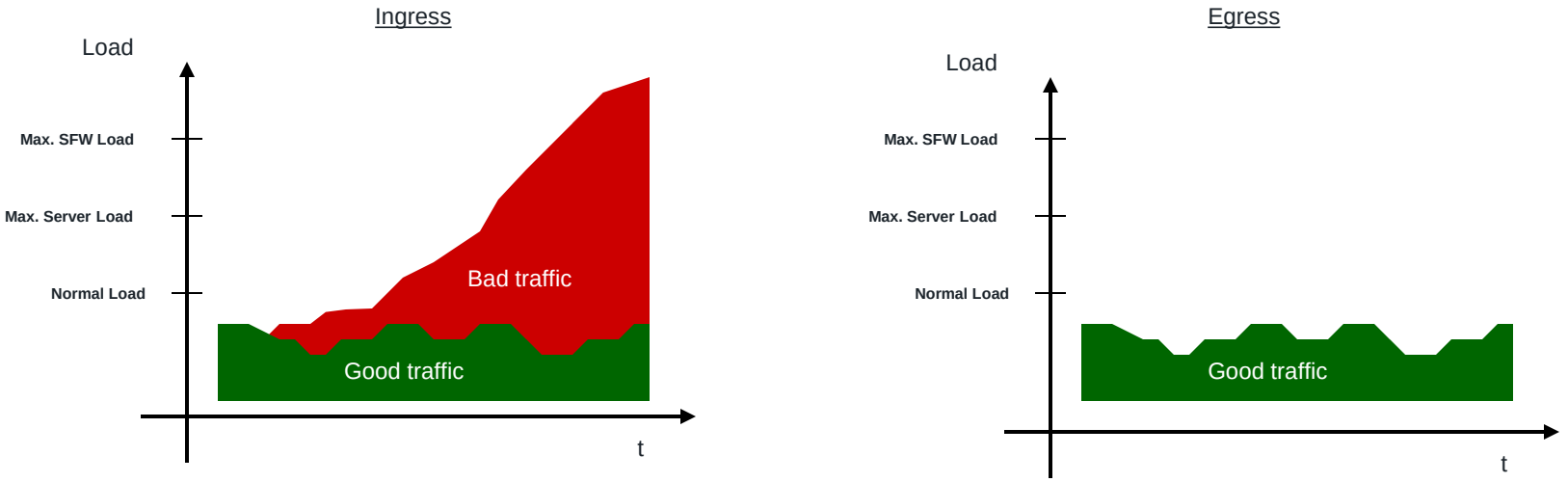
VoIP & UC Technology and its Complexity



VoIP Protection Features Summary

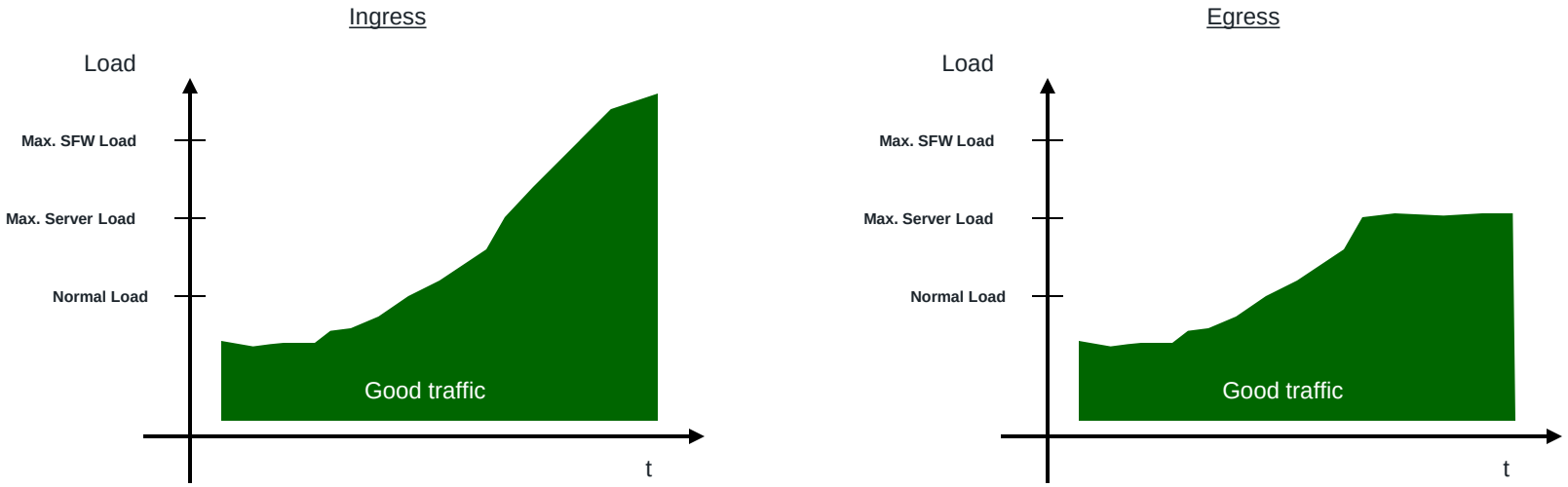
- **Stateful SIP tracking**
  - The SIP SFW tracks the SIP session over it's lifespan. A SIP-Session (or SIP dialog) normally is established after the SIP INVITE procedure. The SIP SFW then tracks this call as a „SIP session". A Session can for instance end by regular BYE procedure (users hang-off the phone) or by another unexpected Signaling or Transport event.
- **SIP per request method message rate limitation**
  - Configurable threshold for SIP message rates per request method. Protects SIP servers from SIP overload and DoS attacks.
- **SIP High Availability (HA)**
  - Allows to configure HA configuration (active-standby) for SIP. Supports failover of SIP sessions in case of an active firewall instance fails.
- **SIP NAT**
  - Various NAT policies can be defined for SIP signal sessions and RTP sessions that are negotiated through the SIP signal session.
- **RTP Pinholing**
  - The SIP SFW opens the respective RTP Ports as long as the SIP session is alive and conforming with the operator security policies.
- **RTP Bypass**
  - Supports configurations with and without RTP pin-holing. May inspect and protect SIP signaling only.
- **SIP NAT with IP address conservation**
  - Performs SIP and RTP aware IP Network Address translation. Preserves the lost IP address information in the SIP/SDP info header for later processing/debugging in the SIP server.
- **SIP Transparent or NAT mode**
  - The SFW supports a transparent mode, where SIP messages are inspected but not modified. Just in case of an attack or overload the SFW becomes visible. The other mode is SIP NAT. In this mode, the SIP header is modified with regard to translation of IP addresses.
- **Support for Geographical Redundancy**
  - Maintains a active-standby SIP server configuration, which even supports geographical distribution. If the active SIP server fails (missing SIP heartbeat messages or SIP traffic) FortiOS will redirect the SIP traffic to a secondary SIP server.
- **SIP command control**
  - The SIP SFW can block SIP methods. SIP methods that can be blocked are: ack, bye, cancel, info, invite, notify, options, publish, refer, register, subscribe, update and „unknown commands".
