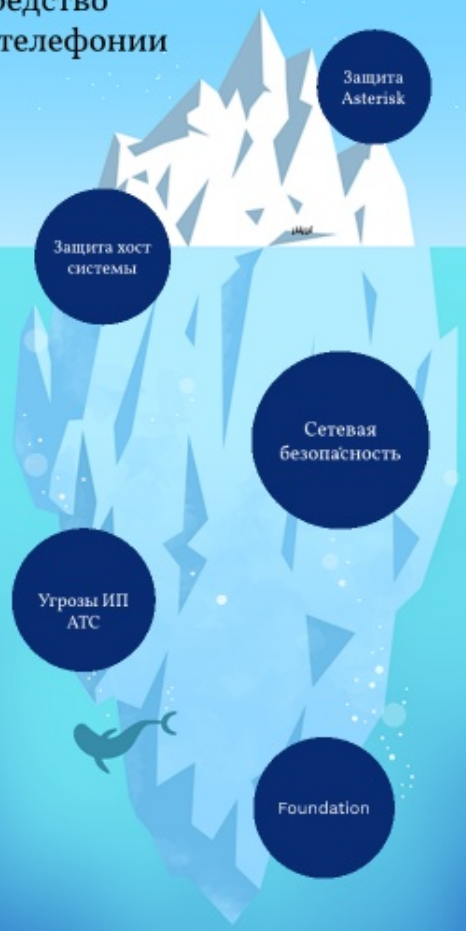




Оборудование Mikrotik как средство безопасности для системы IP телефонии

Vladislav Istratii
MTI Link



О НАС

Vladislav Istratiy:

- В IT с 1998 года
- С 2011г. тренер по Asterisk
- MTCNA, MTCRE, MTCWE, MTCTCE, MTCIPv6E
- СМО MTI-Group LLC ; MTI-Link LLC

MTI-Group & MTI-Link:

- Системная интеграция
- Производство сетевого оборудования STYX Communication
- Разработка ПО
- Центр обучения по MikroTik ROS, Asterisk в РФ
- Дистрибьютор ProCell
- Brands: MikroTik, STYX Communication, Setrann, Mupssoft, ProCell antennas

Наша
команда

Нам
доверяют

Наша команда

Руководящий состав



Irina Tsyapa
CEO "MTI Group" LLC



Vladislav Istratii
CMO "MTI Group" LLC



Oleg Tsyapa
CTO "MTI Group" LLC



Sergey Chernosvitov
Head Programmer

Нам доверяют

наши клиенты





Оборудование Mikrotik как средство безопасности для системы IP телефонии

Vladislav Istratii
MTI Link



Вектор атаки

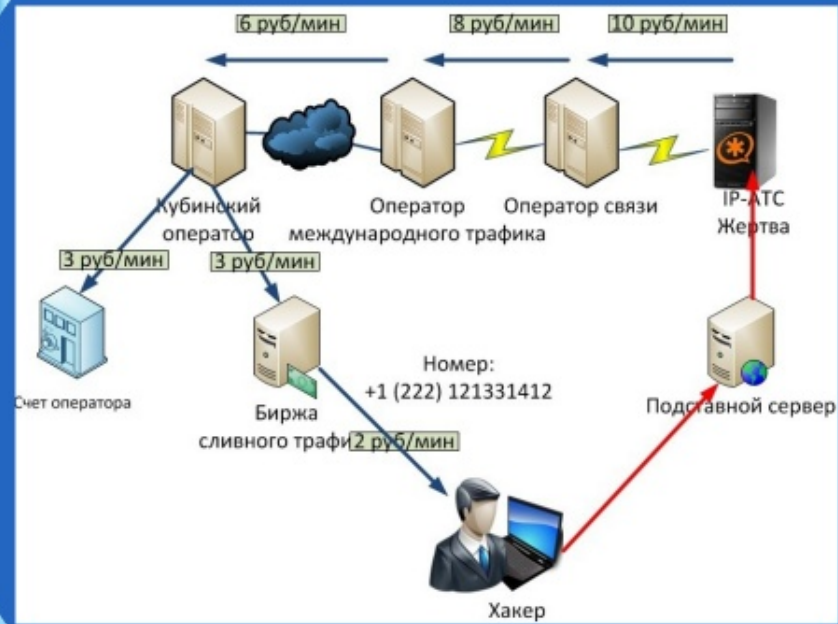
При построении системы безопасности для решений в области IP-телефонии важно осознавать возникающие риски. В общем случае их можно выделить следующим образом:

- Нарушение конфиденциальности и искажение содержимого. Перехват сессии.
- Проникновение в сеть организации через уязвимости, появившиеся при разворачивании IP-телефонии.
- Действия, направленные на ухудшение сервисов (Dos-атаки).
- Перепродажа трафика (Toll-Fraud).

