тайная канцелярия

ВНЕДРЕНИЕ IPSEC

РАССМОТРИМ ДВА НАИБОЛЕЕ ЧАСТО ИСПОЛЬЗУЕМЫХ СЦЕНАРИЯ ВЧС (ВИРТУАЛЬНЫХ ЧАСТНЫХ СЕТЕЙ) — «ХОСТ В ХОСТ» И «ХОСТ В СЕТЬ», ПРЕДВАРИТЕЛЬНО БОЛЕЕ ДЕТАЛЬНО РАССМОТРЕВ НЕКОТОРЫЕ ТЕОРЕТИЧЕСКИЕ АСПЕКТЫ IPSEC

КОНСТАНТИН ГАВРИЛЕНКО
{директор компании Архонт}

→ **IPSec** — наиболее признанный, поддерживаемый и стандартизированный из всех протоколов ВЧС на сегодняшний день. Для обеспечения совместной работы различных устройств в гетерогенной сети он подходит лучше прочих, так как основан на полностью открытых стандартах. В отличие от других ВЧС-протоколов, IPSec работает на третьем уровне и может защищать любой ИП-трафик. При его применении совместно с другими протоколами туннелирования на втором уровне, такими как Л2ТП, также появляется возможность защиты в том числе и не ИП-трафика.

→ **внутреннее устройство IPSec.** Нельзя говорить об IPSec'е, как об одном протоколе. На самом деле, под протоколом IPSec подразумевается набор стандартов и черновиков (drafts). Вот основные:

— AH (AUTHENTICATED HEADER) ЗАГОЛОВОК АУТЕНТИФИКАЦИИ, ОБЕСПЕЧИВАЮЩИЙ АУТЕНТИФИКАЦИЮ ИСТОЧНИКА ДАННЫХ, ЦЕЛОСТНОСТЬ И ЗАЩИТУ ОТ АТАК ПОВТОРНОГО ВОСПРОИЗВЕДЕНИЯ.

- ESP (ENCAPSULATED SECURITY PAYLOAD) БЕЗОПАСНО ИНКАПСУЛИРОВАННАЯ ПОЛЕЗНАЯ НАГРУЗКА, ОБЕСПЕЧИВАЮЩАЯ АУТЕНТИФИКАЦИЮ ИСТОЧНИКА ДАННЫХ, ЦЕЛОСТНОСТЬ, ЗАЩИТУ ОТ АТАК ПОВТОРНОГО ВОСПРОИЗВЕДЕНИЯ, КОНФИДЕНЦИАЛЬНОСТЬ ДАННЫХ И, В НЕКОТОРЫХ ТИПАХ ПРИМЕНЕНИЯ, СКРЫТНОСТЬ УПРАВЛЕНИЯ ПОТОКОМ.
- IPCOMP (IP PAYLOAD COMPRESSION PROTOCOL) ПРОТОКОЛ АВТОМАТИЧЕСКОГО СЖАТИЯ ДАННЫХ ПЕРЕД ШИФРАЦИЕЙ. ПОТЕНЦИАЛЬНО УСТРАНЯЕТ НЕГАТИВНОЕ ВЛИЯНИЕ ИНКАПСУЛЯЦИИ ДАННЫХ И СОКРАЩАЕТ ОБЪЕМ ТРАНСЛИРУЕМОЙ ИНФОРМАЦИИ.
- IKE (INTERNET KEY EXCHANGE) МЕХАНИЗМ БЕЗОПАСНОГО АВТОМАТИЧЕСКОГО ОБМЕНА КЛЮЧАМИ, ПРЕДОСТАВЛЯЮЩИЙ СРЕДСТВА СОГЛАСОВАНИЯ КРИПТОГРАФИЧЕСКОГО АЛГОРИТМА И ОТВЕЧАЮЩИЙ ЗА РАСПРЕДЕЛЕНИЕ КЛЮЧЕЙ, ИСПОЛЬЗУЕМЫХ ДЛЯ ШИФРОВАНИЯ ДАННЫХ.

Существуют два режима работы IPSec-соединения: туннельный и транспортный. Транспортный режим работы используется исключительно для защиты соединения между двумя хостами, шифруя только полезные данные в пакете. Туннельный режим работы шифрует весь передаваемый ИП-пакет, вместе с полезными данными, ИП-опциями, исходным и конечным адресом, добавляя новые ИП-заголовки, позволяя создавать защищенное соединение между несколькими сетями. Настоятельно рекомендую использовать туннельный режим работы ESP IPSec, так как он обеспечивает наибольший уровень конфиденциальности передаваемых данных, хотя и увеличивает пакет на несколько дополнительных байтов.

