ČESKÉ VYSOKÉ UČENÍ TECHNICKÉ V PRAZE
FAKULTA ELEKTROTECHNICKÁ

DIPLOMOVÁ PRÁCE

2015 **Patrik Havrila**

ČESKÉ VYSOKÉ UČENÍ TECHNICKÉ V PRAZE
Fakulta elektrotechnická
Katedra telekomunikační techniky

Bezpečnost SIP PBX

Diplomant: **Patrik Havrila**
Vedoucí práce: **Ing. Ján Kučerák**

Leden 2015

Čestné prehlásenie

Čestne vyhlasujem, že predkladanú diplomovú prácu Bezpečnost SIP PBX som napísal samostatne, pod odborným vedením vedúceho diplomovej práce, konzultanta a za použitia literatúry uvedenej v bibliografii. Ďalej prehlasujem, že nemám žiadne námietky proti požičiavaniu alebo zverejňovaniu mojej diplomovej práce alebo jej časti so súhlasom katedry.

Dátum: 5. 1. 2015

……..……
podpis diplomanta

České vysoké učení technické v Praze
Fakulta elektrotechnická

katedra telekomunikační techniky

ZADÁNÍ DIPLOMOVÉ PRÁCE

Student: **Bc. Havrila Patrik**

Studijní program:
Obor: Sítě elektronických komunikací

Název tématu: **Bezpečnost SIP PBX**

Pokyny pro vypracování:

Zhodnoťte z hlediska bezpečnosti možnosti nasazení na trhu dostupných zařízení SBC-Session Border Controller do architektury NGN sítě na bázi protokolu SIP a to jak na úrovni NNI (Network to Network Interface) tak UNI (User to Network Interface). Popište aktuální možnosti zabezpečení v Avaya Aura architektuře. Zhodnoťte možnosti útoku na tuto architekturu a pokuste se navrhnout možné způsoby zvýšení její odolnosti.

Seznam odborné literatury:

[1] Schulzrinne, H. et. al. RTP: A Transport Protocol for Real-Time Applications. RFC3550. July 2003.
[2] Rosenberg, J. et. al. SIP: Session Initiation Protocol. RFC3261. June 2002
[3] Schulzrinne, H. et. al. Real Time Streaming Protocol (RTSP), RFC2326. April 1998.

Vedoucí: Ing. Ján Kučerák

Platnost zadání: do konce zimního semestru 2014/2015

[redacted]
prof. Ing. Boris Simák, CSc.
vedoucí katedry

ČESKÉ VYSOKÉ UČENÍ TECHNICKÉ V PRAZE Fakulta elektrotechnická
L.S.

[redacted]
prof. Ing. Pavel Ripka, CSc.
děkan

V Praze dne 20. 11. 2013

Abstrakt v SJ

V tejto diplomovej práci je riešená problematika VoIP. Konkrétne ide o protokol SIP. Zaoberá sa zhodnotením možností nasadenia na trhu dostupných zariadení SBC. Zhrňuje všeobecný pohľad na SBC, ujasňuje dôvody a možnosti jeho použitia na úrovni Network-to-Network Interface a User-to-Network Interface. Popisuje základné SIP útoky a následné zabezpečenie proti ním. Takisto popisuje bezpečnostné mechanizmy a možnosti zabezpečenia Avaya Aura architektúry, ktorá sa skladá zo serverov Avaya Session Manager a Avaya System Manager. Sústredí sa aj na jej praktické zabezpečenie, a to pomocou všetkých dostupných bezpečnostných prvkov vrátane Avaya Session Border Controller for Enterprise.

Kľúčové slová

VoIP, SIP, NGN, Unnified Communications, Avaya Aura, Session Border Controller, Session Manager, System Manager

Abstrakt v AJ

Main topic of this diploma thesis is the VoIP especially the SIP. It deals with the assessment of SBC deployment available on the market. This diploma thesis summarizes SBC as a product from all of the possible views to one general description. Clarifies possible usage and security threads at Network-to-Network Interface and User-to-Network Interface. Describes basic SIP attacks and main defense against them. Also describes security mechanisms and security options to secure Avaya Aura architecture consist of Avaya Session Manager and Avaya System Manager servers. The aim is on practical securing by all available secure features included by Avaya Session Border Controller for Enterprise.

Kľúčové slová v AJ

VoIP, SIP, NGN, Unnified Communications, Avaya Aura, Session Border Controller, Session Manager, System Manager

Poďakovanie

Týmto by som chcel poďakovať vedúcemu diplomovej práce Ing. Jánovi Kučerákovi za cenné rady pri písaní práce. Ďalej by som chcel poďakovať môjmu konzultantovi Ing. Josefovi Čechovi za všetku poskytnutú pomoc a skúsenosti. Takisto by som chcel poďakovať aj firme Algotech za poskytnutie všetkého potrebného vybavenia k diplomovej práci.

Obsah

Zoznam obrázkov **9**
Zoznam tabuliek **10**
Zoznam symbolov a skratiek **11**
Slovník termínov **12**
Úvod **13**
1 Bezpečnosť VoIP **15**
1.1 Typy útokov proti SIP 16
1.1.1 Denial-of-Service – Odmietnutie služby 17
1.1.2 Toll Fraud – Theft of the Service 18
1.1.3 Eavesdropping 18
1.2 Zabezpečenie protokolu SIP 18
1.2.1 Heslo a kontrola prístupu 19
1.2.2 Šifrovanie 20
1.2.3 Autentizácia a autorizácia 21
1.3 BYOD 21
2 Session Border Controller **23**
2.1 Potreba SBC 25
2.1.1 NNI - SIP trunk k operátorovi 25
2.1.2 UNI - Remote workers 27
2.2 Možnosti zapojenia SBC 28
2.2.1 Topológia Two-wire 29
2.2.2 Topológia One-wire 29
2.2.3 Demilitarized Zone - DMZ 30
2.2.4 SBC High Availability (HA) 30
2.3 Vyber správneho SBC 32
3 Avaya Aura architektúra **33**
3.1 Avaya Aura Session Border Controller for Enterprise 34
3.1.1 Funkcie Avaya SBCE 34
3.1.2 Bezpečnostné špecifikácie Avaya SBCE 35
3.2 Avaya Aura Session Manager 38
3.2.1 Bezpečnosť 40
3.3 Avaya Aura System Manager 43

3.4 SIP Klienti 43
4 Praktická časť 45
4.1 Implementácia Avaya Aura a Inštalácia Avaya SBCE 45
4.1.1 Adresovanie siete 45
4.1.2 Inštalácia a základné nastavenie SBC 46
4.2 Možnosti útoku a spôsoby zabezpečenia 48
4.2.1 Návrh bezpečnej architektúry 49
4.2.2 Zabezpečenie komunikácie 52
4.2.3 Kontrola prístupu (Autorizácia a autentifikácia) 53
4.2.4 Šifrovanie 53
4.2.5 Nastavenie SIP firewallu v SM 54
4.2.6 Nastavenie Firewallu v SBC 58
4.2.7 Topology hiding 61
4.2.8 Ďalšie zabezpečenie 62
5 Záver 63
Zoznam použitej literatúry 64
Príloha A – Ukážky z útokov 66
Priloha B – Certifikáty ..... Chyba! Záložka není definována.

Zoznam obrázkov

Obr. 1 Klasifikácia rôznych typov DoS útoku [4] ... 18
Obr. 2 Hop-by-Hop TLS medzi UA a Proxy serverom ... 20
Obr. 3 Registračná procedúra pomocou digest-autentizácie ... 21
Obr. 4 Vnútorná architektúra SBC ... 23
Obr. 5 Typy SBC ... 24
Obr. 6 SIP trunk [15] ... 26
Obr. 7 Útok z pohľadu útočníka bez SBC ... 26
Obr. 8 Útok z pohľadu útočníka s nasadeným SBC ... 27
Obr. 9 Remote Workers [15] ... 28
Obr. 10 Zapojenie Two-wire [15] ... 29
Obr. 11 Zapojenie One-wire [15] ... 30
Obr. 12 DMZ ... 30
Obr. 13 Detailné zapojenie Avaya Aura SBCE v HA [15] ... 31
Obr. 14 Zjednodušené zapojenie v HA [15] ... 31
Obr. 15 Avaya Aura architektúra ... 33
Obr. 16 Ochrana IP-PBX pred útokmi ... 36
Obr. 17 SM ako centrum SIP siete [20] ... 39
Obr. 18 Fyzické zapojenie SBC [26] ... 47
Obr. 19 Základné nastavenie SBC ... 47
Obr. 20 Natavenie Server Flows ... 48
Obr. 21 Nastavenie Subscriber Flows ... 48
Obr. 22 SBC za Firewallom ... 49
Obr. 23 SBC pred Firewallom ... 50
Obr. 24 Bezpečné zapojenie ... 51
Obr. 25 Signalizácia pri zapojení len jedného rozhrania ... 51
Obr. 26 Single Source DoS ... 59
Obr. 27 Phone DoS/DDoS ... 60
Obr. 28 Stealth DoS/DDoS ... 60
Obr. 29 Call Walking ... 60
Obr. 30 Domain DoS ... 61
Obr. 31 Topology hiding ... 61

Zoznam tabuliek

Tab. 1 Bezpečnostné vrstvy [1] 16
Tab. 2 Špecifikácie Avaya Aura podľa jednotlivých verzií [20] 34
Tab. 3 Parametre počtu konkurenčných hovorov pre Avaya SBCE [15] 35
Tab. 4 Zoznam použitých portov [22] 37
Tab. 5 Inštalované Scrubber balíčky v Avaya SBCE [21] 38
Tab. 6 Porovnanie SM a SBC pre pripojenie k SIP operátorovi [23] 42
Tab. 7 Kapacita SMGR [25] 43
Tab. 8 Adresovanie siete 45
Tab. 9 Doby trvania prelomenia hesla 52
Tab. 10 Nastavenie Firewallu 57

Zoznam Grafov

Graf 1 Závislosť vyťaženie CPU SM od času – s vypnutým SIP firewallom 55
Graf 2 Závislosť počtu správ od času – s vypnutým SM SIP firewallom 55
Graf 3 Pomer úspešných a neúspešných hovorov počas simulácie DoS útoku 56
Graf 4 Závislosť vyťaženia CPU SM od času – so zapnutým SIP firewallom 56
Graf 5 Závislosť vyťaženia CPU SBC od času – s vypnutým SBC SIP firewallom 58
Graf 6 Závislosť vyťaženia CPU SM od času – so zapojeným SBC 59

Zoznam symbolov a skratiek

ASBCE	Avaya Session Border Controller for Enterprise
B2BUA	Back-to-back User Agent
BYOD	Bring Your Own Device
CA	Certifikačná autorita
CM	Communication Manager
DDoS	Distributed Denial of Service
DMZ	Demilizarizovaná zóna
DNS	Domain Name System
DoS	Denial of Service
EMS	Element Management System
FTP	File transfer Protocol
HA	High Availability
HTTP	Hypertext Transfer Protocol
IP	Internet Protocol
LAN	Local Area Network
NAT	Network Address Translation
NGN	Next Generation Network
NNI	Network to Network Interface
PBX	Private Branch Exchange
PSTN	Public Switched Telephony Network
RPM	Red Hat Package Manager
RTP	Real-time Transport Protocol
SBC	Session Border Controller
SIP	Session Initiation Protocol
SM	Session Manager
SMGR	System Manager
SRTP	Secure Real-time Transport Protocol
TCP	Transmission Control Protocol
TLS	Transport Layer Security
UA	User Agent
UAC	User Agent Client
UAS	User Agent Server
UDP	User Datagram Protocol
UNI	User to Network Interface
URI	Uniform Resource Identifier
VLAN	Virtual Local Area Network
VoIP	Voice over Internet Protocol
VPN	Virtual Private Network
WAN	Wide Area Network

Slovník termínov

Firewall je sieťové zariadenie alebo softvér, ktorého úlohou je oddeliť siete s rôznymi prístupovými právami a kontrolovať dátový tok medzi týmito sieťami.

Kodek je počítačový program, ktorý dokáže transformovať dátový tok alebo signál. Slovo vzniklo zložením počiatočných slov kodér a dekodér resp. kompresia a dekompresia.

Koncové zariadenie je zariadenie, ktoré je použité ako rozhranie medzi človekom a komunikačnou sieťou.

Multimédia je označenie pre digitálny obsah, ktoré je kombináciu viacerých druhov audiovizuálneho obsahu.

Paket označuje v informatike blok dát prenášaný v počítačových sieťach založených na prepojovaní paketov.

Rozhranie je bod, v ktorom je vytvorené spojenie medzi dvoma elementmi tak, aby spolu mohli navzájom pracovať.

Server je v informatike všeobecne označenie pre počítač, ktorý poskytuje nejaké služby, alebo počítačový program, ktorý tieto služby realizuje.

SIP Proxy je zariadenie, ktoré smeruje SIP požiadavku na správne miesto, autentizuje, autorizuje užívateľov k rôznym službám a poskytuje rôzne služby.

SIP Redirect server je user agent server, ktorý generuje 3xx odpovede na požiadavky ktoré prijme, nasmerovaním klienta ku kontaktovaniu inej množiny URI adries.

SIP registrar je server ktorý prijme SIP REGISTER požiadavku a uloží ju do databázy známej ako Location Service.

SIP Trunk je spôsob pripojenia privátnej ústredne do internetu.

SIP URI je adresná schéma signalizačného protokolu SIP, ktorá umožňuje volanie ostaným osobám.

Telefónna ústredňa je zariadenie, ktoré zaisťuje spojovanie telefónnych hovorov .

VoIP sieť je systém navzájom prepojených VoIP elementov v počítačovej sieti, ktoré medzi sebou komunikujú signalizačnými protokolmi.

Úvod

V diplomovej práci sa budem zaoberať aktuálnym zhodnotením nasadenia SBC do NGN architektúry. Popíšem aktuálny stav a spôsob zabezpečenia PBX pracujúcich na protokole SIP, konkrétne Avaya Aura architektúru. Budem sa zaoberať všetkými dostupnými prvkami, ktoré systém zabezpečujú.

Diplomová práca bude predpokladať základné znalosti z oblasti SIP signalizačného protokolu. Pokúsim sa vecne zodpovedať na otázky, ktoré by si mohla klásť organizácia alebo firma rozhodujúca sa nad implementáciou SBC do praxe. Budem tiež riešiť otázky ohľadom samotného SBC, i samotné bezpečnostné hľadisko SBC. V texte sa preto nebudem podrobne zaoberať základnými vlastnosťami protokolu SIP, ale svoju pozornosť zameriam na praktické zabezpečenie Avaya Aura NGN siete.

Práca je rozdelená do štyroch kapitol, jednotlivé kapitoly sa členia na teoretickú a praktickú časť. V úvode práce oboznámim čitateľa s čo najširším spektrom bezpečnostných otázok, spomeniem tiež všeobecné bezpečnostné mechanizmy protokolu SIP a prejdem až k tým, ktoré Avaya priamo ponúka.

Cieľom teoretickej časti bude popísanie aktuálneho stavu zabezpečenia PBX systémov pracujúcich na protokole SIP. Priblížim architektúru zapojenia z pohľadu bezpečnosti, otestujem jednotlivé metódy zabezpečenia a následne zhodnotím ochranu systému.

V praktickej časti práce ponúknem aj návod, ako nastaviť základné zabezpečenie a to v kombinácií Avaya Aura Session Manager a Avaya Session Border Controller for Enterprise.

V prvej kapitole sa budem zaoberať celkovou VoIP bezpečnosťou, opíšem základné útoky a možnosti zabezpečenia protokolu SIP. Spomeniem aj najvážnejšie útoky akými sú DoS, Toll Fraud a Eavesdropping. Z pohľadu VoIP bezpečnosti spomeniem i čoraz rozšírenejší trend BYOD, ktorého implementáciu ponúka aj Avaya Session Border Controller for Enterprise, a ktorý tak zvyšuje atraktivitu jeho použitia.

Druhá kapitola bude patriť SBC, ktoré zadefinujem, popíšem jeho potrebu, možnosti zapojenia a v neposlednom rade aj jeho správny výber. Táto kapitola vysvetľuje čo vlastne pojem SBC znamená a čo môže SBC poskytnúť. Na SBC sa budem pozerať hlavne z bezpečnostného hľadiska, ale popíšem aj všetky možné funkcie SBC. Spolu s prvou kapitolou budú tieto dve kapitoly tvoriť teoretický základ diplomovej práce, ktorý dopomôže k lepšiemu porozumeniu praktickej časti práce.

V tretej kapitole rozoberiem pojem Avaya Aura. Popíšem jednotlivé prvky hlavne z pohľadu bezpečnosti. Zadefinujem Avaya Aura Session Border Controller for Enterprise, ktorý je ochranným prvkom celej Avaya Aura architektúry. Poviem o tom, ako a kam ho v sieti uložiť. Malú časť kapitoly venujem aj SIP klientom od firmy Avaya. Táto kapitola bude chýbajúcim kúskom skladačky medzi teoretickou a praktickou časťou, ktorá ozrejmí použitú Avaya technológiu, jej vlastnosti a katalógové informácie.

Posledná, štvrtá, kapitola tvorí praktickú časť diplomovej práce. Popíšem implementáciu testovacej Avaya Aura architektúry i implementáciu a konfiguráciu Avaya Aura SBCE pre ochranu trunkov a vnútornej siete.

Štvrtá kapitola diplomovej práce sa prelína s diplomovou prácou môjho kolegu, Ondru Kováře, kde testovanie jednotlivých metód zabezpečenia bude našim spoločným bodom. Ondra Kovář bude na navrhnutú architektúru útočiť a ja sa budem snažiť jeho útokom ubrániť. A tak budeme skúmať celkový dopad rôznych útokov na architektúru

Avaya Aura. Na základe získaných výsledkov zhodnotím možnosti zabezpečenia tejto architektúry a pokúsim sa navrhnúť prípadné zlepšenia jej ochrany.

1 Bezpečnosť VoIP

Na trhu, v oblasti telekomunikácií, sa stávame svedkami kedy je technológia VoIP stále populárnejšou. S týmto spôsobom komunikácie sa dostáva do popredia aj protokol SIP.

Protokol SIP slúži ako dorozumievací prostriedok na vytváranie, modifikáciu a ukončovanie relácií v IP sieťach. Zahŕňa telefónne hovory, konferencie a multimediálny prenos hlasu, videa a správ. O tento protokol sa začína zaujímať stále väčšie množstvo ľudí, či už ide o sieťových odborníkov, pracujúcich pre poskytovateľov dátových služieb, malých prevádzkovateľov VoIP pobočkových ústrední alebo len o obyčajných ľudí, ktorý sa týmto spôsobom snažia znížiť svoje výdavky spojené s telefonovaním.

Pri takejto narastajúcej populárnosti je veľmi dôležité zaoberať sa aj otázkou bezpečnosti v IP telefónii. Tá je dnes výzvou, a to hlavne preto, lebo je priamo pripojená k internetu, ktorý je z pohľadu zabezpečenia dát a ochrany súkromia hrozbou. Každý kto sa zaoberá problematikou bezpečnosti vie, že pripojenie k internetu je rizikom. Exituje mnoho prípadov kedy boli internetové služby kompromitované, boli ukradnuté/zneužité citlivé informácie alebo sa vyskytla nedostupnosť služby z dôvodu jej zahltenia. Netreba sa nechať zmiasť tým, že sofistikované bezpečnostné riešenia dokážu zabrániť útokom na sieť. Dokonca aj virtuálne hradby najbezpečnejších sietí sveta čelia útokom a neraz aj podľahnú.

To ale pomáha identifikovať slabé miesta a zaujať voči ním patričné stanovisko. Preto je štúdium zraniteľnosti SIP protokolu dôležitou súčasťou, ktorá by mala viesť k lepšiemu porozumeniu VoIP a hlavne k zníženiu bezpečnostného rizika. V tejto oblasti je aktívna organizácia IETF, ktorá vyvíja a neustále pridáva rôzne vylepšenia a záplaty proti sieťovým útokom. Tie prispievajú k lepšiemu a bezpečnejšiemu chodu protokolu SIP. Veľa zostáva priamo na pleciach prevádzkovateľov sietí a sieťových administrátorov, ktorí si týchto záplat a vylepšení musia byť vedomí.

V problematike bezpečnosti je úplne v poriadku ak sa firma alebo organizácia stane do určitej miery paranoidnou. Pod paranoidnosťou myslím, že firma hľadá všetky slabé miesta a možnosti odkiaľ útok môže prísť. Príčinou útoku môže byť LAN sieť, nezabezpečené servery, bezpečnostné diery v serverových operačných systémoch, ale aj nepremyslený dizajn architektúry, infraštruktúry, ponechaná základná konfigurácia alebo základné heslá. Tieto slabé miesta je potrebné v čo najkratšom čase odhaliť a zabezpečiť.

Existuje veľa možností zabezpečenia VoIP siete - autentizácia, šifrovanie paketov a bezpečná architektúra. Jednou z nich je aj nasadenie SBC ako tzv. SIP firewall, ktorý bráni nežiaducej SIP prevádzke preniknúť do vnútra siete, a ktorým sa budem ďalej v tejto diplomovej práci zaoberať.

Nebolo by však rozumné myslieť si, že jediné SBC, ako bezpečnostný prvok zabráni všetkým útokom, pretože nejaká časť príde určite aj zvnútra. Preto bezpečnostné riešenie musí byť implementované tak zvonku ako aj zvnútra siete. Na úrovni NNI a rovnako aj na úrovni UNI. Dokonca aj vonkajšie útoky môžu využiť nesprávnu konfiguráciu siete alebo nejaké slabé miesta, ktoré v konečnom dôsledku môžu a nemusia mať s protokolom SIP nič spoločné.

1.1 Typy útokov proti SIP

Ako také útoky vyzerajú? Existuje mnoho tipov útokov, niektoré sú sieťové, iné útočia na slabiny šifrovacieho algoritmu, operačného systému, fyzického zapojenia alebo bezpečnostných pravidiel danej organizácie. SIP sa nachádza až na samom vrchu tejto pomyselnej pyramídy (Tab. 1). Preto jeho bezpečnosť sa spolieha na všetky tieto vrstvy pod ním a je taká silná ako ten najslabší prvok. Slabiny a zabezpečenia týchto vrstiev sú dnes už celkom známe, popísané a pravidelne sa vyvíjajú rôzne záplaty a vylepšenia.

Mojou úlohou v diplomovej práci je popísať možnosti zabezpečenia práve tejto najvyššej VoIP vrstvy. Pochopeniu všetkých možností zabezpečenia predchádza pochopenie útokov. Z tohto dôvodu sa v tejto kapitole budem sústrediť práve na tie útoky a zabezpečenia proti ním, ktoré sa týkajú priamo SIP protokolu.

Tab. 1 Bezpečnostné vrstvy [1]

	Bezpečnostné vrstvy	Typ útoku na danú bezpečnostnú vrstvu
6.	VoIP	DoS/DDoS, Toll Fraud, Eavesdropping, Fuzzing
5.	Bezpečnosť OS	Pretečenie zásobníka, Červy, Konfigurácia, Pád OS
4.	Bezpečnosť podporných služieb	SQL Injection,
3.	Sieťová bezpečnosť	Sin Flood, SYN Flood, Ping of Death, Paketová búrka
2.	Fyzická bezpečnosť	Shutdown, Reboot
1.	Bezpečnostná politika	Slabé heslá

Jednou z prvých vecí, ktorá človeka napadne ak sa začne zaoberať útokmi je, zamyslieť sa nad dôvodmi, ktoré vedú útočníka k zlomyseľnej činnosti. Tieto dôvody sú tými istými, ktoré vedú útočníkov útočiť aj na obyčajné telefóne siete. Či už v minulosti alebo v súčasnosti, tak ľuďom šlo vždy hlavne o finančný prospech, a to napríklad metódami Toll Fraud, krádežou informácií alebo identity. Takíto ľudia nemajú strach z odhalenia. Medzi ďalšie dôvody patrí snaha znepríjemniť užívateľom využívanie nejakej služby alebo znehodnotiť službu operátora, a to zaťažením siete vysokou prevádzkou. [2]

Existuje mnoho útokov proti službe SIP, niektoré sú účinnejšie, a niektoré naopak menej. Všetko závisí hlavne na tom, čo útočník od svojho útoku požaduje. Typy útokov proti službe SIP je možné všeobecne kategorizovať [3]:

- **Prelomenie registrácie** - vydávanie sa útočníka za niekoho iného. Ide o jeden z najčastejších útokov, v ktorom útočník neoprávnene využíva SIP služby. Prelomenie registrácie môže byť dosiahnuté slovníkovým útokom alebo útokom hrubou silou na heslo legitímneho užívateľa. Tak isto môže byť prelomená registrácia odchytením platnej registrácie účastníka, z ktorej je možné vyčítať meno a heslo.
- **Privlastnenie identity servera** - útočník sa snaží dostať do komunikácie medzi SIP server (SIP Proxy, SIP registrar alebo Redirect) a UA. Útočník bude schopný odpočúvať, kontrolovať alebo presmerovať všetku prevádzku prechádzajúcu cez takýto kompromitovaný SIP server.