Toll-Fraud

Шаги к
безопасности

Toll-Fraud



Защита IP АТС включает в себя:

- Организацию сетевой безопасности
- Структуру сети
- Обработку сообщений, логов
- Настройку Asterisk
- План маршрутизации звонков
- Настройку безопасности ОС Linux
- Безопасность периферийных устройств
- Административную организация



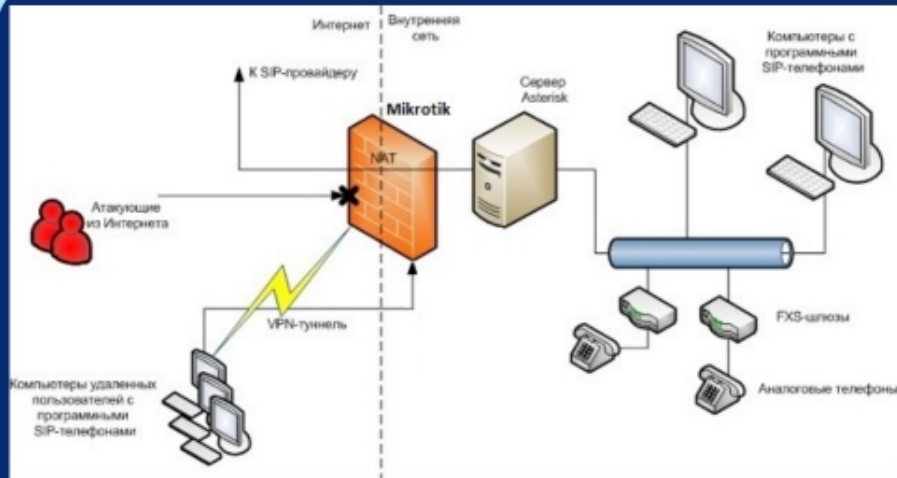


Оборудование Mikrotik как средство безопасности для системы IP телефонии

Vladislav Istratii
MTI Link



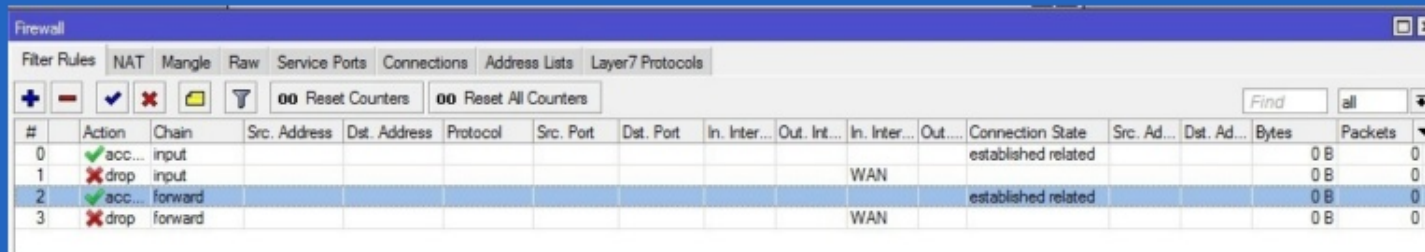
Сетевая безопасность



Firewall

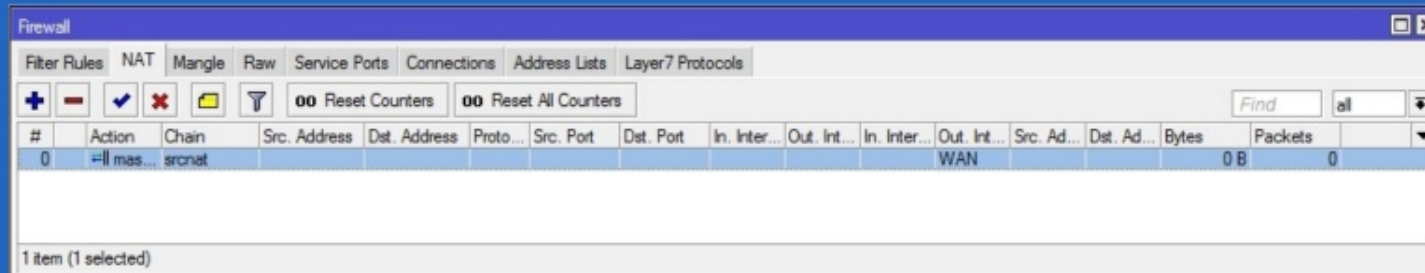
Структура сети

Firewall (Basic)



