Поддержка IKEv2 и аппаратное ускорение в продуктах MikroTik

Maris Bulans
MikroTik, Latvija

MUM
Март 2017

Вкратце

- IKEv1 vs IKEv2
- Маршрутизаторы с аппаратным ускорением
- Советы по повышению производительности
- Советы по безопасности

Что такое IKE

- Internet Key Exchange
- Протокол для установки SA (security association)
- Демон IKE имеет доступ к данным конфигурации и аутентификации
- IKE обычно работает на UDP/500 UDP/4500
- IKE установление соединения использует kerniel ipsec stack
- Ядро перехватывает соответствующие пакеты и выполняет шифрование / дешифрование

IKEv1 vs IKEv2

- IKEv1
  - Несколько режимов обмена
  - Обмен сообщениями зависит от режима (9 сообщений в основном режиме)
  - PSK и RSA-Sig аутентификация
  - Точки должны использовать один и тот же метод auth
  - Требуется точное соглашение о селекторе трафика
  - Требуется соглашение о lifetime
  - Rekey – не определен
  - NAT-T: Определяется как расширение
  - DPD: Определяется как расширение
  - RoadWarrior: (для производителей mode-conf, xauth)

IKEv1 vs IKEv2

- IKEv2
  - Режимы обмена устарели
  - Упрощенный обмен, всего 4 сообщения
  - PSK и RSA-Sig аутентификация
  - Асимметричная аутентификация
  - Сужение селектора трафика разрешено
  - Lifetime не нужны
  - Rekey – Определен
  - NAT-T: Поддерживается по умолчанию
  - DPD: Поддерживается по умолчанию
  - RoadWarrior: поддерживается EAP и config payload(CP)
  - Сопротивление ДОС улучшено (не устанавливается соединение пока точка не верифицирована)
  - MOBIKE (В настоящее время не реализовано)

IKEv2 Конфигурация

- Новый IKE2 exchange mode
- Игнорируемые параметры:
  - proposal-check
  - compatibility-options
  - lifebytes
  - xauth
- Mode-conf Используется для определения CP (configuration payload)

```
[admin@rack1_b3] /ip ipsec peer> add  address=1.1.1.1 exchange-mode=ike2 secret=123
[admin@rack1_b3] /ip ipsec peer> print
Flags: X - disabled, D - dynamic, R - responder
 0     address=1.1.1.1/32 auth-method=pre-shared-key secret="123" generate-policy=no
       policy-template-group=default exchange-mode=ike2 send-initial-contact=yes
       hash-algorithm=sha1 enc-algorithm=aes-128,3des dh-group=modp1024
       dpd-interval=2m
```

Интересные факты

- Улучшен формат отладки
- Может выступать в роли реле EAP
- Поддержка EAP-Only режима
- Может создавать политики с помощью level=unique
- Несколько клиентов за одним и тем же публичным IP-адресом теперь работают
- Аутентификация как xauth для ike2 (Работает только с ROS)
- RouterOS сейчас экспортирует pkcs12

IKEv2 RoadWarrior пример

```
/radius
add address=192.168.88.10 service=ipsec
#
/ip pool
add name=rw ranges=192.168.99.2-192.168.99.10
#
/ip ipsec mode-config
add address-pool=rw address-prefix-length=32 name=ike2
/ip ipsec peer
add auth-method=eap-radius certificate=none exchange-mode=ike2 generate-policy=\
    port-strict passive=yes
```

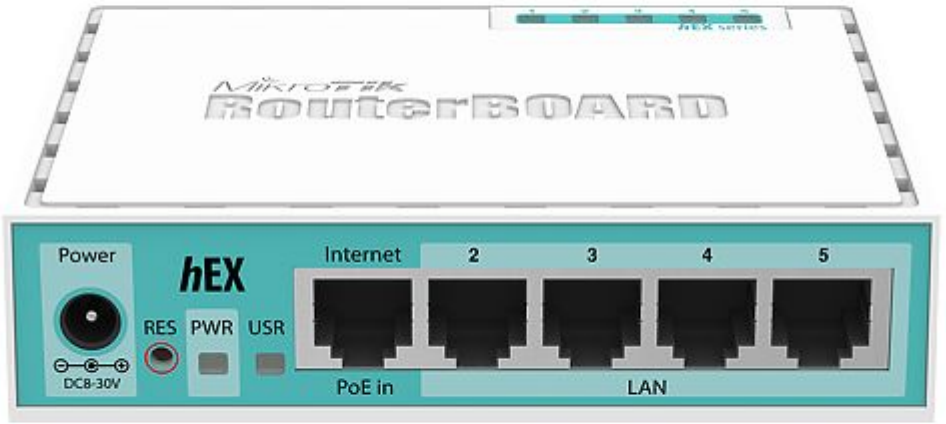
Аппаратное ускорение

Программное обеспечение медленно:

- MIPS 20-40Mbps
- Другие CPUs около 120Mbps на ядро
- x86 зависит от CPU (AES-NI не поддерживается)

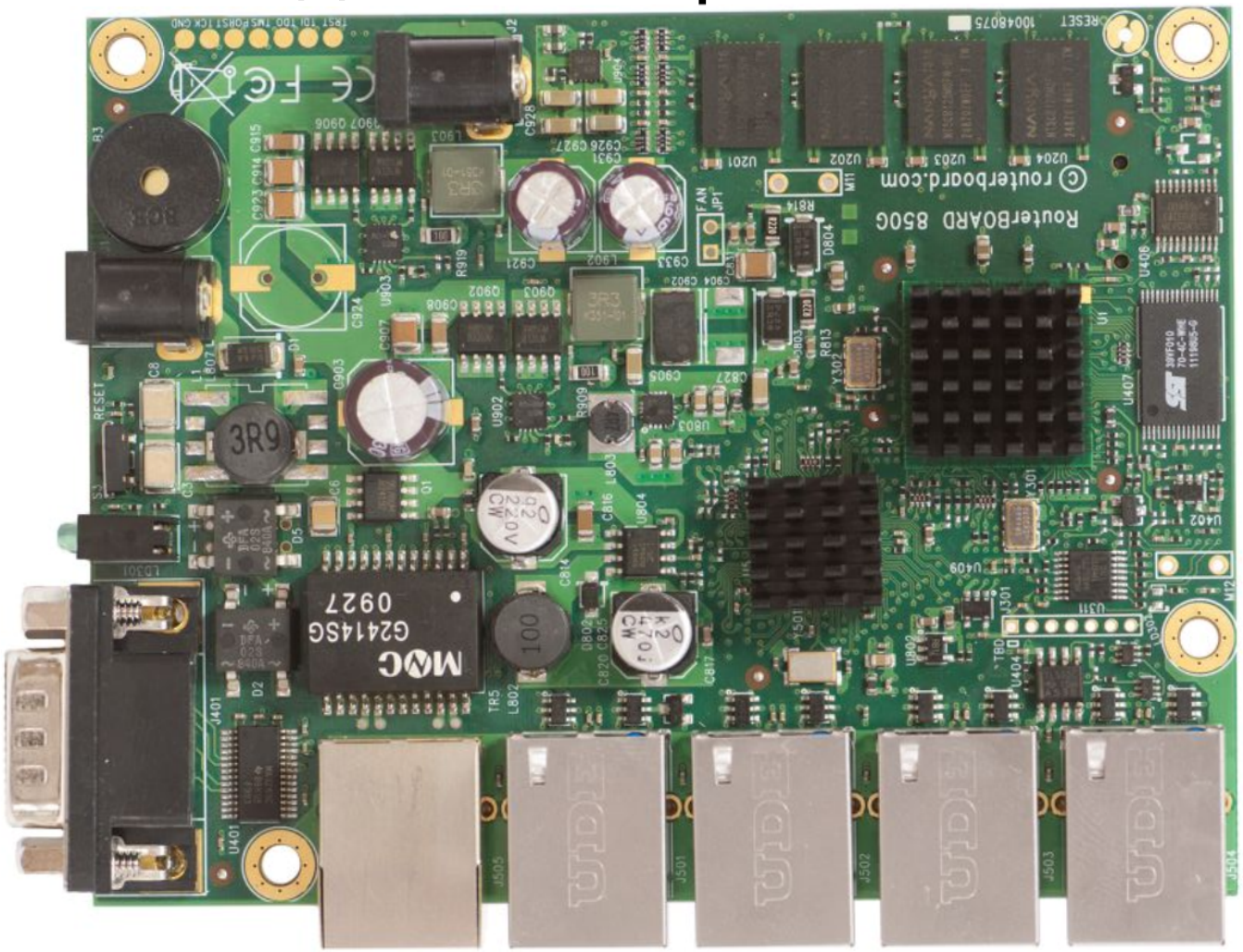
Аппаратное ускорение

HEX v3 (до 450Mbps)