- **Manipulácia so správou** - odchytenie a modifikáciu SIP hlavičky.
- **Manipulácia s reláciou** - do tejto kategórie patrí napríklad odchytenie časti komunikácie a na základe získaných informácií a vhodného nástroja je možné zrušiť BYE útokom práve prebiehajúcu reláciu.
- **DoS útoky.**

V dnešnej dobe, dobe internetu, už nie je problém vyhľadať si informácie o danom type útoku a svojpomocne takýto útok zrealizovať.

Nech už je dôvod útočníka akýkoľvek, tak s vysokou pravdepodobnosťou si vyberie jeden z niekoľkých najčastejšie používaných útokov, ktorými môžu byť DoS/DDoS, Toll Fraud, Man in the Middle, Eavesdropping, Theft of Service, Impersonation, Credential and Identity Theft, Hijacking alebo Fuzzing.

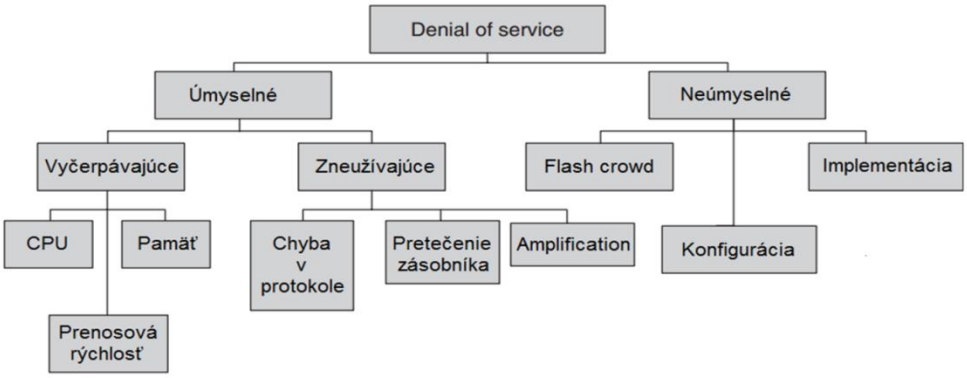
1.1.1 Denial-of-Service – Odmietnutie služby

Táto technika útoku, tzv. odmietnutie služby, sa snaží platným účastníkom zabrániť používať danú službu. Dochádza k zaplaveniu servera požiadavkami realizovanými veľkým počtom neužitočných paketov, ktoré zahlcujú pamäť CPU alebo prenosovú rýchlosť kanála. Týmto útokom dôjdu serveru vlastné prostriedky pre poskytovanie danej služby, a to vedie zvyčajne k znemožneniu obslúženia platných účastníkov alebo pádu služby.

Medzi útoky typu Denial-of-Service patrí aj použitie malého množstva škodlivých paketov, ktoré sú navrhnuté na zneužitie zraniteľných miest softwaru služby. Útočník týmto spôsobom nad ňou zvyčajne preberá kontrolu alebo znemožní odoslanie platnej požiadavky. Kvôli zvýšeniu obtiažnosti sledovania a objavenia zdroja tohto útoku sa takýto útok väčšinou prevádza distribučným spôsobom. V takomto prípade sú veľké počty systémov v internete ovládané útočníkom a tie následne zahlcujú obeť [4].

Môžeme rozlišovať medzi úmyselnými, neúmyselnými alebo záškodníckymi DoS útokmi. Rozdelenie je zobrazené na Obr. 1. Zatiaľ čo neúmyselné DoS útoky sú často výsledkom implementácie alebo konfiguračnej chyby, tak tie zlomyseľné sú zahájené útočníkmi úmyselne. Tieto útoky môžu byť ďalej rozdelené do vyčerpávajúcich (tzv. flooding) útokov a do útokov, ktoré zneužívajú zraniteľné miesta protokolu (tzv. misuse) [4].

Ďalším hľadiskom, z ktorého sa na útoky je možné pozerať sú útoky priame a nepriame. Priame útoky spočívajú v priamom napadnutí obete posielaním veľkého množstva požiadaviek alebo zneužitím určitej bezpečnostnej chyby. Nepriame zvyčajne útočia na nejaké podporné služby. Takouto službou môže byť napríklad DNS alebo databáza používaná obeťou. V tomto prípade nemusí služba vykazovať žiadne známky útoku, ale jej funkčnosť už nie je taká, aká bola zamýšľaná. [4][1]



Obr. 1 Klasifikácia rôznych typov DoS útoku [4]

1.1.2 Toll Fraud – Theft of the Service

Toll Fraud je v oblasti telekomunikácií a VoIP celosvetovo rozšíreným problémom. Je to útok, v ktorom útočník využije slabinu VoIP zabezpečenia a získa prístup k volaniam, ktoré je ďalej schopný lacno predať. Tieto volania potom často krát smerujú práve do krajín, v ktorých sú poplatky za takéto hovory drahé. Odpoveď na otázku prečo takéto hovory nezastaví už priamo operátor je taká, že operátor nedokáže rozlíšiť či ten hovor je od firmy, zákazníka alebo je to útok typu Toll Fraud. Takýto hovor je prenášaný cez rôznych IXC (Inter-Exchange Carriers) - telekomunikační operátori prenášajúci hovory na veľké vzdialenosti. Každý z nich musí platiť svoju časť pri prenášaní hovoru. V prípade volania do exotickej krajiny musí jeden operátor platiť tomu druhému, a to bez ohľadu na to, či je to Toll Fraud útok alebo nie. [1]

Podľa americkej CFCA (asociácia zaoberajúca sa útokmi Toll Fraud) bola celková spôsobená škoda vo výške $4.96 miliárd amerických dolárov. [5] Človek má, po prečítaní takejto správy tendenciu neprikladať jej veľkú vážnosť a povedať si, že: „Mne sa to nemôže stať.“ Je dobré vedieť o týchto hrozbách, neskrývať sa pred nimi a zaujať voči ním patričné stanovisko.

1.1.3 Eavesdropping

Typ útoku, ktorý monitoruje a odpočúva SIP reláciu. Môže ísť o signalizáciu, média alebo indikáciu toho, kto s kým hovorí. SIP správa obsahuje signalizačné správy, ktoré pozostávajú z údajov ako identita, kontaktná adresa, bezpečnostné kľúče a ďalšie užitočné informácie pre vytvorenie relácie, ktoré sa napríklad pomocou voľne dostupného programu Wireshark dajú jednoducho odchytiť, prečítať a následne jednoducho zneužiť. Tieto informácie by mali byť z pohľadu bezpečnosti vhodným spôsobom utajené. [6]

1.2 Zabezpečenie protokolu SIP

Ak bude firma rozmýšľať o stavbe bezpečnej SIP siete, potrebuje vziať do úvahy štyri rôzne oblasti, v ktorých zabezpečenie bude použité.

Ako prvé je potrebné zabezpečiť SIP signalizáciu. Prioritou číslo dva by bola ochrana RTP streamu prenášaného cez sieť. Potom je tu zaistenie toho, že SIP entita je naozaj tá, za ktorú sa vydáva. A ako posledné je vytvorenie bezpečného pripojenia k

internetu na okraji siete. V tejto kapitole sa preto budem snažiť popísať rôzne metódy zabezpečenia protokolu SIP.[7]

Pri návrhu a implementácii siete je nutné použiť bezpečnostné opatrenia, ktoré dokážu uspokojiť požiadavky bezpečnej siete. Medzi základné bezpečnostné mechanizmy patrí [8]:

- **Autentizácia** – proces overenia identity účastníka. Vyžaduje použitie hesla kedykoľvek keď sa užívateľ pripojí do siete, a tak zaháji registráciu užívateľa v sieti.
- **Autorizácia** – oprávnenie prístupu. Vyžaduje dopytovanie sa databázy na základne údajov o účastníkovi, o službách, ktoré je účastník autorizovaný používať. Tieto údaje pozostávajú z privátnej a verejnej identity účastníka. Autorizácia môže byť kvôli zefektívneniu súčasťou autentifikácie.
- **Dôvernosť** – čo znamená, že k informáciám a dátam majú prístup len oprávnení účastníci, konverzácia nemôže byť špehovaná a účastníci si môžu slobodne vymieňať informácie (napríklad telefonovať) bez toho, aby boli odchytené niekým iným.
- **Celistvosť** – zaistenie, že informácia nebola zničená, stratená alebo modifikovaná. Je veľmi jednoduché získať prístup k nezabezpečenej SIP správe a predtým než bude doručená, tak zmeniť jej obsah. Napríklad za účelom zmeny služby a doručovacieho miesta.
- **Súkromie** – zaistenie anonymity účastníka (skrývanie IP adresy).
- **Dostupnosť** – zaistenie dostupnosti služby.
- **Nepopierateľnosť** – zaisťuje, aby po tom čo účastník službu použil, tak nemohol poprieť využitie danej služby.

Toto sú len všeobecne definované bezpečnostné mechanizmy, ktoré tvoria základ špecifických bezpečnostných implementácií v sieti SIP. Na nich sú postavené všetky bezpečnostné mechanizmy opísané v nasledujúcich podkapitolách. V nich som sa nezaoberal bezpečnostnými mechanizmami, S/MIME, PGP a Secure SIP, pretože tieto mechanizmy nie sú použité v Avaya Aura architektúre.

1.2.1 Heslo a kontrola prístupu

Heslo patrí k najzákladnejším a najviac prehliadaným bezpečnostným prvkom. Heslá sú nepríjemnou záležitosťou a nikto sa s nimi nerád zaoberá pokiaľ sa chce prihlásiť k svojmu SIP účtu.

Problémom s heslami je ich správa, napr. implementáciu starnutia hesla, ktorá zvyšuje bezpečnosť. Je to pravidelná zmena hesla, ktorá sa týka účastníkov alebo kritických sieťových prvkov.

Niekto si svoje heslo mení pravidelne, iní vôbec. Možno to vyzerá triviálne, ale niektorí správcovia sietí si heslá na svojich zariadenia pravidelne vôbec nemenia, nech sa jedná o brány, smerovače alebo iné sieťové zariadenia. Dokonca nechávajú štandardné heslá, ktoré sú veľmi dobré zdokumentované a ďalej šírené pomocou internetu, a to môže viesť k tzv. Toll Fraud útoku [8].

Prvým najzákladnejším a nevyhnutným krokom k bezpečnejšej sieti je zmena základného hesla a jeho pravidelná aktualizácia. Je potrebné mať taktiež čo najdlhšie a najzložitejšie heslá.

1.2.2 Šifrovanie

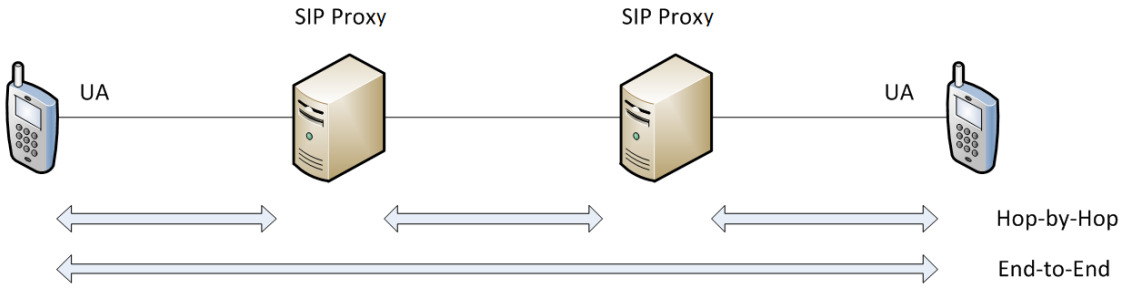
SIP signalizácia sa v sieti šíri ako tzv. „plain text“ čo z anglického prekladu znamená *prostý text*. Ten je možné pomocou sieťových nástrojov, napríklad Wireshark, veľmi jednoducho odchytiť. Preto je z hľadiska bezpečnosti potrebné uvažovať aj o šifrovaní takéhoto prostého textu.

Šifrovanie je jedným z bezpečnostných prvkov, ktoré rieši mnoho problémov a jedna z najlepších ciest, ako preventívne zamedziť nežiaducemu prečítaniu správy naprieč sieťou na ceste k jej prijímateľovi.

RFC 3261 [9] v tomto prípade štandardizuje použitie TLS pre proxy servery, redirect servery a registrar. Taktiež sa odporúča jeho použitie pre UA. Pri použití TLS vznikne dôverné spojenie na transportnej vrstve OSI modelu. TLS je schopné poskytnúť ochranu SIP komunikácie proti strate celistvosti, dôvernosti (kap. 1.2) a proti opakovanému generovaniu SIP správy.

TLS sa používa na Hop-by-Hop báze (Obr. 2) medzi UA a proxy alebo medzi UA a call severom. Ak budem uvažovať o relácii medzi dvomi UA a dvomi proxy servermi, podľa Obr. 2, tak každý z týchto tzv. „hopov“ bude rôznou TLS reláciou. TLS tunel je v signalizačnej ceste zostavovaný nezávisle medzi všetkými koncovými bodmi. V každom spojení je možné použiť rôzne bezpečnostné certifikáty, rôzne hash funkcie a šifrovacie algoritmy. Vo výsledku bude zaistená celistvosť a dôvernosť pri prechode cez každú SIP entitu na signalizačnej ceste, ale obsah SIP správy bude viditeľný pre obe sip proxy. [2]

V reálnom použití je však veľmi ťažké dokázať, že v signalizačnej ceste pri telefonovaní cez internet bol medzi všetkými sip entitami vybudovaný TLS tunel. Význam jeho použitia je hlavne medzi UA a proxy serverom, ktoré spravuje sieťový operátor, a ktoré má pod svojou kontrolou. Takto je možné zabezpečiť to, že hovory v jeho sieti nebudú odpočúvané.



Obr. 2 Hop-by-Hop TLS medzi UA a Proxy serverom

Čo sa šifrovania týka, tak tu patrí nielen šifrovanie signalizácie pomocou TLS ale aj šifrovanie médií. Avaya podporuje šifrovanie pomocou SRTP [10]. Je to šifrovaný RTP prenos. Takýto prenos nemôže byť odpočúvaný, a to jednoduchým odchytením

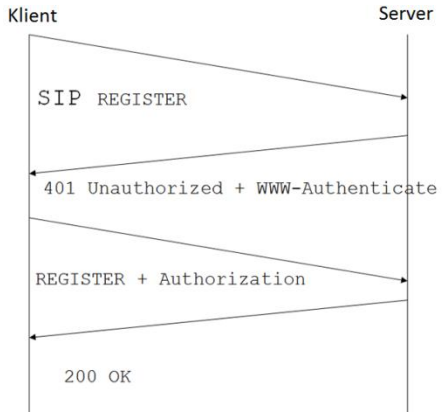
komunikácie pomocou programu Whireshark. Útočník nebude poznať kľúč, ktorým je komunikácia šifrovaná, a preto si daný hovor nebude môcť prehrať.

1.2.3 Autentizácia a autorizácia

Jedným zo základných bezpečnostných mechanizmov je aj autentizácia. Dôvodom potreby autentizácie je overenie identity toho s kým komunikujeme. Taktiež zabezpečuje to, že to čo prijímateľ prijme je to čo odosielateľ odoslal (celistvosť). Tak isto zabraňuje neautorizovanej registrácií.

SIP špecifikuje niekoľko druhov autentizácie. Tá najzákladnejšia má anglický názov „basic“ a originálne pochádza z protokolu HTTP. Táto autentizácia prenáša užívateľove prihlasovacie údaje v čistom texte zakódovaná do base-64, takže pre útočníka by vôbec nebolo problémom získať používateľovo heslo. Základná autentizácia neobsahuje žiadne zabezpečovacie mechanizmy a je jednoducho zneužiteľná. Je však možné použiť základnú autentizáciu aj bezpečne, a to v určitých prípadoch. Kde by komunikáciu chránil napríklad TLS tunel. Aj napriek tomu by však mali byť použité digest alebo silnejšie autentizačné metódy. [2]

Z pohľadu bezpečnosti neexistuje dôvod nepoužiť digest autentizáciu, ktorá tak ako aj na klienta, tak aj na server kladie len minimálne požiadavky. Digest autentizácia vychádza z protokolu HTTP a používa sa na autentizáciu medzi UA a proxy serverom alebo naopak. Kvôli bezpečnosti využíva tzv. „nonce“ alebo jednorázovo generovaný kľúč. Používateľove prihlasovacie údaje sú zvyčajne hashované pomocou MD5. MD5 hash tvorí používateľské meno, heslo, realm a nonce. Môže byť použitý len pod špecifickou doménou. Popis toho ako taká autentizácia funguje je zobrazený na Obr. 3. Táto autentizácia nemusí byť iba súčasťou REGISTER požiadavky ale aj INVITE a BYE. [11]



Obr. 3 Registračná procedúra pomocou digest-autentizácie

1.3 BYOD

Dnešná doba prináša obrovský bum vo výrobe a vývoji nových mobilných zariadení (tabletov, telefónov). Tie sa stávajú novodobým trendom a všetok vývoj sa začína točiť okolo nich. Bolo by veľkou škodou ak by si zamestnanec firmy kúpil svoje vlastné zariadenie, napríklad tablet a nemohol ho používať v rámci firmy. To doteraz

bolo možné ale takéto zariadenie muselo byť prísne monitorované, pretože z pohľadu siete sa stávalo hrozbou. Ani sám používateľ nemusel vedieť o tom, aký škodlivý softvér si tam nevedomky nainštaloval.

To je už ale minulosťou. SIP ponúka možnosť nainštalovať si na svoje zariadenie vlastného SIP klienta a týmto klientom byť pripojený k firemnej sieti. Tento trend sa nazýva Bring Your Own Device (BYOD). Takéto zariadenie už nemusí podliehať prísnej kontrole, pretože už to nie je ten tablet alebo mobilný telefón, ktorý sa pomocou VPN pripája k firemnej sieti ale SIP aplikácia. Tá môže ponúknuť široké možnosti komunikácie – telefonovanie, videohovor, konferencia, videokonferencia, prezenčný systém alebo zdieľanie pracovnej plochy za účelom prezentácie. [12]

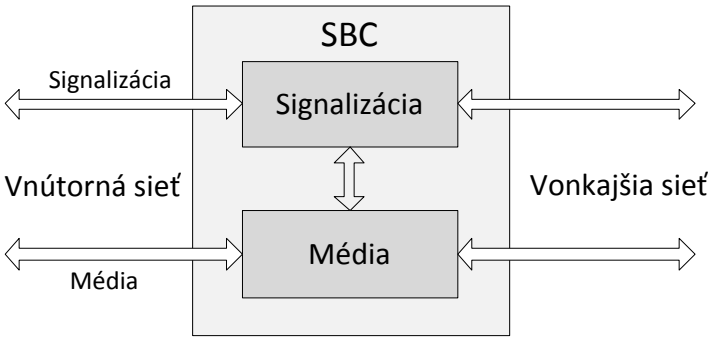
Dnes je možné si nainštalovať na IOS, Android alebo Windows Phone svojho vlastného SIP klienta a reagovať na hovory vo firme práve ním - UNI (User to Network Interface). Bezpečnosť v tomto prípade nebude problém pod podmienkou, ak celá komunikácia z vlastných zariadení bude prechádzať cez SBC. Ten prepustí len platnú SIP komunikáciu, vrátane médií a do internej siete sa nič cudzie nemôže dostať. Takto medzi organizáciou a vlastným zariadením odpadne potreba VPN tunela. Už nebude potrebné zabezpečiť celé zariadenie a následné monitorovanie inštalovaných aplikácií ako pri VPN. V tomto prípade ide len o zabezpečenie SIP aplikácie. [12]

2 Session Border Controller

Session Border Controller (SBC) je SIP B2BUA entita, ktorá je všeobecne známa ako hranica medzi privátnou a verejnou sieťou. SBC prijíma žiadosti ako UAS a potom ich ďalej preposiela ako UAC. Tvorí akýsi SIP firewall, ktorý zabraňuje nežiaducej prevádzke ohroziť sieť.

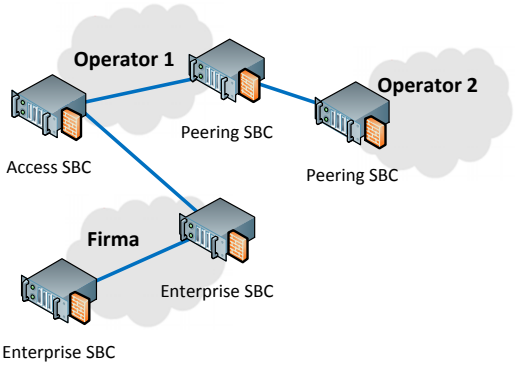
V súčasnosti každý VoIP operátor, ku ktorému sa firma pripojí bude mať na svojom okraji siete vždy nejaké SBC, ktorým si bude chrániť svoju vlastnú sieť. Preto je potrebné zvážiť použitie SBC aj na okraji internej siete. Každý kto spravuje sieť, ju chce mať pod čo najväčšou kontrolou. Táto kontrola zahŕňa aj takú zdravú nedôveru voči VoIP operátorovi, ktorý môže ale nemusí ochrániť firemnú internú sieť od vonkajších útokov. Preto prvým bezpečnostným prvkom v sieti by malo byť vlastné SBC, ktoré má sieťový administrátor pod svojou kontrolou.

Termín SBC je relatívne nešpecifikovaný, pretože zatiaľ nie je štandardizovaný. SBC typicky spracováva signalizáciu médií, často modifikuje hlavičky a časti tela správy SIP, ktoré SIP Proxy nemajú dovolené modifikovať. Taktiež zvyčajne sedí na hranici medzi vnútornou a vonkajšou sieťou, kde dáva pozor, kontroluje a chráni prevádzku, ktorá smeruje z vonkajšej siete (nedôveryhodnej) do vnútornej (dôveryhodnej). SBC je konfigurované a spravované organizáciou, ktorá spravuje aj vnútornú sieť. Na Obr. 4 je znázornená vnútorná architektúra SBC, ktorá zahŕňa časť spracúvajúcu média a časť spracúvajúcu signalizáciu. [13]



Obr. 4 Vnútorná architektúra SBC

SBC sa delí na podnikové, prístupové a peering SBC (Obr. 5). Podnikové SBC je štandardné SBC, ktoré oddeľuje internú sieť firmy od operátora. To je pripojené k prístupovému SBC, ktoré má už v správe VoIP operátor. Peering SBC sú navzájom prepojení operátori.



Obr. 5 Typy SBC

SBC je zariadenie, ktoré disponuje niekoľkými funkciami [13][14]:

SIP Firewall

Vo svojej podstate je SBC akýmsi SIP firewallom, ktorý prepúšťa iba správne formátované SIP správy. Dokáže zastaviť DoS a DDoS útok, obsahuje white list a black list IP adries, monitoruje zlyhané pokusy o prihlásenie sa a poskytuje prevenciu proti zahlcovacím útokom.

Topology hiding

Jednou z ďalších výhod SBC je, že dokáže poskytnúť „topology hiding" - skrývanie topológie, ktoré funguje ako Network Addresses Translation (NAT). NAT nám zaistí mapovanie privátnej IP adresy na niekoľko málo verejných. To spôsobí, že vnútro siete je zvonku neviditeľné.

Interoperablita

Je to schopnosť rôznych systémov spolu vzájomne spolupracovať. SBC poskytuje možnosť meniť a manipulovať so SIP správami, ktoré cez neho prechádzajú. To znamená, že môže zmeniť obsah takejto správy manipulovaním hlavičiek. Táto funkcia sa využíva hlavne pri naviazaní komunikácie s rôznymi SIP telefónmi, servermi a trunkami od rôznych operátorov. Veľmi často sa stáva, že rôzne SIP siete majú svoj vlastný formát SIP signalizácie, a preto by siete spolu, bez nejakého prvku medzi nimi nedokázali navzájom dorozumievať. Netýka sa to len rôznych sietí, ale aj rôznych výrobcov (napríklad Cisco a Avaya).

Prekódovanie

Je jazykový preklad, ktorý je vyžadovaný vtedy ak sa medzi sieťami používajú rôzne jazykové prostriedky, ktoré chcú spolu komunikovať ale používajú rôzne jazyky. Napríklad zmena signalizácie H.323 na SIP alebo potreba zmeny z jedného kodeku na druhý (z G.729 na G.711). Ďalšie možnosti zahŕňajú preklad IPV6 na IPV4, SRTP na RTP alebo TLS na SIP.

Smerovanie hovorov

SBC dokáže taktiež smerovať SIP signalizáciu v sieti. Táto možnosť vie byť nápomocná ak v sieti používame viac ústrední alebo iných SIP prvkov.

Dynamická manipulácia signalizácie

SBC používa dynamickú manipuláciu SIP signalizačných správ, ktorá dovoľuje pridať, zmeniť alebo vymazať ľubovoľnú SIP hlavičku v SIP správe. Táto funkcia sa v Avaya SCB využíva pomocou skriptovacieho jazyka zvaný SigMa.