Firewall Connections tab showing active connections. The table includes columns for #, Action, Chain, Src. Address, Dst. Address, Protocol, Src. Port, Dst. Port, In. Inter..., Out. Int..., In. Inter..., Out..., Connection State, Src. Ad..., Dst. Ad..., Bytes, and Packets.

#	Action	Chain	Src. Address	Dst. Address	Protocol	Src. Port	Dst. Port	In. Inter...	Out. Int...	In. Inter...	Out...	Connection State	Src. Ad...	Dst. Ad...	Bytes	Packets
0	✓ acc...	input										established related			0 B	0
1	✗ drop	input								WAN					0 B	0
2	✓ acc...	forward										established related			0 B	0
3	✗ drop	forward								WAN					0 B	0



Firewall Connections tab showing a single selected connection. The table includes columns for #, Action, Chain, Src. Address, Dst. Address, Proto..., Src. Port, Dst. Port, In. Inter..., Out. Int..., In. Inter..., Out. Int..., Src. Ad..., Dst. Ad..., Bytes, and Packets.

#	Action	Chain	Src. Address	Dst. Address	Proto...	Src. Port	Dst. Port	In. Inter...	Out. Int...	In. Inter...	Out. Int...	Src. Ad...	Dst. Ad...	Bytes	Packets
0	=ll mas...	srcnat									WAN			0 B	0

1 item (1 selected)

SIP.CONF
nat=comedia,force_rport

Firewall DST-NAT

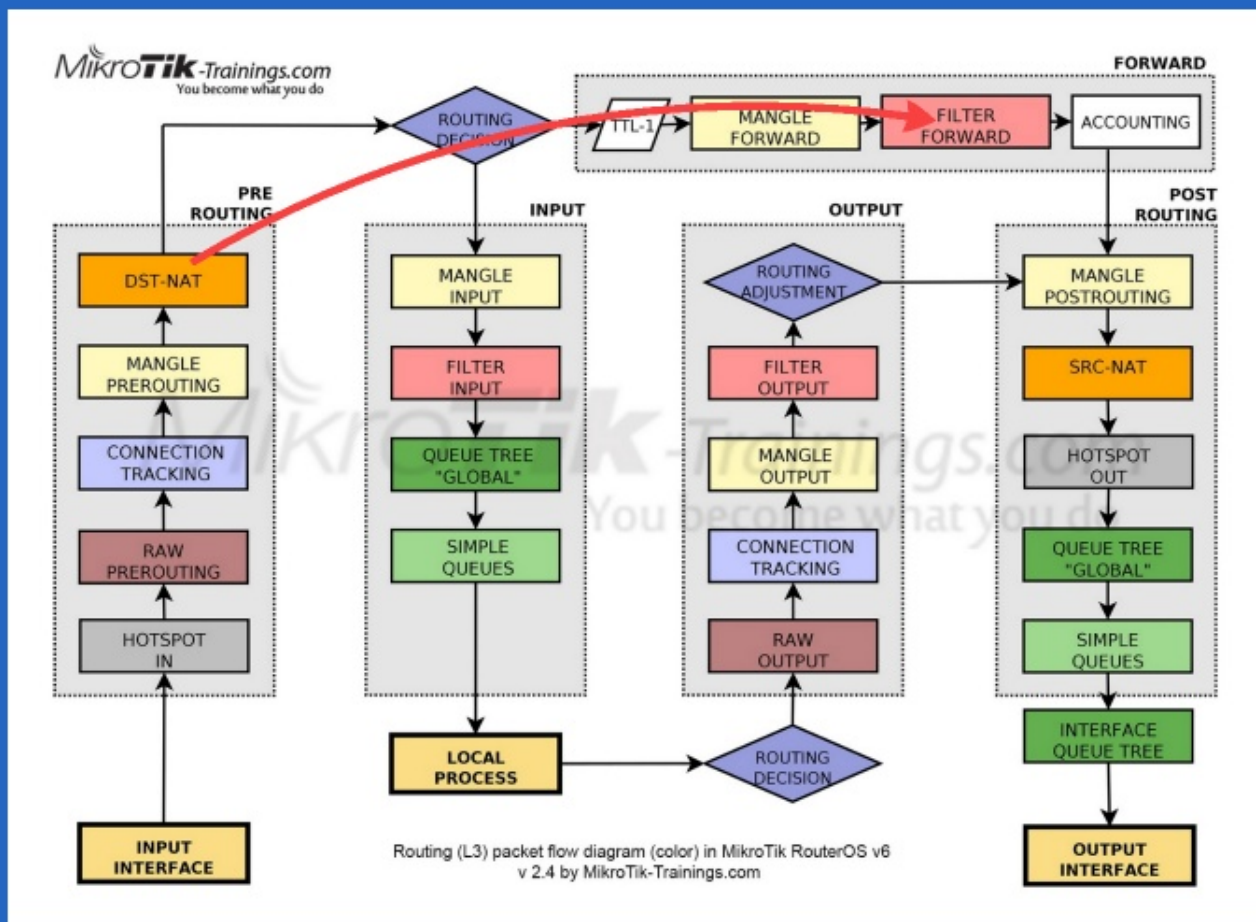
#	Action	Chain	Src. Address	Dst. Address	Protocol	Src. P...	Dst. Port	In. Inte...	Out. I...	In. I...	Out. Int...	Src. Ad...	Dst. Ad...	To Addresses	Bytes	Packets
0	mas...	srcnat									WAN			10.10.105.2	0 B	0
1	dst...	dstnat	185.45.152.174	1.1.1.2	17 (udp)		5060,10000-20000							10.10.105.2	0 B	0