- **SIP communication logging**
  - The SIP SFW supports logging to a FortiAnalyzer. The Logfiles will show up in the „Content Archive" section under the VoIP Tab.
- **Hardware accelerated RTP processing**
  - In cases where RTP is pin-holed by a FortiOS Carrier™ device, it needs to be understood that RTP packets can be very small (around 100bytes or less), sensitive to processing latency, packet loss or jitter (packet delay variation). FortiGate devices can offload RTP packet processing to HW assistance (FortiASIC). This will greatly enhance the overall throughput and will give the firewall device a multiple GE wirespeed (1 Gbps) VoIP security solution.
- **Media Inactivity**
  - In some case SIP signaling is established, but the voice bearer (RTP) is broken. The SIP SFW supports optionally the detection of Media Inactivity that cleans the SIP call context in the SFW once there's no RTP anymore for a specific time.
- **SIP over IPv6**
  - Supports Signaling Firewall for SIP messages using IPv6 transport. Limited to SIP over IPv6 in SIP transparent mode (no SIP/RTP NAT of IPv6 to IPv4)
- **IP Topology Hiding**
  - IP topology of a network can be hidden through NAT and NAPT manipulation of IP and SIP level addressing.
- **Deep SIP header inspection**
  - Deep SIP header syntax inspection. Prevents from many SIP Fuzzing attacks with malformed SIP message headers. User configurable bypass and response message options. SIP conformance violations can be logged with the FortiAnalyzer.
- **Hosted NAT traversal**
  - Resolves IP address issue in SIP-SDP header due to NAT-PT in far end firewall. Important feature for VoIP access networks.

Expected DoS Protection



- **Expected counter action**
- **Detect malicious packets and discard them**
- **Prevent the SIP server from DoS related traffic**
- **Do not impact the transport of “good messages”**
- **Provide “blacklisting” of malicious IP sources**
- **DoS attack may consist of**
  - **SIP flooding attack (sending 10,000s of messages per second)**
  - **Packet storms**
  - **Flooding with malformed packets.**
  - **Flooding with spoofed identities of random IP addresses**
  - **L3-4 Dos attacks (e.g. TCP Sync attacks, etc)**
  - **Distributed DoS (e.g from botnets)**

