



IP-ATC Asterisk: Безопасность

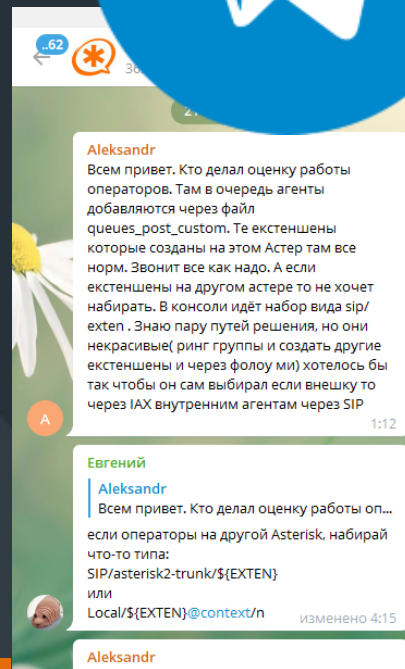
Как выстроить контур защиты

Подключайтесь к Telegram

Задавайте свои вопросы и общайтесь
с коллегами в Telegram-канале

@asterisker

Авторы наиболее продуктивных и
полезных вопросов и комментариев
получат ценные призы от спонсоров



А запись будет?

ДА



VOXLINK: ASTERISK
ПРОФЕССИОНАЛЬНО

Запись придет по почте всем, кто подписан
а также будет на канале Asterisker

Взлом IP-АТС. Кому и для чего это нужно?

Взлом VoIP – один из самых удобных способов монетизации для хакера.

Взломанная АТС дает злоумышленнику:

1. Звонки за ваш счет (и счет – на миллионы)
2. Звонки «ложного минирования»
3. Слив вашей базы
4. Прослушивание ваших звонков



Возможные причины уязвимости АТС:

1. Misconfiguration
2. Слабые пароли
3. Отсутствие IPTables
4. Голый ... (сетевухой) в Интернет
5. FreePBX наружу 80-ми портами (баги в PHP)
6. И ряд других проблем...



Возможные причины уязвимости АТС

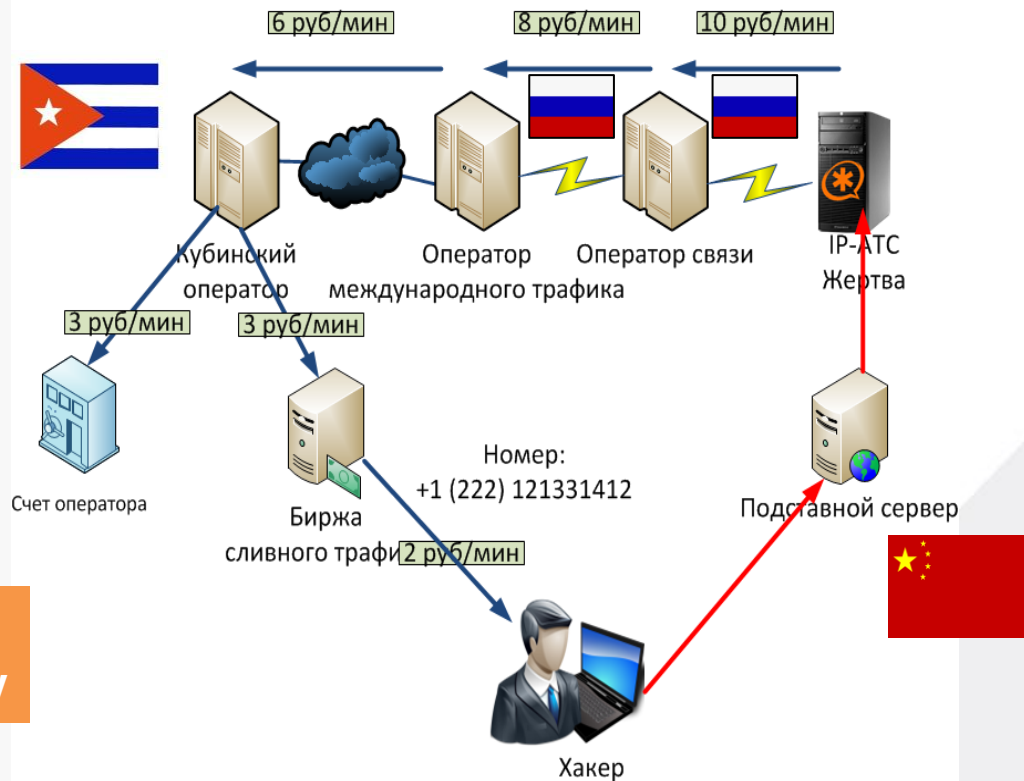


Как я вижу
безопасность
своего Asterisk

Как безопасность
моего Asterisk
видит опытный хакер

Принципы взлома

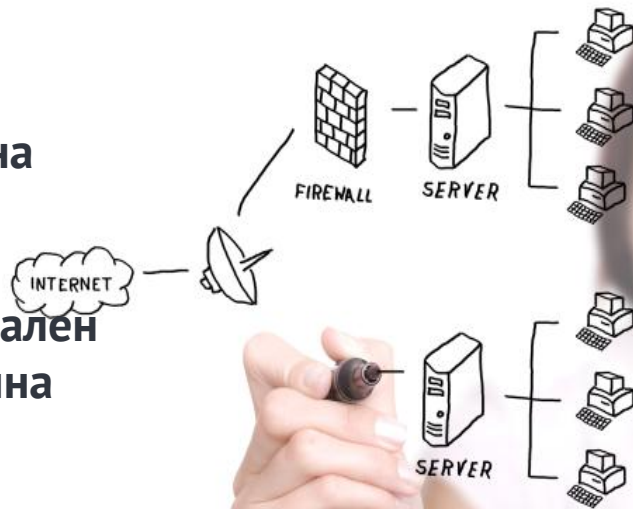
Основная схема –
перепродажа VoIP-
трафика



У вас были взломы?
Напишите, на какую сумму

Безопасен ли Asterisk?

- Инструментарий защиты Asterisk сильнее, чем у многих конкурентов
- Система защиты строится на нескольких уровнях
- Уровень безопасности Asterisk прямопропорционален уровню компетенции админа



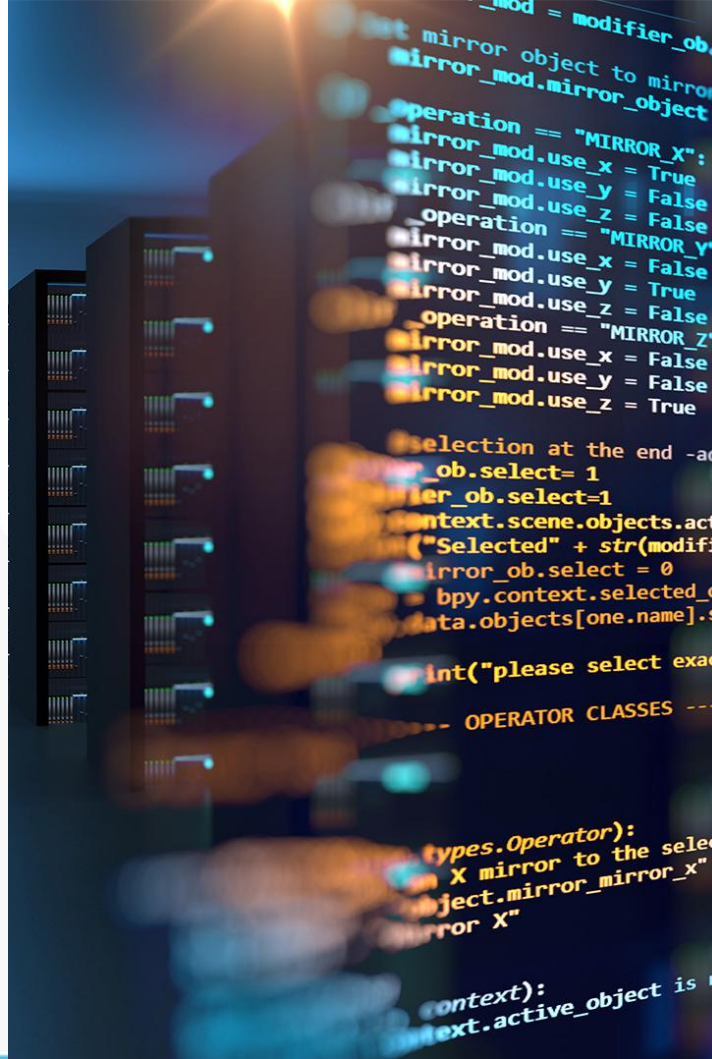
Безопасен ли Asterisk?

Так же стоит отметить, что много бед бывает от пионеров-интеграторов



Уровни защиты IP-АТС

1. Сетевая защита (IPTables + VPN + VLAN)
2. Защита конфигурации Asterisk (SIP + modules)
3. Защита подсистем (сертификаты + обновление)
4. Защита периферии
5. Административные меры
6. Мониторинг (логи + системы мониторинга)
7. Дополнительные средства защиты



IPTables



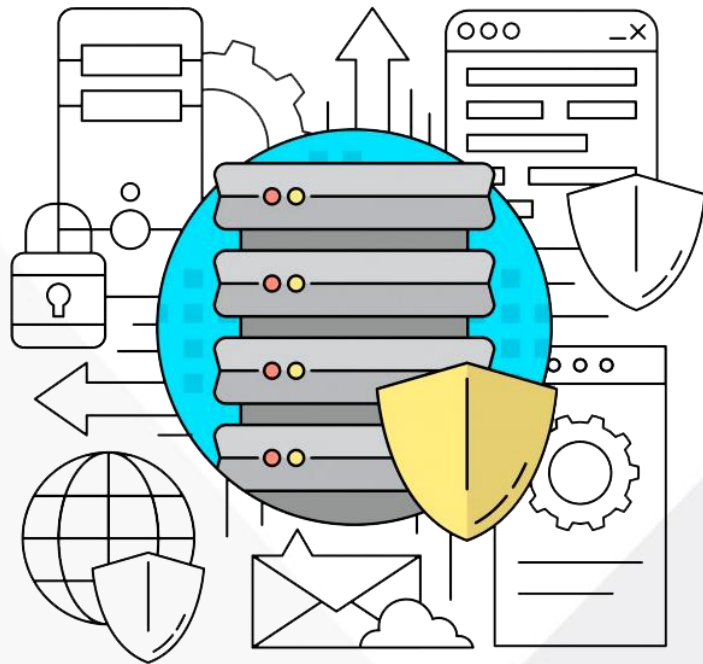
Сетевая защита

IPTables - мощный и гибкий сетевой firewall Linux (входит по умолчанию)

Управляется простыми командами

Принцип работы предельно прост:

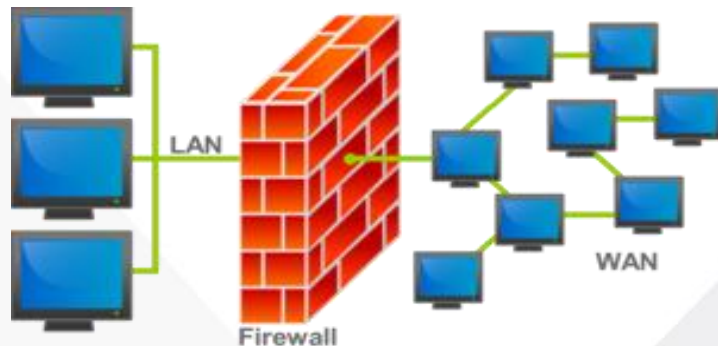
1. Создаем цепочки и наполняем их соответствующими IP-адресами
2. «Гоним» трафик в эти цепочки
3. Если трафик не попал ни в одну, то удаляем его