При использовании автоматического режима обмена ключами, создание туннеля происходит в два этапа. В процессе первой фазы соединения происходит формирование ISAKMP SA (соглашения о защите протокола безопасности в интернете и управлении ключами), включая установление аутентификации и защиты IPSec-узлов, согласование политики для защиты обмена информацией, выработку защитного ключа через протокол Диффи-Хельмана и установку туннеля для дальнейших переговоров второй фазы. В процессе второй фазы согласования формируется IPSec SA, включая согласование параметров SA для протокола IPSec, выработку SA для протокола IPSec, периодическую ротацию ключей шифрования.

ДЛЯ СТАТЬИ ИСПОЛЬЗОВАЛОСЬ ПОСЛЕДНЕЕ СТАБИЛЬНОЕ 2.6.16 ЯДРО, IPSEC-TOOLS 0.6.5 И IPROUTE2 2.6.16

Наиболее распространенные методы взаимной аутентификации сторон включают использование предварительно разделенного ключа (PSK) или цифровых сертификатов типа X.509. Оба метода имеют свои преимущества. Хотя считается, что использование цифровых сертификатов — более безопасное решение, но стоит ли утруждать себя созданием CA, выпиской сертификатов и CRL, если нужно соединить только два хоста?

→ **выбор IPSec'a.** На данный момент существует две имплементации IPSec-стэка для Линукса и три вида пользовательского интерфейса. Начиная с 2.6.x версии, ядро Линукса приобрело встроенную поддержку IPSec'a (NETKEY), портированную с FreeBSD, и пользовательский интерфейс, предоставляемый ipsec-tools. Для предыдущих версий ядра (2.2.x и 2.4.x) поддержка протокола IPSec осуществлялась через программный пакет FreeSWAN (KLIPS как часть кернела, и Pluto — как пользовательский интерфейс), который сейчас перешел в новую реинкарнацию и называется OpenSWAN. Третьим пользовательским интерфейсом является Isakmpd, портированный на Линукс с OpenBSD — наименее распространенное решение.

Хотя NETKEY — значительно более молодой стэк, чем KLIPS, и имеет меньшую функциональность, он все равно был интегрирован в текущее древо ядра, в основном из-за различных «политических» проблем, окружающих KLIPS, а также из-за более «чистого» кода.

→ **подготовка к установке.** Большинство современных дистрибутивов базируются на 2.6.x ядре и имеют как предустановленную поддержку IPSec'a в ядре, так и набор утилит в своих системах управления пакетами.

Опустим стандартный процесс сборки и установки, сконцентрировавшись непосредственно на самом процессе конфигурации.

проверь, что в конфигурационном файле ядра следующие опции отмечены для включения в ядро или выбраны как модули

```
CONFIG_XFRM=y          CONFIG_CRYPTO_MD5=y
CONFIG_
XFRM_USER=m            CONFIG_CRYPTO_SHA1=m
CONFIG_NET_KEY=m       CONFIG_CRYPTO_SHA256=m
CONFIG_INET_AH=m       CONFIG_CRYPTO_SHA512=m
CONFIG_INET_ESP=m      CONFIG_CRYPTO_DES=y
CONFIG_
INET_IPCOMP=m          CONFIG_CRYPTO_AES=m
CONFIG_
INET_TUNNEL=m          CONFIG_CRYPTO_DEFLATE=m
```

проверь, что два хоста, между которыми ты собираешься устанавливать туннель, не имеют никаких препятствий для связи (если установлен брандмауэр, то разреши соединения на UDP-порты 500, 4500 и протоколы 50 и 51)

```
iptables -A INPUT -i eth0 -p 50 -j ACCEPT
iptables -A INPUT -i eth0 -p 51 -j ACCEPT
iptables -A INPUT -i eth0 -p udp --
dport 500 -j ACCEPT
iptables -A INPUT -i eth0 -p udp --
dport 4500 -j ACCEPT
```

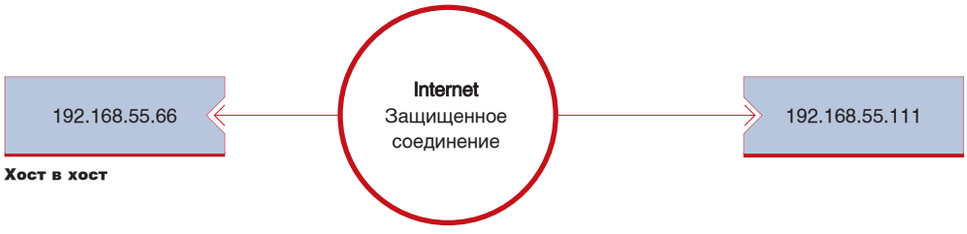
для отделения потока трафика, пришедшего через IPSec-туннель, необходимо пометить входящие ESP-пакеты и разрешить беспрепятственный доступ или перенаправить их в отдельную таблицу

```
iptables -t mangle -A PREROUTING -i
eth0 -p esp -j MARK --set-mark 50
iptables -A INPUT -i eth0 -m mark --
mark 50 -j ACCEPT
```

→ **конфигурация «хост в хост».** Существует достаточно возможностей установления безопасного соединения между двумя статическими хостами, начиная с использования SSH для защиты административного канала управления или инкапсуляции всего трафика в PPP-канал связи с последующей защитой через SSH или SSL. Хотя наиболее простым и правильным решением в данном случае будет установка «хост в хост» IPSec-соединения, используя PSK для аутентификации сторон.