2 items (1 selected)

#	Action	Chain	Src. Address	Dst. Address	Protocol	Src. Port	Dst. Port	In. Inter...	Out. I...	In. Inter...	Out...	Connection State	Src. Ad...	Dst. Ad...	Address List	Timeout	Bytes	Packets
0	acc...	input										established related					0 B	0
1	drop	input							WAN								0 B	0
2	acc...	forward										established related					0 B	0
3	acc...	forward	185.45.152.174	10.10.105.2	17 (udp)		5060,10000-20000										0 B	0
4	drop	forward							WAN								0 B	0

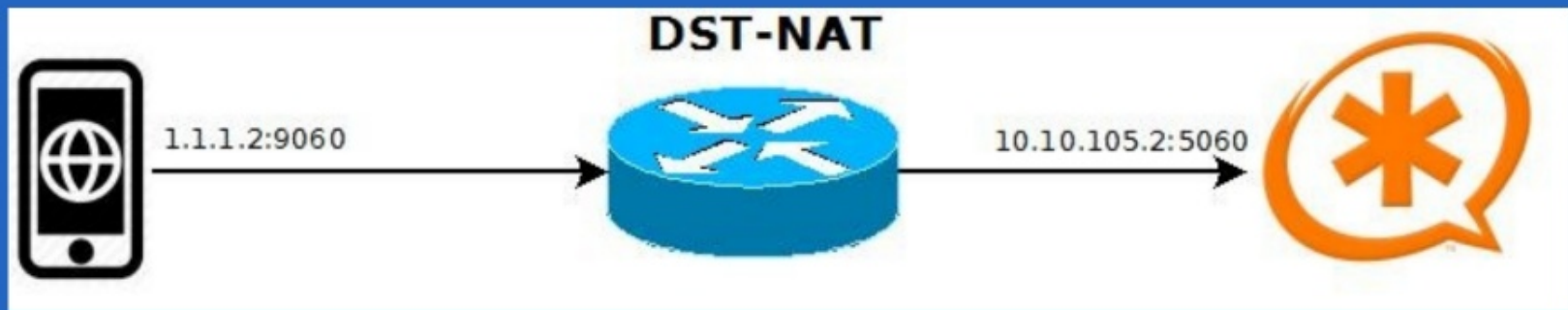
5 items

SIP.CONF
nat=comedia,force_rport



Хочешь такую? Подходи к нашему стенду и возьми бесплатно.

Firewall Honeypot



Firewall Honeypot

The image displays three screenshots of the Mikrotik WinBox Firewall configuration interface, illustrating a honeypot setup.