2.1 Potreba SBC

Potreba SBC sa nemusí primárne vzťahovať len na bezpečnosť. To je len jedna z funkcií, ktoré SBC ponúka. V čom sa teda líši klasické SBC od firewallu? Tradičný firewall nedokáže zabrániť zahlteniu ústredne SIP požiadavkami, otvárať a zatvárať média porty podľa SIP signalizácie, sledovať stav relácie. Nedokáže zabezpečiť kompatibilitu medzi rôznymi SIP sieťami. V konečnom dôsledku závisí potreba SBC len na danej organizácii. Predsa len sa jedná o určitú finančnú položku. Dôvody potreby SBC sa preto pokúsim stručne popísať v nasledujúcich podkapitolách.

Na potrebu SBC sa pozriem z dvoch hlavných pohľadov. Tieto dva pohľady sa delia na úrovne NNI a UNI.

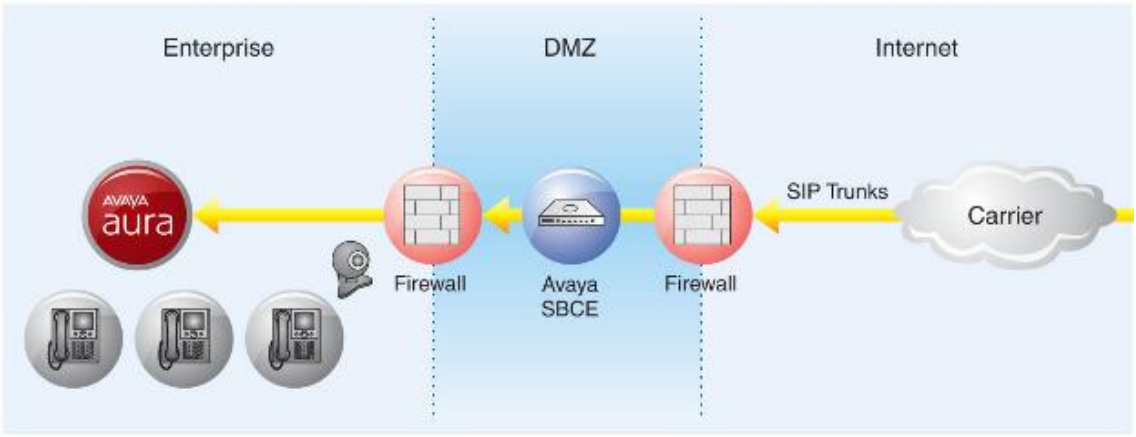
2.1.1 NNI - SIP trunk k operátorovi

SIP trunk sa stáva čoraz obľúbenejším spôsobom pripojenia k operátorovi a postupne nahrádza drahé tradičné telefónne linky T1/E1. Takto dosiahne firma ten istý výsledok za menej peňazí. Jediným problémom ostáva iba bezpečnosť, na ktorú sa pri SIP trunku kladie oveľa väčší dôraz.

Niektoré firmy sú ešte aj teraz pripojené pomocou T1/E1 liniek, pretože neveria IP telefónii a boja sa pripojiť svoju sieť do verejnej siete. Chcú mať bezpečnosť siete pod kontrolou aspoň takto. Toto riešenie je ale oproti SIP tunku drahšie. Preto pri správnom zabezpečení siete pomocou SBC je možné mať zabezpečené pripojenie a k tomu aj ušetriť peniaze za tieto linky.

Bezpečnosť SIP trunku

Dnes si asi nikto nedokáže predstaviť, že by pripojil svoju privátnu sieť do tej verejnej bez toho, aby medzi toto spojene vložil nejaký firewall. Takéto pripojenie by predstavovalo riziko útoku a to isté platí aj pre SIP. Nákup nového SBC zhltne určitú položku vo finančnom rozpočte. Niektoré firmy si poriadne premyslia či túto položku do svojho finančného rozpočtu vôbec zahrnú a budú vznikať rôzne argumenty proti nasadeniu SBC. Niekto by sa vedel obhájiť aj tým, že je pripojený k operátorovi, ktorý ho dokáže ochrániť. To je sčasti pravda, takýto operátor disponuje schopnosťou odhaliť a včas zamedziť nejakým druhom útokov (hlavne DoS/DDoS). Prečo sa ale spoliehať len na operátora, ak je možnosť mať bezpečnosť svojej siete vo vlastných rukách, ktorá je ešte znásobená tým, že o túto bezpečnosť sa stará aj operátor?

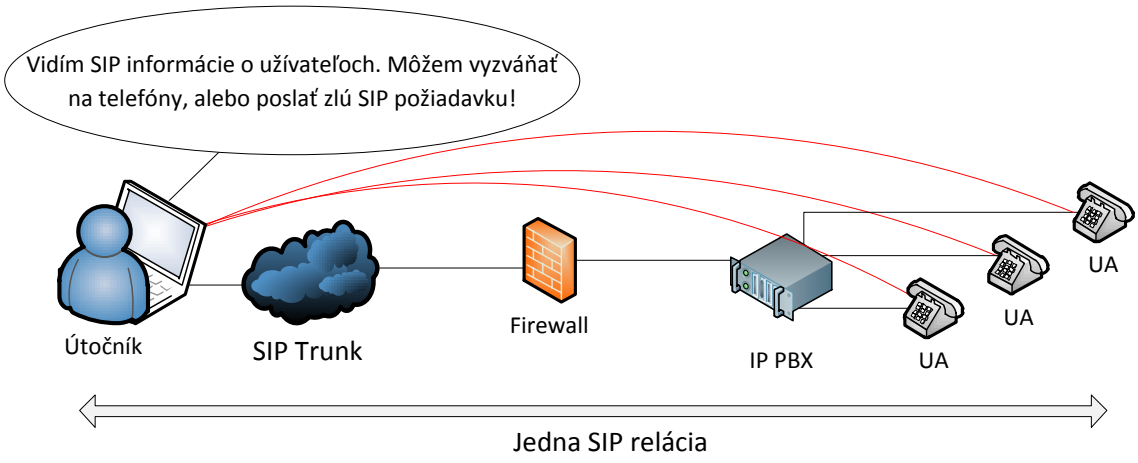


Obr. 6 SIP trunk [15]

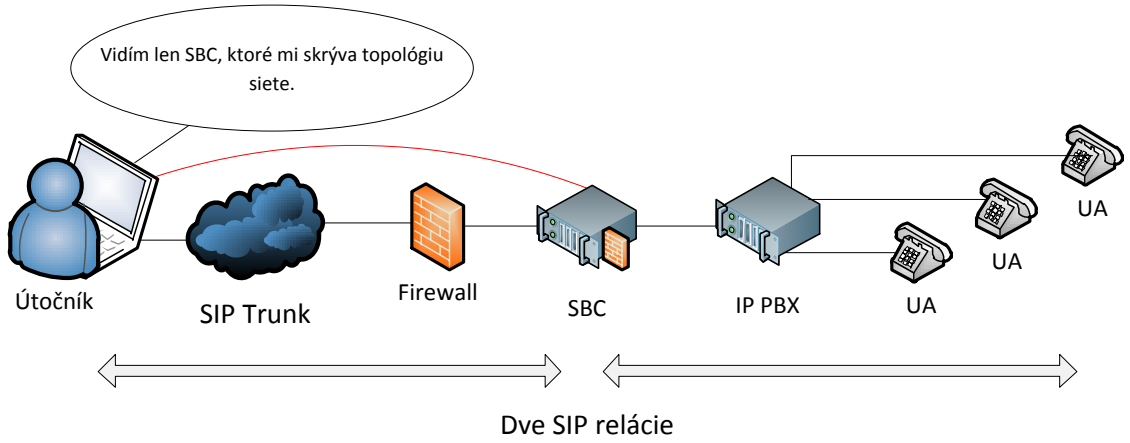
Porovnávaním sieťovej bezpečnosti s VoIP bezpečnosťou je vidieť, že tá VoIP je iná. Nasadením firewallu je možné zamedziť útokom orientovaným na tretiu a štvrtú vrstvu OSI modelu. Keďže SIP je určený pracovať na najvyššej aplikačnej vrstve, tak takýto útok firewall nedokáže ochrániť. Je potrebné si uvedomiť, že bezpečnosť VoIP sa od tej klasickej líši. Vystavením nechránenej VoIP siete do internetu vzniká riziko toho, že útočník dokáže zo SIP hlavičiek vyčítať o sieti kľúčové informácie. Tieto informácie môže ľahko použiť k napadnutiu. Zachytením hocijakej SIP relácie ju môže odpočúvať, pozmeniť, posielať škodlivé požiadavky alebo len tak vyzváňať na telefóny.

Čo sa teda stane ak na hranicu siete príde SBC? Z pohľadu bezpečnosti to, že útočník už nebude schopný prečítať a istým spôsobom zneužiť informácie zo SIP správ, ktoré z internej siete odchádzajú. SBC pozmení SIP hlavičky tak, že ich nahradí za také, ktoré pre útočníka nebudú mať nijakú hodnotu. V prípade, že by tam to SBC nebolo je útočník schopný vidieť určité detaily o volajúcom, napríklad jeho IP adresu. Na tú potom môže záškodnícky vyzváňať. Naopak, v prípade, že je SBC nasadené bude útočník vidieť len IP adresu SBC a všetko ostatné bude pre neho skryté.

Dôvodom je to, že pri použití SBC sa bude jeden hovor fyzicky skladať z dvoch relácií. Útočník bude vidieť len reláciu po hranicu SBC, tá druhá, ktorá obsahuje cenné informácie o infraštruktúre vnútornej siete, bude pre neho vďaka tej druhej relácii utajená.



Obr. 7 Útok z pohľadu útočníka bez SBC



Obr. 8 Útok z pohľadu útočníka s nasadeným SBC

Funkčnosť

V niektorých prípadoch nemusí byť použité SBC len kvôli bezpečnosti. Potreba SBC vychádza taktiež aj z hľadiska funkčnosti. Pretože vďaka SBC je možné používať všetky funkcie popísané v kap. 2, a tak isto aj funkcie z nich vychádzajúce napr.:

- UDP/TLS – TLS s operátorom, UDP v sieti,
- spracovanie viacerých registrácií od účastníka zatiaľ čo voči ústredni sa zaregistruje len raz,
- v niektorých SBC je možné aj účtovať hovory,
- nastavenie určitého maximálneho počtu hovorov od daného užívateľa.

2.1.2 UNI - Remote workers

Komunikácia je jeden z najvýraznejších faktorov úspešnosti firmy. Ocitáme sa vo svete kedy sa jeden človek nedokáže postarať o celý komplexný projekt. Určite bude potrebovať pomoc od ostatných ľudí, a preto s nimi musí ostať v kontakte.

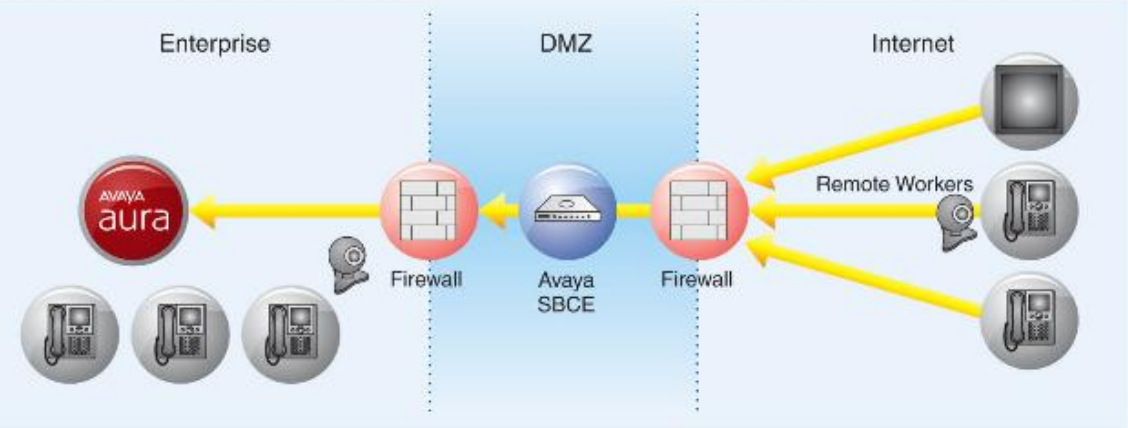
Firma, v ktorej spolu zamestnanci môžu pohodlne komunikovať má vysoké predpoklady rastu. Komunikácia nebude problém ak sa títo ľudia budú každý deň osobne stretávať alebo budú aspoň v jednej budove, kde náklady na komunikáciu sú zanedbateľné. Takýto svet ale začína byť postupne minulosťou. Ľudia začínajú viac cestovať a vzďaľovať sa od sídla firmy i na druhú stranu planéty. V tomto bode sa začína komunikácia zhoršovať a ľudia sú nútení využívať relatívne lacné internetové spojenie a s ním spojenú technológiu VoIP. To prináša radu bezpečnostných rizík.

V predchádzajúcom prípade bolo použitie SBC otázne, ale odôvodnené. V tomto prípade, kedy sa firma rozhodne využiť funkčnosť protokolu SIP, ktorou je vzdialený prístup k firemnej SIP sieti, tak použitie SBC je nutnosťou. SBC bude jediné zariadenie, ktoré bude stáť medzi internetom a privátnou sieťou alebo medzi potenciálne nebezpečným zariadením a ústredňou.

Možnosti protokolu SIP sa stále vyvíjajú a s tým sa vyvíja aj firemná komunikácia, kde firemný zamestnanci často pracujú z domu alebo si nosia do práce vlastné zariadenia (BYOD). Tento vzrastajúci trend je vo svete SIP novinkou a pestrým rozšírením možností modernej firmy, ale zároveň aj veľkou bezpečnostnou hrozbou.

Túto situáciu popisuje nasledujúci príklad, v ktorom firemný zamestnanec pracujúci z domu alebo na služobnej ceste potrebuje komunikovať so svojím kolegom v tej istej firme. Doteraz mohol disponovať zvýhodneným paušálom od operátora, ale pri väčšom počte takýchto zamestnancov to už nemusí byť pre firmu zanedbateľná položka. Firemný zamestnanec bude mať s veľkou pravdepodobnosťou prístup k internetu. Populárnou možnosťou je použitie virtuálnej privátnej siete, tzv. VPN, táto možnosť je ale nepraktická pretože sa vzťahuje na celé zariadenie, s ktorým sa pripájame k sieti. SIP preto ponúka možnosť, tzv. remote worker, kde firemný zamestnanec sa so svojím SIP klientom zo svojho vlastného počítača a so svojím internetovým pripojením prihlási do firemnej siete a bez žiadnych ďalších finančných nákladov komunikuje s ostatnými zamestnancami firmy.

Takýto SIP klient sa registruje pomocou internetu na SBC, ktoré túto SIP registráciu skontroluje a predá ďalej ústredni, v tomto prípade to bude Avaya Aura Session Manager. Týmto odpadá potreba VPN SIP komunikácie, zjednoduší sa vzdialený prístup k sieti a otvoria sa nové možnosti firmy. V konečnom dôsledku sem okrem volania patria aj videohovory, prezenčný systém, zdieľanie plochy, konferencie a videokonferencie.



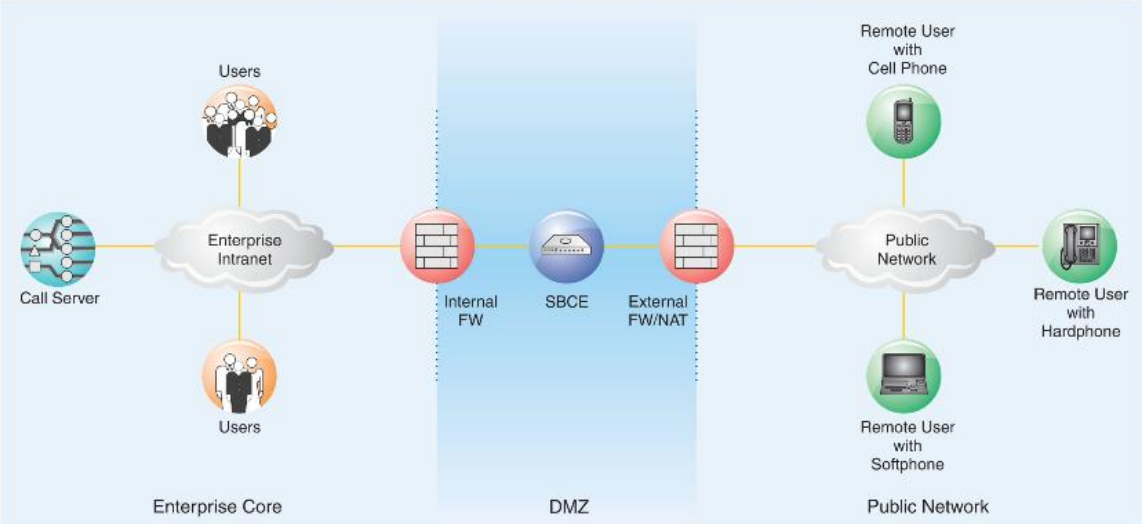
Obr. 9 Remote Workers [15]

2.2 Možnosti zapojenia SBC

Architektúra siete i uloženie SBC je dôležitým prvkom. SBC je možné zapojiť ako Two-wire a One-wire. Výber vhodnej topológie závisí od bezpečnostných potrieb a požiadaviek organizácie. Žiadne z týchto zapojení nepridáva zbytočnú latenciu. Obe zapojenia je z bezpečnostného hľadiska potrebné vložiť do DMZ. [15]

2.2.1 Topológia Two-wire

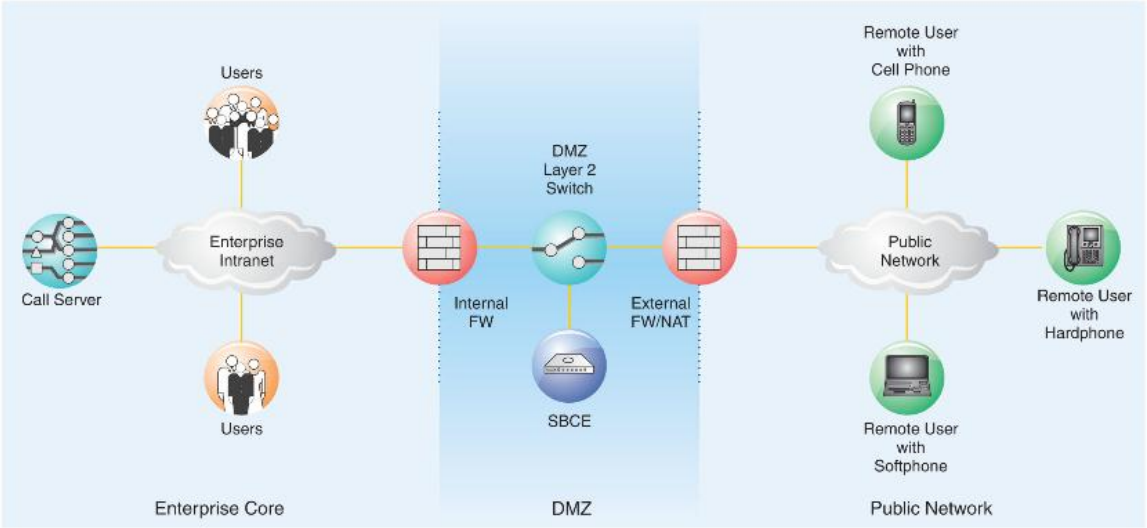
V Táto topológia je jedna z najjednoduchších a najzákladnejších možností, ako zapojiť SBC. To je umiestnené v DMZ medzi interným a externým firewallom - priamo na linke medzi ústredňou a internetom. V tomto prípade ponúka SBC hraničnú kontrolu SIP prevádzky. Zahŕňa SIP firewall, NAT, spravovanie a kontrola prístupu. Tieto funkcie sú založené na bezpečnostných opatreniach firmy. Nezávisle na nich je táto topológia schopná chrániť aj proti útokom ako DoS, spoofing, stealth útoky a hlasový SPAM. [15]



Obr. 10 Zapojenie Two-wire [15]

2.2.2 Topológia One-wire

V topológií typu One-wire je SBC tak isto uložené v DMZ, ale od predchádzajúceho zapojenia sa líši v uložení, a to že už nie je priamo na linke medzi ústredňou a verejnou sieťou. V tomto prípade je však SIP smerovanie nastavené tak, aby všetky SIP komunikácia prechádzala cez SBC. [15]

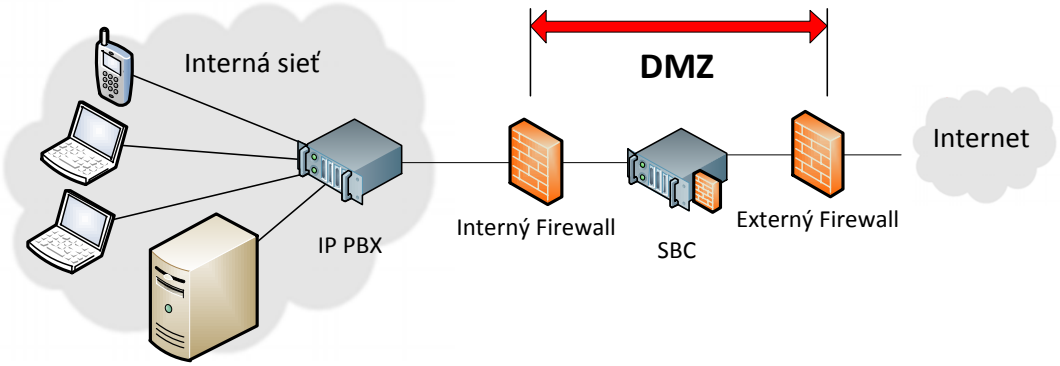


Obr. 11 Zapojenie One-wire [15]

2.2.3 Demilitarized Zone - DMZ

DMZ je fyzická alebo logická podsieť a znamená demilitarizovanú zónu. Dôvodom použitia DMZ je zvýšenie bezpečnosti.

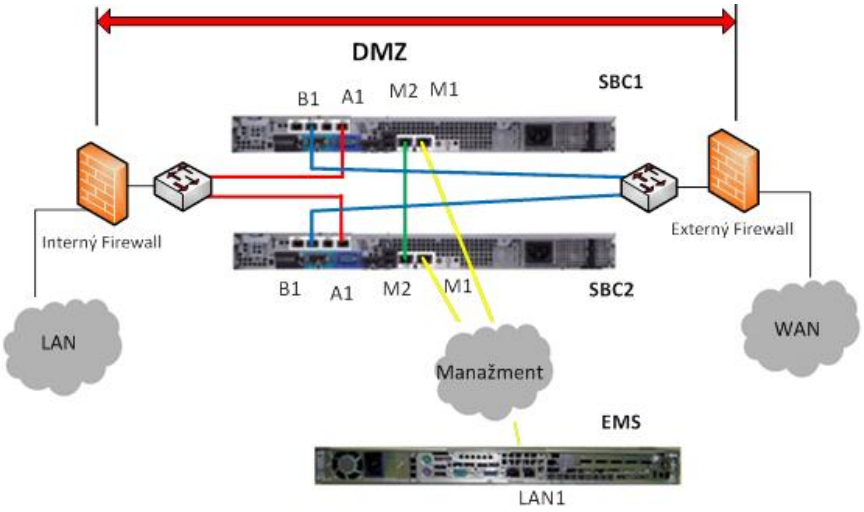
Ide o podsieť, ktorá síce patrí k organizácii, ale je to izolovaná sieť, ktorá oddeľuje LAN od WAN. Je to sieť, do ktorej sa vložia servery, ktoré potrebujú priamo komunikovať s externou nedôveryhodnou WAN sieťou. V prípade mojej diplomovej práce sa to týka SBC, ktoré tu bude uložené. Táto sieť síce bude chránená firewallom, ale stále má priamy prístup k internetu. To znamená, že ak aj náhodou bude kompromitovaná útočníkom zvonku, tak internej sieti sa nič nestane, tá bude aj naďalej funkčná. Výhodou DMZ je taktiež priama kontrola nad servermi v nej. [16]



Obr. 12 DMZ

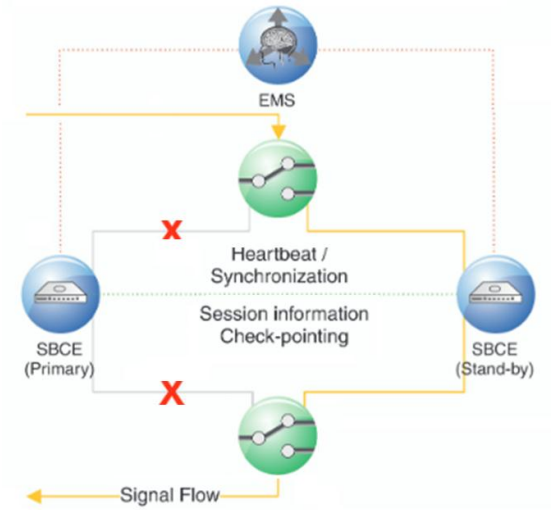
2.2.4 SBC High Availability (HA)

Väčšina SBC môže byť nakonfigurovaná v dvoch módoch. Pre jednoduchosť som sa doteraz zaoberal len jedným z nich tzv. standalone. Celú prácu vykonáva len jeden hardware a v prípade poruchy alebo nečakaného výpadku SBC môže byť celá komunikácia prechádzajúca práve cez toto SBC v ohrození alebo stratená.