Сетевая защита

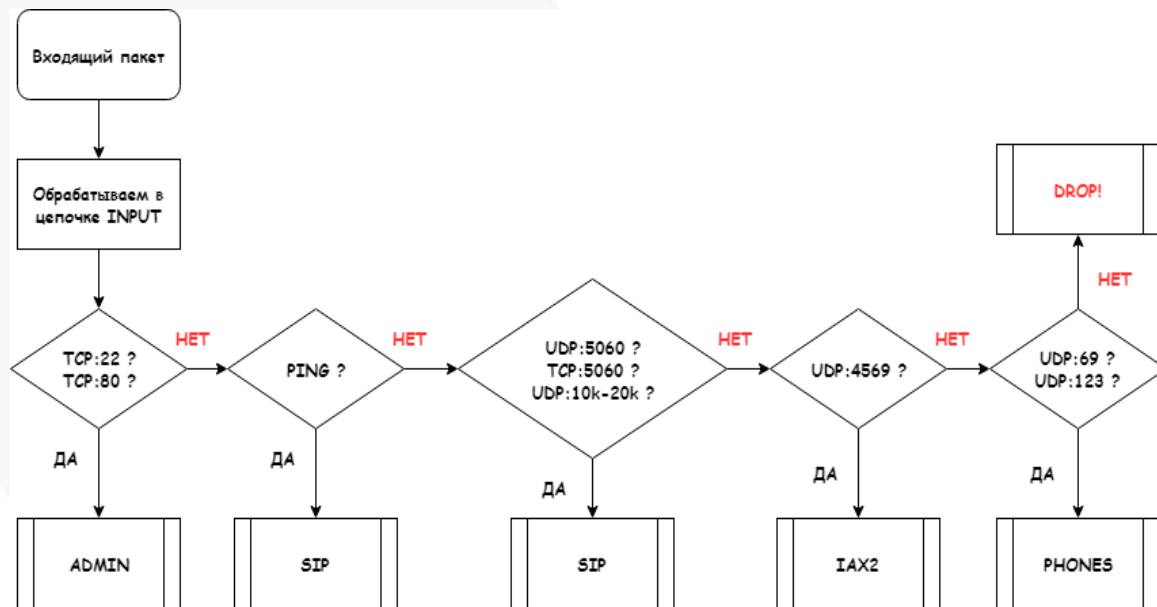
Пример работы с IPTables

- `chkconfig iptables add` – добавляем в автозагрузку
- `service iptables start` – запускаем iptables
- `iptables -L` – просмотр действующих правил
- `iptables -N ADMIN` – создаем новую цепочку
- `iptables -A ADMIN -i eth0 -s 192.168.10.0/24 -j ACCEPT` – добавляем в цепочку правило
- `iptables-save > somefile.txt`
- `nano somefile.txt`
- `iptables-restore < somefile.txt`
- `service iptables save`



Сетевая защита

Пример работы IPTables в виде диаграммы для цепочки INPUT



Сетевая защита

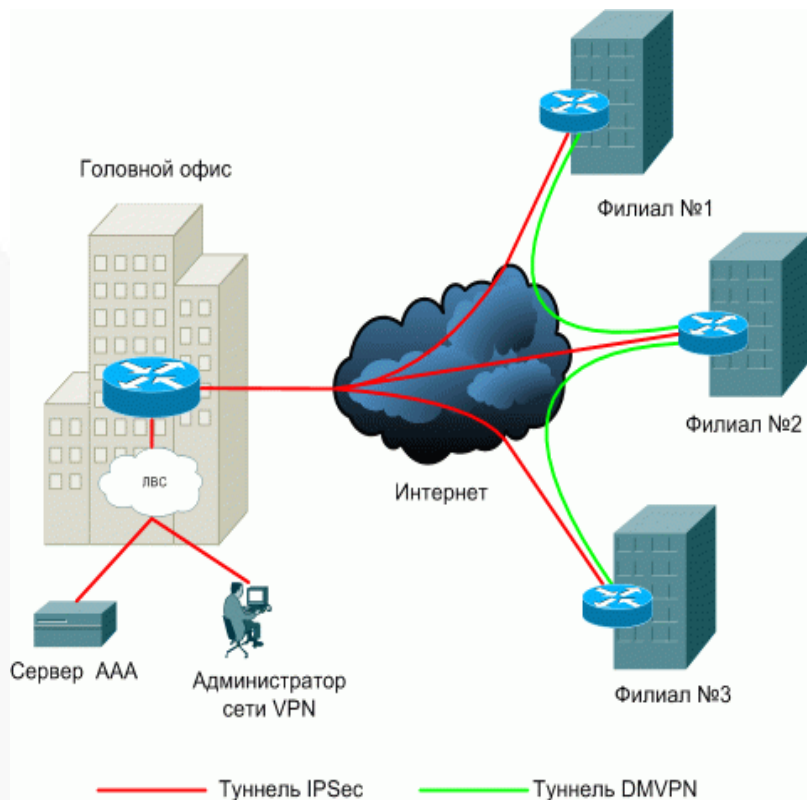
Удаленные сети: VPN

Проблема: удаленные устройства подключаются по публичным сетям

Последствия:

- Перехват трафика
- Публикация SIP-сервера

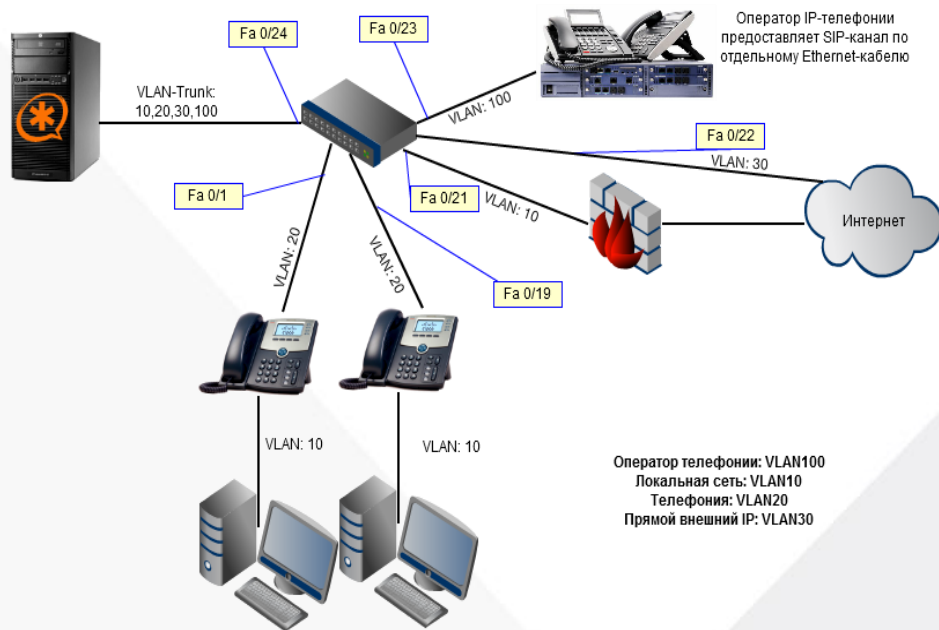
Решение: объединение всех подразделений компании в общую VPN-сеть



Сетевая защита

VLAN – виртуальная локальная сеть

- Основная задача – разделение сети данных и сети телефонии
- Для реализации необходим управляемый коммутатор



Fail2Ban



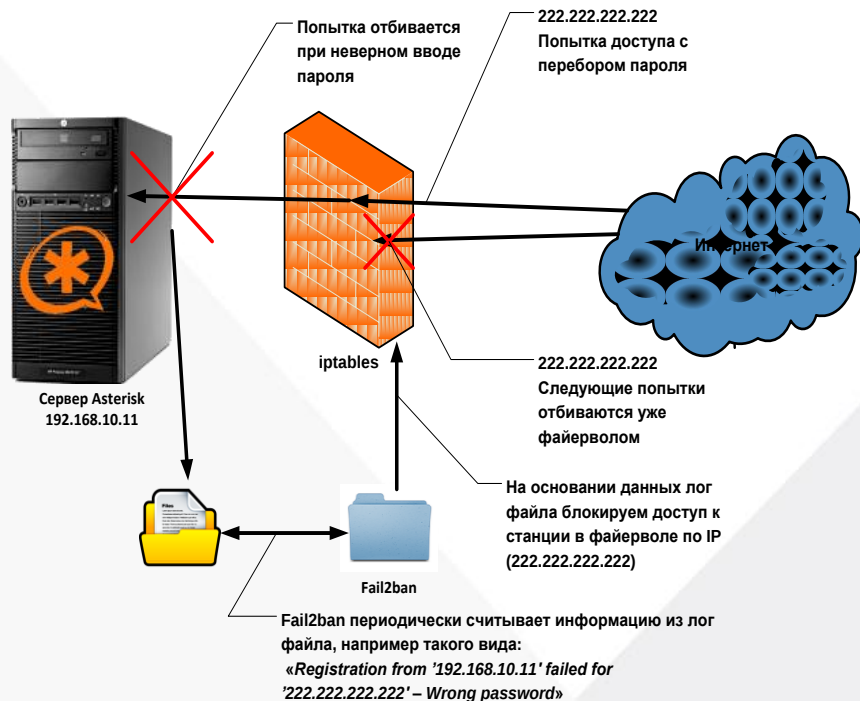
Fail2Ban – главный убийца сканеров и ботов (и невнимательных админов)



Сетевая защита: Fail2Ban

Fail2Ban – внешняя система защиты от перебора паролей (BruteForce)

- Принцип работы – Чтение логов и обнаружение попыток входа
- Работает со службами:
 1. Asterisk
 2. SSH
 3. Apache
 4. FTP и пр.



Сетевая защита: Fail2Ban

Конфигурация Fail2Ban производится в файлах:

- `/etc/fail2ban/jail.conf`
- `/etc/fail2ban/action.d/iptables.conf`
- `/etc/fail2ban/filter.d/asterisk.conf`
- `/etc/fail2ban/filter.d/sshd.conf`



Сетевая защита: Fail2Ban

/etc/fail2ban/jail.conf

```
[DEFAULT]
ignoreip = 127.0.0.1 10.10.0.0/16
bantime = 86400
findtime = 600
maxretry = 3
backend = auto

[asterisk-iptables]
enabled = true
filter = asterisk
action = iptables-allports[name=SIP, protocol=all]
        sendmail-whois[name=SIP, dest=log@voxlink.ru, sender=fail2ban@voxlink.ru]
logpath = /var/log/asterisk/fail2ban
maxretry = 5
bantime = 86400

[ssh-iptables]
enabled = true
filter = sshd
action = iptables[name=SSH, port=ssh, protocol=tcp]
        sendmail-whois[name=SSH, dest=log@voxlink.ru, sender=fail2ban@voxlink.ru]
logpath = /var/log/secure
maxretry = 3

[apache-tcpwrapper]
enabled = true
filter = apache-auth
action = iptables-allports[name=PBX-GUI, port=http, protocol=tcp]
        sendmail-whois[name=PBX-GUI, dest=log@voxlink.ru, sender=fail2ban@voxlink.ru]
logpath = /var/log/httpd/error_log
maxretry = 3
```



Сетевая защита: Fail2Ban

/etc/fail2ban/action.d/iptables.conf

```
[Definition]

# Option: actionstart
# Notes.: command executed once at the start of Fail2Ban.
# Values: CMD
#
actionstart = iptables -N fail2ban-<name>
              iptables -A fail2ban-<name> -j RETURN
              iptables -I INPUT -p <protocol> --dport <port> -j fail2ban-<name>

# Option: actionstop
# Notes.: command executed once at the end of Fail2Ban
# Values: CMD
#
actionstop = iptables -D INPUT -p <protocol> --dport <port> -j fail2ban-<name>
              iptables -F fail2ban-<name>
              iptables -X fail2ban-<name>

# Option: actioncheck
# Notes.: command executed once before each actionban command
# Values: CMD
#
actioncheck = iptables -n -L INPUT | grep -q fail2ban-<name>

# Option: actionban
# Notes.: command executed when banning an IP. Take care that the
#         command is executed with Fail2Ban user rights.
# Tags:   <ip> IP address
#         <failures> number of failures
#         <time> unix timestamp of the ban time
# Values: CMD
#
actionban = iptables -I fail2ban-<name> 1 -s <ip> -j DROP

# Option: actionunban
# Notes.: command executed when unbanning an IP. Take care that the
#         command is executed with Fail2Ban user rights.
# Tags:   <ip> IP address
#         <failures> number of failures
#         <time> unix timestamp of the ban time
# Values: CMD
#
actionunban = iptables -D fail2ban-<name> -s <ip> -j DROP
```



Сетевая защита: Fail2Ban

/etc/fail2ban/filter.d/asterisk.conf

```
failregex = Registration from '.*' failed for '<HOST>(:[0-9]{1,5})?' - Wrong password
            Registration from '.*' failed for '<HOST>(:[0-9]{1,5})?' - No matching peer found
            Registration from '.*' failed for '<HOST>(:[0-9]{1,5})?' - Device does not match ACL
            Registration from '.*' failed for '<HOST>(:[0-9]{1,5})?' - Username/auth name mismatch
            Registration from '.*' failed for '<HOST>(:[0-9]{1,5})?' - Peer is not supposed to register
            NOTICE.* <HOST> failed to authenticate as '.*'$
            NOTICE.* *: No registration for peer '.*' (from <HOST>)
            NOTICE.* *: Host <HOST> failed MD5 authentication for '.*' (.)
            VERBOSE.* logger.c: -- .*IP/<HOST>-.* Playing 'ss-noservice' (language '.*')
```

/etc/fail2ban/filter.d/sshd.conf

```
failregex = ^%(__prefix_line)s(?:error: PAM: )?Authentication failure for .* from <HOST>\s*$
            ^%(__prefix_line)s(?:error: PAM: )?User not known to the underlying authentication module for .* from <HOST>\s*$
            ^%(__prefix_line)sFailed(?:password|publickey) for .* from <HOST>(:? port \d*)?(?: ssh\d*)?$
            ^%(__prefix_line)sROOT LOGIN REFUSED.* FROM <HOST>\s*$
            ^%(__prefix_line)s[il](?:llegal|nvalid) user .* from <HOST>\s*$
            ^%(__prefix_line)sUser \S+ from <HOST> not allowed because not listed in AllowUsers$
            ^%(__prefix_line)sauthentication failure; logname=\S* uid=\S* euid=\S* tty=\S* ruser=\S* rhost=<HOST>(:?\s+user=.)?\s*$
            ^%(__prefix_line)srefused connect from \S+ \((<HOST>)\)\s*$
            ^%(__prefix_line)sAddress <HOST> .* POSSIBLE BREAK-IN ATTEMPT!\s*$
            ^%(__prefix_line)sUser \S+ from <HOST> not allowed because none of user's groups are listed in AllowGroups$
```