Ракун — достаточно сложный в конфигурации демон с огромным количеством опций, большинство из которых, к счастью, можно оставить по умолчанию, что значительно облегчает задачу.

В первую очередь нужно установить пароль. Значение ключа устанавливается в файле psk.txt (проверь, чтобы права доступа были 400, -r-------- 1 root root, иначе Ракун не запустится).



Хост в хост

генерирование случайного ключа

```
arhontus / # dd if=/dev/random bs=16
count=1 | xxd -ps
1+0 records in
1+0 records out
16 bytes (16 B) copied, 4.4e-05
seconds, 364 kB/s
cc0c6778f478f5aff03caa38779090c1
```

помести ключ в файл psk.txt

```
arhontus racoon # cat psk.txt
192.168.55.66
cc0c6778f478f5aff03caa38779090c1
```

В первом столбце указывается идентификатор хоста, будь-то ИП-адрес или имя хоста, а во втором — сам ключ. Такую же операцию проведи и на втором хосте, заменив ИП на противоположный.

Далее необходимо задать политику безопасности IPSec, а именно: какие каналы коммуникации необходимо защитить, и каким образом будет осуществляться защита соединения. Политику безопасности возможно определить для хостов и для направления соединения, а также и на уровне сокета, которым пользуется программа. При запуске Ракун не пытается немедленно установить соединение, а ждет уведомления от ядра о том, что данное соединение становится активным и нуждается в защите, после чего инициирует обмен ключами.

как правило, конфигурация политики безопасности заносится в файл ipsec.conf или setkey.conf (зависит от особенностей дистрибутива)

```
arhontus racoon # cat ipsec.conf
#!/usr/sbin/setkey -f
# Flush the SAD and SPD
flush;
spdflush;
spdadd 192.168.55.111/32
192.168.55.66/32 any -P out ipsec
 ipcomp/transport//use
 esp/transport//unique;
spdadd 192.168.55.66/32
192.168.55.111/32 any -P in ipsec
 ipcomp/transport//use
 esp/transport//unique;
```

В данном примере мы создали две политики, описывающие входящий и исходящий трафик, для двухсторонней коммуникации с соседним хостом. В зависимости от используемого режима протокола и алгоритма шифрования, конечный отправляемый пакет увеличивается в размере. Соответственно, для уменьшения количества передаваемых данных, а так же для того, чтобы избежать ненужной фрагментации пакетов, мы сначала сжимаем пакет и только потом его шифруем, что и отображено в файле конфигурации. Ты неограничен в выборе используемой комбинации протоколов (AH, ESP, IPCOMP) и, ради эксперимента, можешь попробовать провести даже двойное шифрование пакета.

настройка конфигурационного файла IKE-демона, чем, собственно, и является Ракун

```
arhontus racoon # cat racoon.conf
path pre_shared_key "/etc/raco-
on/psk.txt";
listen {
 isakmp 192.168.55.111 [500];
  isakmp_natt 192.168.55.111 [4500];
 strict_address;
 }

remote 192.168.55.66 {
 exchange_mode main;
 my_identifier address;
 peers_identifier address;
 verify_identifier on;

 dpd_delay 60;
 proposal {
  lifetime time 120 min;
  encryption_algorithm rijndael256;
  hash_algorithm sha256;
  authentication_method pre_shared_key;
  dh_group modp4096;
  }
 proposal_check strict;
}

sainfo anonymous {
 lifetime time 30 minutes;
 encryption_algorithm rijndael;
 authentication_algorithm hmac_sha1;
 compression_algorithm deflate;
 pfs_group modp2048;
}
```

SPECIAL МНЕНИЕ

КОНСТАНТИН ГАВРИЛЕНКО
Консультант по безопасности, директор компании Архонт. Соавтор книг: «Wi-Фу: Секреты беспроводного взлома» и «Секреты Хакеров: Безопасность сетей Циско».

КАКОВО ИСТИННОЕ ПРЕДНАЗНАЧЕНИЕ VPN (VIRTUAL PRIVATE NETWORK)?