Obr. 13 Detailné zapojenie Avaya Aura SBCE v HA [15]

Druhý mód je High Availability konfigurácia, kde celé SBC pozostáva z dvoch rovnako nakonfigurovaných serverov a tretieho (EMS), ktorý tieto dva spravuje a synchronizuje. Celá prevádzka prechádza cez oba SBC servery, kde jeden je aktívny a druhý je jeho kópia v reálnom čase. Tieto dva SBC majú rovnako nakonfigurované verejné a privátne adresy, avšak tie sú používané len v aktívnom SBC. V dobe kedy nastane výpadok aktívneho SBC, druhé v okamihu schopného prevziať IP adresy a následne aj kontrolu nad všetkou práve prebiehajúcou komunikáciou. [15]



Obr. 14 Zjednodušené zapojenie v HA [15]

2.3 Vyber správneho SBC

Existuje niekoľko kritérií podľa ktorých je možné si vybrať to správne SBC. SBC je relatívne nový produkt a keďže nie je presne štandardizovaný, tak všetci výrobcovia disponujú veľkou voľnosťou pri jeho dizajne.

Asi najdôležitejším kritériom pri výbere bude kapacita SBC. Ide o počet súbežných hovorov, ktoré je schopné SBC odbaviť. Na trhu sa SBC, podľa kapacity, delia do troch kategórií. Kategória pre malé, stredné a pre veľké firmy. Pre predstavu sa rozsahy počtov relácií pre malé firmy pohybujú od 96 - 500. Pre stredné od 500 do 6 000. SBC s najväčšou kapacitou sú od 6 000 do 64 000. Každý výrobca ponúka SBC s rôznym počtom relácií.

Ďalšími kritériami by mohla byť funkčnosť SBC či ponuka HA alebo šifrovanie hlasu a signalizácie. Otázkou môžu byť aj použité kodeky, ktoré SBC podporuje alebo či vie previesť H.323 signalizáciu do SIP. Tiež ako vyzerá manažment SBC či je jednoduché ho konfigurovať napríklad cez webové rozhranie alebo sa konfiguruje cez príkazový riadok. S konfiguráciu ide ruka v ruke otázka podpory od výrobcu. [17]

Významnú úlohu zohráva samozrejme aj bezpečnosť a spôsob akým je schopné zvládnuť útoky. Do úvahy prichádza aj možnosť nastavenia prahovej hranice pri DoS útokoch a následné informovanie o podozrivom správaní sa v sieti. Správny výber preto výrazne závisí od požiadaviek zákazníka. Myslím si, že dobrým porozumením potrieb zákazníka a možnosti dostupných SBC sa dá dospieť k tým najdôležitejším kritériám pre danú firmu. [17]

Najznámejšími výrobcami SBC, ku ktorým som sa dopátral sú: Avaya, AudioCodes, Genband, Sonus, Cisco, Acme, Mediant, Edgewater Networks, Frafos a Squire Technologies. Každý z nich ponúka niekoľko SBC produktov, ktorými sa snaží pokryť trh čo najširšie.

3 Avaya Aura architektúra

Avaya Aura je názov komunikačného riešenia od firmy Avaya, ktoré predstavuje komunikáciu zabezpečenú pomocou protokolu SIP. Poskytuje tzv. „Unnified communication“ (UC) čo z anglického názvu znamená *zjednotenú komunikáciu*.

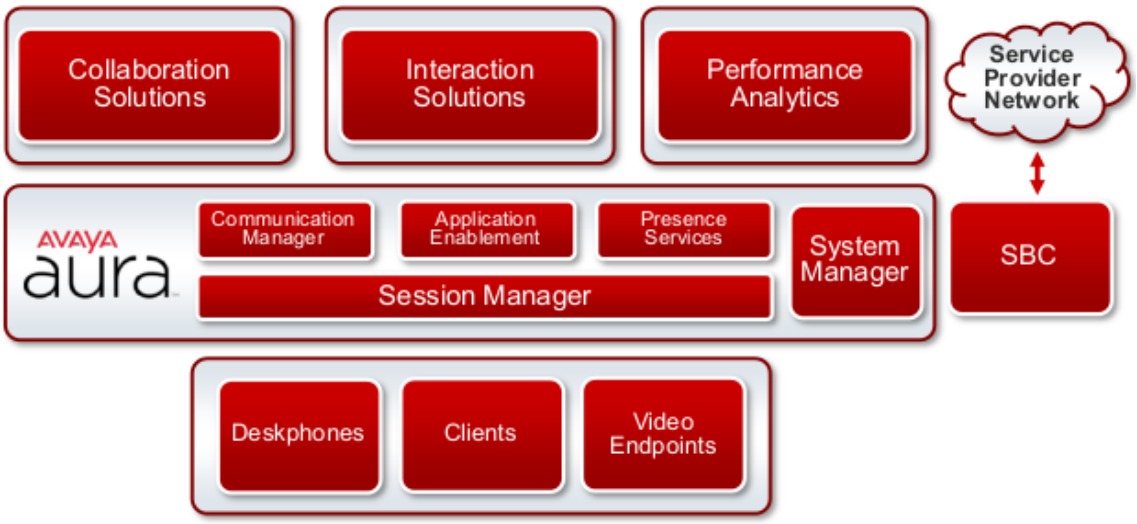
UC pozostáva z komunikácie v reálnom čase k čomu patrí: posielanie rýchlych správ (chat), prezencia, VoIP, videokonferencia, zdieľanie plochy, zdieľanie dát, kontrola hovorov, rozpoznávanie reči. Do komunikácie, ktorá neprebieha v reálnom čase patrí: hlasová schránka, e-mail, SMS a fax. Zároveň podporuje aj H.323 telefoniu. [18]

Avaya Aura architektúra sa skladá z piatich základných serverov: Communication Manager, Application Enablement, Presence, System Manager a Session Manager. Zaoberal som sa len dvoma z nich - System Manager a Session Manager, ktoré mi k zabezpečeniu obyčajného telefónneho spojenia medzi pár klientmi úplne stačilo. V sieti som mal dva SM zapojené v HA, ktoré boli manažované z pomocou SMGR.

Prístup k týmto serverom som získali od firmy Algotech, ktoré už boli nasadené a pripojené do testovacej prevádzky. Prvým krokom bolo spoznávanie a možnosti nastavenia celej tejto architektúry. K ďalším testom bolo potrebné nainštalovať, nastaviť a k celej sieti pripojiť Session Border Controller (SBC).

Všetky tieto servery používajú operačný systém Red Hat Enterprise Linux, ktorého bezpečnosť bola firmou Avaya vylepšená, a to odstránením nepoužívaných Red Hat Packet Management (RPM) balíčkov. Dôvodom je to, že IP telefónia od firmy Avaya nevyžaduje všetky RPM poskytované Red Hat-om, ktoré by mohli byť bezpečnostnou hrozbou.

K zisteniu všetkých RPM balíčkov, ktoré sú v danom serveri použité je možné použiť príkaz *rmp-qa*. Kvôli minimalizácii sieťovo založených útokov sú povolené len porty potrebné k telefónnym aplikáciám. Už v základe sú vypnuté menej bezpečné služby ako napríklad TELNET a FTP, ktoré prenášajú nezašifrované prihlasovacie údaje. Namiesto nich sú použité SSH, SCP a SFTP. Taktiež nie je možné použiť štandardnú kombináciu kláves CTRL-ALT-DELETE k reštartovaniu servera. [19]



Obr. 15 Avaya Aura architektúra

Tab. 2 Špecifikácie Avaya Aura podľa jednotlivých verzií [20]

Kapacita/počet	Maximálny limit			
	Release 6.0	Release 6.1	Release 6.2	Release 6.3.8
Celkový počet SIP používateľov	50 000	100 000	100 000	125 000
SIP koncové zariadenia	100 000	100 000	250 000	250 000
Počet používateľov na SM	10 000	12 000	12 000	12 000
Počet používateľov na CM	18 000	18 000	36 000	35 000
Používatelia z funkciou Shared Control na SM	1 000	7 500	7 500	7 500
Počet SM	6	10	10	12
Simultánne relácie	65 000	80 000	90 000	90 000
Registrácie za sekundu na SM	N/A	N/A	800	800
Počet CM	500	500	500	500
Počet SIP domén	1 000	1 000	1 000	1 000
Dial pattern/Smerovanie	250 000	300 000	300 000	300 000

3.1 Avaya Aura Session Border Controller for Enterprise

Avaya Session Border Controller for Enterprise (SBCE) nepatrí síce priamo do Avaya Aura architektúry, no je jedným z jej bezpečnostných prvkov, ktorý zabezpečuje komunikáciu v reálnom čase smerujúcu za hranice internej siete. Poskytuje niekoľko zabezpečovacích mechanizmov a pracuje v dvoch typoch prevádzky. Jedným je SIP trunk a tým druhým je tzv. „remote worker“ - vzdialené pripojenie, ktoré rozširuje komunikačné možnosti firmy a tu patrí aj trend BYOD. Vo svojej podstate je SBCE akýmsi doplnkom do Avaya Aura architektúry, ktorý pridáva celému prostrediu ďalšie prídavné funkcie a zvyšuje jeho celkovú bezpečnosť.

Skladá sa z dvoch komponentov [21]: Avaya SBCE a Avaya Element Management System (EMS). V závislosti na veľkosti siete a požiadaviek služby je možné rozmiestniť SBCE buď do tzv. „standalone“ konfigurácie, kde je Avaya SBCE a EMS na tom istom fyzickom serveri. Potom je tu konfigurácia typu „multiple server,“ kde sú EMS a Avaya SBC rozdelené na dva fyzické servery. Takéto EMS dokáže spravovať aj viacero Avaya SBCE v sieti. Nakoniec existuje aj možnosť HA konfigurácie (kap. 2.2.4) kedy je potrebné mať dva servery pre Avaya SBCE (primárny a sekundárny) a jeden pre EMS. [21]

3.1.1 Funkcie Avaya SBCE

Z funkčného hľadiska sa Avaya SBCE delí na časť spracovávajúcu signalizáciu a na časť, ktorá spracováva média (Obr. 4). Signalizačná časť vytvára 2 ms latenciu na celkovej signalizačnej trase End-to-End (Obr. 2) a stará sa o funkcie akými sú šifrovanie TLS, manažment bezpečnostných kľúčov, overovanie SIP správ, ochrana internej siete, QoS a v neposlednom rade aj smerovanie do rôznych ústrední v sieti. Časť, ktorá spracováva média je zodpovedná za ich riadenie a správu (napr. správa použitých kodekov, šifrovania SRTP alebo detekcia anomálií v RTP prenose). [21]

Tab. 3 Parametre počtu konkurenčných hovorov pre Avaya SBCE [15]

	Trunk		Remote Workers	
	Nezašifrované	Zašifrované	Nezašifrované	Zašifrované
Počet konkurenčných hovorov	5000	1000	2000	1000

Tieto špecifikácie z Tab. 3 podľa [15] platia za predpokladu, že:

- parametre servera - Dell PowerEdge R210 II, štvorjadrový procesor Intel Xeon E3-1220 (3,1GHz, 8MB cache), 8GB DDR3 1600MHz (až 32GB), 6x1Gb Ethernet,
- špecifikovaný kodek – kodek G711 s 20ms paketovým intervalom a všetky relácie sú audio relácie,
- model hovoru – použitý model SIP RFC pre model hovoru v trunkovom type prevádzky,
- konfigurácia Avaya SBCE – sú použité iba základné nastavenia a všetky bezpečnostné mechanizmy sú vypnuté.

3.1.2 Bezpečnostné špecifikácie Avaya SBCE

Bezpečnostný produkt od firmy Avaya chráni pred nasledujúcimi útokmi [22]:

- neoprávnený prístup alebo modifikácia správ,
- odcudzenie dát,
- DoS útoky,
- vírusy a červy.

K zabráneniu týmto hrozbám je použitá stratégia skladajúca za z troch bezpečnostných častí, ktorými sú: bezpečnosť návrhu, základné zabezpečenie a zabezpečenie komunikácie. [22]

Bezpečnosť návrhu

Bezpečnosť návrhu spočíva v rozdelení sietí do bezpečnostných zón, respektíve do rôznych jednoúčelových LAN alebo VLAN sietí pre určitú funkciu [19]:

- manažment sieť – manažment rozhranie SBC, ktoré slúži na konfiguráciu celého SBC,
- verejná sieť – PSTN alebo internet,
- privátna sieť – vnútorná sieť firmy.

Tieto rôzne bezpečnostné zóny nepotrebujú a nemali by byť medzi sebou prepojené, pretože každá z nich je určená k prenášaniu špecifického typu dát.

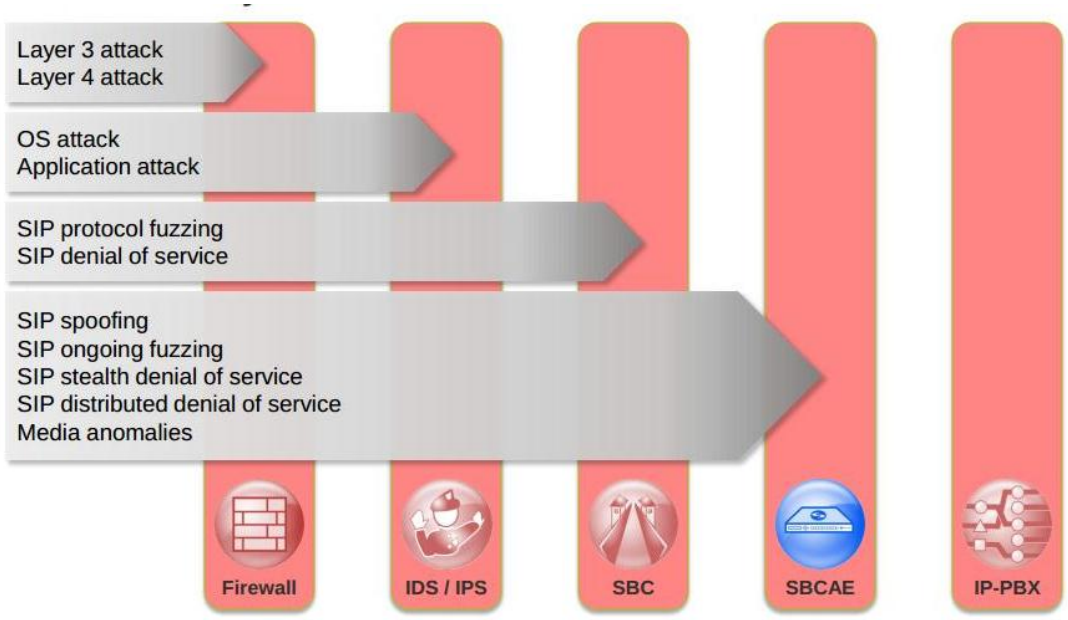
Základné zabezpečenie

Toto zabezpečenie sa týka operačného systému. Tým je v prípade Avaya SBCE Red Hat Enterprise Linux, ktorý nedisponuje žiadnymi nadbytočnými funkciami. Má len limitovaný počet portov a služieb, ktoré sú potrebné pre telefónne aplikácie, a ktoré závisia od počtu pripojených účastníkov. Takáto redukcia nepotrebných funkcií prispieva k zníženiu počtu bezpečnostných aktualizácií a záplat. [19]

Zabezpečenie komunikácie

Komunikácia môže byť zabezpečená šifrovaním (signalizácie a médií) a to konkrétne TLS/SRTP alebo kontrolou prístupu. Kritéria použité pre kontrolu prístupu zahŕňajú zdrojovú podsieť, účastníka, URI skupinu alebo konkrétnu použitú SIP aplikáciu. [19]

V prípade šifrovania médií pomocou SRTP Avaya SBCE podporuje prechod z práve šifrovaného SRTP na RTP, a to z dôvodu nízkej šírky pásma alebo v prípade keď to cieľový server nepodporuje. Podporuje aj opačný prechod z RTP na SRTP a modifikáciu kľúčov pomocou REINVITE. [21]



Obr. 16 Ochrana IP-PBX pred útokmi

Avaya SBCE ako bezpečnostný produkt zaisťuje integritu všetkých IP aplikácií v reálnom čase. Stará sa o celkovú bezpečnosť celej Avaya Aura architektúry, spoľahlivosť a dostupnosť, a to pomocou nasledujúcich troch funkcií [15]:

- **Monitorovanie** - poskytovanie kompletného bezpečnostného monitorovania, ktoré zahŕňa všetky aspekty UC siete vrátane koncových zariadení, ústrední, média brán a aplikačných serverov. K monitorovaniu poskytuje grafické rozhranie, ktoré sa nazýva EMS Web Interface. Toto rozhranie potom monitoruje a koordinuje bezpečnostné aktivity všetkých Avaya SBCE v sieti.
- **Detekcia** - detekčné schopnosti dynamických a adaptívnych algoritmov k detegovaniu rôznych anomálií v sieti. Detekcia týchto anomálií sa vzťahuje pre rôzne časové úseky dňa (dopoludnie, predpoludnie, noc) a víkendu. Sem spadá aj detekcia anomálií v obsahu SIP signalizačných správ.
- **Ochrana** - ide o poskytovanie ochrany blokovaním útokov zatiaľ čo je platná SIP komunikácia prepúšťaná ďalej.

Taktiež chráni pred útokmi tretej, štvrtej vrstvy a skenovaniu portov. Napríklad zahŕňa IP firewall, ktorý zabráni preniknutiu neželanej prevádzky do vnútra siete. Ďalej disponuje prevenciou zahltenia paketmi ICMP alebo TCP SYN, kde v prípade detekcie zablokuje po určitý čas zdroj takéhoto útoku. Tak isto po špecifickú dobu zablokuje účastníka, ktorý zahájil skenovanie dostupných portov v SBC. [21]

Tab. 4 Zoznam použitých portov [22]

Rozhranie	Pripojenie	Služba	Protokol	Port
Verejný Interface	SIP UA	Web Conf.	TCP	843
		LDAP	TCP	636
		LDAPs	TCP	636
		SIP	TCP/UDP	5060
		SIP	TLS	5061
		Média	RTP	35000-40000
		IM	TCP	5222
		FW Download	HTTP	80
		FW Download	HTTPS	443
		PPM	HTTP	80
		PPM	HTTPS	443
	SIP PSTN Provider	SIP	TCP/UDP	5060
		SIP	TLS	5061
Privátny Interface	SM SIP Proxy / Access Elements /PPM	SIP	TCP/UDP	5060
		SIP	TLS	5061
		PPM	HTTP	80
		PPM	HTTPS	443
	Media Gateways / Phones	Media	RTP	35000-40000
	Web Conf. Server	Web Conf.	TCP	843
	Utility Server		HTTP	80
			HTTPS	443
Manažment Interface	EMS	NTP	UDP	123
		Syslog	TCP/UDP	514
		Open VPN	UDP	1194
		HTTPS	TCP	443
		SSH	TCP	222
	DNS Server		TCP/UDP	53
	Syslog Server		TCP/UDP	514
	Admin Terminal	SSH	TCP	222
		HTTPS	TCP	443
	SNMP		UDP	161
			UDP	162

Dôležitým bezpečnostným prvkom je zabezpečenie proti DoS/DDoS útokom. Toto zabezpečenie sa vzťahuje buď k typu prevádzky, a to k remote workers, ku SIP trunku alebo jedno pravidlo vzťahujúce sa zároveň k obom typom prevádzky. Ďalším prvkom je aj zakrytie topológie, ktoré zmení kľúčové parametre SIP správy, aby znemožnil neautorizovanému prístupu útočníka k informáciám o sieti.

Do kategórie bezpečnosti patrí aj Protocol Scrubber, ktorý kontroluje prichádzajúcu prevádzku použitím štatistických mechanizmov a chráni pred škodlivými alebo zle formátovanými správami. Protocol Scrubber overuje napríklad sekvenciu správ, formátovanie správ, kontroluje dĺžku jednotlivých hlavičiek. Správy, ktoré Protocol Scrubber vyhodnotí ako chybné a zároveň škodlivé budú zahodené. Naopak správy, ktoré sú chybné, a ktoré nevyhodnotí ako škodlivé budú opravné. Tieto pravidlá sa vzťahujú na použitý typ prevádzky (SIP trunk alebo remote workers) a sú pripravené spoločnosťou Avaya, užívateľ ich môže meniť len minimálne. Avšak je dovolené inštalovať prídavné Protocol Scrubber balíčky. [21]

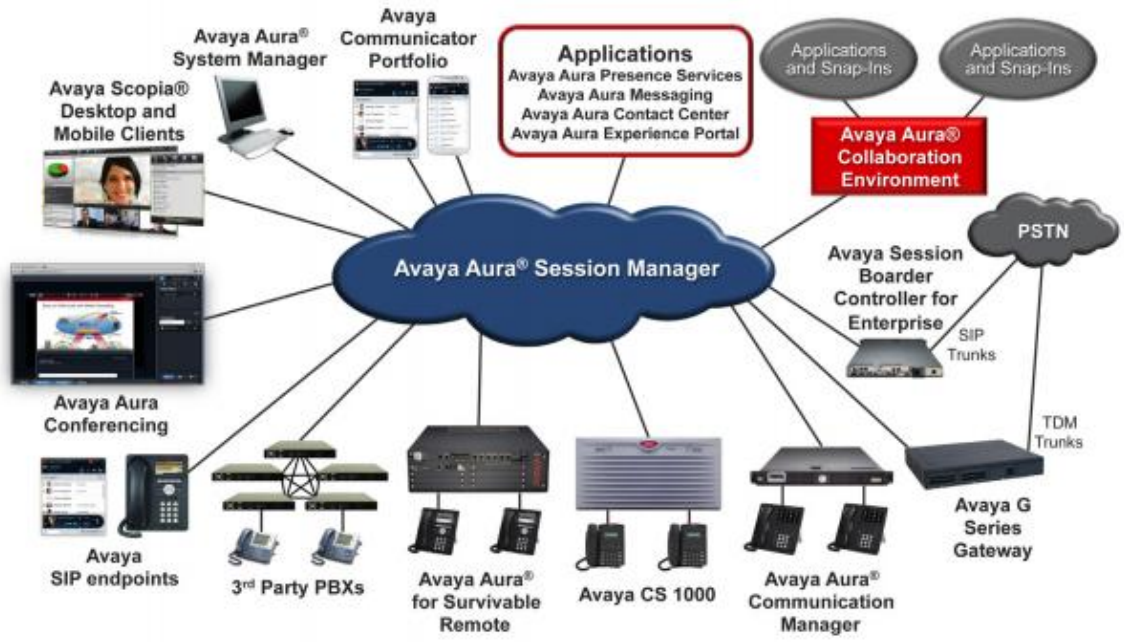
Tab. 5 Inštalované Scrubber balíčky v Avaya SBCE [21]

Balíček	Popis	Použitie v SBC móde
SPKF0001 - Syntax	Pravidlá založené na RFC 3261	Trunk
SPKF0002 - Protos	Pravidlá založená na teste SIP Protos	Trunk, Remote worker
SPKF0003 - OCS	Pravidlá pre MS OCS/MS Lync	-
SPKF0004 - Avaya	Pravidlá pre Avaya	Remote worker

3.2 Avaya Aura Session Manager

Vo firemnom prostredí môže byť spravovanie VoIP komunikácií v reálnom čase komplikované a drahé, a to najmä vtedy, ak organizácia používa niekoľko komunikačných ústrední, ktorých vzájomné prepojenie môže byť zložité.

Session Manager (SM) dokáže spravovať pripojenia ku všetkým týmto ústredňam a SIP aplikáciám. Session Manager (SM) je SIP telefónna ústredňa, ktorá naprieč celou sieťou spravuje účastníkov, aplikácie, ostatné ústredne a všetku komunikáciu medzi nimi. Spolupracuje s ostatými ústredňami v sieti a účastníkom poskytuje pripojenie a komunikáciu v reálnom čase bez ohľadu na to, kde sa v sieti nachádzajú. SM je v sieti SIP Proxy a zároveň aj Registrar serverom. Taktiež ide o kľúčový prvok, ktorý vystupuje z radu obyčajnej telefónie a posúva sieť k Unnified Communications.



Obr. 17 SM ako centrum SIP siete [20]

Poskytuje smerovanie hovorov medzi rôznymi poskytovateľmi služieb, a to na základe číslovacieho plánu alebo IP adresy. Smerovanie hovorov je možné nastaviť podľa záťaže siete, poruchy siete alebo doby kedy sú hovory uskutočnené. Podľa time-of-day a time-of-week smeruje hovory na základe najnižšej ceny. To má názov *Least-cost routing*. V prípade nejakej poruchy v sieti vyberá alternatívne smerovanie (*Alternate routing).* Nakoniec disponuje ešte funkciami rovnomerného rozdelenia záťaže (*Load ballancing*) a presmerovaním hovorov kedy je vyčerpaná šírka pásma danej linky (*Call admission control*). Taktiež poskytuje, respektíve, doručuje aplikácie naprieč celou sieťou. [23]

Spravuje číslovacie plány, poskytuje rôzne monitorovacie nástroje, napríklad status pripojených SIP entít, komunikačné profily všetkých užívateľov a indikácia registrácie užívateľa, spravovanie použitia šírky pásma. K SM patria aj systémové nástroje akým je SIP trace a SIP monitoring.