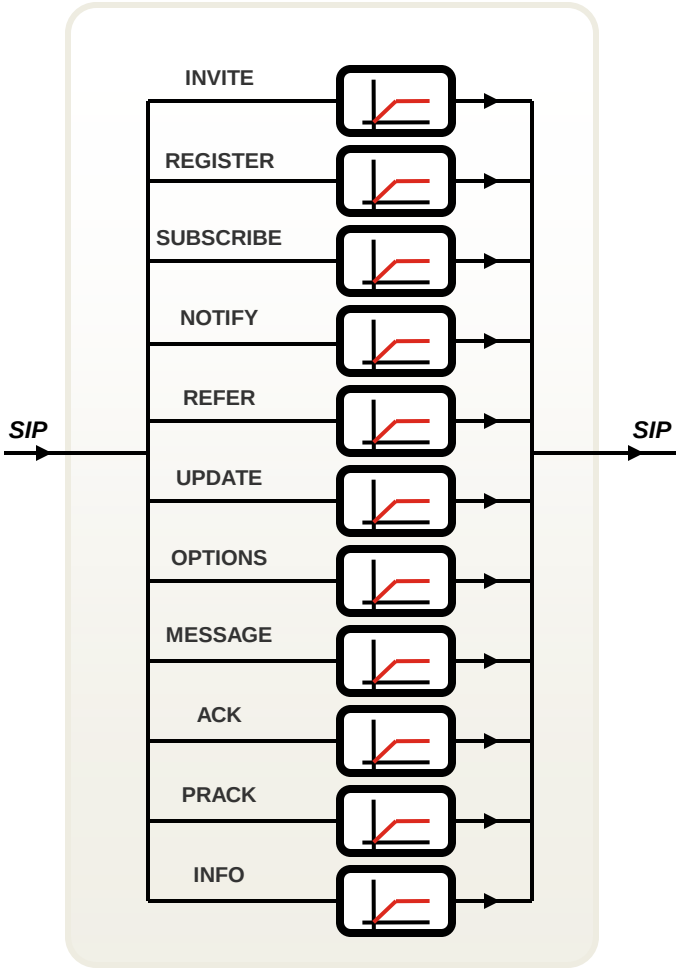
Expected Overload Protection



Overload Protection

- **Throttle SIP messages to specified limits of the corresponding SIP server**
- **Requires discard of good SIP messages**
- **Therefore discard with a drop precedence**
  - **Start with SIP messages of low importance, then higher ones.**
- **Maintain existing SIP dialogs at highest priority**
- **Allow server specific message throttling with a per SIP method rate limitation**

VoIP Security – Per Method Rate Limitation



- SIP message rate limitation
- Individually configurable per SIP method
- When threshold is hit additional messages with this method will be discarded
- Prevents SIP server from getting overloaded by flash crowds or Denial-of-Service attacks.
- May block some methods at all (with extra “block” option)
- Can be disabled (unlimited rate)

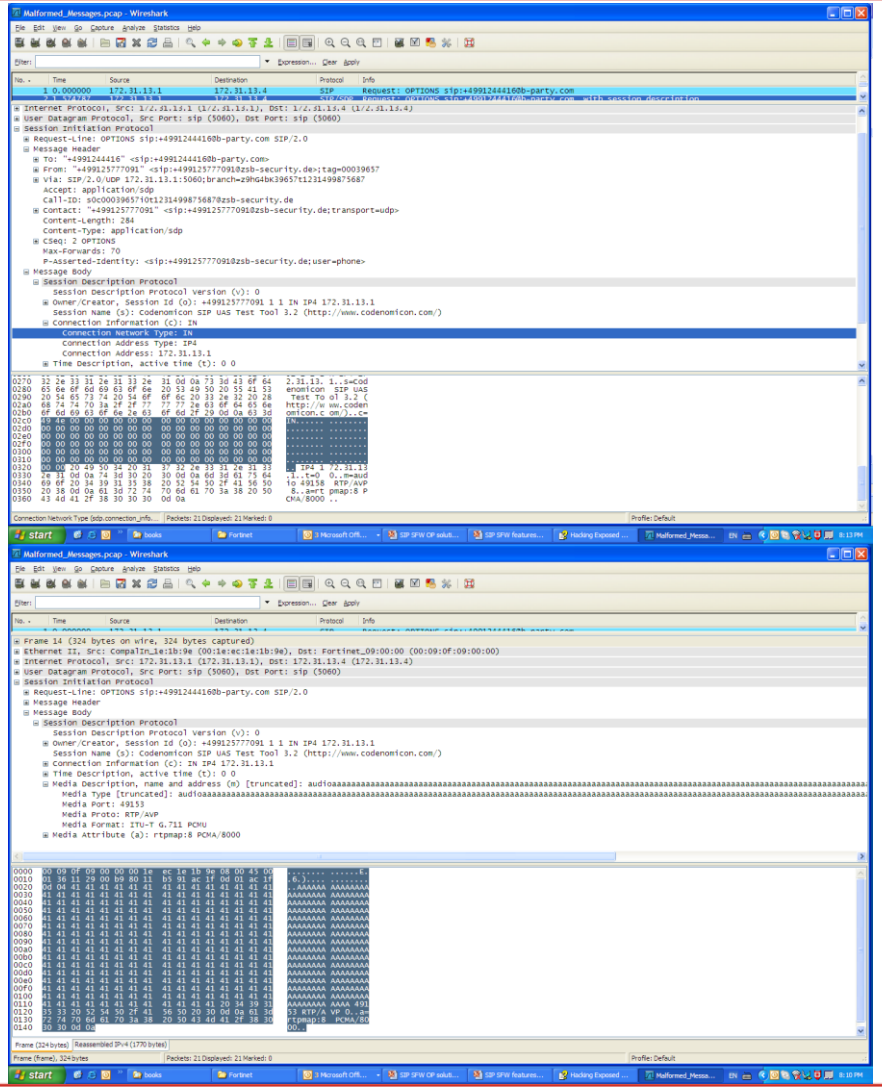
VoIP Fuzzing

SIP Fuzzing attacks

- **Buffer overflows**
- **Format String vulnerability**
- **Integer Overflow**
- **Endless loops and logical errors**
  - **Packet Fragmentation**
  - **Firmware vulnerability**
- **Often, VoIP Fuzzing is combined with DoS**

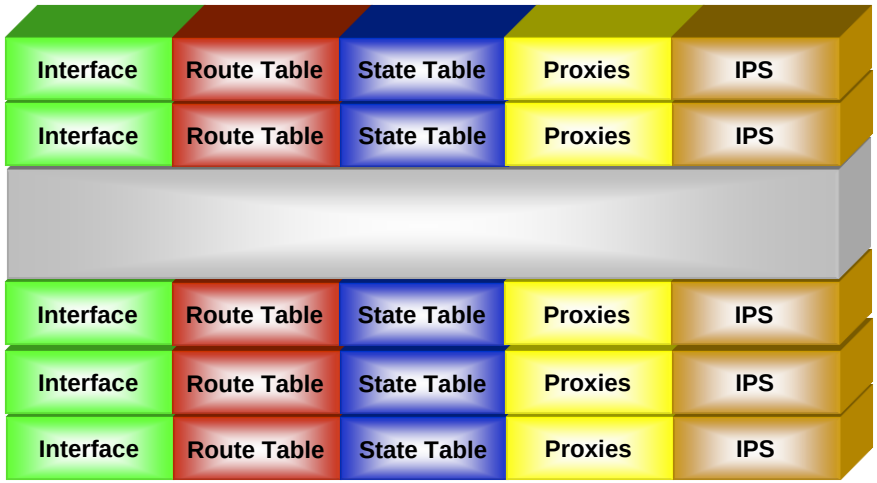
Expected Counter Measurement

- **Detect malicious messages**
- **Discard them or**
- **Replace the dangerous fields**