В те давние времена, когда интернет был доступен ограниченному количеству пользователей, в основном академической направленности, особых вопросов о конфиденциальности передаваемых данных не возникало. С ростом количества пользователей и приходом громадных корпораций претерпела изменения и сама природа интернета. Из академического инструмента она превратилась в глобальную распределенную Сеть, в которой хранится и передается огромное количество конфиденциальных данных и проводится множество финансовых транзакций.

Такие изменения не могли долго оставаться без внимания лиц, пытающихся извлечь выгоду из доступа к конфиденциальной информации. Соответственно, с особой остротой встал вопрос безопасной передачи данных. Одно из возможных решений этой проблемы — развертывание ВЧС. Их применение оправдано по двум мотивам:

— стремление сократить расходы, например, заменив безопасные линии дозвона для удаленных корпоративных пользователей на доступ через IPSec;

— желание обеспечить конфиденциальность передаваемых данных между узлами сети во враждебном окружении, например, защита коммуникаций между клиентом и точкой беспроводного доступа.

Обычная конфигурация хранится в файле racoon.conf. В нем содержится описание особенностей всех туннелей, для которых необходима автоматическая генерация ключей.

Теперь более подробно рассмотрим используемые опции:

- PATH PRE_SHARED_KEY
  МЕСТОНАХОЖДЕНИЕ ФАЙЛА С КЛЮЧАМИ;
- ISAKMP 192.168.55.111 [500]
  АДРЕС, НА КОТОРОМ БУДЕТ СЛУШАТЬ ДЕМОН IKE;
- ISAKMP_NATT 192.168.55.111 [4500]
  АДРЕС, НА КОТОРОМ БУДЕТ СЛУШАТЬ ДЕМОН IKE В РЕЖИМЕ РАБОТЫ ЧЕРЕЗ NAT;
- STRICT_ADDRESS
  УКАЗЫВАЕТ, ЧТО ИНТЕРФЕЙС ДОЛЖЕН ПРИСУТСТВОВАТЬ ПЕРЕД НАЧАЛОМ РАБОТЫ;
- REMOTE 192.168.55.6
  ОТКРЫВАЕТ СЕКЦИЮ КОНФИГУРАЦИИ ОТДЕЛЬНО ВЗЯТОГО ТУННЕЛЯ И УКАЗЫВАЕТ АДРЕС СОСЕДА IPSEC-ТУННЕЛЯ;
- EXCHANGE_MODE MAIN
  ОПРЕДЕЛЯЕТ РЕЖИМ РАБОТЫ ПЕРВОЙ ФАЗЫ;
- MY_IDENTIFIER ADDRESS
  ПОСЫЛАЕМЫЙ ИДЕНТИФИКАТОР;
- PEERS_IDENTIFIER ADDRESS
  ОЖИДАЕМЫЙ ИДЕНТИФИКАТОР СОСЕДА;
- VERIFY_IDENTIFIER ON
  ВКЛЮЧЕНИЕ ПРОВЕРКИ ИДЕНТИФИКАТОРА СОСЕДА;
- DPD_DELAY 60
  ОПРЕДЕЛЕНИЕ ИНТЕРВАЛА РАБОТЫ РЕЖИМА ОБНАРУЖЕНИЯ НЕРАБОТАЮЩЕГО ХОСТА;
- PROPOSAL
  ОТКРЫВАЕТ СЕКЦИЮ КОНФИГУРАЦИИ ПАРАМЕТРОВ ПРЕДЛОЖЕНИЯ ПЕРВОЙ ФАЗЫ;
- LIFETIME TIME 120 MIN
  ВРЕМЯ ЖИЗНИ КЛЮЧА ШИФРОВАНИЯ ПЕРВОЙ ФАЗЫ;
- ENCRYPTION_ALGORITHM RIJNDAEL256
  АЛГОРИТМ ШИФРОВАНИЯ, ИСПОЛЬЗУЕМЫЙ В ПРОЦЕССЕ ПЕРВОЙ ФАЗЫ;
- HASH_ALGORITHM SHA256
  АЛГОРИТМ ХЭШИРОВАНИЯ, ИСПОЛЬЗУЕМЫЙ В ПРОЦЕССЕ ПЕРВОЙ ФАЗЫ;
- AUTHENTICATION_METHOD PRE_SHARED_KEY
  ИСПОЛЬЗУЕМЫЙ МЕТОД АУТЕНТИФИКАЦИИ;
- DH_GROUP MODP4096
  ПАРАМЕТРЫ ФУНКЦИИ ИДЕАЛЬНОЙ СЕКРЕТНОСТИ ПЕРЕНАПРАВЛЕНИЯ ПЕРВОЙ ФАЗЫ;
- PROPOSAL_CHECK STRICT
  ОПРЕДЕЛЯЕТ УРОВЕНЬ СООТВЕТСТВИЯ ДВУХ ПРЕДЛОЖЕНИЙ;
- SAINFO ANONYMOUS {
  ОТКРЫВАЕТ СЕКЦИЮ КОНФИГУРАЦИИ ПАРАМЕТРОВ ПРЕДЛОЖЕНИЯ ВТОРОЙ ФАЗЫ;
- LIFETIME TIME 30 MINUTES
  ВРЕМЯ ЖИЗНИ КЛЮЧА ШИФРОВАНИЯ;
- ENCRYPTION_ALGORITHM RIJNDAEL
  АЛГОРИТМ ШИФРОВАНИЯ, ИСПОЛЬЗУЕМЫЙ В ПРОЦЕССЕ ВТОРОЙ ФАЗЫ;
- AUTHENTICATION_ALGORITHM HMAC_SHA1
  АЛГОРИТМ ХЭШИРОВАНИЯ, ИСПОЛЬЗУЕМЫЙ В ПРОЦЕССЕ ВТОРОЙ ФАЗЫ;
- COMPRESSION_ALGORITHM DEFLATE
  АЛГОРИТМ СЖАТИЯ, ИСПОЛЬЗУЕМЫЙ В ПРОЦЕССЕ ВТОРОЙ ФАЗЫ;
- PFS_GROUP MODP2048
  ПАРАМЕТРЫ ФУНКЦИИ ИДЕАЛЬНОЙ СЕКРЕТНОСТИ ПЕРЕНАПРАВЛЕНИЯ ВТОРОЙ ФАЗЫ.