Top Screenshot: Firewall Rule Configuration

#	Action	Chain	Src. Address	Dst. Address	Proto...	Src. Port	Dst. Port	In. Inter...	Out. Int...	In. Inter...	Out. Int...	Src. Address List	Dst. Ad...	Bytes	Packets
0	✗ drop	prerouting										Scanners		0 B	0

Middle Screenshot: Firewall Rule Configuration (Detailed)

#	Action	Chain	Src. Address	Dst. Address	Protocol	Src. P...	Dst. Port	In. Inte...	Out. I...	In. I...	Out. Int...	Src. Ad...	Dst. Ad...	To Addresses	To Ports	Bytes	Packets
0	mas...	srcnat									WAN					0 B	0
1	dst...	dstnat	185.45.152.174	1.1.1.2	17 (udp)		5060,10000-20000							10.10.105.2		0 B	0
2	dst...	dstnat		1.1.1.2	17 (udp)		9060							10.10.105.2		5060	0 B

Bottom Screenshot: Firewall Log Configuration

#	Action	Chain	Src. Address	Dst. Address	Protocol	Src. Port	Dst. Port	In. Inter...	Out. I...	In. Inter...	Out. Int...	Connection State	Src. Ad...	Dst. Ad...	Address List	Timeout	Bytes	Packets
0	acc...	input										established related					0 B	0
1	add...	input		1.1.1.1	17 (udp)		9060								Scanners	1d 00:00:00	0 B	0
2	add...	input		1.1.1.3	17 (udp)		9060								Scanners	1d 00:00:00	0 B	0
3	✗ drop	input									WAN						0 B	0
4	acc...	forward										established related					0 B	0
5	acc...	forward		10.10.105.2	17 (udp)		5060,10000-20000										0 B	0
6	✗ drop	forward									WAN						0 B	0

Структура сети





Оборудование Mikrotik как средство безопасности для системы IP телефонии

Vladislav Istratii
MTI Link



Защита хост системы

- SSH
- IPTABLES
- Fail2Ban



SSH

IPTABLES

Fail2Ban

SSH

```
/etc/ssh/sshd_config
```

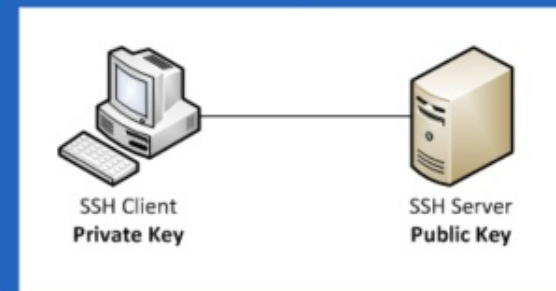
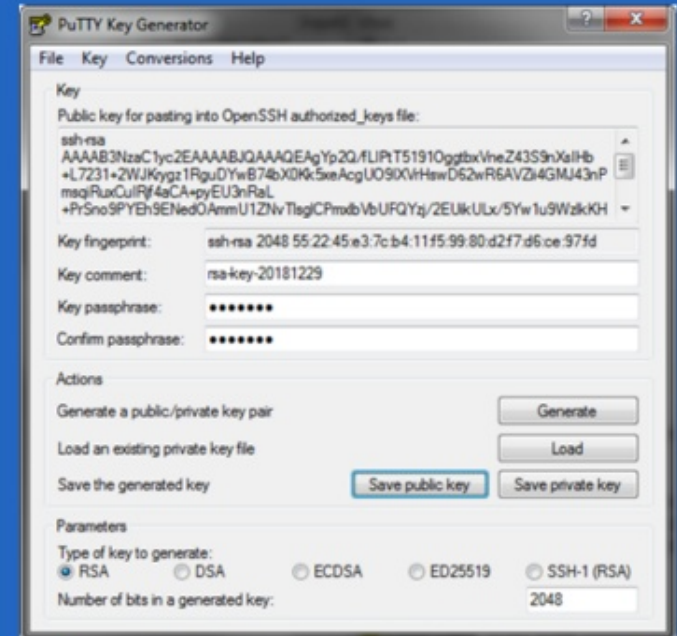
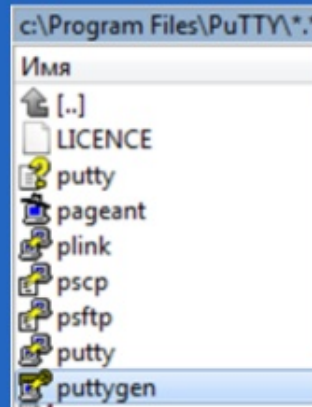
```
...  
Port 6262  
...  
PasswordAuthentication yes  
...  
PermitRootLogin no  
...  
PubkeyAuthentication yes
```

```
mkdir ~/.ssh
```

```
#Импорт публичного ключа
```

```
ssh-keygen -i -f key >> .ssh/authorized_keys
```