Virtual Domains

- SIP SFW policies configurable per Virtual Domain (VDOM)
- Allows individual configuration per external VoIP network interface
- Overlapping address space within the same hardware platform
- Multiple Public/Private peers

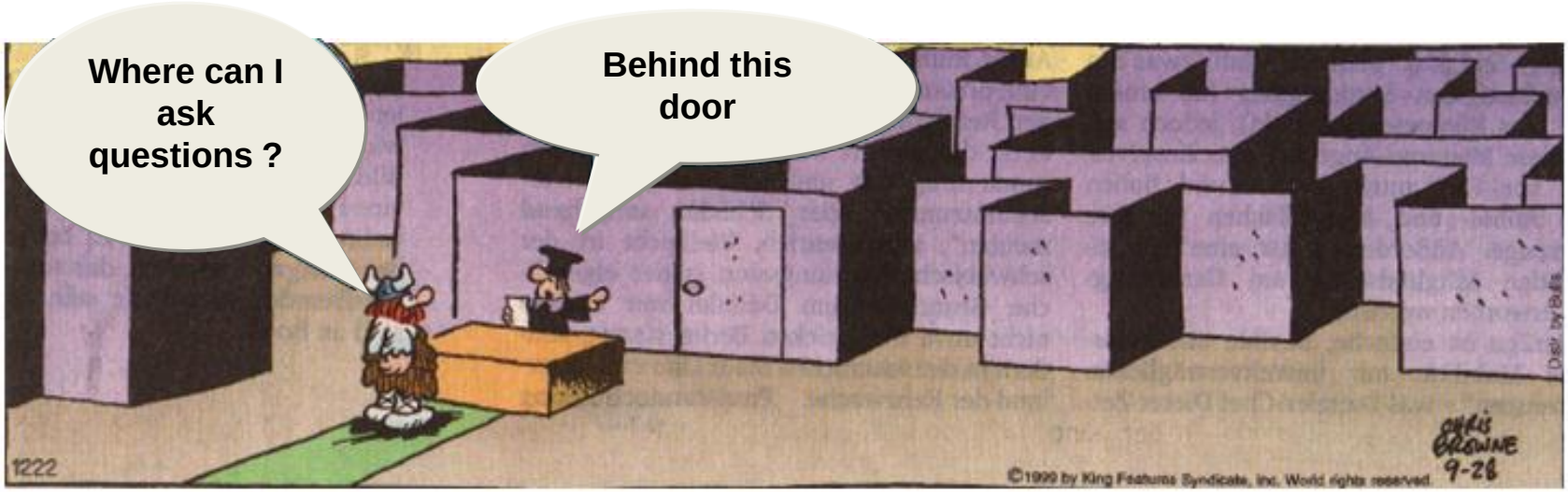


Up to 500 VDOMs supported per physical FortiCarrier device
(250 VDOMs Max when using full UTM)

MANAGED SECURITY

VOICE SECURITY

MOBILE SECURITY


Where can I ask questions ?
Behind this door
1222
©1999 by King Features Syndicate, Inc. World rights reserved.
9-28

Thank You

Backup

VoIP Protection Features FOS 4 MR1

VoIP Features in FortiOS Carrier 4.0 MR1	
Stateful SIP tracking	The SIP SFW tracks the SIP session over it‘s lifespan. A SIP-Session (or SIP dialog) normally is established after the SIP INVITE procedure. The SIP SFW then tracks this call as a „SIP session“. A Session can for instance end by regular BYE procedure (users hang-off the phone) or by another unexpected Signaling or Transport event.
SIP per request method message rate limitation	Configurable threshold for SIP message rates per request method. Protects SIP servers from SIP overload and DoS attacks.
SIP High Availability (HA)	Allows to configure HA configuration (active-standby) for SIP. Supports failover of SIP sessions in case of an active firewall instance fails.
SIP NAT	Various NAT policies can be defined for SIP signal sessions and RTP sessions that are negotiated through the SIP signal session.
RTP Pinholing	The SIP SFW opens the respective RTP Ports as long as the SIP session is alive and conforming with the operator security policies.

VoIP Protection Features FOS 4 MR1

VoIP Features in FortiOS Carrier 4.0 MR1	
RTP Bypass	Supports configurations with and without RTP pin-holing. May inspect and protect SIP signaling only.
SIP NAT with IP address conservation	Performs SIP and RTP aware IP Network Address translation. Preserves the lost IP address information in the SIP/SDP info header for later processing/debugging in the SIP server.
SIP Transparent or NAT mode	The SFW supports a transparent mode, where SIP messages are inspected but not modified. Just in case of an attack or overload the SFW becomes visible. The other mode is SIP NAT. In this mode, the SIP header is modified with regard to translation of IP addresses.
Support for Geographical Redundancy	Maintains a active-standby SIP server configuration, which even supports geographical distribution. If the active SIP server fails (missing SIP heartbeat messages or SIP traffic) FortiOS will redirect the SIP traffic to a secondary SIP server.