Стоит отметить, что для второй фазы были выбраны менее мощные алгоритмы шифрования и хэширования, так как они используются непосредственно для шифрования отправляемого трафика, что, в свою очередь, сказывается на производительности системы. В зависимости от мощности и архитектуры процессора, необходимой пропускной способности и желаемого уровня безопасности данных, различные алгоритмы будут более или менее приемлемы в каждой конкретной ситуации. Включение режима сжатия данных так же добавляет дополнительную нагрузку на центральный процессор, но при подходящем для компрессии типе данных, ты можешь обеспечить значительный прирост скорости передачи.

Не забудь, что файлы конфигурации должны, за исключением ИП-адресов, зеркально отображать себя на обоих хостах. Иначе возможны несостыковки в политиках безопасности, что приведет к невозможности согласования параметров туннеля.

для установки политик безопасности

```
arhontus racoon # setkey -f ./ipsec.conf
```

запуск демона Ракун

```
arhontus racoon # racoon -f ./racoon.conf -F -v
```

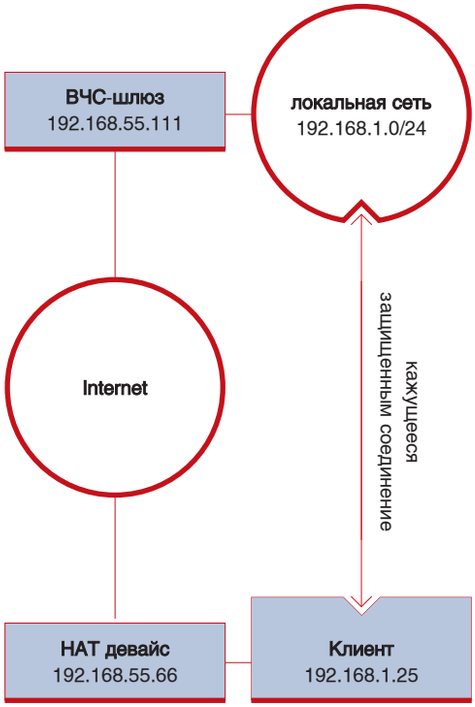
соединение инициировано простым пингом

```
arhontus racoon # ping -c 1 192.168.55.66

May 21 14:18:44 pingo racoon: INFO:
respond new phase 1 negotiation:
192.168.55.111[500]<=>192.168.55.66[500]
May 21 14:18:44 pingo racoon: INFO:
begin Identity Protection mode.
May 21 14:18:44 pingo racoon: INFO:
received Vendor ID: DPD
May 21 14:18:45 pingo racoon: INFO:
ISAKMP-SA established
192.168.55.111[500]-192.168.55.66[500]
spi:8dc4793f80eb71da:b0fd7a67799645da
May 21 14:18:47 pingo racoon: INFO:
respond new phase 2 negotiation:
192.168.55.111[500]<=>192.168.55.66[500]
May 21 14:18:47 pingo racoon: INFO:
IPsec-SA established: ESP/Transport
192.168.55.66[0]->192.168.55.111[0]
spi=26208972(0x18feacc)
May 21 14:18:47 pingo racoon: INFO:
IPsec-SA established: IPCOMP/Transport
192.168.55.66[0]->192.168.55.111[0]
spi=11347(0x2c53)
May 21 14:18:47 pingo racoon: INFO:
IPsec-SA established: ESP/Transport
192.168.55.111[0]->192.168.55.66[0]
spi=64639354(0x3da517a)
May 21 14:18:47 pingo racoon: INFO:
IPsec-SA established: IPCOMP/Transport
192.168.55.111[0]->192.168.55.66[0]
spi=20799(0x513f)
```