Сетевая защита: HoneyPot

HoneyPot – по сути это ресурс, задача которого отдаться хакеру, принять атаку, быть взломанным и рассказать нам в подробностях об этом

- Можно разместить ловушку для ip-адреса на порту Asterisk (например 5060), которая сразу будет банить любые обращения.
- Так же можно разместить ловушку например на MikroTik, если сеть с IP-АТС находится за NAT'ом (принцип примерно одинаковый)



Сетевая защита: CHECKDOMAIN

```
[root@localhost ~]# iptables -l -nv
Chain INPUT (policy DROP 129 packets, 16984 bytes)
pkts bytes target prot opt in out source destination
0 0 REJECT tcp -- * * 0.0.0.0/0 0.0.0.0/0 multiport dports 80,443 match-set f2b-httpd-auth src reject-with top-reset
0 0 REJECT tcp -- * * 0.0.0.0/0 0.0.0.0/0 multiport dports 22 match-set f2b-ssh-auth src reject-with top-reset
0 0 DROP all -- * * 0.0.0.0/0 0.0.0.0/0 match-set f2b-asterisk-auth src
44 34373 CHECKDOMAIN udp -- * * 0.0.0.0/0 0.0.0.0/0 udp dpt:5060 STRING match "REGISTER sip:" ALSO name bn TO 65535
36 27485 CHECKDOMAIN udp -- * * 0.0.0.0/0 0.0.0.0/0 udp dpt:5060 STRING match "INVITE sip:" ALSO name bn TO 65535
0 0 LOGGING tcp -- * * 0.0.0.0/0 0.0.0.0/0 state NEW top flags:0x17/0x02 reject-with top-reset
6 6960 DROP tcp -- * * 0.0.0.0/0 0.0.0.0/0 state NEW top flags:0x17/0x02
7000 12M ACCEPT all -- * * 0.0.0.0/0 0.0.0.0/0 state RELATED,ESTABLISHED
0 0 LOGGING tcp -- * * 0.0.0.0/0 0.0.0.0/0 state INVALID
0 0 DROP all -- * * 0.0.0.0/0 0.0.0.0/0 match-set blacklisted_nets src
25 1500 ACCEPT all -- !o * * 0.0.0.0/0 0.0.0.0/0
0 0 ADMIN icmp -- * * 0.0.0.0/0 0.0.0.0/0 icmp type 8
0 0 ADMIN tcp -- * * 0.0.0.0/0 0.0.0.0/0 tcp dpt:22
0 0 ADMIN tcp -- * * 0.0.0.0/0 0.0.0.0/0 tcp dpt:80
41 2132 ADMIN tcp -- * * 0.0.0.0/0 0.0.0.0/0 tcp dpt:443
0 0 SIP icmp -- * * 0.0.0.0/0 0.0.0.0/0 icmp type 8
0 0 SIP udp -- * * 0.0.0.0/0 0.0.0.0/0 udp dpt:5060
12 804 SIP udp -- * * 0.0.0.0/0 0.0.0.0/0 udp dpt:5060
0 0 SIP tcp -- * * 0.0.0.0/0 0.0.0.0/0 tcp dpt:5060
0 0 SIP tcp -- * * 0.0.0.0/0 0.0.0.0/0 tcp dpt:5061
0 0 SIP udp -- * * 0.0.0.0/0 0.0.0.0/0 udp dpt:36600:39999
0 0 IMX2 udp -- * * 0.0.0.0/0 0.0.0.0/0 udp dpt:4569
0 0 PHONES udp -- * * 0.0.0.0/0 0.0.0.0/0 udp dpt:69
0 0 PHONES tcp -- * * 0.0.0.0/0 0.0.0.0/0 tcp dpt:1989
0 0 PHONES udp -- * * 0.0.0.0/0 0.0.0.0/0 udp dpt:123
0 0 PHONES tcp -- * * 0.0.0.0/0 0.0.0.0/0 tcp dpt:80
0 0 ACCEPT icmp -- * * 0.0.0.0/0 0.0.0.0/0 icmp type 3 code 4
0 0 ACCEPT icmp -- * * 0.0.0.0/0 0.0.0.0/0 icmp type 11
0 0 ACCEPT icmp -- * * 0.0.0.0/0 0.0.0.0/0 icmp type 8 limit: avg 5/sec burst 5

Chain FORWARD (policy DROP 0 packets, 0 bytes)
pkts bytes target prot opt in out source destination

Chain OUTPUT (policy ACCEPT 5734 packets, 3173K bytes)
pkts bytes target prot opt in out source destination

Chain ADMIN (4 references)
pkts bytes target prot opt in out source destination
41 2132 VOXLINK all -- * * 0.0.0.0/0 0.0.0.0/0
41 2132 ACCEPT all -- eth0 * 192.168.178.4 0.0.0.0/0
0 0 RETURN all -- * * 0.0.0.0/0 0.0.0.0/0

Chain CHECKDOMAIN (2 references)
pkts bytes target prot opt in out source destination
80 61858 PHONES all -- * * 0.0.0.0/0 0.0.0.0/0
0 0 ACCEPT udp -- * * IP-адрес оператора связи 0.0.0.0/0 udp dpt:5060
22 17654 ACCEPT udp -- * * 0.0.0.0/0 0.0.0.0/0 udp dpt:5060 STRING match "Доменное имя" ALSO name bn TO 65535
36 27485 DROP udp -- * * 0.0.0.0/0 0.0.0.0/0 udp dpt:5060
```

Защита удалённых абонентов на АТС с помощью доменного имени и iptables

Для реализации необходимо:

1. Создать цепочку CHECKDOMAIN
2. Включить в нее цепочку для телефонов
3. Разрешить подключение по порту для указанного доменного имени и для ip-адреса оператора связи
4. Остальные подключения DROP'ать
5. Правило DROP обязательно должно быть в самом конце цепочки, но до правила RETURN



Сетевая защита: GEOIP



Определите регионы, которые вам важны.
Все остальные – забаньте на уровне
IPTables

Asterisk на внешнем IP.



Может ли Asterisk
на внешнем IP
быть
безопасным?



VOXLINK: ASTERISK
ПРОФЕССИОНАЛЬНО

Следующий шаг: Защита конфигурации Asterisk

Защита конфигурации Asterisk

Смена порта SIP

Проблема: если порт 5060 доступен из WAN, то он обязательно станет объектом BruteForce-атаки

Решение: смена порта директивой в sip.conf

- [general]
- bindport=5090



Смена порта 5060:



Защита конфигурации Asterisk

/etc/asterik/sip.conf

```
[general]
alwaysauthreject=yes //сообщение 401 Unauthorized
allowguest=no //запрещаем гостевые SIP-соединения
bindaddr=192.168.0.1
bindport=5090 //меняем порт
[101]
permit/deny=192.168.0.0/255.255.255.0 //разрешаем
или запрещаем сети
secret=nvi438NB8f3fsjffg //сложный пароль
call-limit=2
context=from-closed //используем различные
КОНТЕКСТЫ
```



Защита конфигурации Asterisk

Защита с помощью диалплана в extensions.conf (запреты вызовов)

```
[allow-all]
exten=>_X.,1,Dial(SIP/operator/${EXTEN})
[from-it]
exten=>_10X.,1,Dial(SIP/${EXTEN})
[from-buch]
exten=>_810.,1,Hangup()
exten=>_.,1,GoTo(allow-all,${EXTEN},1)
[from-boss]
exten=>_.,1,GoTo(allow-all,${EXTEN},1)
```

Разделение абонентов на контексты

```
[101]
context=from-it
[102]
context=from-buch
[103]
context=from-boss
```



Защита конфигурации Asterisk

Маскировка SIP

`/etc/asterisk/sip_general_custom.conf`

`useragent=ChuckNorrisPBX`

`realm=ChuckNorrisPBX`

`sdpsexp=ChuckNorrisPBX`



VOXLINK: ASTERISK

ПРОФЕССИОНАЛЬНО

А что насчет защиты PJSIP

Вряд ли кто-то лучше **Николая Шакина** сможет об этом рассказать, поэтому смотрите по ссылке его выступление с AsterConf-2019:

<http://tiny.cc/pjsip>

А мы пока продолжим дальше



*Нет, это не Николай



VOXLINK: ASTERISK
ПРОФЕССИОНАЛЬНО

ASTERCONF

ЕЖЕГОДНАЯ КОНФЕРЕНЦИЯ ПО ASTERISK



ДЛИТЕЛЬНОСТЬ:
2 дня



ПЕРИОДИЧНОСТЬ:
1 РАЗ В ГОД (СЕНТЯБРЬ)



СТОИМОСТЬ
3,000 РУБЛЕЙ



ПРОГРАММА И РЕГИСТРАЦИЯ:
<http://asterconf.ru>



Защита конфигурации Asterisk

Информирование о попытках звонков на 810.

exten => _810.,Playback(zapret-zvonkov)

same => n,System(echo \${EXTEN}> mail -s "8-10 ALARM!!!" admin@ya.ru)

same => n,Hangup()



Защита конфигурации Asterisk

Ограничение на право звонков по времени

```
Gotolftime(9:00-18:00|mon-fri|*|*?menu1,s,1)
```

```
[from-it]  
exten=>_810.,1,GoTo(mail-info,{EXTEN},1)  
exten=>_,1,Gotolftime(9:00-18:00|mon-fri|*|*?allow-all,{EXTEN},1)  
exten=>_,n, Playback(zapret-zvonkov)
```

```
[mail-info]  
exten => _X.,Playback(zapret-zvonkov)  
same => n,System(echo ${EXTEN}> mail -s "8-10 ALARM!!!" admin@ya.ru)  
same => n,Hangup()
```

```
[allow-all]  
exten=>_X.,1,Dial(SIP/operator/${EXTEN})  
exten=>_10X.,1,Dial(SIP/${EXTEN})
```



Защита конфигурации Asterisk

Ограничение на право звонков по времени

AdminApplicationsConnectivityDashboardReportsSettingsUCP

Outbound Routes

Edit Route

Route SettingsDial PatternsImport/Export PatternsAdditional Settings

Route Name ⓘ

MN

Route CID ⓘ

Override Extension ⓘ

YesNo

Route Password ⓘ

Route Type ⓘ

EmergencyIntra-Company

Music On Hold? ⓘ

default

Time Group ⓘ

0800-2000 Monday-Friday

If this route should only be available during certain times then it should always be available.

---Permanent Route---
0800-1700 ALL
0800-1700 Monday-Friday
0800-1700 Saturday-Sunday
0800-2000 ALL
0800-2000 Monday-Friday
0800-2000 Saturday-Sunday
0900-1800 ALL
0900-1800 Monday-Friday
0900-1800 Saturday-Sunday
1000-1900 ALL
1000-1900 Monday-Friday
1000-1900 Saturday-Sunday
Russian Holidays
Add New Time Group...

Route Position ⓘ

Trunk Sequence for Matched Routes ⓘ

Optional Destination on Congestion ⓘ

> SubmitDuplicateResetDelete



Защита конфигурации Asterisk

Защита динамических абонентов

Проблема: абонент подключается с внешних динамических IP.