VoIP Protection Features FOS 4 MR1

VoIP Features in FortiOS Carrier 4.0 MR1	
SIP command control	The SIP SFW can block SIP methods. SIP methods that can be blocked are: ack, bye, cancel, info, invite, notify, options, publish, refer, register, subscribe, update and „unknown commands“.
SIP communication logging	The SIP SFW supports logging to a FortiAnalyzer. The Logfiles will show up in the „Content Archive“ section under the VoIP Tab.
Hardware accelerated RTP processing	In cases where RTP is pin-holed by a FortiOS Carrier™ device, it needs to be understood that RTP packets can be very small (around 100bytes or less), sensitive to processing latency, packet loss or jitter (packet delay variation). FortiGate devices can offload RTP packet processing to HW assistance (FortiASIC). This will greatly enhance the overall throughput and will give the firewall device a multiple GE wirespeed (1 Gbps) VoIP security solution.

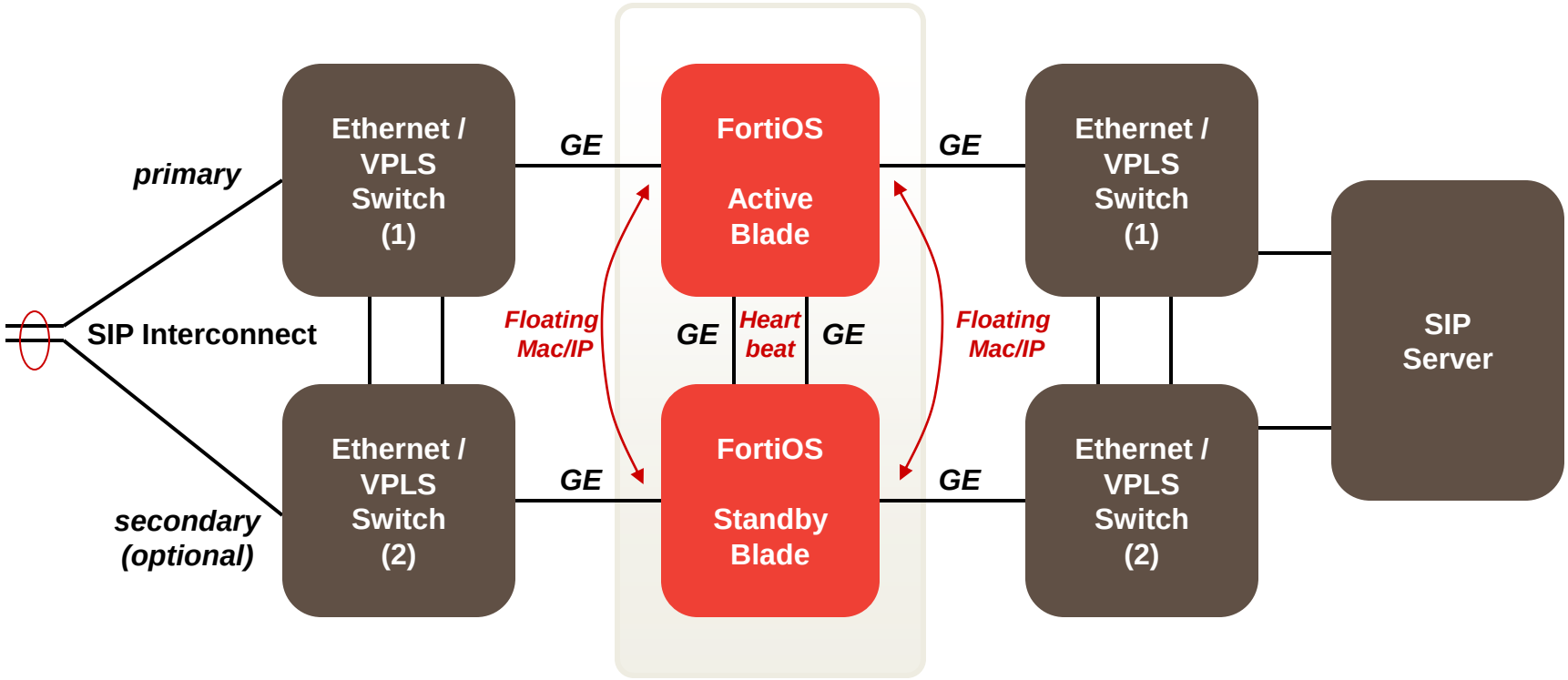
VoIP Protection Features FOS 4 MR1

VoIP Features in FortiOS Carrier 4.0 MR1	
Media Inactivity	In some case SIP signaling is established, but the voice bearer (RTP) is broken. The SIP SFW supports optionally the detection of Media Inactivity that cleans the SIP call context in the SFW once there‘s no RTP anymore for a specific time.
SIP over IPv6	Supports Signaling Firewall for SIP messages using IPv6 transport. Limited to SIP over IPv6 in SIP transparent mode (no SIP/RTP NAT of IPv6 to IPv4).
IP Topology Hiding	IP topology of a network can be hidden through NAT and NAPT manipulation of IP and SIP level addressing.