→ **конфигурация «хост в сеть».** Часто возникает ситуация, когда клиенту необходим доступ к ресурсам сети, но он использует динамический доступ к интернету посредством дозвона, беспроводного хот-спота и т.д. Заранее невозможно прописать его динамический ИП в политике безопасности для установки туннеля, поэтому для аутентификации таких хостов приходится применять другие методы.

Рассмотрим пример настройки ВЧС-шлюза для приема соединений таких клиентов, используя аутентификацию через x509 сертификаты, проверку их подлинности через центральный CA и использование поддержки режима работы через NAT- устройства.

→ **пример конфигурации сервера.** Опустим детальное описание настройки x509 сертификатов, благо, об этом существует достаточное количество информации как в Сети, так и в печатных изданиях, которых предостаточно в книжных магазинах. Вкратце, используя openssl, необходимо



Хост в сеть

создать свой CA (центр сертификации), а затем — подписанные сертификаты для сервера и для каждого из клиентов. Для контроля годности сертификатов необходимо выпустить CRL (список аннулирования сертификатов). Теперь помести открытый сертификат CA, а также открытую и секретную части сертификата сервера и CRL в директорию, используемую Ракуном, или сделай символический линк к директории по умолчанию (/etc/racoon/certs/).

чтобы openssl мог найти CA и CRL, их надо переименовать или слинковать к их хэшу

```
arhontus certs # ln -s cacert.pem
`openssl x509 -in cacert.pem -noout -hash`.0
arhontus certs # ln -s rootca.crl
`openssl crl -in rootca.crl -noout -hash`.r0
```

директория с сертификатами на сервере

```
arhontus certs # ls -1
8bc54ff5.0 -> cacert.pem
8bc54ff5.r0 -> rootca.crl
cacert.pem -> /etc/ssl/cacert.pem
rootca.crl -> /etc/ssl/rootca.crl
stalin.arhont.com.crt
stalin.arhont.com.key
```

файл описания политик безопасности (ipsec.conf)

```
arhontus racoon # cat ipsec.conf
#!/usr/sbin/setkey -f

# Flush the SAD and SPD
flush;
spdflush;
```

файл настройки Ракуна

```
arhontus racoon # cat racoon.conf
path certificate "/etc/racoon/certs";

listen {
 isakmp 192.168.55.111 [500];
 isakmp_natt 192.168.55.111 [4500];
 strict_address;
 }

remote anonymous {
 exchange_mode aggressive;
 generate_policy on;
 nat_traversal force;
 ike_frag on;
 esp_frag 552;
 dpd_delay 60;

 ca_type x509 "cacert.pem";
 certificate_type x509
"stalin.arhont.com.crt"
"stalin.arhont.com.key";
 verify_cert on;

 my_identifier asn1dn;
 peers_identifier asn1dn;
 verify_identifier off;

 proposal {
   lifetime time 120 min;
   encryption_algorithm rijndael256;
   hash_algorithm sha256;
   authentication_method hybrid_rsa_server;
   dh_group modp4096;
   }
 proposal_check claim;
}

mode_cfg {
 network4 192.168.1.1;
 pool_size 128;
 auth_source system;
 dns4 192.168.1.121;
 banner "/etc/racoon/motd";
}

sainfo anonymous {
 lifetime time 30 minutes;
 encryption_algorithm rijndael;
 authentication_algorithm hmac_sha1;
 compression_algorithm deflate;
 pfs_group modp2048;
}
```

Итак, теперь приступим к более подробному рассмотрению новых опций, которые будем использовать:

— `PATH CERTIFICATE "/ETC/RACOON/CERTS"`
МЕСТОНАХОЖДЕНИЕ ДИРЕКТОРИИ С СЕРТИФИКАТАМИ;

— `REMOTE ANONYMOUS {`
ОТКРЫВАЕТ СЕКЦИЮ КОНФИГУРАЦИИ ТУННЕЛЕЙ, ДЛЯ КОТОРЫХ НЕ ПРОПИСАНА ПОЛИТИКА;

— `GENERATE_POLICY ON`
ВКЛЮЧАЕТ РЕЖИМ УСТАНОВЛЕНИЯ ПОЛИТИКИ БЕЗОПАСНОСТИ, ПОЛУЧЕННОЙ ОТ КЛИЕНТА;