Tento SM je možné použiť v stredne veľkých a veľkých organizáciách, kde v prípade nedostatku výkonu jedného servera je možné pridávať ďalšie SM servery, a to až do počtu 12. Všetky tieto SM sú potom kvôli jednoduchosti spravované iba jediným SMGR.

Momentálne existujú 2 typy serverov, ktoré je možné použiť ako SM. Oba sú od firmy HP [23]:

- Avaya Common Servers Release 1- HP ProLiant DL360 G7 Power Edge R610 servers
  - je schopný spravovať 10 000 užívateľov počas bežnej prevádzky.
  - 100 relácií za sekundu (360 000 za hodinu)
  - 90 000 konkurenčných SIP relácií
- Avaya common Servers Release 1 - HP ProLiant DL360p G8 Power Edge R610 servers
  - je schopný spravovať 21 500užívateľov počas bežnej prevádzky.

- 150 relácií za sekundu (540 za hodinu)
- 160 konkurenčných SIP relácií

3.2.1 Bezpečnosť

Bezpečnosť sieťovej vrstvy

SM podporuje VLAN segregáciu SIP a SIP manažment sietí. SM má oddelené manažérske rozhranie k manažment komunikácii medzi SM a SMGR. SIP manažment rozhranie sa nachádza v inej VLAN ako obyčajné SIP rozhranie, tak isto nie je možné k nemu pristúpiť zo SIP siete. SMGR je prístupný len cez manažment VLAN.

SM používa IPTables sieťový firewall kvôli ochrane proti sieťovým DoS útokom a k otvoreniu všetkých používaných TCP/UDP portov. Nepoužívané porty sú už od základu zakázané. Firewall pravidlá sú nakonfigurované automaticky už počas inštalácie a poskytuje ochranu proti nasledujúcim sieťovým útokom [19]:

- TCP Syn Flood,
- IP Options,
- ICMP timestamps,
- ICMP Redirects,
- Source Routed Packets,
- Reverse Path Forwarding,
- neplatné IP pakety,
- škodlivé IP pakety.

Bezpečnosť SIP

SM používa firewall aj na aplikačnej vrstve k ochrane proti SIP DoS útokom. Všetka zašifrovaná prevádzka pomocou TLS je rozšifrovaná ešte predtým než prejde cez SIP firewall. Ten poskytuje nasledujúce akcie [19]:

- Flood - ochrana pred záplavou SIP správ od špecifického zdroja,
- Advanced Flood Protection - táto ochrana vie detekovať alebo zmierniť útok z práve prebiehajúcej sip komunikácie z vopred definovaných zdrojov útoku,
- Rate-Limiting - toto pravidlo nastavuje limitovanie počtu SIP správ v určitom časovom intervale pri určitej prekročenej prevádzke,
- Rate-Blocking - blokuje všetku prevádzku z útočiaceho SIP zdroja, a to v prípade keď prevádzka dosiahne určitú medznú hranicu,
- Signature detection - je možné nastaviť detekciu SIP správ, ktoré budú pri nájdení nejakého hľadaného výrazu zahodené. To platí pre hlavičku, tak ako aj pre telo SIP správy.

SIP firewall sleduje SIP správy. Pri prekročení daného množstva týchto správ za určitý čas je možné vo firewalle použiť jednu z definovaných akcií [19]. Počet týchto pravidiel nie je nijako zvlášť obmedzený. Jedno takéto SIP firewall pravidlo z Tab. 10 sa skladá z nasledujúcich častí, ktoré je možné navzájom nezávisle definovať. Týmito časťami sú [24]:

General

Tu sa povoľuje a zakazuje dané pravidlo, názov pravidla log (či to bude alarm alebo len záznam) a nakoniec Action type. V Action type je na výber z rôznych možností:

- No Action– žiadna akcia sa po pri aktivovaní pravidla nevykoná, táto možnosť sa používa v prípade, že chceme generovať alarm alebo záznam do logu,
- Permit – pri aktivovaní tejto akcie je prevádzka pustená ďalej cez firewall bez toho, aby bola nejako obmedzená,
- Drop – podľa nastavených treshold parametrov začne zahadzovať SIP prevádzku,
- Rate Block – podľa nastavených treshold parametrov začne blokovať SIP prevádzku,
- Rate Limit– podľa nastavených treshold parametrov začne limitovať SIP prevádzku.

IP Layer Match

Nastavenie SIP Firewallu, ktorý sa vzťahuje na Protocol (UDP, TLS, TCP), špecifickú IP adresu a rozsah portov.

SIP Layer Match

Tu je možné nastaviť to, ktoré SIP hlavičky (SIP telo) budú kontrolované a aký výraz sa v nich v nich bude hľadať. Hľadaný výraz je možné definovať ako string alebo regular expression.

IP/SIP Layer Match

Je možné nastaviť iba pri Rate Limit alebo Rate Blok. V tejto časti sa nastavuje to, čo bude SIP Firewall (aké hlavičky) sledovať:

- IP adresu
- Port
- From
- To
- Contact
- Request

Treshold

Nastavenie hraničných hodnôt, pri ktorých sa pravidlo aktivuje a doby, počas ktorej bude trvať.

Connections

Nastavenie dôveryhodnej, nedôveryhodnej SIP entity alebo o UA.

K zablokovaniu alebo povoleniu určitých IP adries má SM k dispozícií Blacklist a Whitelist.

Blakclist je možné použiť v prípade, známeho zdroja DoS útoku alebo nejakej škodlivej správy. Každá SIP správa prichádzajúca z IP adresy umiestnenej v Blackliste, bude zahodená, a to bez výraznejšieho vyťaženia CPU.

Whitelist je zas presný opak. Ten funguje tak, že každá SIP správa, ktorá prichádza z IP adresy v ňom uloženej bude posunutá ďalej na spracovanie, a to bez toho, aby boli aplikované ďalšie firewall pravidlá. Funkciu Whitelistu je možné použiť v prípade ak vieme, že z danej SIP entity nám nemôže hroziť žiadny útok. To spôsobí zníženie záťaže CPU. Napríklad ak Avaya CM je priamo pripojená k SM, tak IP adresa CM môže byť daná do Whitelistu, ale len v prípade, že aj SIP entity za CM sú dôveryhodné.

SM je k operátorovi možné pripojiť aj priamo, a to bez použitia SBC. Dobré nastavenie firewallu si dokáže poradiť so SIP útokmi, celková kontrola nad týmto spojením a jeho bezpečnosť je však nižšia ako v prípade SBC.

Tab. 6 Porovnanie SM a SBC pre pripojenie k SIP operátorovi [23]

Vlastnosti	SBC	Session Manager
Bezpečnosť	Chráni sieť a všetky ostatné zariadenie pred DoS a DDoS útokom	Chráni servery a aplikácie Unnified Communication pred DoS a SIP DoS útokom
	Pomocou šifrovania (Médií a signalizácie) chráni identitu a súkromie SIP konverzácie.	Podporuje šifrovanie médií k zabezpečeniu hlasu
	Uplatňuje pravidla kontroly prístupu, a to limitovaním počtu prichádzajúcich relácií od SIP operátora	Pomocou SMGR uplatňuje pravidla kontroly prístupu a autentizácie účastníkov.
	K utajeniu topológie a vnútrosieťových koncových staníc poskytuje Sieťový preklad adries (NAT).	Neposkytuje sieťový preklad adries. Spolieha sa na to, že to za neho spraví SBC
	Kontroluje prevádzku, zabezpečuje ochranu proti vírusom a červom z vonkajšej siete. To zahŕňa kontrolu paketov.	Kontroluje SIP prevádzku a vo vnútri siete zabraňuje škodlivým správam k dosiahnutiu danej aplikácie
Konektivita	Podporuje 2000 konkurenčných SIP relácií.	Podporuje 20 000 konkurenčných SIP relácií
	Podporuje manipuláciu čísla, URI a signalizácie.	Podporuje manipuláciu čísla, URI a signalizácie.
	Zabezpečuje prepojenie šifrovaných a nešifrovaných relácií. Taktiež zabezpečuje prepojenie rôznymi SIP a medzi SIP a H.323.	Zabezpečuje prepojenie šifrovaných (TLS) a nešifrovaných relácií.
	Poskytuje preklad adries medzi privátnymi a verejnými alebo medzi IPv4 a IPv6	Neposkytuje preklad adries.
	Poskytuje SDP a DTMF manipuláciu a prekódovanie	N/A

3.3 Avaya Aura System Manager

System Manager (SMGR) je bezpečný centralizovaný systém, ktorý poskytuje správu celej VoIP siete. Tá zahŕňa správu používateľov, správu volacieho plánu, smerovanie hovorov a v neposlednom rade aj monitorovanie výkonu a porúch. Pomocou grafického webového rozhrania zabezpečuje správu všetkých Avaya severov, ktoré patria do skupiny Avaya Aura. V mojom prípade som ho použil k manažovaniu SM a celej mojej VoIP siete. Priamo do SM som pristupoval len pomocou CLI a to za účelom sledovania práve prebiehajúcej prevádzky v reálnom čase. K nastaveniu SM som pristupovali cez SMGR.

Výhodou SMGR je to, že je jediný riadiaci bod v celej sieti. V prípade veľkej siete znižuje jej komplexnosť. Relatívne jednoduchým nastavením sa snaží čo najviac zamedziť konfiguračným chybám. Operačným systémom CentOS s balíčkami Avaya Aura systémovej platformy. [25]

Tab. 7 Kapacita SMGR [25]

Kapacita	Maximálny limit
Administrátorské prihlásenia	250
Súčasné administrátorské prihlásenia	50
Koncové zariadenia	250 000
SIP koncové zariadenia	125 000
Koncový užívatelia	250 000
Mailboxy	250 000
Kontakty jedného užívateľa	250
Verejné kontakty	1 000
Kontaktný list jedného užívateľa	1
Skupiny	300
Členovia v skupine	400
Elementy	25 000
Communication Manager	500
Session Manager	12
Gateway	2 000
Role	200
Role jedného užívateľa	10

3.4 SIP Klienti

Pri písaní diplomovej práce som prišiel do kontaktu aj s Avaya SIP klientmi. Jedným z nich bol stolný telefón Avaya 9601 SIP IP Deskphone, ktorý je možné používať ako SIP a aj ako H.323 telefón. Tento telefón slúži ako terminál. Jeho funkcie ako napr. telefónny zoznam sa nevzťahujú k telefónu ako takému. Účastník sa môže prihlásiť na akýkoľvek telefón a vždy bude mať prístup k svojím osobným nastaveniam a k adresáru. Je napájaný funkciou PoE. Disponuje ešte druhým 10/100 Eternetovým portom pre pripojenie počítača a následné zredukovanie kabeláže na pracovnom stole.

Druhým Avaya SIP klientom, s ktorými som prišiel do kontaktu je Avaya One-X Communicator. Ten je tzv. „softphone“, čo je softvérový SIP klient, ktorý zvláda prenos hlasu, videa, e-mailu, hlasovej schránky a faxu. Užívateľovi poskytuje jednoduchý a intuitívny prístup ku každodennej komunikácii. Existuje verzia pre osobný počítač a mobilná verzia pre iOS, Android a Windows Phone. Pri inštalácii Avaya One-X Communicator na vlastný mobilný telefón alebo počítač (BYOD v kap. 1.3) je potrebné zvážiť zabezpečenie pomocou SBC.

4 Praktická časť

V tejto kapitole sa budem venovať praktickej časti diplomovej práce. Tu zhodnotím možnosti útoku a spôsoby zvýšenia bezpečnosti v Avaya Aura architektúre.

Všetko potrebné vybavenie vrátane serverov mi bolo poskytnuté firmou Algotech. Tá už mala nainštalované testovacie prostredie, ktoré obsahovalo nainštalovaný SM a SMGR. Tieto servery obsahovali základnú sieťovú konfiguráciu. Čo sa SBC týka, tak ten som si do daného testovacieho prostredia doinštaloval a nakonfiguroval sám.

4.1 Implementácia Avaya Aura a Inštalácia Avaya SBCE

Celú testovaciu Avaya Aura architektúru reprezentovali v mojom prípade SM a SMGR. V sieti bol pripojený aj CM, no ten už bol v ostrej prevádzke a vo firme Algotech spravoval všetku komunikáciu medzi H.323 telefónmi. Jenou z mojích úloh bola konfigurácia Avaya Aura serverov a pripojenia SBC ako ochranného prvku. Návodom k tejto konfigurácii mi boli aplikačné poznámky od firmy Avaya, ku ktorým som dostali prístup cez firmu Algotech. Počas implementácie sa často vyskytli aj nepredvídateľné konfiguračné problémy. Pri riešení vážnejších takýchto konfiguračných problémov, mi výrazne pomohli Avaya Online Support.

4.1.1 Adresovanie siete

Tab. 8 Adresovanie siete

Server	Zariadenie	IP adresa	Maska	Brána
System Manager	SMGR	192.168.25.80	/24	192.168.25.1
Session Manager	SM (Session Manager) SM - CLI	192.168.25.87 192.168.25.85	/24 /24	192.168.25.1 192.168.25.1
Session Border Controller	SBC - M1 SBC - A1 SBC - B1	10.10.11.101 172.16.15.12 91.241.11.237	/24 /24 /29	10.10.11.1 172.16.15.1 91.241.11.233
DNS prim. **DNS sec.** **NTP server**		172.16.2.10 172.16.2.16 172.16.2.12		
UA	SIP klient	DHCP	DHCP	DHCP

V Tab. 8 sú uvedené všetky IP adresy, ktoré som v Avaya Aura architektúre použil. IP adresa 91.241.11.237 bola verejná a všetky ostatné použité IP adresy boli privátne.

Použité servery – tieto servery boli zo skupiny Common Servers Release 1**:**

- **SM** - HP ProLiant DL360 G7, štvorjadrový procesor Intel Xeon E5620 (2,4 GHz, 12MB cache), 12GB (3x4GB) DDR3 1333MHz, 4x1Gb Ethernet, HDD 2x 300GB.
- **SBC** - Dell PowerEdge R210 II, štvorjadrový procesor Intel Xeon E3-1220 (3,1GHz, 8MB cache), 8GB DDR3 1600MHz (až 32GB), 6x1Gb Ethernet

- **SMGR** - HP ProLiant DL360 G7, štvorjadrový procesor Intel Xeon E5620 (2,4 GHz, 12MB cache), 12GB (3x4GB) DDR3 1333MHz, 4x1Gb Ethernet, HDD 2x 300GB

Použitý SIP klienti:

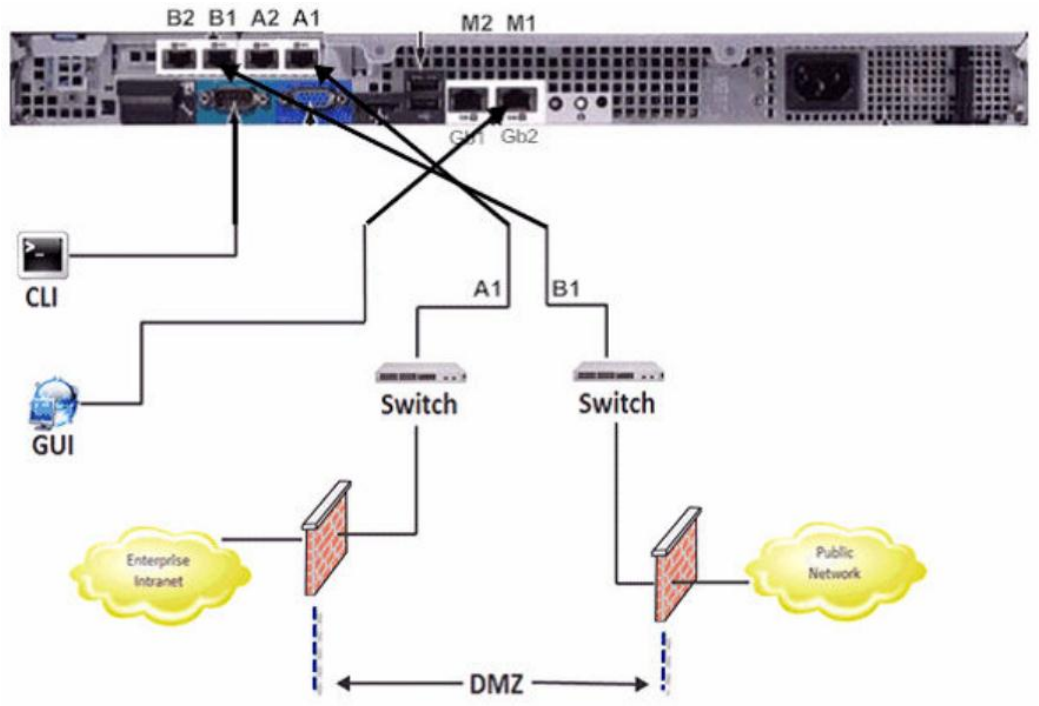
- Avaya One-X Communicator
- Avaya 9601 SIP IP Deskphone
- Empathy
- Linphone

4.1.2 Inštalácia a základné nastavenie SBC

K pripojeniu na server som použili sériový port (CLI Obr. 18), program Putty s rýchlosťou 19200 Bd. Po chvíli mi server ponúkol možnosti bootovania. Bootoval som z USB disku, na ktorom bol skopírovaný systém *Avaya Session Border Controller for Enterprise Release 6.2.1.Q16 FP1 Service Pack 1 GA*. Približne po hodine inštalácie sa server spýtal na jeho základnú konfiguráciu, kde bolo potrebné zadať IP adresu, masku siete a bránu pre port M1. Tento port bude slúžiť ako manažment SBC. V ďalšom kroku sa server spýtal na meno domény siete, DNS a NTP server.

Inštalácia bola vykonaná bez fyzického pripojenia k sieti a SBC sa nutne potrebovalo pripojiť k NTP serveru, tak ten som podľa Tab. 8 pripojili k smerovaču Cisco. Tam som na interface0/0 nastavili IP adresu brány a na interface0/1 IP adresu NTP servera. Na smerovači som vykonal príkaz „*ntp master*“ a SBC si týmto mohlo zosynchronizovať čas. Nakoniec bol na SBC nainštalovaný najnovší patch, a to *Release 6.2.1.Q18.* Po dokončení inštaláci bolo SBC pripravené na odvoz do serverovne. Každý ďalší prístup k SBC už bol vykonávaný vzdialene.

Z pohľadu zvýšenia bezpečnosti je vhodné zvoliť čo najsilnejšie prístupové heslo pre administrátorský účet a heslo si bezpečne uchovať. SBC ponúka možnosť nakonfigurovať viacerých užívateľov čo sa hodí v prípade, keď je potrebné dať administrátorský prístup viacerým ľuďom. Noví užívatelia môžu byť nakonfigurovaní s rôznymi právami. Vo väčšej firme je takto možné dať prístup ku konfigurácii viacerým ľuďom a stále mať SBC plne pod kontrolou.



Obr. 18 Fyzické zapojenie SBC [26]

- A1 – Externá sieť
- B1 – interná sieť
- M1 – manažment SBC
- CLI – sériový port

System Information: SBC_TEST

General Configuration

Appliance Name	SBC_TEST
Box Type	SIP
Deployment Mode	Proxy

Device Configuration

HA Mode	No
Two Bypass Mode	No

Network Configuration

IP	Public IP	Netmask	Gateway	Interface
172.16.15.12	172.16.15.12	255.255.255.0	172.16.15.1	A1
91.241.11.237	91.241.11.237	255.255.255.248	91.241.11.233	B1

DNS Configuration

Primary DNS	172.16.2.10
Secondary DNS	172.16.2.16
DNS Location	DMZ
DNS Client IP	172.16.15.12

Management IP(s)

IP	10.10.11.101

Obr. 19 Základné nastavenie SBC

View Flow: CallServer1

Criteria

Flow Name	CallServer1
Server Configuration	CallServer1
URI Group	*
Transport	*
Remote Subnet	*
Received Interface	External

Profile

Signaling Interface	TrunkUserInternalSignaling
Media Interface	TrunkInternalMedia
End Point Policy Group	default-low
Routing Profile	CallServer1
Topology Hiding Profile	default
File Transfer Profile	None

Obr. 20 Natavenie Server Flows

View Flow: avaya

Criteria

Flow Name	avaya
URI Group	*
User Agent	*
Source Subnet	*
Via Host	*
Contact Host	*
Signaling Interface	External

Optional Settings

Topology Hiding Profile	default
Phone Interworking Profile	Avaya-Ru
TLS Client Profile	None
RADIUS Profile	None
File Transfer Profile	None
Signaling Manipulation Script	None

Profile

Source	Subscriber
Methods Allowed Before REGISTER	
User Agent	*
Media Interface	TrunkExternalMedia
End Point Policy Group	default-low
Routing Profile	CallServer1

Obr. 21 Nastavenie Subscriber Flows

4.2 Možnosti útoku a spôsoby zabezpečenia

Na zabezpečenie Avaya Aura architektúry som sa pozeral z troch pohľadov (kap. 3.1.2). Zaoberal som sa hlavne bezpečnosťou architektúry zapojenia a zabezpečením komunikácie. Tretiemu z bezpečnostných pohľadov (základné zabezpečenie, ktoré sa týkalo viac operačného systému ako SIP) som sa v tejto diplomovej práci nevenoval.

Popisujem však všetky dostupné VoIP bezpečnostné mechanizmy, ktoré Avaya Aura spolu s Avaya SBCE spolu ponúkajú.

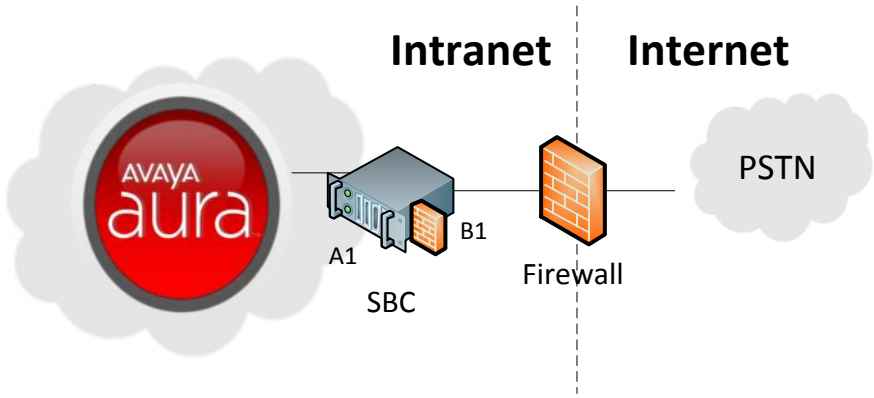
4.2.1 Návrh bezpečnej architektúry

Predtým než sa bude sieťový administrátor zaoberať rôznym nastavením zabezpečenia komunikácie bude musieť riešiť spôsob zapojenia Avaya Aura architektúry v siete. Pod týmto sa myslí hlavne zapojenie SBC, a to ako bezpečnostného prvku Avaya Aura architektúry. Nastavenie bezpečnosti príde na rad až vo chvíli, keď bude celá architektúra fyzicky zapojená a nakonfigurovaná.

V kap. 2.2 som opísal možnosti zapojenia SBC v sieti. V tejto kapitole sa pozriem na to, ktorá z týchto možností je z pohľadu bezpečnosti najoptimalnejšia, a ako by sa táto bezpečnosť ešte dala zvýšiť.

Nebolo by vhodné pripojiť ústredňu priamo k internetu lebo každý útok na túto ústredňu by mohol ovplyvniť funkčnosť SIP služieb. Preto úplne najjednoduchším zapojením by bolo zapojenie, kedy je SBC umiestnené na okraji siete a jedna strana je pripojená k internetu alebo k operátorovi a tá druhá k ústredni. Takto vytvorí SBC hraničný prvok medzi internetom a ústredňou, ktorý bol akýmsi nárazníkom. Zatiaľ čo bude SBC vyčerpávať svoje zdroje na obranu pred hrozbami z internetu, tak ústredňa je aj naďalej schopná ničím nerušene vykonávať svoju prácu.

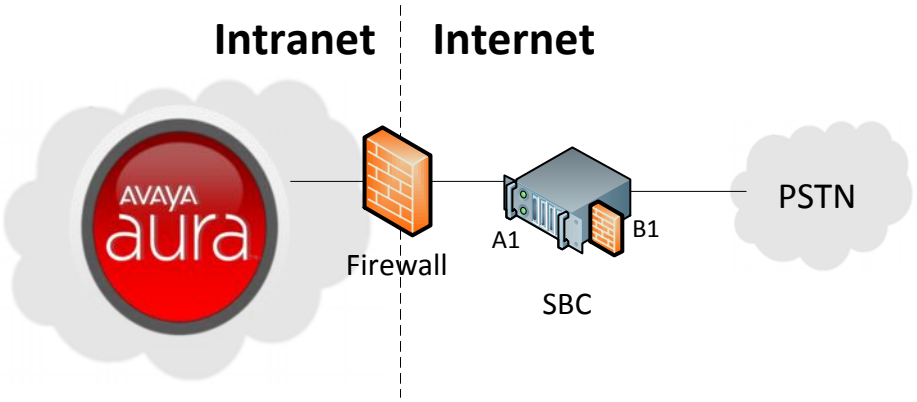
Toto základné zapojenie je vhodné ďalej zabezpečiť firewallom, ktorý by bol umiestnený buď pred, alebo za SBC. Rozhodnutie toho aké postavenie medzi sebou SBC alebo firewall zaujmú závisí od bezpečnostných zásad aké firma používa a spôsobom využitia SBC (kap. 2.2). Napríklad či firma používa SIP trunk alebo remote workers. V prípade, že má firma nadefinované bezpečnostné pravidlo, v ktorom stojí že firewall je jediné zariadenie, ktoré rozhodne o tom čo do siete pustí a čo nie, tak pôjde SBC za neho.