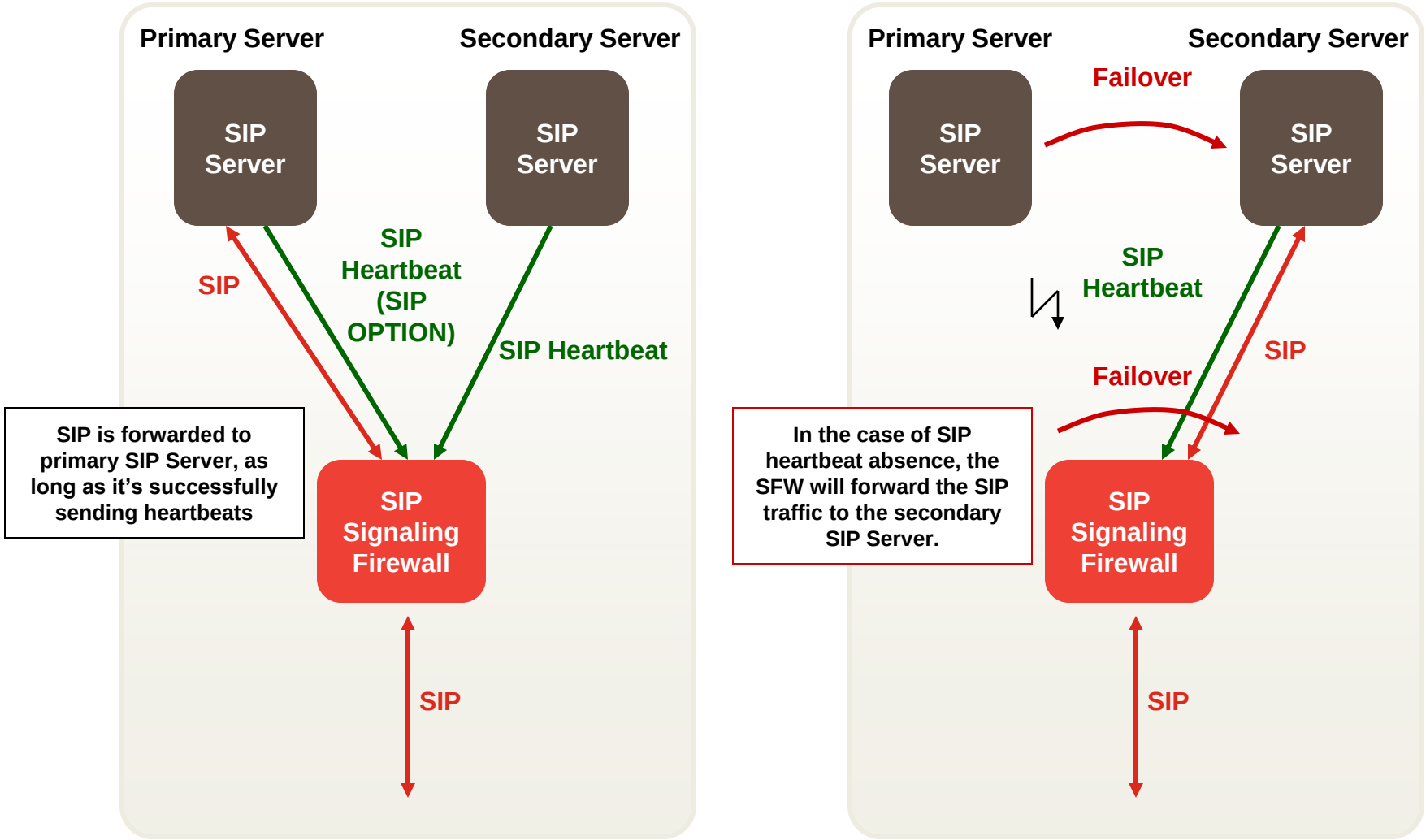
IPS – Intrusion Prevent and Detection

- Fortinet's IPS is SIP aware
  - SIP decode is available
- Allows attack prevention and detection with a signature database.
- Signature updates available from Fortinet's FortiGuard service with a very short response time.
- Customer signatures allow service personell to write their own prevention or detection rules
  - Could be used for the quickest reaction to a sudden security threat
- SIP aware IPS customer signature example from a customer:
  - *F-SBID(--name "SIP.Proxy.Require.Header.Buffer.Overflow"; --protocol udp; --service SIP; --flow from_client; --pattern "OPTIONS|20|sip|3a|"; --no_case; --context uri; --within 12,context; --pattern "Proxy-Require|3a 20|"; --no_case; --distance 8; --within 500; --context header; --pattern !"|0a|"; --within_abs 500;)*
  - *This signature blocks OPTION messages with a "Proxy-Require" field.*