— `NAT_TRAVERSAL FORCE`
ИСПОЛЬЗОВАНИЕ МЕХАНИЗМА ПРЕОДОЛЕНИЯ NAT ВО ВСЕХ СЛУЧАЯХ;

— `IKE_FRAG ON`
ВКЛЮЧЕНИЕ РЕЖИМА ПОДДЕРЖКИ ФРАГМЕНТАЦИИ IKE;

— `ESP_FRAG 552`
ВКЛЮЧЕНИЕ РЕЖИМА ПОДДЕРЖКИ ФРАГМЕНТАЦИИ ПАКЕТА ДО ИНКАПСУЛЯЦИИ В ESP;

— `CA_TYPE X509 "CACERT.PEM"`
ИМЯ ФАЙЛА CA;

— `CERTIFICATE_TYPE X509 "STALIN.ARHONT.COM.CRT" "STALIN.ARHONT.COM.KEY"`
ТИП И ИМЯ ОТКРЫТОГО СЕРТИФИКАТА И СЕКРЕТНОГО КЛЮЧА СЕРВЕРА;

— `VERIFY_CERT ON`
ВКЛЮЧЕНИЕ ПОДДЕРЖКИ ПРОВЕРКИ СЕРТИФИКАТА КЛИЕНТА;

— `AUTHENTICATION_METHOD HYBRID_RSA_SERVER`
ВЫБОР HYBRID_RSA_SERVER МЕТОДА АУТЕНТИФИКАЦИИ;

— `MODE_CFG {`
ОТКРЫТИЕ СЕКЦИИ КОНФИГУРАЦИИ ИНФОРМАЦИИ ДЛЯ КЛИЕНТА;

— `NETWORK4 192.168.1.1`
ОПРЕДЕЛЕНИЕ РЯДА ИП-АДРЕСОВ, НАЗНАЧАЕМЫХ КЛИЕНТАМ;

— `POOL_SIZE 128`
РАЗМЕР РЯДА ИП-АДРЕСОВ, НАЗНАЧАЕМЫХ КЛИЕНТАМ;

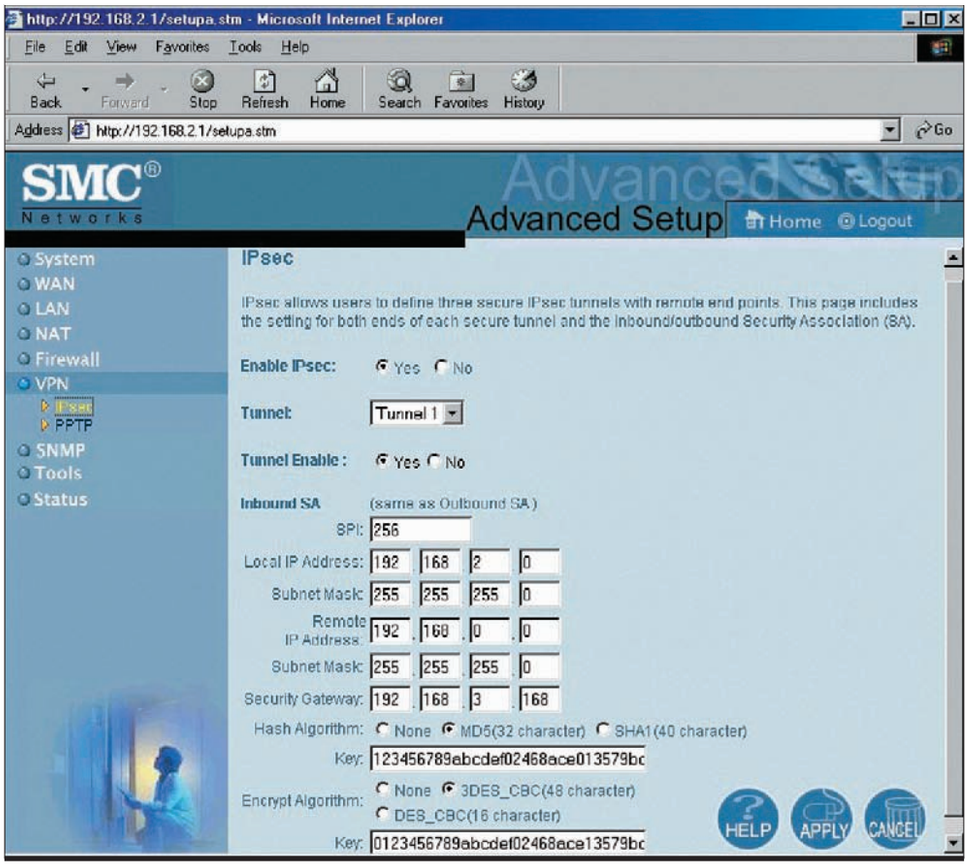
— `AUTH_SOURCE SYSTEM`
МЕХАНИЗМ АУТЕНТИФИКАЦИИ;

— `DNS4 192.168.1.121`
ИП-АДРЕС DNS-СЕРВЕРА, НАЗНАЧАЕМОГО КЛИЕНТАМ;

— `BANNER "/ETC/RACOON/MOTD"`
ПУТЬ К ФАЙЛУ ЗАГОЛОВКА, ПЕРЕДАВАЕМОМУ КЛИЕНТАМ.