Ограничение permit/deny – невозможно

Решение: используем контекст, в котором ограничиваем звонки на международные направления (целиком или по PIN-коду)



Защита конфигурации Asterisk

Отключение лишних модулей Asterisk

Выбираем заведомо ненужные модули и
отключаем их в конфигурационном файле
`/etc/asterisk/modules.conf`

`noload = res_pjsip_endpoint_identifier_anonymous.so`

`noload = res_pjsip_messaging.so`

`noload = res_pjsip_pidf.so`

`noload = res_pjsip_session.so`

`noload = func_pjsip_endpoint.so`

`noload = res_pjsip_endpoint_identifier_ip.so`

`noload = res_pjsip_mwi.so`

`noload = res_pjsip_pubsub.so`

`noload = res_pjsip.so`

`noload = res_pjsip_acl.so`

`noload = res_pjsip_endpoint_identifier_user.so`

`noload = res_pjsip_nat.so`

`noload = res_pjsip_refer.so`

`noload = res_pjsip_t38.so`

`noload = res_pjsip_authenticator_digest.so`

`noload = res_pjsip_exten_state.so`

`noload = res_pjsip_notify.so`

`noload = res_pjsip_registrar_expire.so`

`noload = res_pjsip_transport_websocket.so`

`noload = res_pjsip_caller_id.so`

`noload = res_pjsip_header_funcs.so`

`noload = res_pjsip_one_touch_record_info.so`

`noload = res_pjsip_registrar.so`

`noload = res_pjsip_diversion.so`

`noload = res_pjsip_log_forwarder.so`

`noload = res_pjsip_outbound_authenticator_digest.so`

`noload = res_pjsip_rfc3326.so`

`noload = res_pjsip_dtmf_info.so`

`noload = res_pjsip_logger.so`

`noload = res_pjsip_outbound_registration.so`

`noload = res_pjsip_sdp_rtp.so`

`noload = res_pjsip_outbound_publish.so`

`noload = res_pjsip_config_wizard.so`



VOXLINK: ASTERISK

ПРОФЕССИОНАЛЬНО



Обсудим защиту подсистем

Защита подсистем

```
[root@hk-met ~]# chkconfig --list
acpid          0:off 1:off 2:on 3:on 4:on 5:on 6:off
asterisk       0:off 1:off 2:off 3:off 4:off 5:off 6:off
atd            0:off 1:off 2:off 3:on 4:on 5:on 6:off
atop           0:off 1:off 2:off 3:off 4:off 5:off 6:off
auditd        0:off 1:off 2:on 3:on 4:on 5:on 6:off
blk-availability 0:off 1:on 2:on 3:on 4:on 5:on 6:off
callmetrix     0:off 1:off 2:on 3:on 4:on 5:on 6:off
corosync       0:off 1:off 2:off 3:off 4:off 5:off 6:off
crond          0:off 1:off 2:on 3:on 4:on 5:on 6:off
dahdi          0:off 1:off 2:on 3:on 4:on 5:on 6:off
dnsmasq        0:off 1:off 2:on 3:on 4:on 5:on 6:off
drbd           0:off 1:off 2:off 3:off 4:off 5:off 6:off
fail2ban       0:off 1:off 2:on 3:on 4:on 5:on 6:off
garb           0:off 1:off 2:off 3:off 4:off 5:off 6:off
heartbeat      0:off 1:off 2:off 3:off 4:off 5:off 6:off
htcacheclean   0:off 1:off 2:off 3:off 4:off 5:off 6:off
htopd          0:off 1:off 2:on 3:on 4:on 5:on 6:off
ip6tables      0:off 1:off 2:on 3:on 4:on 5:on 6:off
ipset          0:off 1:off 2:on 3:on 4:on 5:on 6:off
iptables       0:off 1:off 2:on 3:on 4:on 5:on 6:off
irqbalance     0:off 1:off 2:off 3:on 4:on 5:on 6:off
iscsi          0:off 1:off 2:off 3:on 4:on 5:on 6:off
isnsd          0:off 1:off 2:off 3:on 4:on 5:on 6:off
lm_sensors     0:off 1:off 2:off 3:off 4:off 5:off 6:off
lvm2-monitor   0:off 1:on 2:on 3:on 4:on 5:on 6:off
mdmmonitor     0:off 1:off 2:on 3:on 4:on 5:on 6:off
multipathd     0:off 1:off 2:off 3:off 4:off 5:off 6:off
myaqa          0:off 1:off 2:on 3:on 4:on 5:on 6:off
netconsole     0:off 1:off 2:off 3:off 4:off 5:off 6:off
netfs          0:off 1:off 2:off 3:off 4:off 5:off 6:off
network        0:off 1:off 2:on 3:on 4:on 5:on 6:off
nfs            0:off 1:off 2:off 3:off 4:off 5:off 6:off
nfs-rdma       0:off 1:off 2:off 3:off 4:off 5:off 6:off
nfslock        0:off 1:off 2:off 3:off 4:off 5:off 6:off
ntpd           0:off 1:off 2:on 3:on 4:on 5:on 6:off
ntpdate        0:off 1:off 2:off 3:off 4:off 5:off 6:off
openvpn        0:off 1:off 2:on 3:on 4:on 5:on 6:off
pandora_agent_daemon 0:off 1:off 2:on 3:on 4:on 5:on 6:off
postfix        0:off 1:off 2:on 3:on 4:on 5:on 6:off
quota_nld      0:off 1:off 2:off 3:off 4:off 5:off 6:off
rsync          0:off 1:off 2:off 3:off 4:off 5:off 6:off
rdma           0:off 1:on 2:on 3:on 4:on 5:on 6:off
restorecond    0:off 1:off 2:off 3:off 4:off 5:off 6:off
rpcbind        0:off 1:off 2:off 3:off 4:off 5:off 6:off
rpcgsd         0:off 1:off 2:off 3:off 4:off 5:off 6:off
rpcidmapd      0:off 1:off 2:off 3:off 4:off 5:off 6:off
rpcsvcgsd      0:off 1:off 2:off 3:off 4:off 5:off 6:off
rsyslog        0:off 1:off 2:on 3:on 4:on 5:on 6:off
saslauthd      0:off 1:off 2:off 3:off 4:off 5:off 6:off
smartd         0:off 1:off 2:off 3:off 4:off 5:off 6:off
snmpd          0:off 1:off 2:off 3:off 4:off 5:off 6:off
snmpttrapd     0:off 1:off 2:off 3:off 4:off 5:off 6:off
sshd           0:off 1:off 2:on 3:on 4:on 5:on 6:off
svnserve       0:off 1:off 2:off 3:off 4:off 5:off 6:off
sysstat        0:off 1:on 2:on 3:on 4:on 5:on 6:off
udev-post      0:off 1:on 2:on 3:on 4:on 5:on 6:off
vsftpd         0:off 1:off 2:off 3:off 4:off 5:off 6:off
winbind        0:off 1:off 2:off 3:off 4:off 5:off 6:off
xinetd         0:off 1:off 2:off 3:on 4:on 5:on 6:off
```

Отключение лишних служб

`chkconfig --list` - просмотр служб

`chkconfig someservice off` – отключение службы

```
xinetd based services:
  chargen-dgram:  off
  chargen-stream: off
  daytime-dgram:  off
  daytime-stream: off
  discard-dgram:  off
  discard-stream: off
  echo-dgram:     off
  echo-stream:    off
  rsync:          off
  tcpmux-server:  off
  tftp:           on
  time-dgram:     off
  time-stream:    off
```

Защита подсистем

Вход по SSH с использованием сертификата

```
login as: root
Authenticating with public key "rsa-key-20191008" from agent
Last login: Fri Oct 25 19:38:06 2019 from [REDACTED]
.....
.... qooo. `OBb      Hostname:
qooo. YQOb. `#VOob `H#A      Date:          Fri 2019-10-25 19:40 +05
g#qobibYgobi#Yoob.i#i.      Uptime:         1:01
H#:`obqI qobH:`qobIiI:      Load average:   0.18 0.19 0.11
H#I `Yoi Yoi: `Yobii.
d#; ioP ioI: iIoiJ      Network interfaces:
d#P AO' AoP Aool      em1
''' dOP .ooP          em2
'''                  tun0
Default gateway: [REDACTED]

Tech Support:
+7 (495) 989-85-33
911
(only phones connected
to this PBX)

Occupied disk space:
/ 4.0G/19G
/dev/shm 0/16G
/boot 31M/283M
/mnt/sda_data 864M/897G

Active calls: 0/100
Processed calls: 39
Asterisk uptime: 4:01
SIP peers online: 73/127

To create FreePBX user or change password, use:
fpbx_passwd -u <user> [-p <password>]
```



Защита подсистем

Генерация SSH-ключа

1. `ssh-keygen -t dsa`
2. Конфиг для `sshd.conf`:
 - `RSAAuthentication yes`
 - `PubkeyAuthentication yes`
 - `PasswordAuthentication no`
3. Скопируйте открытый ключ на сервер



Защита подсистем

Ограничение доступа к Apache

ServerSignature Off

ServerTokens Prod

```
<Directory>
```

```
Order Deny,Allow
```

```
Deny from all
```

```
Allow from 192.168.10.0/24
```

```
<Directory>
```



VOXLINK: ASTERISK

ПРОФЕССИОНАЛЬНО

Защита подсистем

Asterisk Manager Interface он же AMI

Контроль учетных записей и ACL в /etc/asterisk/manager.conf

```
;
; AMI - Asterisk Manager interface
;
; FreePBX needs this to be enabled. Note that if you enable it on a different IP, you need
; to assure that this can't be reached from un-authorized hosts with the ACL settings (permit/deny).
; Also, remember to configure non-default port or IP-addresses in amportal.conf.
;
; The AMI connection is used both by the portal and the operator's panel in FreePBX.
;
; FreePBX assumes an AMI connection to localhost:5038 by default.
;
[general]
enabled = yes
port = 5038
bindaddr = 0.0.0.0
displayconnects=no ;only effects 1.6+

[admin]
secret = 0fe461bea5d1bbacd2fc8123d01
deny=0.0.0.0/0.0.0.0
permit=127.0.0.1/255.255.255.0
read = system,call,log,verbose,command,agent,user,config,command,dtmf,reporting,cdr,dialplan,originate,message
write = system,call,log,verbose,command,agent,user,config,command,dtmf,reporting,cdr,dialplan,originate,message
writetimeout = 5000

#include manager_additional.conf
#include manager_custom.conf
```



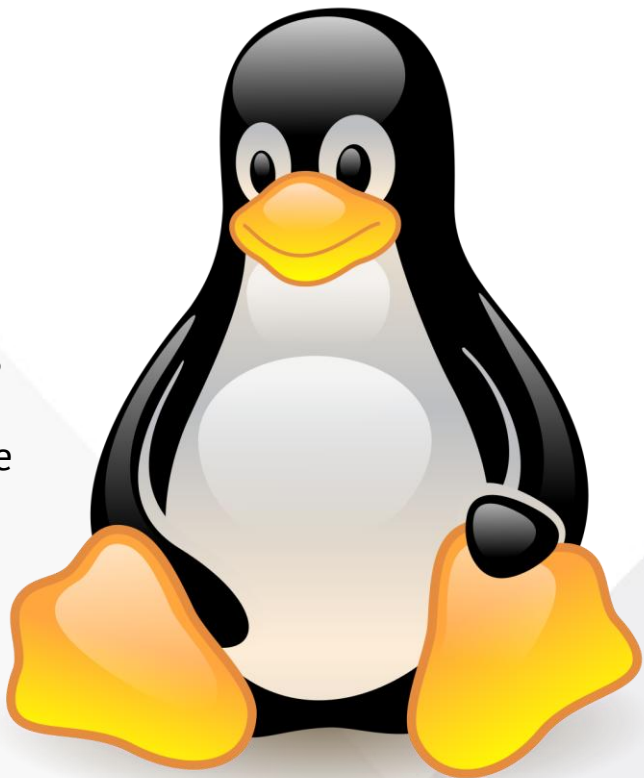
Защита подсистем

Обновление системы

При «ручной» установке необходимо обновить Linux до момента установки.

На работающей системе необходимо проводить обновление, предварительно сделав бэкап. Желательно сначала протестировать обновление на виртуальной машине, так как переход на новые версии опасен проблемами с совместимостью конфигураций

Само обновление простое:
yum update -y



Защита подсистем

Обновление Asterisk

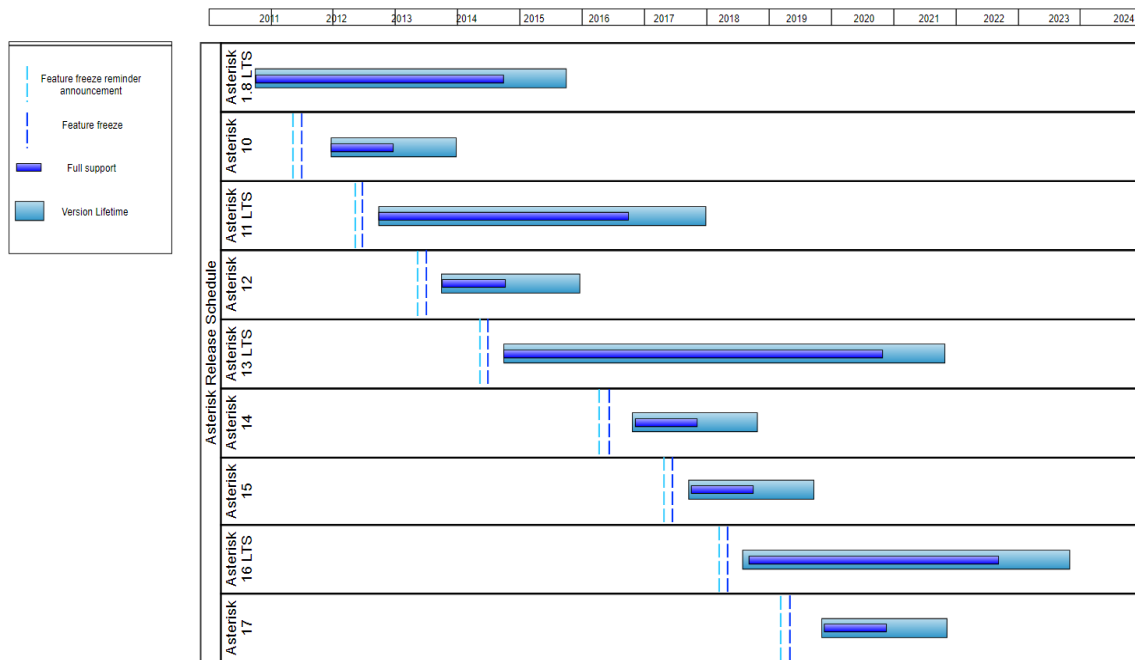
Целесообразно проводить обновление Asterisk только в том случае, если новая версия решает проблемы безопасности, которые можно использовать в вашей конфигурации