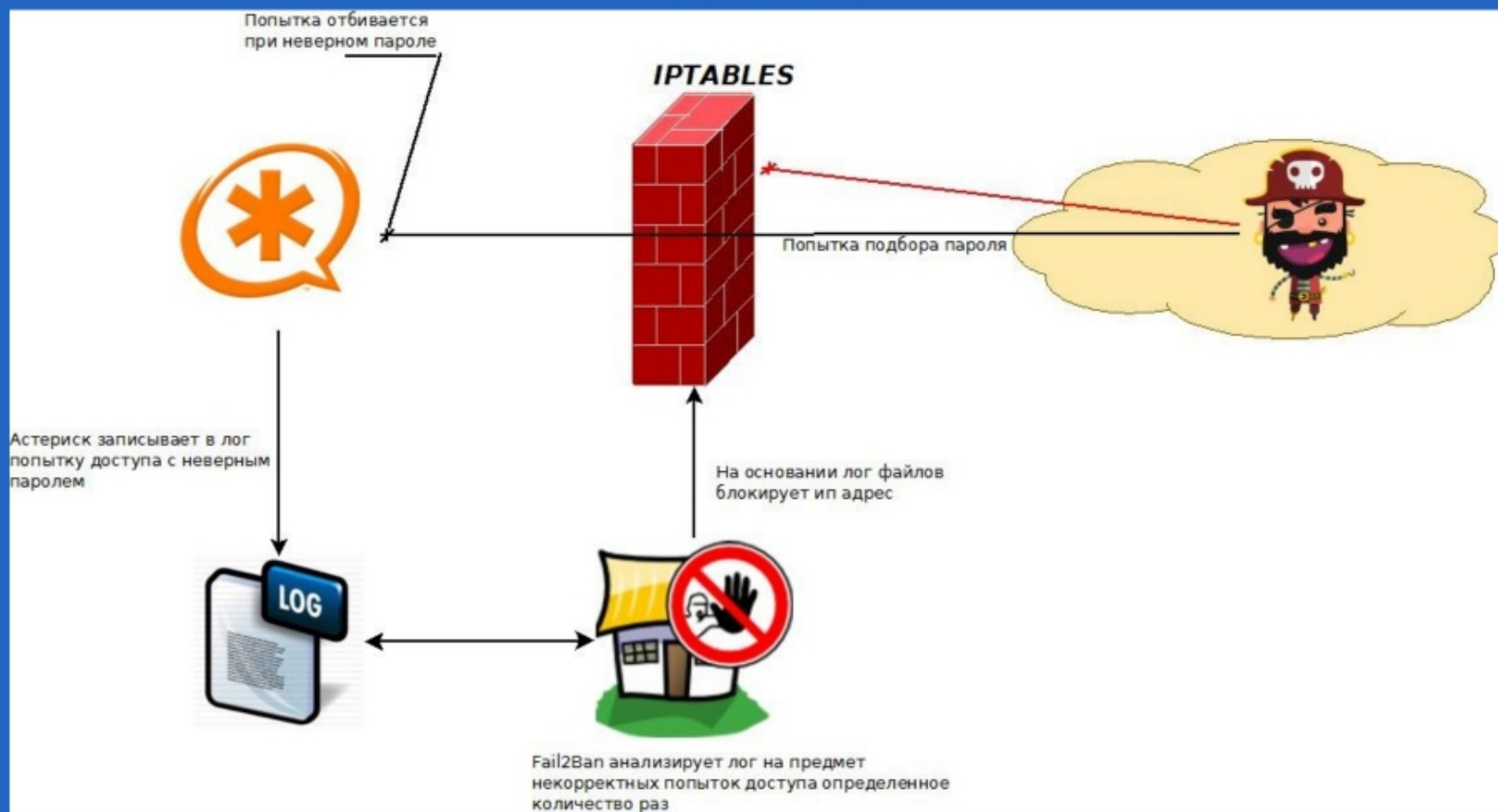
```
chmod og-rwx -Rc ~/.ssh
```



IPTABLES

- `iptables -N input-voip` ← Создаем цепочку файервола
- `iptables -A INPUT -i lo -j ACCEPT` ← Разрешаем трафик по интерфейсу
- `iptables -A INPUT -p icmp -j ACCEPT` ← Разрешаем ICMP трафик (а можно и не разрешать)
-
- `iptables -A INPUT -p udp --dport 5060 -j input-voip`
`iptables -A INPUT -p tcp --dport 5060:5061 -j input-voip` ← При попытке доступа на данные порты перенаправляем в цепочку input-voip
`iptables -A INPUT -p udp --dport 10000:20000 -j input-voip`
`iptables -A INPUT -p udp --dport 4569 -j input-voip`
`iptables -A INPUT -p tcp --dport 22 -j input-voip`
-
- `iptables -A INPUT -p icmp -m state --state RELATED,ESTABLISHED -j ACCEPT`
`iptables -A INPUT -p tcp -m state --state RELATED,ESTABLISHED -j ACCEPT` ← Разрешаем пакеты RELATED, ESTABLISHED
`iptables -A INPUT -p udp -m state --state RELATED,ESTABLISHED -j ACCEPT`
-
- `iptables -A input-voip -s 10.10.105.0/24 -j ACCEPT` ← Цепочка input-voip, где мы проверяем совпадает ли ип адрес запроса с разрешенными
`iptables -A input-voip -s 185.45.152.174 -j ACCEPT`
-
- `iptables -A INPUT -j DROP` ← Блокируем все остальное
`iptables -A FORWARD -j DROP`

Fail2Ban





Оборудование Mikrotik как средство безопасности для системы IP телефонии

Vladislav Istratii
MTI Link



Защита Asterisk

- Безопасная конфигурация sip.conf
- Защита dialplan`ом
- Защита оконечных устройств
- Упреждающие действия



Sip.conf

Dialplan

Оборудование

Упреждающие
действия

Вопросы

Sip.conf

```
[general]
;Изменение порта udp
bindport = 7799

;Запретить отправлять сообщения о несуществующем
пользователе
alwaysauthreject=yes

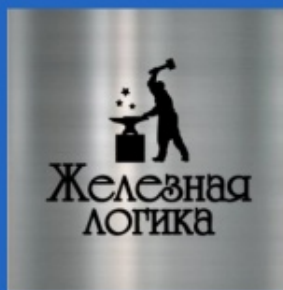
#Маскируем АТС
useragent=Panasonic