Obr. 22 SBC za Firewallom

Rovnako je výhodné uložiť SBC za firewall v prípade, že je použitá funkcia remote workers, ktorá využíva viac než SIP komunikáciu. Naopak, ak sa jedná len o použitie SIP trunku tak môže byť SBC aj pred firewallom. Takúto spoluprácu firewallu a SBC je ďalej nutné nakonfigurovať tak, aby prenos médií a všetka komunikácia na portoch 5060 (UDP) a 5061 (TLS) šla priamo k SBC a nebola ďalej

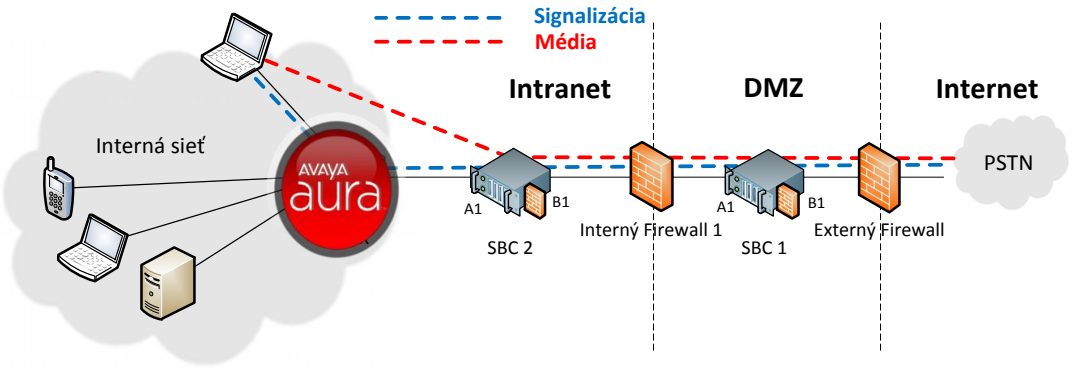
spracovávaná firewallom. Tak isto je vhodné oddeliť SIP komunikáciu do osobitnej VLAN.



Obr. 23 SBC pred Firewallom

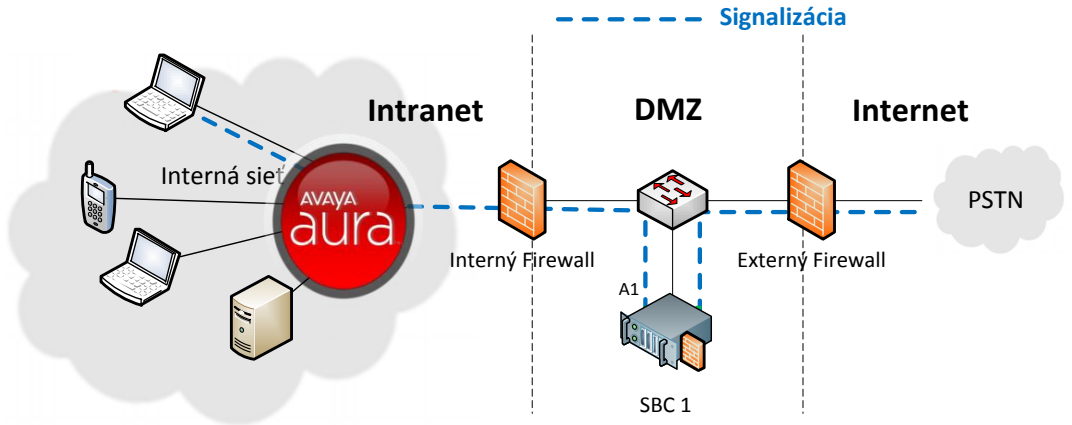
Ešte bezpečnejším spôsobom zapojenia je uloženie SBC do DMZ, ktorá pridáva ďalšiu pomyselnú bezpečnostnú vrstvu. Ide o nasadenie SBC medzi interný a externý firewall oddelených do rôznych LAN sietí. Takto útočník zaútočí iba na servery, ktoré sa nachádzajú v DMZ. Všetko čo je za ňou, vrátane ústredne je pre neho skryté. Toto konkrétne zapojenie je doporučené aj firmou Avaya [15].

Posledným spôsobom ako zapojiť SBC je zapojenie viacerých SBC za sebou (Obr. 24). Zapojenie, ktorého silná stránka je v tom, že vo firewalle nie je potrebné povoľovať všetky možné porty pre média a týmto sa zníži počet používaných portov. V tomto prípade stačí medzi oboma SBC nastaviť trunk. Komunikácia prebiehajúca týmto trunkom prejde cez firewall len jedným portom. Ide hlavne o média, pre ktoré musia byť v internom firewalle povolené porty. Cez firewall medzi SBC1 a SBC 2 bude prechádzať signalizácia média iba jedným portom. Média sú priamo preposielané k UA až druhým SBC 2. Vzniká scenár back-to-back-to-back komunikácie (B2B2B). V tomto spôsobe zapojenia stačí aj na internom firewalle povoliť iba jeden port pre trunk. Toto zapojenie ma výhodu v jednoduchšej konfigurácii a správe firewallu. Nevýhodou ostáva potreba dvoch SBC a to predstavuje kúpu ďalšieho hardvéru. (to však pre firmu nemusí byť veľmi výhodné). Iná situácia nastane v prípade virtualizácie SBC, kde už nebude potrebné zakúpiť nový drahý server. Avaya už začala podporovať virtualizáciu SBC v dobe písania tejto diplomovej práca.



Obr. 24 Bezpečné zapojenie

Spomenul by som ešte jedno zapojenie. Nepatrí do kategórie tých v úvodzovkách „najbezpečnejších“, ale v určitých prípadoch môže byť nápomocné. Je to zapojenie kedy je z portov A1, B1, A2, B2 použitý iba jeden z nich, a to A1. SBC je v tomto prípade nakonfigurované prijať prevádzku týmto jedným portom a po spracovaní ju tým istým portom presmerovať ďalej k ústredni. Konfigurácia Avaya SBC túto možnosť povoľuje. Výhodou by bolo napríklad uvoľnenie jedného portu. Pri tejto komunikácii je nutné nastaviť smerovanie v sieti tak, aby všetka SIP prevádzka prešla cez SBC.



Obr. 25 Signalizácia pri zapojení len jedného rozhrania

Všetky tieto zapojenia sú typu NNI a SBC je uložené na hranici siete. V internej sieti a v zapojení typu UNI už nejde o SIP trunk, ale priamo užívatelia sa pripájajú na SM cez SBC vo vnútri siete. Toto zapojenie v prípade Avaya Aura však nemusí byť veľmi efektívne. Svoj účel to síce splní, ale všetkých účastníkov je možné týmto spôsobom pripojiť aj priamo k SM, ktorý prípadné DoS/DDoS útoky z vnútra siete dokáže odraziť. Pri písaní tejto diplomovej práce som sa nestretol s potrebou použiť SBC vo vnútri siete, bez toho aby bolo nakonfigurované v móde remote workers a v inom prípade ako pri trende BYOD. Správnou konfiguráciou SIP firewallu v SM, a pri priamom pripojení účastníkov v internej sieti, je možné aj bez SBC dosiahnuť bezproblémový a bezpečný chod siete. Iné by to bolo v prípade remote workers kedy sa účastníci pripájajú z internetu a SBC je umiestené na okraji siete.

Posledným bezpečnostným prvkom, ktorý sa týka architektúry siete, a ktorý je určite vhodné použiť, je zapojenie SBC do HA. V prípade výpadku jedného SBC prevezme jeho činnosť to druhé. V tomto prípade sú potrebné 3 servery. Dva SBC a jeden riadiaci server, ktorý tieto 2 SBC synchronizuje a v prípade problému odstaví nefunkčné SBC a na jeho miesto dosadí to funkčné. Avaya ponúka túto možnosť už pri inštalácii SBC.

4.2.2 Zabezpečenie komunikácie

Z pohľadu zabezpečenia komunikácie ide o celú škálu mechanizmov použitých k tomuto účelu. Použitím, správnym nastavením a kombináciou všetkých z nich vznikne relatívne celkom zabezpečená sieť. Vravíme relatívne, pretože sieť je taká bezpečná ako zabezpečenie toho najslabšieho článku v nej. Existuje stále veľa možností ako VoIP napadnúť, a to pokojne aj útokom na nižšej vrstve podľa Tab. 1.

Prvým z mechanizmov použitým k zabezpečeniu komunikácie je autorizácia. Avaya používa už v základnom nastavení digest autorizáciu. Tá zabráni útočníkovi k jeho nežiaducemu prístupu a to tým, že na prihlásenie bude potrebovať meno a heslo. Je nutné však používať kvalitné heslá, ktoré nebude možné pomocou metódy hrubej sily odhaliť. To v prípade soft SIP klienta nie je problém. Problém nastáva pri telefónoch Avaya.

V telefónoch Avaya, s ktorými som prišiel do kontaktu môže byť dĺžka a zložitosť hesla slabinou celej siete, pretože tieto telefóny podporujú len číselné heslá, a to s dĺžkou maximálne 8 miest. Predpokladám, že nie každý si zvolí maximálnu dĺžku hesla. Napríklad také 4 miestne heslo je pri nesprávne nastavenom firewallu možné prelomiť pomocou metódy hrubej sily s dnes úplne obyčajným notebookom (Dual Core 2,2 GHz, 4GB RAM) do niekoľkých sekúnd.

K overeniu tohto tvrdenia som použil skript (kolekciu skriptov) napísaný v jazyku Python, ktorý sa volá SIP Vicious [27]. V mojom prípade som použili konkrétne skript s názvom *svcrack* - bruteforce utilita, ktorá skúšala všetky možné číselné kombinácie hesiel. Na základe tohto výsledku som prepočítal dobu prelomenia pre rôzny počet cifier. Prepočítané odhady pri rôzne dlhých heslách sú zobrazené v Tab. 9. Tabuľka nezobrazuje presné doby trvania odhadu hesla, je to len približný odhad.

Tomuto sa však dá zamedziť konfiguráciou maximálneho počtu registračných pokusov, ktoré má SIP účastník povolené v určitej dobe vyčerpať. Toto nastavenie sa vzťahuje na nastavenie firewallu a je bližšie popísané v kapitolách týkajúcich sa SIP firewallu. Konkrétne ide o SIP firewall pravidlá - Obmedzenie a alarm vysokého počtu REGISTER od jedného UA a jednej IP (Tab. 10).

Tab. 9 Doby trvania prelomenia hesla

Počet cifier hesla	Približná doba prelomenia hesla
4 - ciferné heslo	20 sekúnd
5 - ciferné heslo	27 minút
6 - ciferné heslo	4,5 hodín
7 - ciferné heslo	2 dni
8 - ciferné heslo	2 týždne

4.2.3 Kontrola prístupu (Autorizácia a autentifikácia)

Oba servery, Avaya SM a tak isto aj Avaya SBCE, používajú digest autorizáciu, ktorú už majú nastavenú a nedá sa v prípade potreby vypnúť. Autorizácia sa používa pri všetkých SIP požiadavkách REGISTER, INVITE a BYE. `WWW-Authenticate` a následná odpoveď `Authorization` vyzerala v mojom prípade nasledovne:

```
WWW-Authenticate: Digest realm="abg.net", qop="auth",
opaque="1234567890abcedef",nonce="14a21a406cbffac10c53c021c503c89e0d2D
77d27c1",algorithm=MD5,stale=false
```

```
Authorization: Digest username="560", realm="abg.net",
nonce="14a21a406cbffac10c53c021c503c89e0d2D77d27c1", uri=sip:ab.net,
response="ebef1c11770521ee589bdac95f36a870", algorithm=MD5,
cnonce="0a4f113b", opaque="1234567890abcedef", qop=auth, nc=00000001
```

Ďalšou funkciou zabezpečujúcou kontrolu prístupu je povolenie prístupu iba určitému klientovi. Táto funkcia je dostupná len v SBC a ide jej o zabránenie použitia neznámeho SIP klienta. Napríklad pri trende BYOD, kde si užívateľ môže nainštalovať SIP klienta podľa svojho vlastného uváženia. Administrátor si to môže ako-tak odkontrolovať v *SBC → Global Parameters → User Agents.* Táto funkcia však nie je nejako výrazne ošetrená, pretože jediné čo robí je porovnávanie zhody názvu v SIP hlavičke *User-Agent* so zadaným názvom v tabuľke. Zabezpečenie sa dá preto veľmi ľahko obísť vhodným prepísaním SIP hlavičky *User-Agent.*

Kontrolu prístupu je možné kontrolovať aj podľa účastníka alebo URI skupiny do ktorej patrí, takto je možné každej skupine alebo účastníkovi nastaviť vlastné práva, smerovanie alebo kontrolu prístupu. Nastavenie: *SBC → Global Parameters → URI Groups.*

4.2.4 Šifrovanie

Oba servery (SM aj SBC) podporujú zabezpečený prenos SIP signalizácie pomocou TLS. Veľa útokov je možné realizovať len vďaka tomu, že v sieti nie je použité šifrovanie. Ak je vo VoIP sieti použité šifrovanie signalizácie tak z bezpečnostného pohľadu odpadne veľké množstvo potenciálnych hrozieb. Šifrovanie signalizácie pomocou TLS je preto z hľadiska bezpečnosti výhodné nasadiť. Lenže existuje niekoľko ďalších uhlov pohľadov kedy to už tak výhodné nie je.

Dôvody sú rôzne, ale medzi tie najhlavnejšie patrí to, že v prípade TLS sa zložito riešia problémy v sieti. SIP prevádzka šifrovaná protokolom TLS je neviditeľná aj pre administrátora, ktorý tam preto radšej nastaví UDP a získa väčší prehľad o dianí v sieti.

Ďalším z dôvodov je zaistenie kompatibility, pretože veľa systémov to nepodporuje. V neposlednom rade ide šifrovanie aj na úkor výkonu, kde pokles počtu hovorov je taký výrazný (napr. Tab. 3), že je pre väčšiu firmu z ekonomického hľadiska výhodnejšie tam to TLS nepoužiť.

Nepoužitím TLS šifrovania zostáva veľké bezpečnostné riziko. Pokiaľ by sieť nebola zabezpečená iným spôsobom, ktorý sa už nemusí priamo týkať SIP signalizácie, tak kdekoľvek v organizácii si útočník nájde voľný kábel a je schopný nahliadnuť do prevádzky siete.

Je potrebné zvážiť použitie TLS a nasadiť ho tam, kde má naozaj význam. Existujú však dôvody kedy je použitie TLS priam samozrejmosťou. Ide o prípad kedy funguje SBC v móde remote workers, a to z dôvodu priameho pripojenia do verejnej siete.

Podporu šifrovaného prenosu médií (SRTP) už podporuje len SBC. SM touto funkciou nedisponuje pretože Session Manager médiá neprenáša. Opäť tu však SRTP pripadá na zváženie. Aj keď zabráni záškodnému odpočúvaniu hovorov, tak organizácia sa pripravuje o použitie nahrávania, čo v niektorých prípadoch (napr. Call centrum) môže byť nevýhoda. V neposlednom rade znižuje počet dostupných konkurenčných SIP relácií.

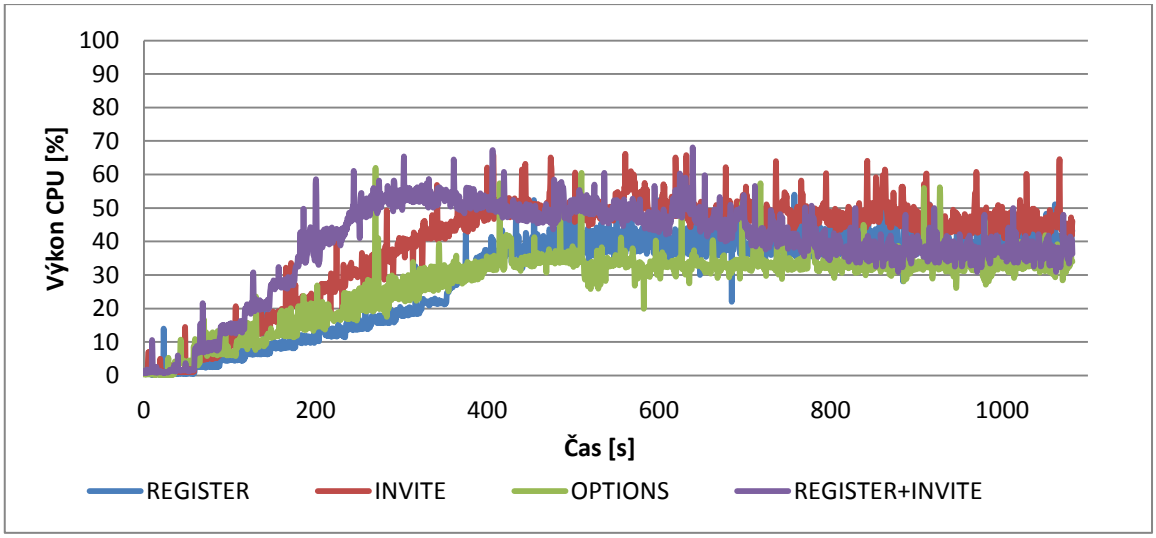
V prípade, že sa organizácia rozhodne použiť šifrovaný prenos SIP signalizácie (TLS) alebo médií (SRTP), tak Avaya odporúča použiť CA certifikáty tretích strán avšak ponúka aj vlastné. Natavenie SRTP je v *SBC → Domain Policies → Media Rules → Media Encryption.* Natavenie TLS v je v *SBC→ TLS Management → Client Profiles*. Daný profil je potom následne potrebné priradiť k Subscriber alebo Server Flows v *SBC → Device Specific Settings → End Poit Flows*. V SM to bude *SM → Routing → Entity Links → Protocol* a certifikáty v *SM → Services → Security → Certificates.*

4.2.5 Nastavenie SIP firewallu v SM

Nastavenie SIP firewallu bude závisieť hlavne od toho, ako sa daný SM správa pri zvýšenej prevádzke. Preto sme s mojím kolegom Ondrou Kovářem, ktorý na moju architektúru útočil, simulovali DoS útok pomocou voľne prístupného programu SIPp a sledovali vyťaženie procesora na SM. Použili sme dva počítače. Oba počítače boli vybavené najnovším procesorom Intel i7 a 16 GB pamäťou RAM. Týmto sa tieto notebooky výkonnostne radili medzi vyššiu triedu.

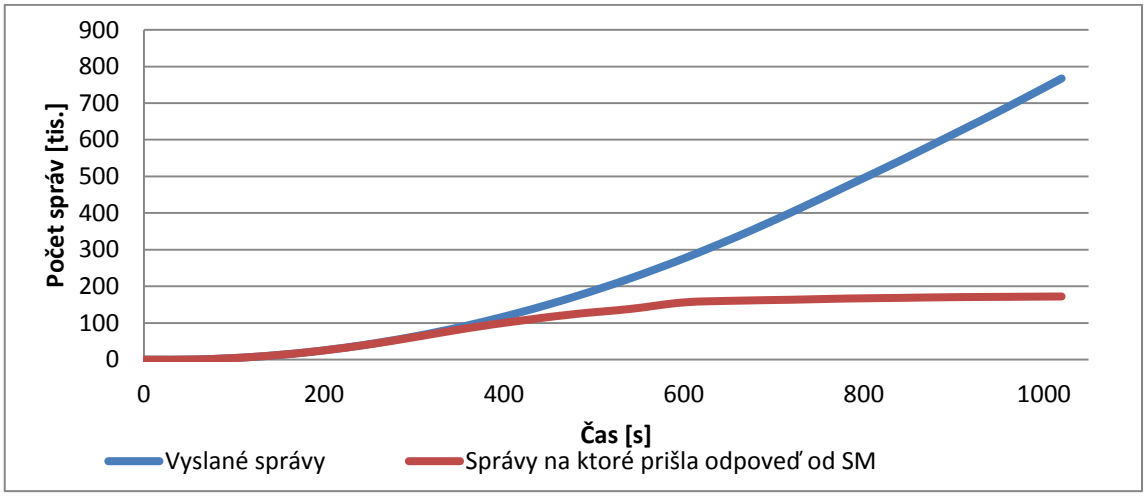
Test sme skúšali najprv s jedným počítačom a potom sme pridali druhý, následne sme pocítili asi 10 % nárast vyťaženia CPU na SM. Tento útok prebiehal tak, že sme z dvoch počítačov, na ktorých bežal SIPp postupne zaplavovali ústredňu SIP prevádzkou. Túto prevádzku tvorili transakcie REGISTER, INVITE, OPTION a nakoniec ešte REGISTER spolu s INVITE. Nakoniec sme ešte pridali tretí počítač, ten sa už radil medzi tie slabšie a žiadny ďalší výrazný nárast vyťaženia CPU už nenastal. Vo výslednom grafe (Graf 1) je vidieť výsledok testu smerovaného na Avaya Aura Session Manger.

Graf 1 Závislosť vyťaženie CPU SM od času – s vypnutým SIP firewallom



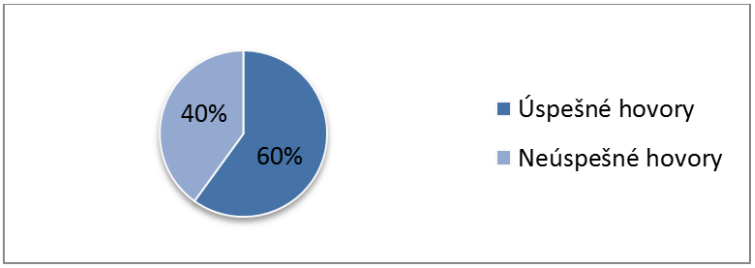
Na grafe (Graf 1) je vidieť, ako sme postupne každých 30 sekúnd navýšili počet odoslaných správ o 100 za sekundu. Počiatočná hodnota bola 10 správ za sekundu. Hodnotu 30 sekúnd sme zvolili preto, lebo pri nej hodnote už bolo vyťaženie procesora po predošlom náraste relatívne ustálené. Takto sme zvyšovali prevádzku až sa hodnota počtu odoslaných správ priblížila k 90 000, počet vyslaných správ je zobrazený v grafe (Graf 2). Je viditeľné, ako po tejto hodnote prestáva SM odpovedať na správy.

Graf 2 Závislosť počtu správ od času – s vypnutým SM SIP firewallom



Počas trvania testu sme skúšali aj obyčajné hovory. Čo vlastne simulovalo účastníka, ktorý sa počas takéhoto DoS útoku snaží niekam dovolať. Volali sme na striedačku z jedného klienta na druhý. Výsledkom nášho testu bolo 12 neúspešných hovorov z 20 (Graf 3). Čím by náš útok už mohol užívateľovi znepríjemniť deň.

Graf 3 Pomer úspešných a neúspešných hovorov počas simulácie DoS útoku



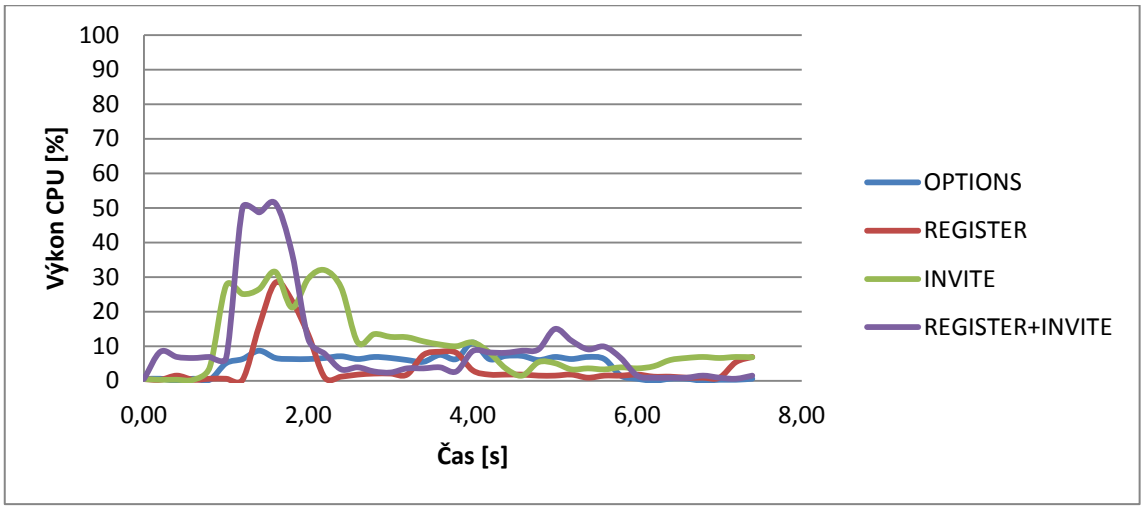
Hodnota 90 000 je maximálny počet SIP relácií, ktoré dokáže SM bez problémov odbaviť a je definovaná spoločnosťou Avaya (kap. 3.2). Táto hodnota nebola fixne daná. Niekedy sme sa dostali aj nad 150 000. Čo svedčí v prospech SM. 90 000 konkurenčných SIP relácií bolo však minimom, ktoré sme potom zohľadnili pri návrhu SIP firewallových pravidiel v SM.