Беспроblemное обновление – в пределах той же мажорной версии (1.8, 10, 11)



Защита подсистем

Версионность Asterisk



Защита подсистем

Обновление FreePBX (13->14)

Перед обновлением так же настоятельно рекомендуется сделать бэкап
В **Dashboard** графической оболочки должно появиться уведомление о доступности новой версии

В консоли сервера выполняем команду: `fwconsole ma downloadinstall versionupgrade`
После установки модуля переходим в интерфейс FreePBX:

- Apply config
- Admin -> 13 to 14 Upgrade Tool
- Check the requirements!
- Выбираем дистрибутив
- Ждем окончания обновления
- Apply config

Чаще всего требуется обновить локальные и коммерческие модули для обновления и зарегистрировать систему

Защита подсистем

Обновление FreePBX (13->14)

Admin Applications Connectivity Dashboard Reports Se

System Overview

Welcome to FreePBX

FreePBX [redacted]
(You can change this name in Advanced Settings)

Summary Sysinfo updated 10 seconds ago

Asterisk	✓
Firewall Configuration	✗
MySQL	✓
Fail2Ban	✓
System Registration	✓
Web Server	✓
System Firewall	✓
Prosody (XMPP)	✓
XMPP Presence	✓

Critical Errors found
Please check for errors in the notification section

1 Новый модуль доступен

Следующие новые модули доступны для скачивания. Кликнуть на значок Удалить справа чтобы удалить это сообщение.
versionupgrade (13.0.1)

Resolve 1 Week, 3 Days, 23 Hours, 53 Minutes, 59 Seconds, Ago

Show All

Admin Applications Connectivity Dashboard Reports Settings UCP Overview Trunk Balance

Welcome to the FreePBX 14 updater

Prepare to experience a whole new way to accomplish Telephony and VoIP

FreePBX 14 provides many exciting new features. [Click here to learn more](#)

1

2 Step 2
Upgrade System

Step 1 Verify System Information

To help us learn more about who is using FreePBX please verify the information below

Distribution

FreePBX Distro (Default)

The distribution of this system. This is defaulted to what FreePBX has determined the system to be. Please change it if it is wrong.

Previous Next

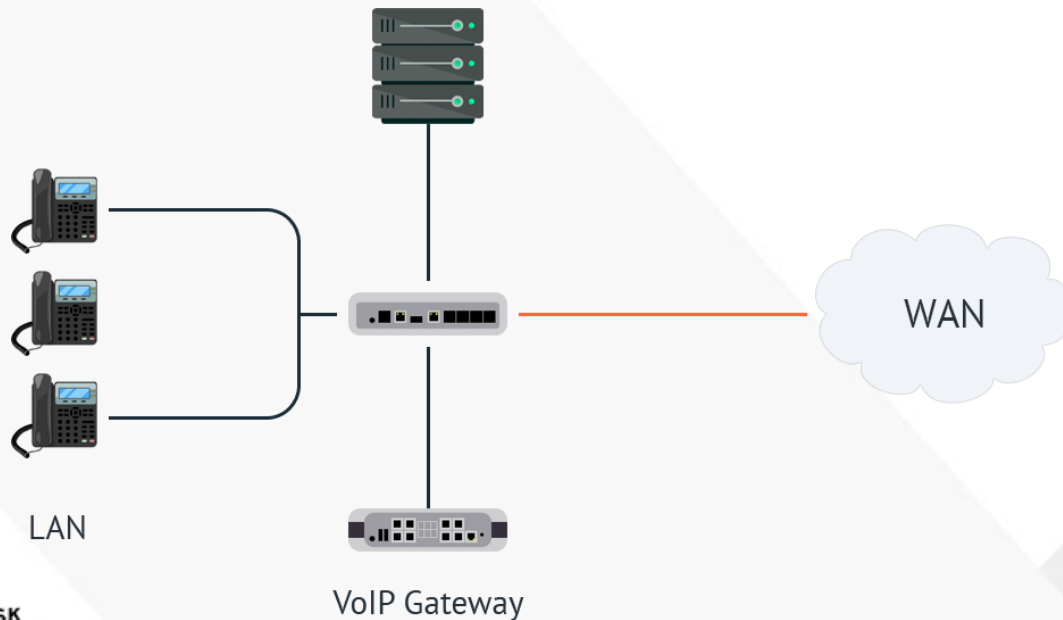


А теперь немного о защите периферии

Защита периферии

Размещение до/после Firewall

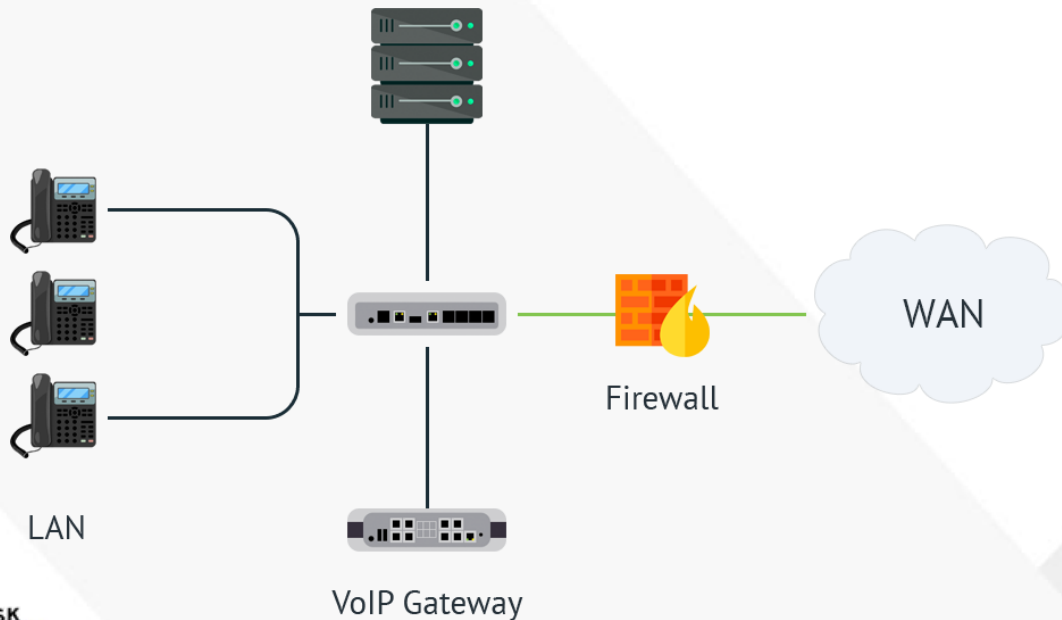
Вот так делать не следует:



Защита периферии

Размещение до/после Firewall

Нужно вот так:



Защита периферии

Пароли на web-интерфейс и/или отключение

Одна из серьезных уязвимостей оборудования это web-интерфейс. Очевидно, что его необходимо защитить хорошим паролем или по возможности вообще отключить.

The screenshot displays the Cisco SPA303 Configuration Utility web interface. The top navigation bar includes 'Small Business', 'cisco', 'SPA303 Configuration Utility', and links for 'User Login', 'basic', and 'adv'. Below this is a tabbed interface with 'Voice', 'Call History', and 'Personal Directory'. The 'System' tab is selected, showing a sub-tabbed interface with 'Info', 'System', 'SIP', 'Provisioning', 'Regional', 'Phone', 'User', and 'Attendant Keys'. The 'System' sub-tab is active, displaying various configuration options. A red box highlights the 'Restricted Access Domains' section, which includes a text input field for 'указываем список доменов с которых запрещен доступ в веб-интерфейс'. Below this are several settings: 'Enable Web Server' (yes), 'Enable Web Admin Access' (yes), 'User Password' (empty), 'SPCP Auto-detect' (yes), and 'Phone-UI-user-mode' (no). To the right, there are fields for 'Web Server Port' (80), 'Admin Passwd' (empty), 'Signaling Protocol' (SIP), and 'Phone-UI-readonly' (no). At the bottom, there are sections for 'Internet Connection Type' (Connection Type: DHCP) and 'Static IP Settings' (Static IP: empty, NetMask: empty). The bottom of the interface features 'Undo All Changes' and 'Submit All Changes' buttons, along with the 'voxlinc' logo.

Info	System	SIP	Provisioning	Regional	Phone	User	Attendant Keys
Ext 1	Ext 2	Ext 3					
Restricted Access Domains указываем список доменов с которых запрещен доступ в веб-интерфейс							
Enable Web Server:		yes		Web Server Port:		80	
Enable Web Admin Access:		yes		Admin Passwd:		Установка пароли администратора	
User Password:		Установка пароли пользователя		Signaling Protocol:		SIP	
SPCP Auto-detect:		yes		Phone-UI-readonly:		no	
Phone-UI-user-mode:		no					
Internet Connection Type							
Connection Type:		DHCP					
Static IP Settings							
Static IP:				NetMask:			
Undo All Changes Submit All Changes							



Защита периферии

Пароли на web-интерфейс и/или отключение

Так же хорошим примером является станция TGP-600 от Panasonic. Её вебка отключена по умолчанию и запускается только с одной из трубок, а время сессии строго ограничено (15 минут)



Защита периферии

Смена сервисных портов

На телефонах и шлюзах рекомендуется менять сервисные порты, например порт SIP с 5060 на любой другой. Это повышает устойчивость к сканированиям.

The screenshot shows the Yealink T21P-E2 web interface. The top navigation bar includes 'Status', 'Account', 'Network', 'Dsskey', 'Features', 'Settings' (selected), 'Directory', and 'Security'. The left sidebar lists configuration options: Preference, Time&Date, Call Display, Upgrade, Auto Provision, Configuration, Dial Plan, Voice, Ring, Tones, Softkey Layout, TR069, Voice Monitoring, SIP (selected), and Power Saving. The main content area is titled 'SIP Config' and contains the following settings:

Setting	Value
SIP Session Timer T1 (0.5~10s)	0.5
SIP Session Timer T2 (2~40s)	4
SIP Session Timer T4 (2.5~60s)	5
Local SIP Port	50753
TLS SIP Port	5061

Buttons for 'Confirm' and 'Cancel' are located below the settings. A 'NOTE' section on the right provides additional information:

SIP Session Timers
SIP session timers T1, T2 and T4 are SIP transaction layer timers defined in RFC 3261.

Timer T1 is an estimate of the Round Trip Time (RTT) of transactions between a SIP client and SIP server.

Timer T2 represents the maximum retransmitting time of any SIP request message.

Timer T4 represents the time the network will take to clear messages between the SIP client and server.

[Click here to get more product documents.](#)

Copyright © 1998-2019 **Inc. All Rights Reserved



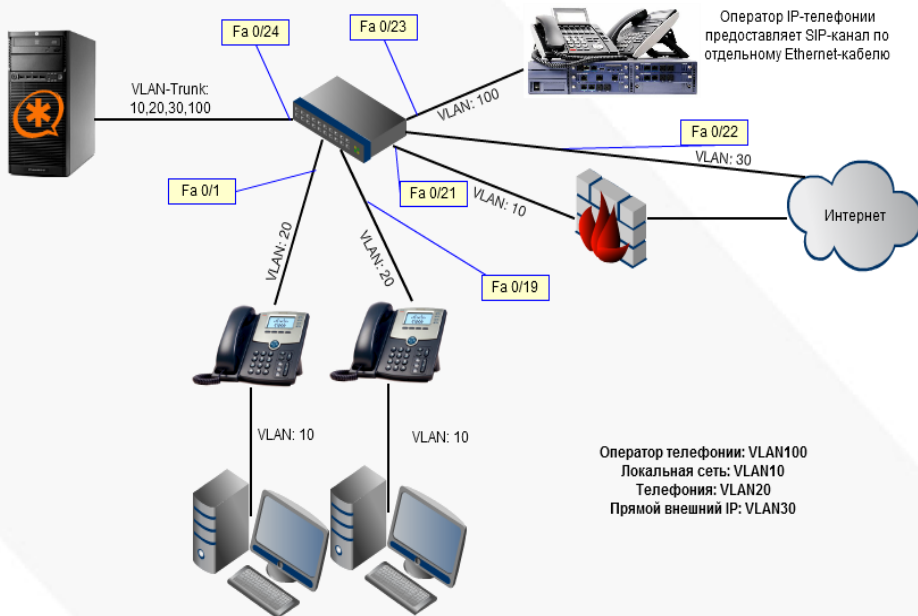
VOXLINK: ASTERISK

ПРОФЕССИОНАЛЬНО

Защита периферии

Голосовой VLAN

Голосовой VLAN используется для выделения VoIP-оборудования в отдельную VLAN-сеть
Для VoIP-фреймов могут быть назначены QoS-атрибуты для приоритезации трафика



Защита периферии

Обновление прошивки

Очень важно всегда поддерживать актуальность ПО на телефонах, т.к. производитель тоже не дремлет и по мере сил убирает известные уязвимости

The screenshot displays the Yealink T21P_F2 web interface. The top navigation bar includes 'Status', 'Account', 'Network', 'Dsskey', 'Features', 'Settings' (selected), 'Directory', and 'Security'. A left sidebar lists various settings: 'Preference', 'Time&Date', 'Call Display', 'Upgrade' (selected), 'Auto Provision', 'Configuration', 'Dial Plan', 'Voice', 'Ring', 'Tones', 'Softkey Layout', 'TR069', 'Voice Monitoring', 'SIP', and 'Power Saving'. The main content area is titled 'Upgrade' and shows the 'Select And Upgrade Firmware' section with a 'Browse...' button. Other sections include 'Version' (Firmware Version: 52.84.0.15, Hardware Version: 52.0.0.0.0.0.0), 'Reset' (Reset to Factory), and 'Reboot' (Reboot). A right sidebar contains a 'NOTE' section with links for 'Reset to Factory Setting', 'Reboot', and 'Upgrading Firmware'. The footer indicates 'Copyright © 1998-2019 **Inc. All Rights Reserved'.