sdowner=Panasonic
sdpsession=Panasonic

[<пользователи>]
;ограничить по ip
deny = 0.0.0.0/0.0.0.0
permit = 192.168.100.0/24
;Использовать стойкий пароль
secret=920332$4nf323;;9asdYioepooALY39mD#dnnw2e
```

secure sip

Dialplan

- Завершать номера расширения Hangup()'ом
- Устанавливать ограничения на максимальное число линий для пользователя
- Устанавливать ограничения на междугородние и международные вызовы
- Настроить cdr для отслеживания расходов
- Устанавливать ограничения по времени суток
- Высылать оповещения на email/sms на дорогие направления
- и т.д.



Защита оконечных устройств

- Используйте отдельную подсеть и ограничивайте доступ в по web/telnet только для администраторов
- Изменяйте стандартные пароли на вход в интерфейс настройки
- Изменяйте пароль для входа в режим конфигурации с клавиатуры телефона
- Отключайте лишний функционал (переадресации, DND), если он не нужен пользователю



Упреждающие действия

Защита через оператора связи

- Установите ограничения на число минут (или расход средств)
- Не держите большую сумму на балансе
- Установите ограничения (звонок по вводу кода) для дорогих направлений
- Настройте уведомления о расходе средств
- Используйте VPN канал (если есть возможность) до оператора

В организации

- Повышение осведомленности персонала
- Регулярная смена паролей
- Обновление АТС и оконечных устройств



Контакты

Интеграция - mti-group.ru
Оборудование - shop.mti-group.ru
Software - mupssoft.com
Обучение - QTraining.ru
Обучение - MikroTik-TrainingS.COM

Corporate - ISP - WISP - DC
STYX - MikroTik - Procell
MUPSBox, MUPS, MTMS, IPCalc
Asterisk, MikroTik, e.t.c
MikroTik

Вопросы?





Оборудование Mikrotik как средство безопасности для системы IP телефонии

Vladislav Istratii
MTI Link