Celý tento test prebiehal s vypnutým SIP firewallom, po jeho nakonfigurovaní už bola situácia odlišná. Priebeh testu je zobrazený v grafe (Graf 4). Na ňom je vidieť, ako po poslaní veľkého množstva správ bol SIP firewall schopný odhaliť a zachytiť náš útok. Polovičné vyťaženie procesora trvalo približne iba jednu sekundu. So serverom sa nič nedialo ani pri ďalšom zvyšovaní počtu záškodníckych SIP správ.

Tu je vidieť, že SIP Firewall zmysel má a to taký, že žiadny legitímny hovor počas tohto útoku, nebol ovplyvnený. V praxi by to znamenalo, že každý účastník by sa bez problémov dovolal aj v prípade, že by sa niekto snažil o zahltenie ústredne.

Nastavenie SIP Firewallu je však relatívne a je taktiež veľmi subjektívnou záležitosťou, pretože každý má iné bezpečnostné požiadavky a každá firma môže mať ináč nastavený DoS limit. Respektíve limit, kedy už firma považuje zvýšenú prevádzku v sieti za DoS útok. Nejaká malá firma s pár telefónni môže už pár INVITE požiadaviek za minútu považovať za útok. Zatiaľ čo pre inú väčšiu firmu nemusia ani stovky INVITE požiadaviek za minútu predstavovať žiadny problém.

Graf 4 Závislosť vyťaženia CPU SM od času – so zapnutým SIP firewallom



V prípade REGISTER SIP správy nemusí ísť len o simuláciu útoku, kde útočník záškodne posiela REGSITER požiadavky, tento test mohol simulovať aj výpadok SM

a jeho následný reštart. Po reštarte SM by sa začali všetci užívatelia naraz registrovať. SM nemal problém aj pri vypnutom SIP firewalle zaregistrovať 500 účastníkov za sekundu. Pri registrácii 1 000 účastníkov za sekundu a vypnutom firewalle už začal na nejaké požiadavky nereagovať, no v konečnom dôsledku by boli všetci užívatelia zaregistrovaní. Pretože užívateľ bude posielať REGISTER pokiaľ sa úspešne nezaregistruje.

V nasledujúcej tabuľke sú prehľadne znázornené všetky použité pravidlá SIP firewallu, ktoré boli pri našom teste použité. Pravidlá je možné kombinovať v ľubovoľnom množstve. Vysvetlenie toho, čo všetky tie pojmy v tabuľke znamenajú je v kap. 3.2.1.

Toto nastavenie je pozmenené základné nastavenie SIP Firewallu od firmy Avaya, ktoré by podľa nej malo byť modifikované len v prípade potreby.

Tab. 10 Nastavenie Firewallu

Názov	Typ akcie	Typ záznamu	Počet správ	Perioda [s]	Timeout [s]
Obmedzenie a alarm vysokého počtu INVITE od jedného UA	Rate Limit	A+Z	90	60	900
Obmedzenie a alarm vysokého počtu REGISTER od jedného UA	Rate Limit	A+Z	10	60	900
Obmedzenie a alarm vysokého počtu OPTIONS od jedného UA	Rate Limit	A+Z	20	60	900
Obmedzenie a alarm vysokého počtu INVITE z jednej IP	Rate Limit	A+Z	360	60	900
Obmedzenie a alarm vysokého počtu REGISTER z jednej IP	Rate Limit	A+Z	60	60	900
Obmedzenie a alarm vysokého počtu OPTIONS z jednej IP	Rate Limit	A+Z	90	60	900
Vysoká prevádzka od jedného UA	Rate Limit	A+Z	800	60	900
Vysoká prevádzka z jednej IP adresy	Rate Limit	A+Z	30 000	60	900

A – Alarm

Z – Záznam do logu

Toto nastavenie Firewallu je možné pri reálnej prevádzke prispôsobiť, no je však potrebné poznať priemerné počty aktívnych užívateľov a aktívnych hovorov. Podľa nich sa potom dajú detekovať prípadné anomálie v sieti. Táto detekcia môže prebiehať napríklad nastavením pravidla Firewallu na požadovaný detekovaný počet správ, ako typ akcie zvoliť No Action a následne zaznamenať do logu SM.

V prípade SM sa SIP firewall nastavuje cez SMGR v sekcii *SM → Network Configuration → SIP Firewall.* Tu je možné definovať rôzne typy nastavenia firewallu (Tab. 10). Tak isto je možné pridať vopred známe IP adresy do Blacklistu alebo

Whitelistu. Po tom, čo sú nadefinované jednotlivé pravidlá SIP firewallu, tak je potrebné ich priradiť k SM a to nastavením: *SM* → *Network Configuration* → *SIP Firewall* → *Označiť Rule Set* → *Assign* → Vybrať SM, na ktorý bude aplikovaný firewall → *Commit.*

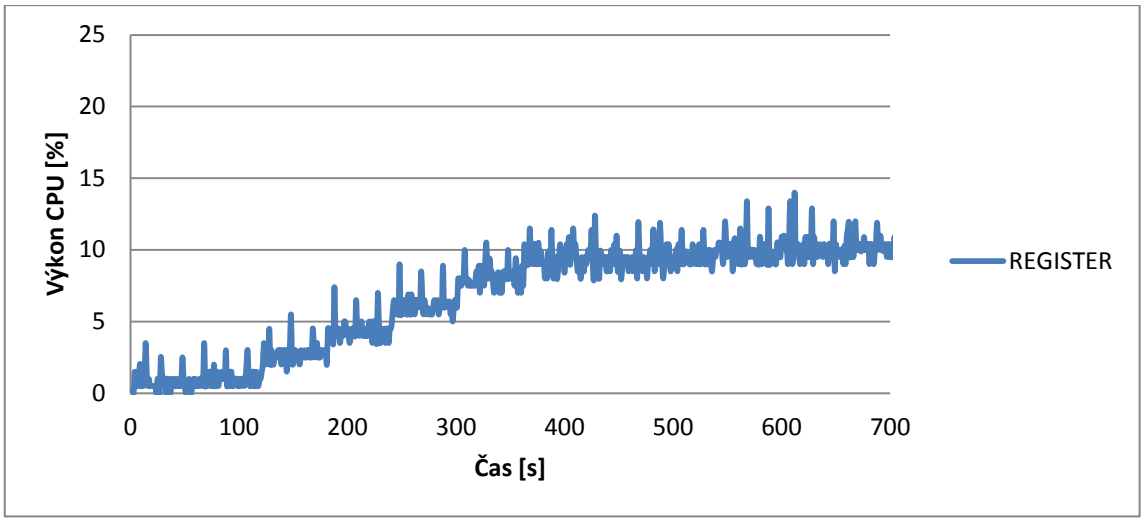
4.2.6 Nastavenie Firewallu v SBC

Rovnaký test aký sme previedli v prípade SM, tak sme testovali aj pri zapojení SBC pred SM. Tento test bol opäť s vypnutým firewallom, tentokrát však už na SBC. Oba servery boli zapojené podľa Obr. 22. a v móde remote worker. Architektúra zapojenia však nemala žiadny vplyv na tento test. Opäť sme použili dva počítače z predchádzajúcej kapitoly a sledovali vyťaženie CPU oboch serverov zobrazené na Graf 5 a Graf 6.

Prevádzka najskôr prechádzala cez SBC (Graf 5) a potom následne do SM (Graf 6). V tomto prípade, však SBC prestalo odbavovať naše záškodnícke správy oveľa skôr ako samotný SM v teste predtým. Počet konkurenčných hovorov sa pohyboval okolo hodnoty 2 000, čo bol maximálny počet remote workers definovaný firmou Avaya podľa Tab. 3.

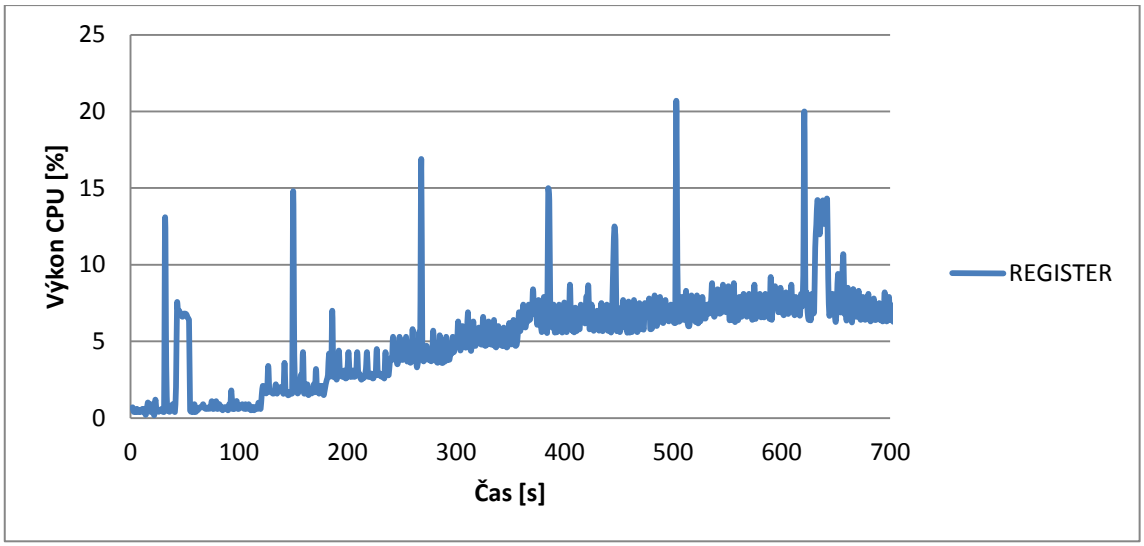
Na grafe je vidieť, že aj keď sa SBC celkom nudil, tak aj tak začal zahadzovať hovory. Z toho je možné vidieť, že SBC neplní rolu len bezpečnostného prvku ale nejaké prostriedky si necháva aj na jeho ostatné funkcie.

Graf 5 Závislosť vyťaženia CPU SBC od času – s vypnutým SBC SIP firewallom



Ďalší graf, Graf 6, zobrazuje prepustenú prevádzku z SBC na SM. Z predošlého testu však vieme, že je schopný zvládnuť oveľa viac. V reálnej prevádzke nebude spracovávať len požiadavky od SBC ale aj priamo pripojených účastníkov. Tých je však s pomocou SBC schopný ochrániť. V prípade útoku budú vyťažené len zdroje SBC a vnútro siete na čele s SM bude ďalej fungovať. Obmedzenie sa bude vzťahovať len na tých pár remote workers pripojených k SBC.

Graf 6 Závislosť vyťaženia CPU SM od času – so zapojeným SBC

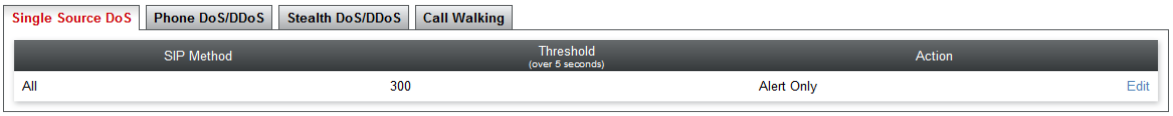


Konfigurácia proti DoS/DDoS útokom v SBC umožňuje jednoducho vytvárať a editovať rôzne pravidlá. Typovo je podobná SM. Nastavuje sa v *SBC → Global Parameters → DoS/DDoS → Edit*. Tu je možné nastaviť:

Single Source DoS

Tento typ útoku je proti jednému alebo viacerým koncovým bodom v sieti, a to práve od jedného zdroja. Toto pravidlo je firmou Avaya nastavené na akciu „Alert Only“, a to upozorniť na všetky správy od jedného zdroja, ktoré prekročia prahové hodnoty 300 SIP správ za 5 sekúnd. Túto hranicu je možné ľubovoľne nastaviť a priradiť jej jednu z nasledujúcich akcií:

- Alert Only – informuje o prekročenej prahovej hranici,
- Block – zablokuje prevádzku ,
- SIP Challenge – zaháji autentizáciu.



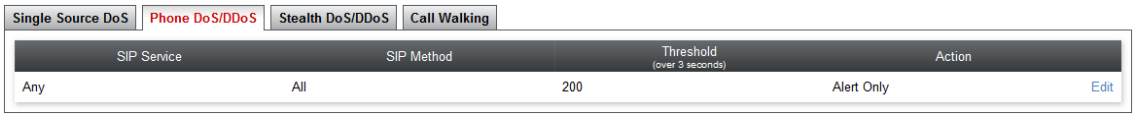
Obr. 26 Single Source DoS

Phone DoS/DDoS

Typ DoS útoku, ktorý útočí práve na jeden koncový bod. V tomto prípade je tak isto možné ľubovoľne nastaviť prahovú hranicu. Základné nastavenie je definované na 200 sip správ za 3 sekundy, ktoré sa vzťahujú na všetky SIP služby a metódy. K prekročeniu prahovej hodnoty je možné priradiť nasledujúce akcie, kde oproti predchádzajúcemu prípade pribudne jedna navyše:

- Alert Only – informuje o prekročenej prahovej hodnoty,
- Block – zablokuje prevádzku,
- SIP Challenge – zaháji autentizáciu,

- Enforce Limits – neblokuje žiadnu prevádzku.

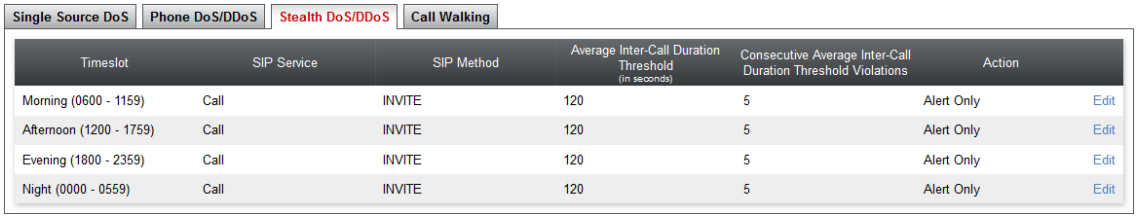


Obr. 27 Phone DoS/DDoS

Stealth DoS/DDoS

Typ DoS útoku, ktorý je smerovaný priamo na jedného koncového užívateľa, kde sa zdroj volania mení. V tomto prípade sa priraďujú jednotlivým časovým oknám rôzne prahové hodnoty. Tieto časové okná sú rozdelené na ráno, popoludnie, večer a noc. Pravidlo sa vzťahuje len na INVITE správy v telefónnych hovoroch. Použité akcie sú:

- Alert Only – informuje o prekročenej prahovej hranice,
- Block – zablokuje prevádzku,
- SIP Challenge – zaháji autentizáciu.

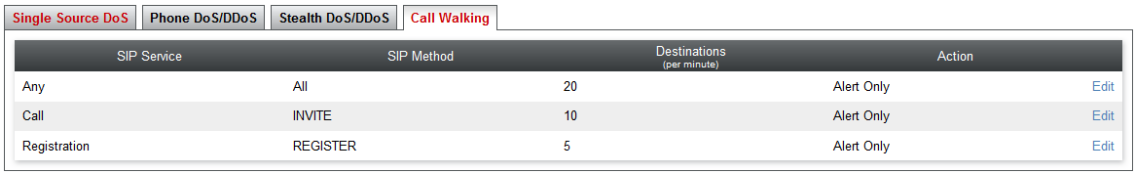


Obr. 28 Stealth DoS/DDoS

Call Walking

Typ DoS útoku, kde útočník z jedného zdroja sekvenčne útočí na niekoľko koncových bodov. Pravidlo sa vzťahuje na všetky SIP správy, kde sa dajú osobitne nastaviť prahové hodnoty pre INVITE a REGISTER. Použité akcie sú opäť:

- Alert Only – informuje o prekročenej prahovej hranice,
- Block – zablokuje prevádzku,
- SIP Challenge – zaháji autentizáciu.



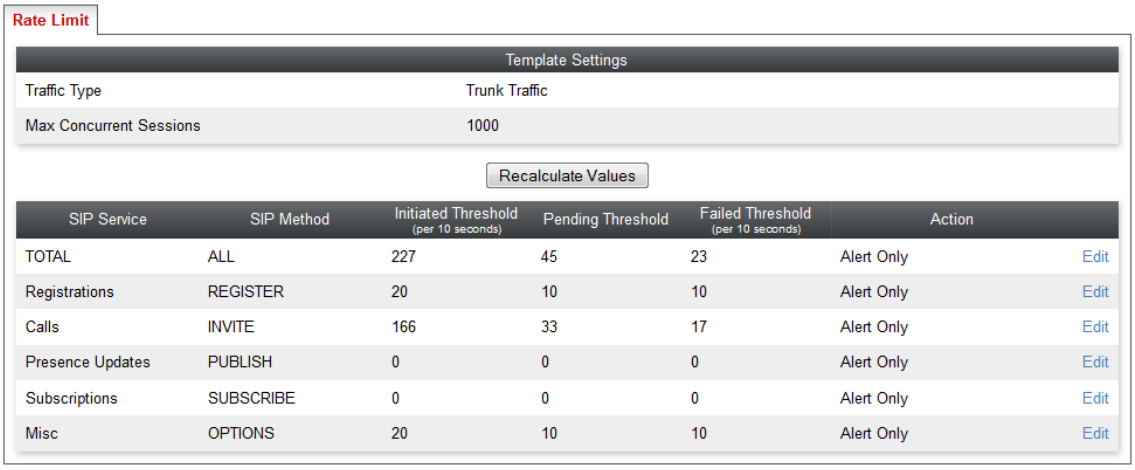
Obr. 29 Call Walking

Domain DoS

Ďalšie DoS nastavenia sú v: *SBC → Global Profiles → Server Configuration → DoS Protection*. Toto nastavenie od základu nie je aktivované preto sa aktivuje: *Advanced →Edit → Enable DoS Protection → Finish* tu ponúka Avaya SBC jednoduchú konfiguráciu DoS pravidiel pri zahltení DoS útokom. Jediný rozdiel oproti predchádzajúcim DoS nastaveniam je, že v tomto prípade sú pravidlá vzťahujúce sa ku

konkrétnemu serveru, ku ktorému sú smerované a až po aplikovaní smerovania. Pretože cieľový SIP server je identifikovaný až potom čo ho SBC nájde vo svojej smerovacej tabuľke. Toto DoS nastavenie je automaticky prepočítané podľa zadaného maximálneho počtu aktívnych relácií. Základné nastavenie sa vzťahuje k 1 000 maximálnym súbežným reláciám (Obr. 30), ktoré v prípade potreby mení. Pri tomto prepočítaní je možné zvoliť typ prevádzky:

- Trunk Traffic,
- Remote Users,
- Tunk Traffic and Remote Users.



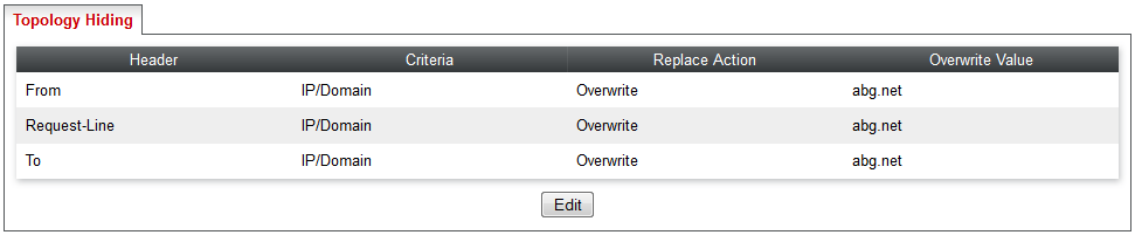
Obr. 30 Domain DoS

Nastavený Domain DoS sa priradí k *SBC → Domain Policies → Security Rules → Domain DoS.* Toto bezpečnostné pravidlo (Security Rules) sa potom priradí k *SBC → Domain Policies → End Point Policy Groups.* End Point Policy Groups nakoniec k *SBC → Device Specific Dettings → End Point Flows → Server Flow.*

4.2.7 Topology hiding

Topology hiding je funkcia poskytovaná serverom Avaya SBCE a umožňuje zmeniť kľúčové SIP správy, obsahujúce určité parametre akými sú IP adresa alebo názov lokálnej domény. Ich zmena potom následne zabráni alebo zamaskuje útočníkovi z verejnej siete jej topológiu.

V SBC je vhodné prepísať tieto SIP hlavičky, ktorými sú: *from, Request-Line* a*To* Obr. 31. Nastavenie funkcie Topology hiding je možné previesť v *SBC→ Global Profiles → Topology Hiding.* Toto nastavenie je možné ľubovoľne modifikovať a v prípade potreby prepísať aj hlavičky *Record-Route, SDP, Via, Reffered-By* a *Refer-To.*



Obr. 31 Topology hiding

4.2.8 Ďalšie zabezpečenie

Avaya SBCE ponuka taktiež aj funkcie Scrubber a Fingerprint, ktoré skúmajú pakety do hĺbky a v prípade nejakej anomálie škodlivé pakety zahodia alebo informujú administrátora alarmom. Obe funkcie bohužiaľ nie je možné ľubovoľne modifikovať. Avaya ich modifikáciu nepovoľuje. Dajú sa len povoliť alebo zakázať. Avaya však odporúča ich používanie [28].

Ich povolenie alebo zakázanie funkcie Scrubber je v *SBC→ Global Parameters → Scrubber.* Povolenie alebo zakázanie funkcie Fingerprint je v *SBC → Global Profiles → Fingerprint.*

5 Záver

V diplomovej práci som sa sústredili hlavne na konkrétne možnosti zabezpečenia Avaya Aura architektúry, tak zvnútra ako aj zvonku siete. Popísal som jednotlivé časti Avaya Aura architektúry, jej komponenty i prvky, ktoré celý systém zabezpečujú. Venoval som sa tiež dostupným bezpečnostným prvkom poskytovaných firmou Avaya.

Práca bola rozdelená na teoretickú a praktickú časť. V prvej, teoretickej, časti práce som sa zaoberal aktuálnym stavom a spôsobmi zabezpečenia PBX systémov založených na protokole SIP, a to nasadením SBC ako hraničného ochranného prvku NGN siete. Snažil som sa zhodnotiť možné hrozby i zabezpečenia proti ním a bezpečnostné trendy pre NGN siete s nasadeným SBC, a to na úrovniach NNI a UNI.

Úroveň NNI znamenala z pohľadu Avaya SBCE pripojenie k VoIP operátorovi SIP trunkom. V rámci UNI išlo o pripojenie, ktoré má názov Remote Workers. Popísal som výhody SBC potreby, dôvody jeho použitia, správny výber a spôsoby jeho zapojenia v NGN sieti, ktoré mali vplyv na jej celkovú bezpečnosť.

V praktickej časti diplomovej práce som sa zaoberal už konkrétnou implementáciou a konfiguráciou testovacej Avaya Aura architektúry. Zároveň som sa venoval implementácii a konfigurácii Avaya SBCE pre ochranu trunku, remote workers, ústredne a BYOD zariadení.

Všetky servery boli poskytnuté firmou Algotech. Praktickú časť som mal rozdelenú spolu s diplomovou prácou môjho kolegu Ondru Kováře. Išlo o koncept, kde sa Ondra Kovář snažil útočiť a ja som sa bránil. Kvôli tomu sme vytvorili testovacie prostredie pre rôzne DoS útoky a vďaka nemu sme namerali údaje a následne ich, ako grafy spracovali do tejto diplomovej práce. Pomocou nich sme overili bezpečnostné možnosti SM aj SBC.

Pri testovaní jednotlivých metód zabezpečenia sme videli správanie ústredne počas útoku. Na základe toho som navrhol patričné opatrenia a zhodnotil jej ochranu. Tieto opatrenia pozostávali z bezpečnostných možností ponúkaných firmou Avaya. Týkalo sa to návrhu bezpečnej architektúry, kontroly prístupu, šifrovania (signalizácie a médií) a nakoniec aj návrhu nastavenia SIP firewallu. Návrh SIP firewallu bol rôzny pre SM a SBC. Pri SBC sa ešte delil na mód, v ktorom bolo SBC nakonfigurované či už SIP trunk alebo Remote Workers.

Cieľom tejto práce bolo vytvoriť referenčné nastavenie proti širokej škále SIP útokov. Pri implementácii všetkých bezpečnostných možností, ktoré Avaya ponúka, a ktorých nastavenie som popísali v tejto práci. Je preto možné povedať, že sieť bude na základe tejto diplomovej práce zabezpečená proti všetkým útokom typu: neautorizovaný prístup, odpočúvanie, DoS/DDoS, Toll Fraud alebo záškodnícka modifikácia správ. Táto práca môže slúžiť aj ako návod alebo aspoň „vodítko“ pri zavádzaní bezpečnostných opatrení do Avaya Aura architektúry.