Fortinet VoIP Security – HA Configuration



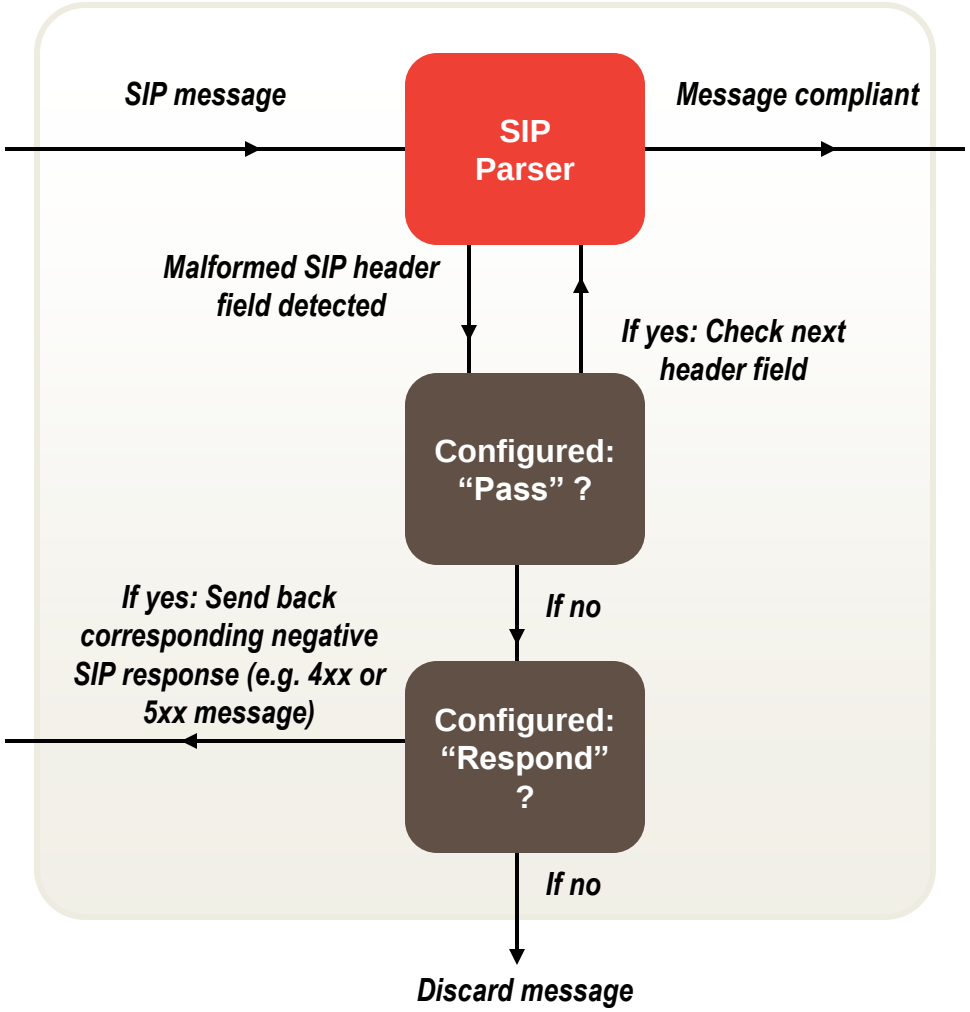
VoIP Security – Geographical Redundancy



VoIP Protection Features FOS 4 MR2

New VoIP Features in FOC and FOS 4.0 MR2	
FOC to FOS SIP feature migration	The enhanced SIP protection feature set of FortiOS Carrier will become available within the standard FortiOS platform. This allows to utilize a larger FortiGate product portfolio and provide more attractive entry models with the low and mid range FortiGate devices.
Deep SIP header inspection	Deep SIP header syntax inspection. Prevents from many SIP Fuzzing attacks with malformed SIP message headers. User configurable bypass and response message options. SIP conformance violations can be logged with the FortiAnalyzer.
Hosted NAT traversal	Resolves IP address issue in SIP-SDP header due to NAT-PT in far end firewall. Important feature for VoIP access networks.

VoIP Security – Deep SIP header Inspection



- Considers the following SIP header fields:
  - Allow, call-id, contact, content-length, content-type, cseq, expires, from, max-forwards, p-asserted-identity, rack, record-route, route, rseq, to, via, request-line
  - SDP/ v=, o=, s=, c=, t=, a=, m=
- Configurable header and body length checks
- Optional logging of message violations to FortiAnalyzer

Fortinet SIP SFW – Two Modes of Operation

Transparent Mode or Stealth Mode

- Inspecting SIP and RTP traffic
- Does not modifies any messages
- Visible only when trusted network is under attack or in overload situations

Active Mode

- Inspecting SIP and RTP traffic
- Performs Network Address Translation (NAT) for SIP and RTP
- Modifies SIP header and SIP body (SDP)
- Visible as SIP Application Level Gateway (ALG) in the network
- Optionally, NAP/T RTP/RTCP packets