Защита периферии

Stealth-mode:
найдите способы сделать
своё периферийное
оборудование
незаметным для любых
сканирований



VOXLINK: ASTERISK
ПРОФЕССИОНАЛЬНО

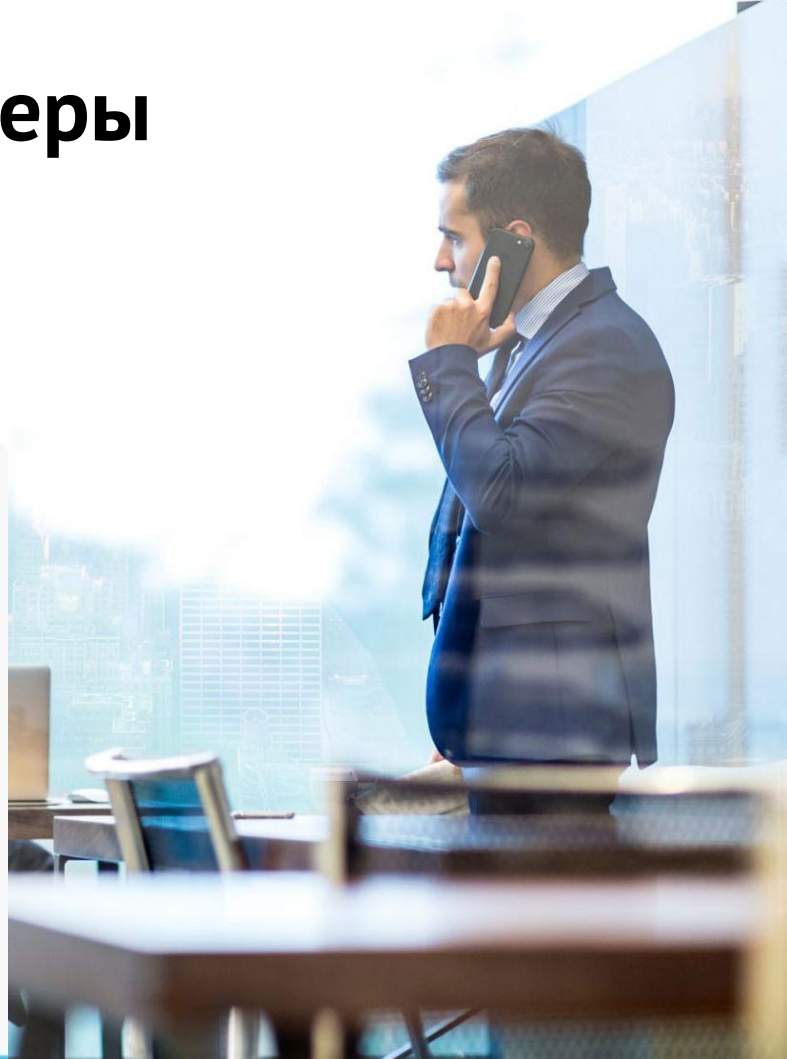


Пара слов об административных мерах защиты IP-АТС

Административные меры

Основные:

- Запрет межгорода на уровне оператора
- Ограничение по IP на транк
- Ограничение на сумму счета или авансовая оплата
- Защита рабочих станций с софтбонами
- Смена паролей при смене сис.админа



Мониторинг

Мониторинг

Мониторинг логов

Для обеспечения безопасности IP-АТС крайне важно следить за логами событий. Так мы будем знать что вообще происходит на станции, пытаются ли ее брутфорсить, поймал ли кого fail2ban, регистрируются ли корректно у нас телефоны, отбиваются ли ошибки по БД и многое другое

Asterisk по умолчанию хранит свои логи в:
/var/log/asterisk/full
Настраивается в:
/etc/asterisk/logger.conf

```
[2019-07-25 06:39:49] WARNING[10537] pbx_config.c: Unable to register extension at line 3743 of /etc/asterisk/extensions_additional.conf
[2019-07-25 06:39:49] WARNING[10537] pbx_config.c: Unable to register extension at line 3744 of /etc/asterisk/extensions_additional.conf
[2019-07-25 06:39:49] WARNING[10537] pbx_config.c: Unable to register extension at line 3745 of /etc/asterisk/extensions_additional.conf
[2019-07-25 06:39:49] WARNING[10537] pbx_config.c: Unable to register extension at line 3760 of /etc/asterisk/extensions_additional.conf
[2019-07-25 06:39:49] WARNING[10537] pbx_config.c: Unable to register extension at line 3761 of /etc/asterisk/extensions_additional.conf
[2019-07-25 06:39:49] WARNING[10537] pbx_config.c: Unable to register extension at line 3762 of /etc/asterisk/extensions_additional.conf
[2019-07-25 06:39:49] WARNING[10537] pbx_config.c: Unable to register extension at line 3763 of /etc/asterisk/extensions_additional.conf
[2019-07-25 06:39:49] WARNING[10537] pbx_config.c: Unable to register extension at line 3764 of /etc/asterisk/extensions_additional.conf
[2019-07-25 06:39:49] WARNING[10537] pbx_config.c: Unable to register extension at line 3765 of /etc/asterisk/extensions_additional.conf
[2019-07-25 06:39:49] WARNING[10537] pbx_config.c: Unable to register extension at line 3766 of /etc/asterisk/extensions_additional.conf
[2019-07-25 06:39:49] WARNING[10537] pbx_config.c: Unable to register extension at line 3767 of /etc/asterisk/extensions_additional.conf
[2019-07-25 06:39:49] WARNING[10537] pbx_config.c: Unable to register extension at line 3768 of /etc/asterisk/extensions_additional.conf
[2019-07-25 06:39:49] WARNING[10537] pbx_config.c: Unable to register extension at line 3769 of /etc/asterisk/extensions_additional.conf
[2019-07-25 06:39:49] WARNING[10537] pbx_config.c: Unable to register extension at line 3770 of /etc/asterisk/extensions_additional.conf
[2019-07-25 06:39:49] WARNING[10537] pbx_config.c: Unable to register extension at line 3771 of /etc/asterisk/extensions_additional.conf
[2019-07-25 06:39:49] WARNING[10537] pbx_config.c: Unable to register extension at line 3802 of /etc/asterisk/extensions_additional.conf
[2019-07-25 06:39:49] WARNING[10537] pbx_config.c: Unable to register extension at line 3803 of /etc/asterisk/extensions_additional.conf
[2019-07-25 06:39:49] WARNING[10537] pbx_config.c: Unable to register extension at line 3804 of /etc/asterisk/extensions_additional.conf
[2019-07-25 06:39:49] WARNING[10537] pbx_config.c: Unable to register extension at line 3805 of /etc/asterisk/extensions_additional.conf
[2019-07-25 06:39:49] WARNING[10537] pbx_config.c: Unable to register extension at line 3806 of /etc/asterisk/extensions_additional.conf
[2019-07-25 06:39:49] WARNING[10537] pbx_config.c: Unable to register extension at line 3807 of /etc/asterisk/extensions_additional.conf
[2019-07-25 06:39:49] WARNING[10537] pbx_config.c: Unable to register extension at line 3808 of /etc/asterisk/extensions_additional.conf
[2019-07-25 06:39:49] WARNING[10537] pbx_config.c: Unable to register extension at line 3809 of /etc/asterisk/extensions_additional.conf
[2019-07-25 06:39:49] WARNING[10537] pbx_config.c: Unable to register extension at line 3810 of /etc/asterisk/extensions_additional.conf
[2019-07-25 06:39:49] WARNING[10537] pbx_config.c: Unable to register extension at line 3811 of /etc/asterisk/extensions_additional.conf
[2019-07-25 06:39:49] WARNING[10537] pbx_config.c: Unable to register extension at line 3812 of /etc/asterisk/extensions_additional.conf
[2019-07-25 06:39:49] WARNING[10537] pbx_config.c: Unable to register extension at line 3813 of /etc/asterisk/extensions_additional.conf
[2019-07-25 06:39:49] WARNING[10537] pbx_config.c: Unable to register extension at line 3814 of /etc/asterisk/extensions_additional.conf
[2019-07-25 06:39:49] WARNING[10537] pbx_config.c: Unable to register extension at line 3815 of /etc/asterisk/extensions_additional.conf
[2019-07-25 06:39:49] WARNING[10537] pbx_config.c: Unable to register extension at line 3816 of /etc/asterisk/extensions_additional.conf
[2019-07-25 06:39:49] WARNING[10537] pbx_config.c: Unable to register extension at line 3817 of /etc/asterisk/extensions_additional.conf
```



Мониторинг

Автоматизация сбора логов Syslog

Протокол syslog и программные средства поддержки обеспечивают запись логов, передачу их на сервер логгирования, сортировку и обработку в зависимости от источника и важности сообщений.

Компонентами системы являются генератор сообщений (устройство или процесс), протокол обмена, коллектор сообщений (collector, syslog server), релей (relay, принимает сообщения от одного или нескольких генераторов и передает одному или нескольким коллекторам или следующим реляям). Генератор (или релей при передаче) не знает является ли приемник релеем или коллектором, может передавать одно сообщение нескольким приемникам, может обрабатывать сообщение самостоятельно (например, записывая в файл)

Мониторинг

Автоматизация сбора логов Syslog+logwatch

logwatch представляет собой framework для написания программ (фильтров) извлечения полезной информации из многочисленных, больших и разноформатных журналов (не только syslog) и формирования отчётов с указанной детализацией за указанный период времени, посылаемых по email

По умолчанию Logwatch охватывает довольно широкий диапазон сервисов. Чтобы просмотреть полный список отслеживаемых сервисов выполняем команду:

- `ls -l /usr/share/logwatch/scripts/services`

```
[root@localhost ~]# ls -l /usr/share/logwatch/scripts/services
total 1184
-rw-r--r-- 1 root root 1570 Mar 22 2017 afpd
-rw-r--r-- 1 root root 65224 Mar 22 2017 amavis
-rw-r--r-- 1 root root 586 Mar 22 2017 arptwatch
-rw-r--r-- 1 root root 9361 Mar 22 2017 audit
-rw-r--r-- 1 root root 4281 Mar 22 2017 automount
-rw-r--r-- 1 root root 1696 Mar 22 2017 autorp
-rw-r--r-- 1 root root 1160 Mar 22 2017 bfd
-rw-r--r-- 1 root root 41178 Mar 22 2017 cisco
-rw-r--r-- 1 root root 3119 Mar 22 2017 clamav
-rw-r--r-- 1 root root 2179 Mar 22 2017 clamav-milter
-rw-r--r-- 1 root root 6965 Mar 22 2017 clam-update
-rw-r--r-- 1 root root 23565 Mar 22 2017 courier
-rw-r--r-- 1 root root 13954 Mar 22 2017 cron
-rw-r--r-- 1 root root 806 Mar 22 2017 denyhosts
-rw-r--r-- 1 root root 6201 Mar 22 2017 dhcpcd
-rw-r--r-- 1 root root 5055 Mar 22 2017 dnsmsec
-rw-r--r-- 1 root root 19007 Mar 22 2017 dovecot
-rw-r--r-- 1 root root 1547 Mar 22 2017 dpkg
-rw-r--r-- 1 root root 3239 Mar 22 2017 emerge
-rw-r--r-- 1 root root 4315 Mar 22 2017 evtapplication
-rw-r--r-- 1 root root 1964 Mar 22 2017 evtsecurity
-rw-r--r-- 1 root root 2364 Mar 22 2017 evtsystem
-rw-r--r-- 1 root root 24041 Mar 22 2017 exim
-rw-r--r-- 1 root root 1067 Mar 22 2017 eximatata
-rw-r--r-- 1 root root 10310 Mar 22 2017 extreme-networks
-rw-r--r-- 1 root root 4842 Mar 22 2017 fail2ban
-rw-r--r-- 1 root root 7254 Mar 22 2017 ftpd-messages
-rw-r--r-- 1 root root 5750 Mar 22 2017 ftpd-xferlog
-rw-r--r-- 1 root root 26024 Mar 22 2017 http
-rw-r--r-- 1 root root 5078 Mar 22 2017 identd
-rw-r--r-- 1 root root 10196 Mar 22 2017 imapd
-rw-r--r-- 1 root root 2894 Mar 22 2017 init
-rw-r--r-- 1 root root 4085 Mar 22 2017 in.qpopper
-rw-r--r-- 1 root root 3305 Mar 22 2017 ipop3d
-rw-r--r-- 1 root root 13637 Mar 22 2017 iptables
-rw-r--r-- 1 root root 5518 Mar 22 2017 ismail
-rw-r--r-- 1 root root 22407 Mar 22 2017 mailscanner
-rw-r--r-- 1 root root 3180 Mar 22 2017 modprobe
-rw-r--r-- 1 root root 3673 Mar 22 2017 mountd
-rw-r--r-- 1 root root 22552 Mar 22 2017 named
-rw-r--r-- 1 root root 14473 Mar 22 2017 netopia
-rw-r--r-- 1 root root 20253 Mar 22 2017 netscreen
-rw-r--r-- 1 root root 4510 Mar 22 2017 oidentd
-rw-r--r-- 1 root root 9830 Mar 22 2017 openvpn
-rw-r--r-- 1 root root 1308 Mar 22 2017 pam
-rw-r--r-- 1 root root 7426 Mar 22 2017 pam_pwdb
-rw-r--r-- 1 root root 14911 Mar 22 2017 pam_unix
-rw-r--r-- 1 root root 4131 Mar 22 2017 php
-rw-r--r-- 1 root root 12533 Mar 22 2017 pix
-rw-r--r-- 1 root root 10850 Mar 22 2017 pluto
-rw-r--r-- 1 root root 14614 Mar 22 2017 pop3
-rw-r--r-- 1 root root 4242 Mar 22 2017 portentry
-rw-r--r-- 1 root root 120440 Mar 22 2017 postfix
-rw-r--r-- 1 root root 2721 Mar 22 2017 pound
-rw-r--r-- 1 root root 9590 Mar 22 2017 proftpd-messages
-rw-r--r-- 1 root root 7290 Mar 22 2017 pureftpd
-rw-r--r-- 1 root root 4988 Mar 22 2017 gmail
-rw-r--r-- 1 root root 3406 Mar 22 2017 gmail-pop3d
-rw-r--r-- 1 root root 2947 Mar 22 2017 gmail-pop3ds
```



Мониторинг

Системы мониторинга (на примере Zabbix)

В крупных сетях, где количество хостов переваливает за несколько десятков, следить за каждым в отдельности — задача не из легких. Для облегчения наблюдения применяются системы мониторинга

Zabbix состоит из:

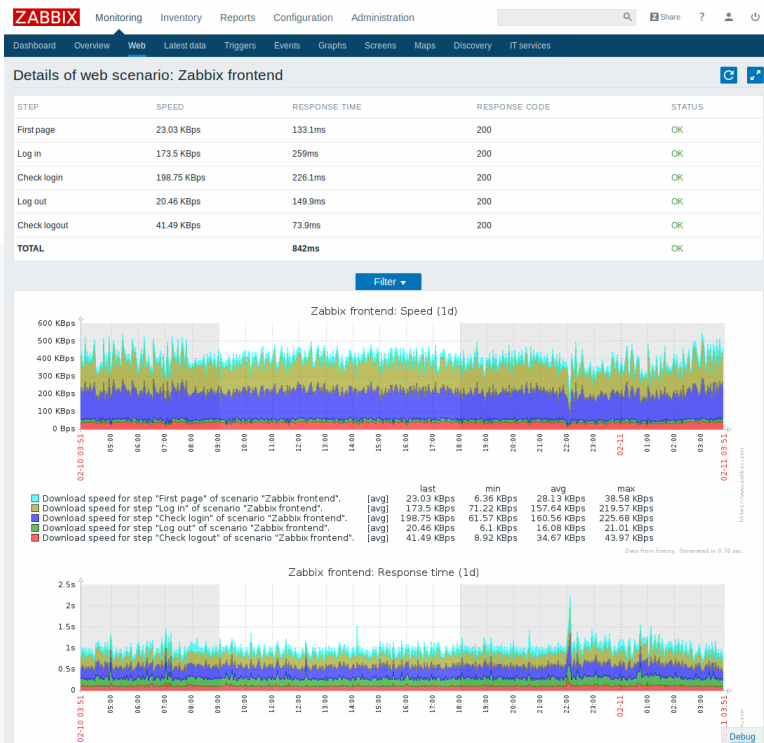
- сервера мониторинга, который выполняет периодическое получение данных, обработку, анализ и запуск скриптов оповещения
- базы данных
- веб-интерфейса
- агента — демона, который запускается на отслеживаемых объектах и предоставляет данные серверу

Мониторинг

Системы мониторинга (на примере Zabbix)

Иногда есть необходимость мониторинга транков, а если этот процесс еще и автоматизировать, то получается вполне себе неплохой инструмент администрирования

Для выполнения данной задачи можно настроить клиент zabbix и подкинуть агенту скрипты



Мониторинг

Системы мониторинга (на примере Zabbix)

Скрипт Trunks.sh

```
#!/bin/sh
number_trunks=`/usr/sbin/asterisk -rx "sip show registry" | grep "SIP registrations" | awk '{print $1}`
reg_trunks=`/usr/sbin/asterisk -rx "sip show registry" | grep Registered | wc -l`
let result=$number_trunks-$reg_trunks
echo $result
```

Этот скрипт необходимо внести в конфигурацию агента, а полученный ключ key=trunks добавить в шаблоны на сервере

UserParameter=trunks,/etc/zabbix/scripts/trunks.sh

```
[root@pbx ~]# zabbix_agentd -t trunks
trunks                                     [t|0]
[root@pbx ~]# █
```



Дополнительные средства защиты от VoxLink

Дополнительные средства защиты от voxlink

Подход нашей компании:

1. Стандартный подход +
2. Система безопасности «Форпост»:
Централизованный контроль
безопасности всех наших клиентов
3. Система безопасности «FakeUserAgent»
(сокращенно - FakeAgent)
Защита от кражи пароля проверкой
UserAgent
4. Система защиты от фрода «CuBAN»
Комплексная оценка «фродовости»
звонка



Дополнительные средства защиты от voxlink

Forpost: централизованный контроль

У нашей компании свыше 600 установленных станций.

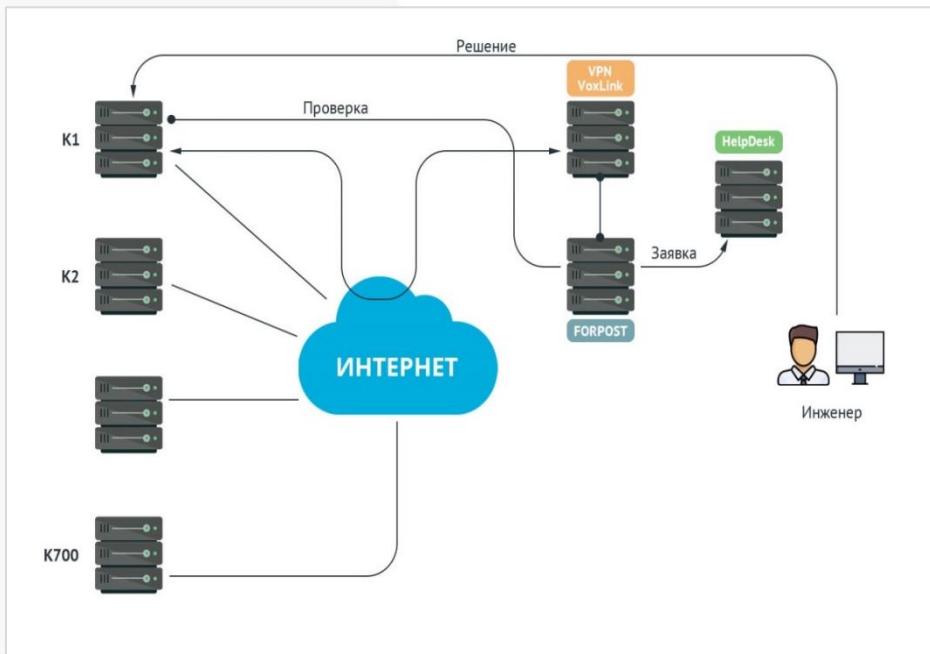
После выполнения проекта мы передаем все доступы админу клиента.

Админы нередко пытаются безопасность уменьшить:

- Создают экстеншены с простыми паролями
- Не меняют пароли на Web и SSH
- Отключают IPTables на время дебага и забывают включить обратно
- Не прописывают ACL (permit/deny)

Дополнительные средства защиты от voxlink

Forpost: централизованный контроль



Дополнительные средства защиты от voxlink

Forpost: централизованный контроль

Что контролируем?

1. IPTables:

1. Вкл/выкл
2. Закрыт ли доступ к 5060, 80, 443, 22, 445 из сети 0.0.0.0/0
3. Default Policy – DROP

2. Настройки Asterisk

1. Alwaysauthreject & allowguest
2. Пароли и их сложность на SIP и IAX2
3. Проверка на лимиты в default context



Дополнительные средства защиты от voxlink

Forpost: централизованный контроль

Что контролируем?

3. Настройки Fail2Ban:

1. Вкл/выкл
2. Наличие цепочек
3. Добавлен в автозапуск

4. Пароли для SSH и HTTPS (отличаются от стандартных)

5. Проверка доступа только по HTTPS

Дополнительные средства защиты от voxlink

Forpost: централизованный контроль

Если срабатывает: (уведомление в HelpDesk)

Главная Заявки База знаний Активы Компании Пользователи Отчеты							
Александр Выход RU							
Все актуальные сервисы (кроме архивных)				Всего 49354 1 из 1975			
☐	№	Ст.	Пр.	Наименование заявки	Заявитель	Срок (план)	Исполнители
☐	52191	!	■■■■	rbx534: проблемы безопасности	log@voxlink.ru	25 сентября, 12:00	Владимир Кортель
☐	52190	!	■■■■	rbx617: проблемы безопасности	log@voxlink.ru	25 сентября, 12:00	Владимир Кортель
☐	52189	!	■■■■	rbx644: проблемы безопасности	log@voxlink.ru	25 сентября, 12:00	Владимир Кортель
☐	52188	!	■■■■	rbx558: проблемы безопасности	log@voxlink.ru	25 сентября, 12:00	Владимир Кортель
☐	52187	!	■■■■	rbx555: проблемы безопасности	log@voxlink.ru	25 сентября, 12:00	Владимир Кортель
☐	52186	!	■■■■	rbx506: проблемы безопасности	log@voxlink.ru	25 сентября, 12:00	Владимир Кортель
☐	52185	!	■■■■	rbx547: проблемы безопасности	log@voxlink.ru	25 сентября, 12:00	Владимир Кортель
☐	52184	!	■■■■	rbx696: проблемы безопасности	log@voxlink.ru	25 сентября, 12:00	Владимир Кортель
☐	52183	!	■■■■	rbx635: проблемы безопасности	log@voxlink.ru	25 сентября, 12:00	Владимир Кортель
☐	52182	!	■■■■	rbx532: проблемы безопасности	log@voxlink.ru	25 сентября, 12:00	Владимир Кортель
☐	52181	!	■■■■	rbx153: проблемы безопасности	log@voxlink.ru	25 сентября, 12:00	Владимир Кортель
☐	52180	!	■■■■	rbx498: проблемы безопасности	log@voxlink.ru	25 сентября, 12:00	Владимир Кортель

Мои фильтры

Нет сохраненных фильтров

Общие фильтры изменить

Бухгалтерия
В работе
В работе Владимир К.
Все заявки
Все кроме закрытых
Закрытые
Закрытые Я
Заявитель Я
Исполнитель Я
Наблюдатель Я
Новые заявки

Действия над заявками

Дополнительные средства защиты от voxlink

Forpost: централизованный контроль

Если срабатывает: (уведомление в HelpDesk)

☐	52186	!	0000	pbx506: проблемы безопасности
☐	52185	!	0000	pbx54
☐	52184	!	0000	pbx69
☐	52183	!	0000	pbx63
☐	52182	!	0000	pbx53
☐	52181	!	0000	pbx15
☐	52180	!	0000	pbx49
☐	52179	!	0000	pbx69
☐	52178	!	0000	pbx51
☐	52177	!	0000	pbx54
☐	52176	!	0000	pbx62
☐	52175	!	0000	pbx59
☐	52174	!	0000	pbx65
☐	52173	!	0000	pbx47
☐	52172	!	0000	pbx60
☐	52171	!	0000	pbx54