➔ **конфигурация клиента.** Процесс конфигурации клиента практически такой же, как и для сервера, за исключением некоторых опций в файле конфигурации Ракуна.

```
dyno racoon # cat racoon.conf
path certificate "/etc/racoon/certs";

listen {
 isakmp 192.168.55.66 [500];
 isakmp_natt 192.168.55.66 [4500];
 strict_address;
 }

remote 192.168.55.111 {
 exchange_mode aggressive;
 nat_traversal force;
 ike_frag on;
 esp_frag 552;
 dpd_delay 60;

 ca_type x509 "cacert.pem";
 certificate_type x509
"berija.arhont.com.crt"
"berija.arhont.com.key";
 verify_cert on;

 my_identifier asn1dn;
 peers_identifier asn1dn;
 verify_identifier off;

 mode_cfg on;
 script "/etc/racoon/phase1-up.sh"
phase1_up;
 script "/etc/racoon/phase1-down.sh"
phase1_down;
 passive off;

 proposal {
  lifetime time 120 min;
  encryption_algorithm rijndael256;
  hash_algorithm sha256;
  authentication_method
hybrid_rsa_client;
  dh_group modp4096;
  }
 proposal_check obey;
}

sainfo anonymous {
 lifetime time 30 minutes;
 encryption_algorithm rijndael;
 authentication_algorithm hmac_sha1;
 compression_algorithm deflate;
 pfs_group modp2048;
}
```



Пример настройки IPSec на роутере

Обзор новых опций в файле конфигурации клиента:

— `MODE_CFG ON`
ВКЛЮЧЕНИЕ РЕЖИМА ЗАПРОСА ОПЦИЙ КЛИЕНТА;

— `SCRIPT "/ETC/RACOON/PHASE1-UP.SH" PHASE1_UP`
ПУТЬ К СКРИПТУ, ИСПОЛЬЗУЕМОМУ ПРИ ВЫПОЛНЕНИИ ПЕРВОЙ ФАЗЫ ОБМЕНА;

— `SCRIPT "/ETC/RACOON/PHASE1-DOWN.SH" PHASE1_DOWN`
ПУТЬ К СКРИПТУ, ИСПОЛЬЗУЕМОМУ ПРИ ОКОНЧАНИИ ПЕРВОЙ ФАЗЫ ОБМЕНА.

После завершения конфигурации клиента запусти демон Ракун. В настоящей конфигурации политика безопасности не прописана, соответственно, ядро не знает, какие пакеты нуждаются в защите, и не инициирует соединение — это нужно сделать вручную.

инициирование туннеля

```
arhontus racoon # racoonctl vpn-connect
-u g_kos 192.168.55.111
Password:
Bound to address 192.168.1.1
=======================================
=====================
# This is a PROTECTED device — UNAUTHO-
RIZED ACCESS IS PROHIBITED! #
```

Для успешного подключения необходимо иметь годный сертификат, подписанный центром сертификации, учетную запись и пароль на ВЧС-шлюзе.

➔ **эпилог.** Всегда имей в виду, что IPSec — достаточно сложный протокол, особенно для начинающего пользователя, что увеличивает вероятность возникновения крупной ошибки. Дополнительные затруднения при установлении соединения могут возникать при использовании различных версий одного продукта и, что более вероятно, различных имплементаций от разных производителей. Начинай с простых решений: меньше вероятность того, что что-нибудь выйдет из под контроля. Не стремись устанавливать самые мощные алгоритмы шифрования. Даже для очень продвинутого хакера проще, и обычно результативнее, попытаться найти уязвимости в ВЧС-шлюзе, чем расшифровать закриптованный пакет. А в случае, если твоими данными заинтересовались спецслужбы, то они скорее всего не станут заниматься криптоанализом трафика, а применят более эффективный метод ректотермального криптоанализа. Так что рассматривай IPSec не как панацею, а только как одну из частей многогранной мозаики систем безопасности C


NM-AIR-WLC6
NOT SUPPORTED
LINK
ACT
PWR
EN
Fast Ethernet 0
Cisco Systems
SYS
ACT
SYS PWR1
AUX PWR1
SYS PWR2
AUX PWR2
PS1