Fortinet SIP SFW – Signaling and Media

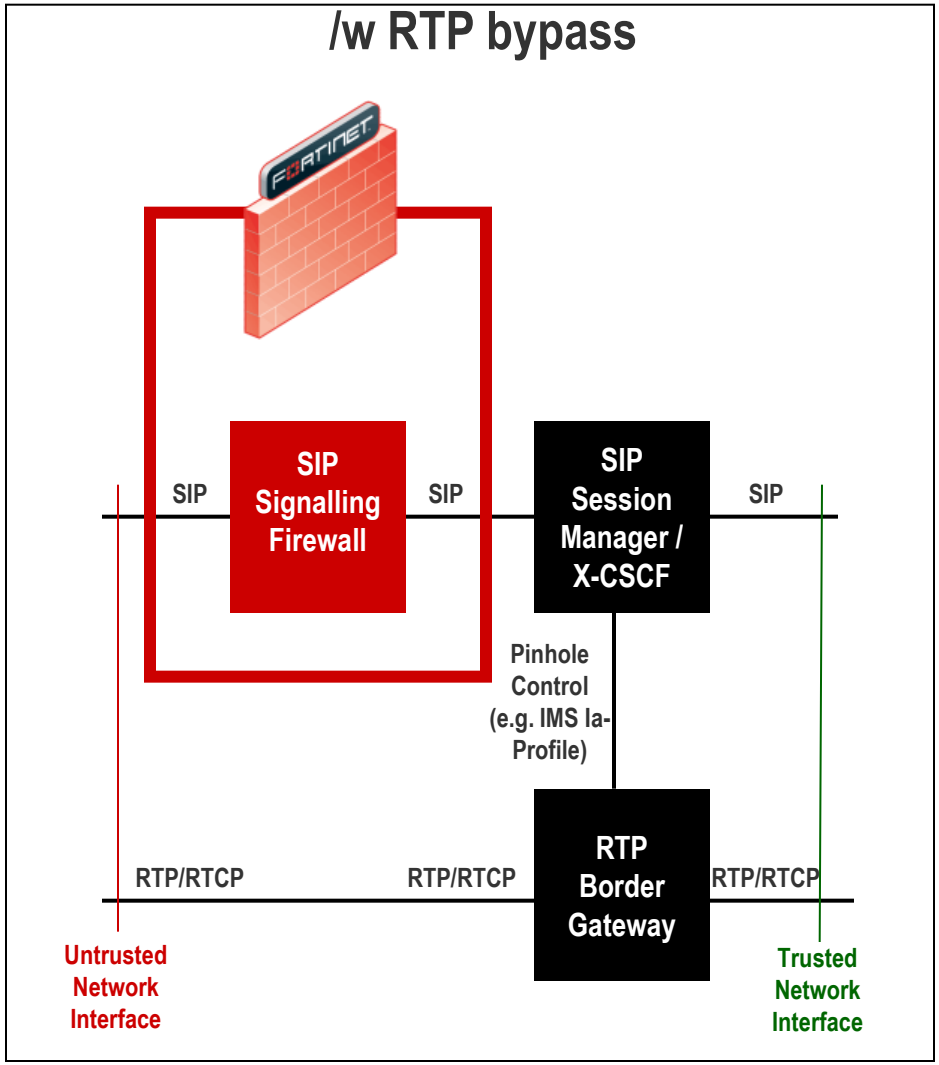
IP network address translation

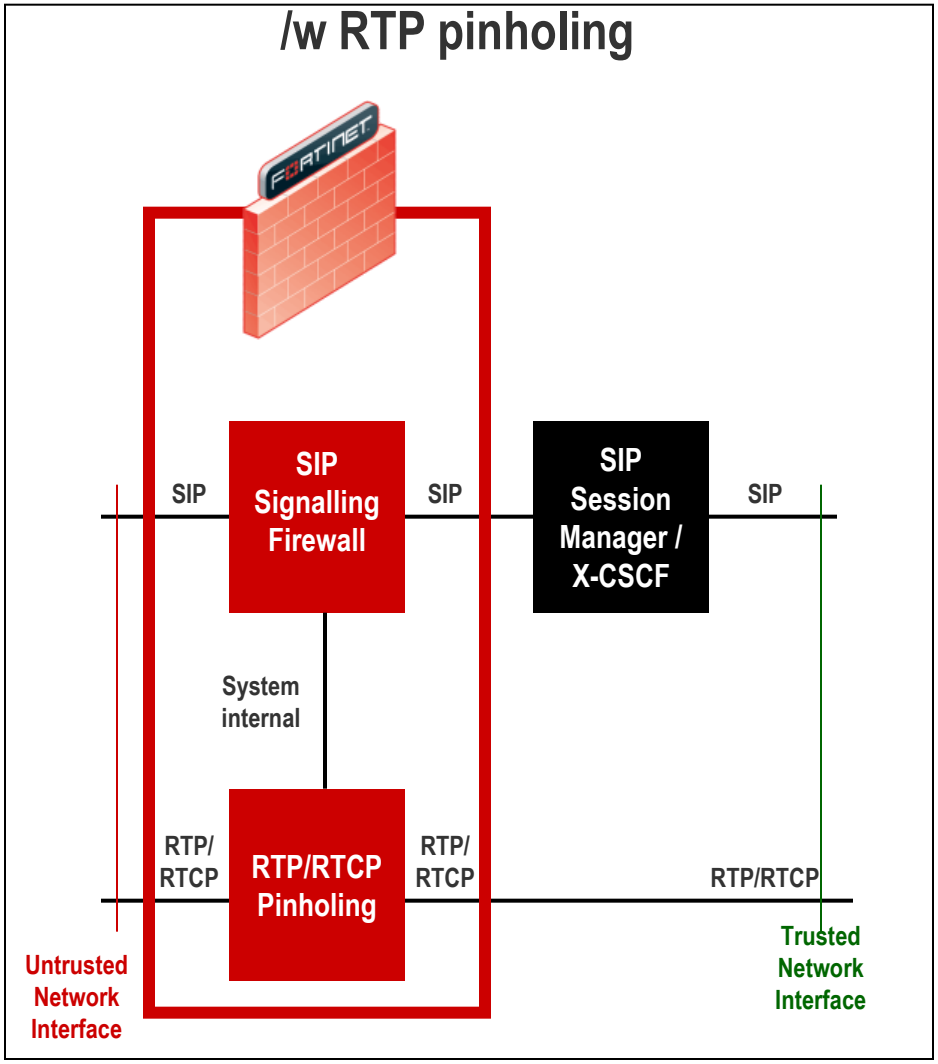
- SIP NAT
  - IP network topology hiding
- Mapping external IP addresses with internal IP address ranges
  - Resolves overlapping IP address between external and internal networks

Media Handling

- Pin-holing of RTP/RTCP
- (Police RTP/RTCP traffic)
- Open and close pin-holes from SIP context
- Hardware acceleration
  - Line rate performance
  - 5 micro seconds latency

SIP SFW Applications





Thank You