Открыл log@voxlink.ru 23 сентября, 09:03 Сервис: Безопасность

ALARM SIP 1003 - permit=0.0.0.0/0.0.0.0 в файле /etc/asterisk/sip_additional.conf
ALARM SIP 1505 - permit=0.0.0.0/0.0.0.0 в файле /etc/asterisk/sip_additional.conf
ALARM SIP 1506 - permit=0.0.0.0/0.0.0.0 в файле /etc/asterisk/sip_additional.conf
ALARM SIP 1525 - permit=0.0.0.0/0.0.0.0 в файле /etc/asterisk/sip_additional.conf
ALARM SIP 1526 - permit=0.0.0.0/0.0.0.0 в файле /etc/asterisk/sip_additional.conf
ALARM SIP 1980 - permit=0.0.0.0/0.0.0.0 в файле /etc/asterisk/sip_additional.conf
ALARM SIP 2101 - permit=0.0.0.0/0.0.0.0 в файле /etc/asterisk/sip_additional.conf
ALARM SIP 2102 - permit=0.0.0.0/0.0.0.0 в файле /etc/asterisk/sip_additional.conf
ALARM SIP 2103 - permit=0.0.0.0/0.0.0.0 в файле /etc/asterisk/sip_additional.conf
ALARM SIP 2104 - permit=0.0.0.0/0.0.0.0 в файле /etc/asterisk/sip_additional.conf
ALARM SIP 2105 - permit=0.0.0.0/0.0.0.0 в файле /etc/asterisk/sip_additional.conf
ALARM SIP 2106 - permit=0.0.0.0/0.0.0.0 в файле /etc/asterisk/sip_additional.conf
ALARM SIP 2107 - permit=0.0.0.0/0.0.0.0 в файле /etc/asterisk/sip_additional.conf
ALARM SIP 2108 - permit=0.0.0.0/0.0.0.0 в файле /etc/asterisk/sip_additional.conf
ALARM SIP 2109 - permit=0.0.0.0/0.0.0.0 в файле /etc/asterisk/sip_additional.conf
ALARM SIP 2110 - permit=0.0.0.0/0.0.0.0 в файле /etc/asterisk/sip_additional.conf
ALARM SIP 2111 - permit=0.0.0.0/0.0.0.0 в файле /etc/asterisk/sip_additional.conf
ALARM SIP 2112 - permit=0.0.0.0/0.0.0.0 в файле /etc/asterisk/sip_additional.conf
ALARM SIP 2113 - permit=0.0.0.0/0.0.0.0 в файле /etc/asterisk/sip_additional.conf
ALARM SIP 2114 - permit=0.0.0.0/0.0.0.0 в файле /etc/asterisk/sip_additional.conf
ALARM SIP 2115 - permit=0.0.0.0/0.0.0.0 в файле /etc/asterisk/sip_additional.conf
ALARM SIP 2116 - permit=0.0.0.0/0.0.0.0 в файле /etc/asterisk/sip_additional.conf
ALARM SIP 2117 - permit=0.0.0.0/0.0.0.0 в файле /etc/asterisk/sip_additional.conf
ALARM SIP 2118 - permit=0.0.0.0/0.0.0.0 в файле /etc/asterisk/sip_additional.conf
ALARM SIP 2119 - permit=0.0.0.0/0.0.0.0 в файле /etc/asterisk/sip_additional.conf
ALARM SIP 2120 - permit=0.0.0.0/0.0.0.0 в файле /etc/asterisk/sip_additional.conf
ALARM SIP 3111 - permit=0.0.0.0/0.0.0.0 в файле /etc/asterisk/sip_additional.conf
ALARM web-админка доступна по HTTP



Дополнительные средства защиты от voxlink

Forpost: централизованный контроль

После срабатывания:

1. Оцениваем, можно ли решить проблему самостоятельно, без привлечения клиента
2. Если без клиента нельзя – то передаем проблему ему или решаем совместно
3. Если можно самостоятельно, то делаем сами. Клиент может и не узнать о том что была угроза.



Как защититься от случаев, когда украден пароль на Extension?

Кейс: на ноутбук директора, на котором стоит сотффон, попал вирус, который украл SIP-пароль.

Директор пользуется ноутбуком из разных стран, звонит по всему миру, из всех часовых поясов.

Защититься ACL-ом, контролем времени, сильным паролем или запретом звонков на МГ/МН – невозможно. VPN или PIN-коды – это лучше, чем ничего, но есть ряд минусов.



Реально ли сделать безопасный экстеншн, на котором даже нет пароля?

(Спойлер: Да)

Дополнительные средства защиты от voxlink

Система FUA (FakeUserAgent)

Может ли взломщик узнать ваш пароль?

Да.

Знает ли он, то для звонка недостаточно одного пароля и знания схему набора?

Нет

Что использует взломщик для аутентификации на вашем сервере:

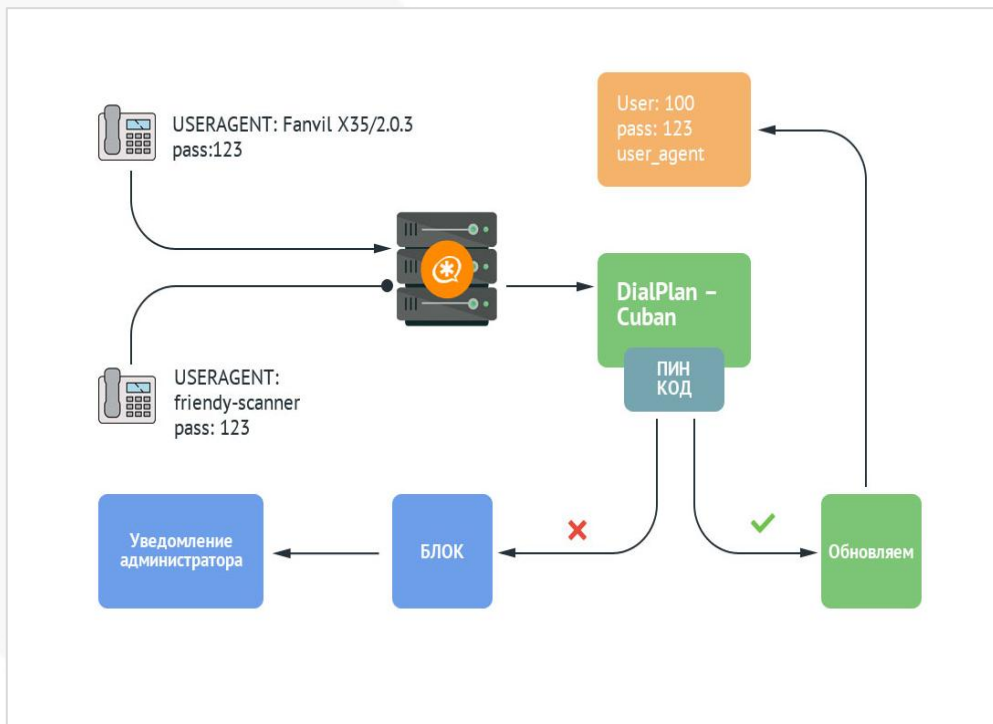
- Extension
- Pass

Что нужно:

- Extention
- Pass
- Useragent

Дополнительные средства защиты от voxlink

Система FUA (FakeUserAgent)



Дополнительные средства защиты от voxlink

Система FUA (FakeUserAgent)

Как работает:

- Запоминаем UA абонента
- Все звонки с этого UA и правильного пароля – разрешаем.
- Звонки с нормальным паролем, но новым UA – отправляем в лимитный контекст
- В контексте запрашиваем ввести пин-код, который позволит добавить новый UA данному юзеру или предлагаем связаться с нашей ТП
- Если несколько попыток ввода пина были безуспешными, то блокируем юзера переносом его в другой контекст, откуда все звонки «идут на мобилу админа»



Дополнительные средства защиты от voxlink

Система FUA (FakeUserAgent)

```
cc Flow 101 1822673854989-247212800226444@10.131.111.86 (Color by Request/Response)  
50 REGISTER sip:10.131.7.21 SIP/2.0  
Via: SIP/2.0/UDP 10.131.111.86:5060;branch=z9hG4bK22872246002240514613;rport  
From: "Sudbina Olga Andreye" <sip:5228@10.131.7.21:5060>;tag=18551792  
To: "Sudbina Olga Andreye" <sip:5228@10.131.7.21:5060>  
Call-ID: 1822673854989-247212800226444@10.131.111.86  
CSeq: 183 REGISTER  
Contact: <sip:5228@10.131.111.86:5060>  
Max-Forwards: 70  
Expires: 3600  
Supported: path  
User-Agent: Fanvil X3S/2.0.3.3049_0c383e190cb8  
Allow: INVITE, ACK, OPTIONS, BYE, CANCEL, REFER, NOTIFY, INFO, PRACK, UPDATE, MESSAGE  
Content-Length: 0
```



Дополнительные средства защиты от voxlink

Система антифрода CuBan

Что делать, если взломали Asterisk, например, через FreePBX и инъектировали свой диалплан? Или если просто не сработала другая защита?

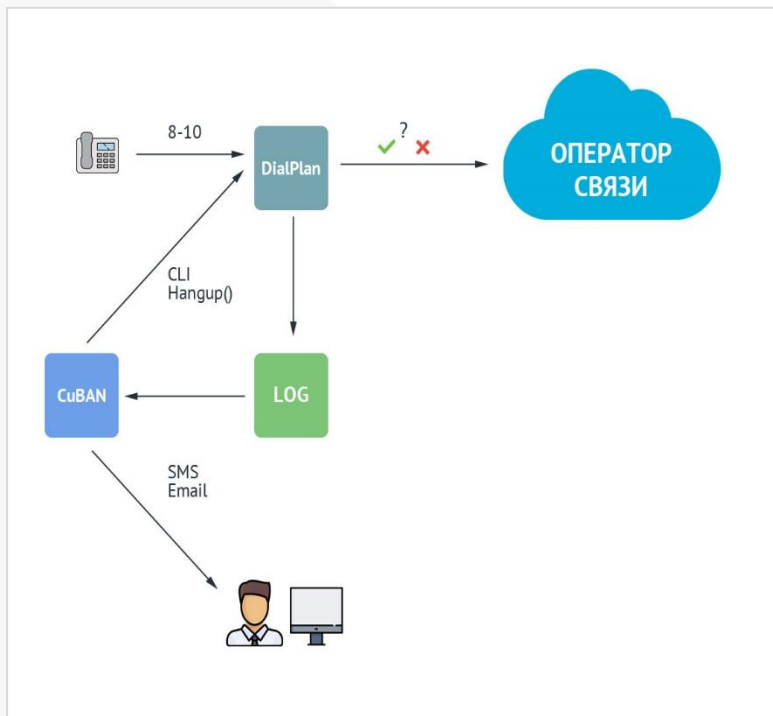
Мы сделали систему CuBan (Cuba + Ban)

Система работает на парсинге логов Asterisk и по сути напоминает Fail2Ban. После срабатывания делает инъекцию Hangup() в «проломленный» контекст.



Дополнительные средства защиты от voxlink

Система антифрода CuBan



Выводы

Asterisk, возможно, самая мощная платформа для реализации собственных инструментов обеспечения безопасности.

Сделать Asterisk безопасным или
оставить «таким как есть» - ваш выбор.



Ваши вопросы?

Вопросы
из онлайн





Беспроводной SIP-DECT телефон KX-TGP600

#1

- SIP-DECT телефон,
- эксклюзивный дизайн,
- цветной ЖКД,
- возможность подключения 8-ми трубок к одной базе,
- поддержка 8-ми линий,
- 8 одновременных разговоров,
- гарантия 5 лет.
- Максимум возможностей для качественной связи.

Спонсор подарка:



Федеральная инженеринговая сеть

MT-TEKHO



Компания MT-TEKHO является Федеральным Техническим Центром АТС Panasonic в России.



VOXLINK: ASTERISK
ПРОФЕССИОНАЛЬНО

— Телефон Fanvil X3SP

#2

ПОДАРКИ



- IP телефон X3SP- Лучший выбор для офиса.
- Цветной экран , высокая надежность, эргономичный дизайн и поддержка звука HD качества, наличие порта POE

Спонсор подарка:



Компания «Телеком Дистрибуция» дистрибьютор Fanvil в России с 20 года. Вам гарантированы : сопровождение сделки от подбора оборудования до окончания срока обслуживания , низкие цены , наличие товара на складе в Москве.



Мерч от VoxLink

- Сумка «TCP-пакет | IP-пакет»
- Кружка VoxLink
- Блокнот и ручка
- Наклейка с логотипом Asterisk

Спонсор подарка:

VoxLink – интегратор систем
IP-телефонии на базе Asterisk

#3

ПОДАРКИ





СПАСИБО ЗА ВНИМАНИЕ!

Грушко Сергей

+7 (926) 350 3163

sergey@voxlink.ru