Čím by sa preto dalo v tejto práci pokračovať? Zaoberal som sa len malými VoIP sieťami, resp. bezpečnostnými princípmi fungujúcimi hlavne v malých sieťach a firmách. Relatívne veľká firma alebo call centru si však nemôže dovoliť použiť len jeden SM alebo len jedno SBC. Pretože sa môže stať, že rôzne časti firmy používajú rôzne bezpečnostné opatrenia. Keďže Avaya podporuje aj dodatočné rozširovanie celej NGN siete, tak pri väčších firmách by v nich bolo potrebné zvážiť použitie viacerých SBC a SM. Pri oboch serveroch je potom potrebné dôsledne zvážiť a odôvodniť ich nový počet a taktiež bezpečnostnú konfiguráciu, ktorá by bola šitá na mieru pre rôzne logické časti veľkej SIP siete. Napríklad rôzne SBC pre DMZ, SBC pre SM a SBC pre Remote Workers.

Zoznam použitej literatúry

[1] DWIVEDI, Himanshu: *Hacking VoIP: protocols, attacks, and countermeasure*s. 2006, No Starch Press, San Francisco. ISBN-10: 1-59327-163-8, ISBN-13: 978-1-59327-163-3.

[2] JOHNSTON, Alan; PISCITELLO, David: *Understanding Voice over IP Security.* 2006 Artech House, INC. ISBN 1-59693-050-0.

[3] RANSOME, James; RITTINGHOUSE, John: *Voice over Internet Protocol (VoIP) Security.* 2005 Elsevier Inc. ISBN 978-1-55558-332-3.

[4] DORGHAM, Sisalem; FLOROIU, John; KUTHAN, Jiri: *SIP Security*. Great Britain 2009, John Wiley & Sons Ltd. ISBN 978-0-470-51636-2 (H/B)

[5] Communications Fraud Control Association (CFCA), *Announces results of worldwide telecom fraud survey.* 4. Októbra 2011, Roseland, NJ. Dostupné na internete: <http://cfca.org/pdf/survey/Global%20Fraud_Loss_Survey2011.pdf>

[6] AHSON, Syed; ILYAS, Mohammad: *SIP Handbook, Services Technologies and Security of SIP*. 2009 Tayor & Francis Group, LLC. ISBN 978-1-4200-6603-6

[7] PROKOP, Andrew: *Building a secure SIP network* [online]. Aktualizované 13. Februára 2014. [cit. 13-09-2014]. Dostupné na internete: <https://andrewjprokop.wordpress.com/2014/02/13/converge2014-building-a-secure-sip-network/>

[8] RUSSEL, Travis: *Session Initiation Protocol (SIP): Controlling Convergent Networks*. Jún 2008 McGraw-Hill. ISBN-10: 0071488529 ISBN-13: 978-0071488525

[9] ROSENBERG, J.; SCHULZRINNE, H.; CAMARILLO, G: *SIP: Session Initiation Protocol.* IETF RFC 3261. Jún 2002. Dostupné na internete: <http://tools.ietf.org/html/rfc3261>.

[10] Baugher, M; McGrew, D; Naslund, M: *The Secure Real-time Transport Protocol (SRTP).* IETF RFC 3711. Marec 2004. Dostupné na internete: <http://www.rfc-base.org/txt/rfc-3711.txt>

[11] THERMOS, Peter; TAKANEN Ari: *Securing VoIP networks. Threats, Vulnerabilities and Countermeasures.* 2008 Boston MA, Pearson Education, Inc. ISBN-13: 978- 0-321-43734-1 ISBN-10: 0-321-43734-9

[12] NIELSEN, Lisa: *7 Myths About BYOD Debunked* [online]. Aktualizované 9.Novembra 2009 [cit. 13-10-2014] Dostupné na internete: <http://thejournal.com/articles/2011/11/09/7-byod-myths.aspx>

[13] HAUTAKORPI, J.; CAMARILLO, G.; PENFIELD, R.; HAWRYLYSHEN, A.; BHATIA, M. (April 2010). *Requirements from SIP (Session Initiation Protocol) Session Border Control Deployments*. IETF RFC 5853. Dostupné na internete: <https://tools.ietf.org/html/rfc5853>.

[14] PROKOP, Andrew: *Why a Sessio Border Controller (SBC).* [online]. Aktualizované 2.Februára 2014. [cit.15-10-2014]. Dostupné na internete:

<https://andrewjprokop.wordpress.com/2014/02/03/why-a-session-border-controller-sbc/>

[15] Dokumentácia: *Avaya Session Border Controller for Enterprise Overview and Specification*. Release 6.2, Issue 2. December 2013 Avaya Inc.

[16] SHINDER, Deb: SolutionBase: *Strengthen network defenses by using a DMZ* [online]. Aktualizované 29. Júna 2005. [cit. 20-10-2014]. Dostupné na internete: <http://www.techrepublic.com/article/solutionbase-strengthen-network-defenses-by-using-a-dmz/>

[17] VoIP News: *10 Questions to Ask Your SBC* [online]. Aktualizované 23. Júla 2012. [cit. 30-10-2014]. Dostupné na internete: <http://www.voip-news.com/articles/voip-blog/10-questions-to-ask-your-sbc-vendor-51985>

[18] PLEASANT, Blair: *What UC is and what it isn't* [online]. Aktulaizované Júl 2008. [cit. 5-11-2014]. Dostupné na internete: <http://searchunifiedcommunications.techtarget.com/feature/What-UC-is-and-isnt>

[19] Dokumentácia: *Security Design in Avaya Aura® Session Manager*. Release 6.3, Október 2013 Avaya Inc.

[20] Dokumentácia: *Avaya Aura ® Session Manager.* Release 6.3, Issue 5, August 2014 Avaya Inc.

[21] Dokumentácia: *Avaya Session Border Controller for Enterprise Overview and Specification.* Release 6.3, Issue 3, Október 2014 Avaya Inc.

[22] Dokumentácia: *Avaya SBCE 6.3 Security Configuration and Best Practices Guide.* Release 6.3, Issue 1.0, Október 2014 Avaya Inc.

[23] Dokumentácia: *Avaya Aura ® Session Manager Overview and Specification.* Release 6.3, Issue 5, August 2014 Avaya Inc.

[24] Dokumentácia: *Administering Avaya Aura® Session Manager*, Release 6.3, Issue 7, September 2014 Avaya Inc.

[25] Dokumentácia: *Avaya Aura® System Manager Security Design,* Release 6.1, Január 2011 Avaya Inc.

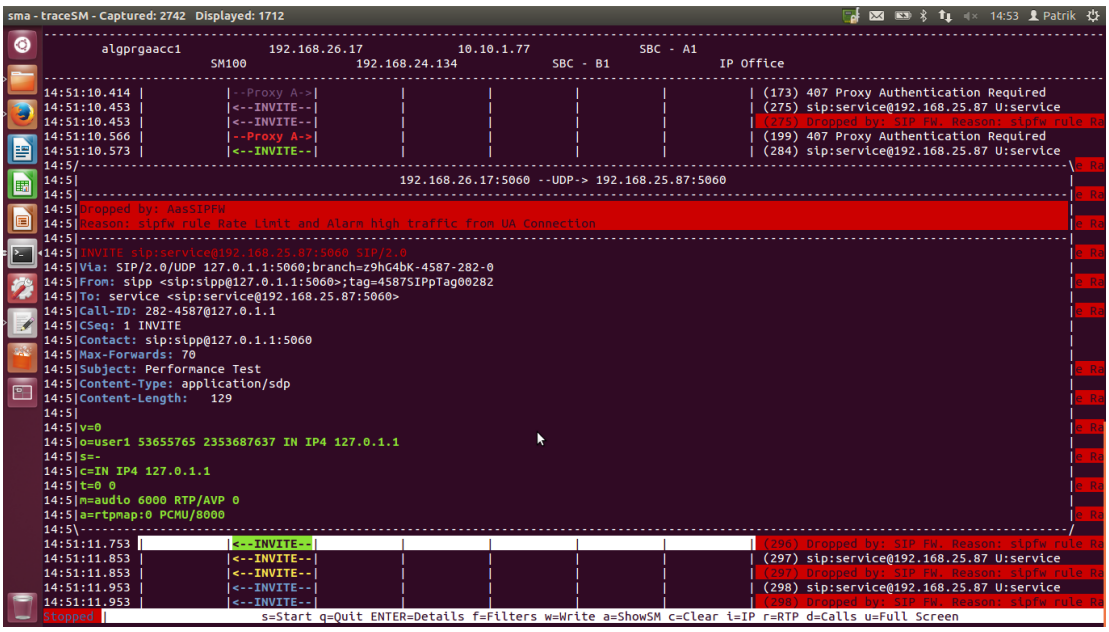
[26] Dokumentácia: *Configuring the Avaya Session Border Controller for IP Office Remote Workers,* September 2013 Avaya Inc.

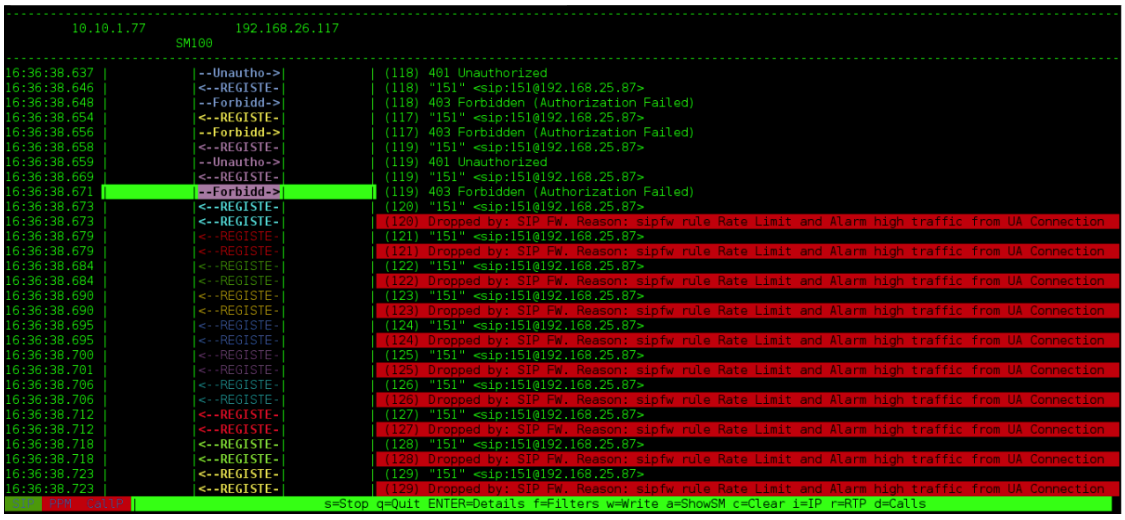
[27] Dokumentácia: SIP Vicious. Dostupné online: <https://code.google.com/p/sipvicious/wiki/GettingStarted>

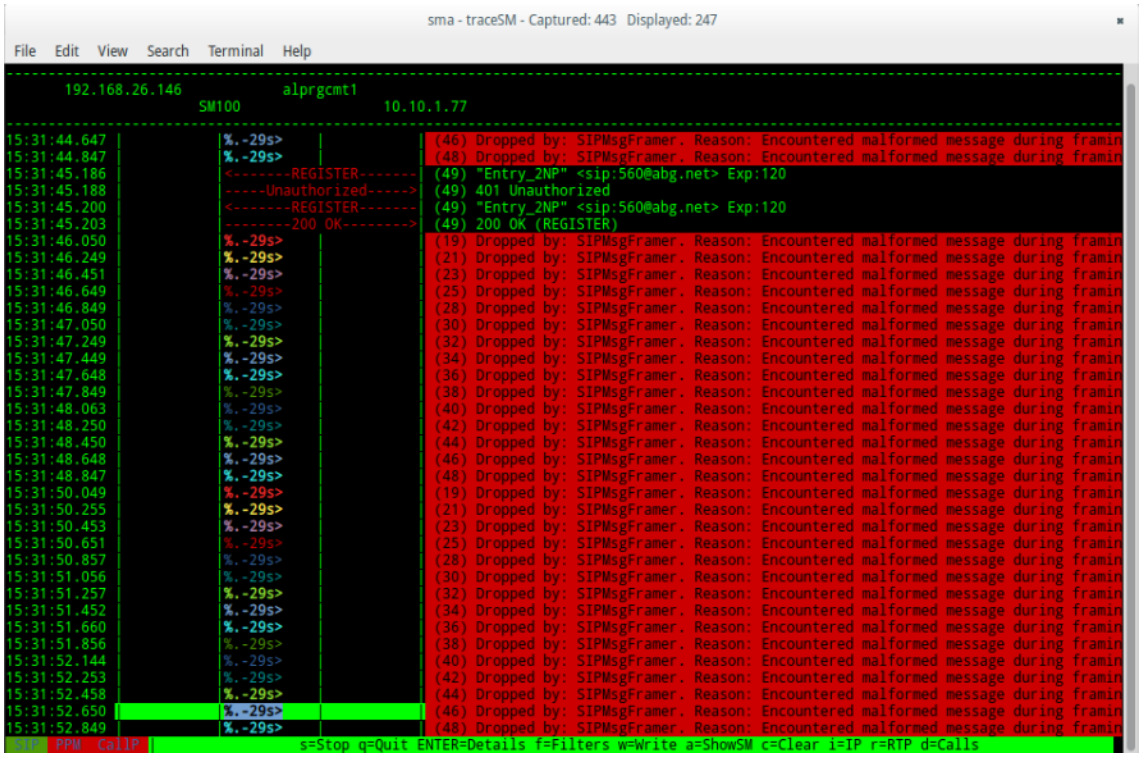
[28] Dokumentácia: *Administering Avaya Session Border Controller for Enterprise.* Release 6.2, Issue 2, Január 2013 Avaya Inc.

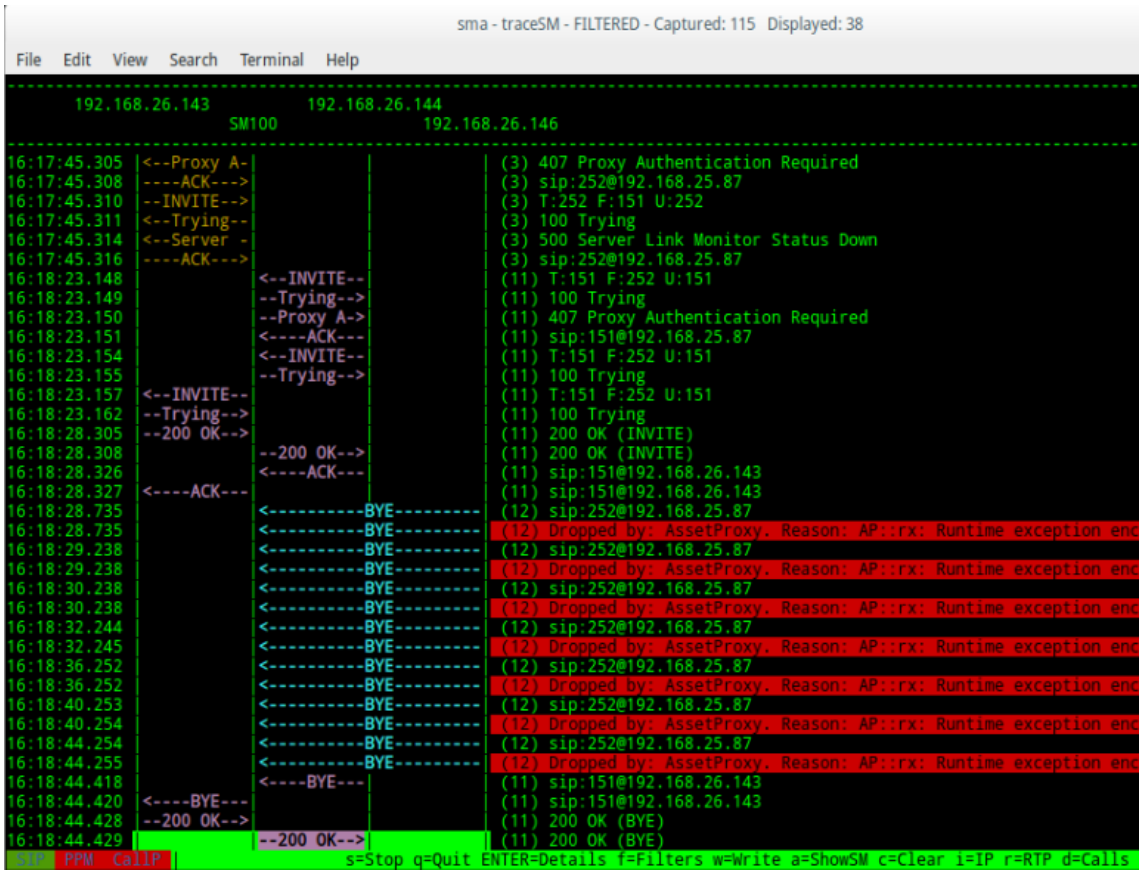
[29] Kuhn, Richard; Walsh, Thomas; Fries, Steffen (January 2005) *Security Considerations for Voice Over IP Systems.* Gaithersburg, Computer Security Division, Information Technology Laboratory, Naitonal Institute of Standards and Technology, Special publication 800-58, MD 20899-8930

Príloha A – Ukážky z útokov






sma - traceSM - Captured: 443 Displayed: 247
File Edit View Search Terminal Help
192.168.26.146 alprgcmt1
SM100 10.10.1.77
15:31:44.647 %.-29s> (46) Dropped by: SIPMsgFramer. Reason: Encountered malformed message during framin
15:31:44.847 %.-29s> (48) Dropped by: SIPMsgFramer. Reason: Encountered malformed message during framin
15:31:45.186 <-------REGISTER------- (49) "Entry_2NP" <sip:560@abg.net> Exp:120
15:31:45.188 -----Unauthorized-----> (49) 401 Unauthorized
15:31:45.200 <-------REGISTER------- (49) "Entry_2NP" <sip:560@abg.net> Exp:120
15:31:45.203 --------200 OK--------> (49) 200 OK (REGISTER)
15:31:46.050 %.-29s> (19) Dropped by: SIPMsgFramer. Reason: Encountered malformed message during framin
15:31:46.249 %.-29s> (21) Dropped by: SIPMsgFramer. Reason: Encountered malformed message during framin
15:31:46.451 %.-29s> (23) Dropped by: SIPMsgFramer. Reason: Encountered malformed message during framin
15:31:46.649 %.-29s> (25) Dropped by: SIPMsgFramer. Reason: Encountered malformed message during framin
15:31:46.849 %.-29s> (28) Dropped by: SIPMsgFramer. Reason: Encountered malformed message during framin
15:31:47.050 %.-29s> (30) Dropped by: SIPMsgFramer. Reason: Encountered malformed message during framin
15:31:47.249 %.-29s> (32) Dropped by: SIPMsgFramer. Reason: Encountered malformed message during framin
15:31:47.449 %.-29s> (34) Dropped by: SIPMsgFramer. Reason: Encountered malformed message during framin
15:31:47.648 %.-29s> (36) Dropped by: SIPMsgFramer. Reason: Encountered malformed message during framin
15:31:47.849 %.-29s> (38) Dropped by: SIPMsgFramer. Reason: Encountered malformed message during framin
15:31:48.063 %.-29s> (40) Dropped by: SIPMsgFramer. Reason: Encountered malformed message during framin
15:31:48.250 %.-29s> (42) Dropped by: SIPMsgFramer. Reason: Encountered malformed message during framin
15:31:48.450 %.-29s> (44) Dropped by: SIPMsgFramer. Reason: Encountered malformed message during framin
15:31:48.648 %.-29s> (46) Dropped by: SIPMsgFramer. Reason: Encountered malformed message during framin
15:31:48.847 %.-29s> (48) Dropped by: SIPMsgFramer. Reason: Encountered malformed message during framin
15:31:50.049 %.-29s> (19) Dropped by: SIPMsgFramer. Reason: Encountered malformed message during framin
15:31:50.255 %.-29s> (21) Dropped by: SIPMsgFramer. Reason: Encountered malformed message during framin
15:31:50.453 %.-29s> (23) Dropped by: SIPMsgFramer. Reason: Encountered malformed message during framin
15:31:50.651 %.-29s> (25) Dropped by: SIPMsgFramer. Reason: Encountered malformed message during framin
15:31:50.857 %.-29s> (28) Dropped by: SIPMsgFramer. Reason: Encountered malformed message during framin
15:31:51.056 %.-29s> (30) Dropped by: SIPMsgFramer. Reason: Encountered malformed message during framin
15:31:51.257 %.-29s> (32) Dropped by: SIPMsgFramer. Reason: Encountered malformed message during framin
15:31:51.452 %.-29s> (34) Dropped by: SIPMsgFramer. Reason: Encountered malformed message during framin
15:31:51.660 %.-29s> (36) Dropped by: SIPMsgFramer. Reason: Encountered malformed message during framin
15:31:51.856 %.-29s> (38) Dropped by: SIPMsgFramer. Reason: Encountered malformed message during framin
15:31:52.144 %.-29s> (40) Dropped by: SIPMsgFramer. Reason: Encountered malformed message during framin
15:31:52.253 %.-29s> (42) Dropped by: SIPMsgFramer. Reason: Encountered malformed message during framin
15:31:52.458 %.-29s> (44) Dropped by: SIPMsgFramer. Reason: Encountered malformed message during framin
15:31:52.650 %.-29s> (46) Dropped by: SIPMsgFramer. Reason: Encountered malformed message during framin
15:31:52.849 %.-29s> (48) Dropped by: SIPMsgFramer. Reason: Encountered malformed message during framin
SIP PPM CallP s=Stop q=Quit ENTER=Details f=Filters w=Write a=ShowSM c=Clear i=IP r=RTP d=Calls


sma - traceSM - FILTERED - Captured: 115 Displayed: 38
File Edit View Search Terminal Help
192.168.26.143 192.168.26.144
SM100 192.168.26.146
16:17:45.305 <--Proxy A- (3) 407 Proxy Authentication Required
16:17:45.308 ----ACK---> (3) sip:252@192.168.25.87
16:17:45.310 --INVITE--> (3) T:252 F:151 U:252
16:17:45.311 <--Trying-- (3) 100 Trying
16:17:45.314 <--Server - (3) 500 Server Link Monitor Status Down
16:17:45.316 ----ACK---> (3) sip:252@192.168.25.87
16:18:23.148 <--INVITE-- (11) T:151 F:252 U:151
16:18:23.149 --Trying--> (11) 100 Trying
16:18:23.150 --Proxy A-> (11) 407 Proxy Authentication Required
16:18:23.151 <----ACK--- (11) sip:151@192.168.25.87
16:18:23.154 <--INVITE-- (11) T:151 F:252 U:151
16:18:23.155 --Trying--> (11) 100 Trying
16:18:23.157 <--INVITE-- (11) T:151 F:252 U:151
16:18:23.162 --Trying--> (11) 100 Trying
16:18:28.305 --200 OK--> (11) 200 OK (INVITE)
16:18:28.308 --200 OK--> (11) 200 OK (INVITE)
16:18:28.326 <----ACK--- (11) sip:151@192.168.26.143
16:18:28.327 <----ACK--- (11) sip:151@192.168.26.143
16:18:28.735 <----------BYE--------- (12) sip:252@192.168.25.87
16:18:28.735 <----------BYE--------- (12) Dropped by: AssetProxy. Reason: AP::rx: Runtime exception enc
16:18:29.238 <----------BYE--------- (12) sip:252@192.168.25.87
16:18:29.238 <----------BYE--------- (12) Dropped by: AssetProxy. Reason: AP::rx: Runtime exception enc
16:18:30.238 <----------BYE--------- (12) sip:252@192.168.25.87
16:18:30.238 <----------BYE--------- (12) Dropped by: AssetProxy. Reason: AP::rx: Runtime exception enc
16:18:32.244 <----------BYE--------- (12) sip:252@192.168.25.87
16:18:32.245 <----------BYE--------- (12) Dropped by: AssetProxy. Reason: AP::rx: Runtime exception enc
16:18:36.252 <----------BYE--------- (12) sip:252@192.168.25.87
16:18:36.252 <----------BYE--------- (12) Dropped by: AssetProxy. Reason: AP::rx: Runtime exception enc
16:18:40.253 <----------BYE--------- (12) sip:252@192.168.25.87
16:18:40.254 <----------BYE--------- (12) Dropped by: AssetProxy. Reason: AP::rx: Runtime exception enc
16:18:44.254 <----------BYE--------- (12) sip:252@192.168.25.87
16:18:44.255 <----------BYE--------- (12) Dropped by: AssetProxy. Reason: AP::rx: Runtime exception enc
16:18:44.418 <----BYE--- (11) sip:151@192.168.26.143
16:18:44.420 <----BYE--- (11) sip:151@192.168.26.143
16:18:44.428 --200 OK--> (11) 200 OK (BYE)
16:18:44.429 --200 OK--> (11) 200 OK (BYE)
SIP PPM CallP s=Stop q=Quit ENTER=Details f=Filters w=Write a=ShowSM c=Clear i=IP r=RTP d=Calls