Аппаратное ускорение

RB 850x2 (до 500Mbps)



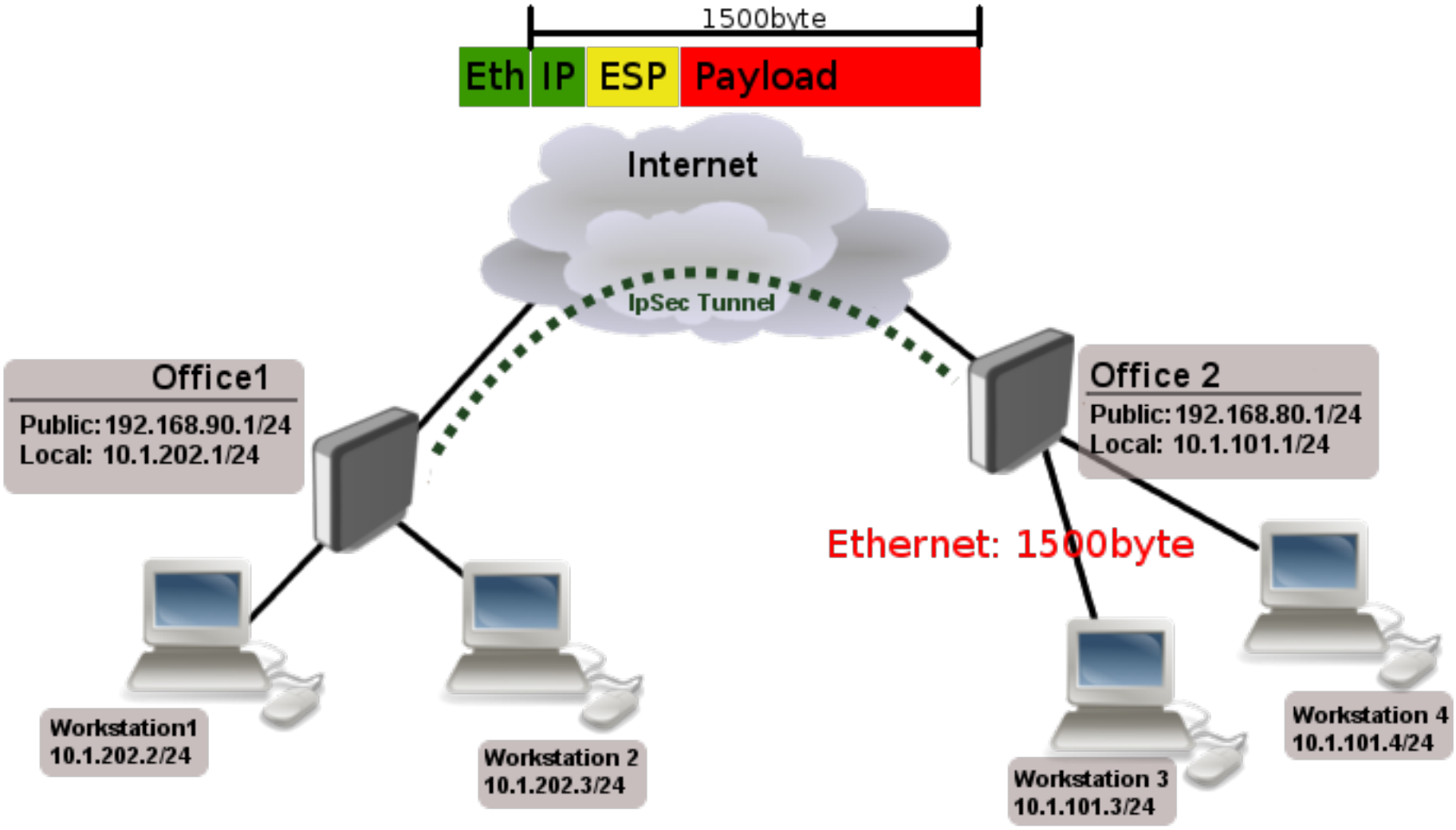
Аппаратное ускорение

RB1100AHx2 (до 750Mbps)

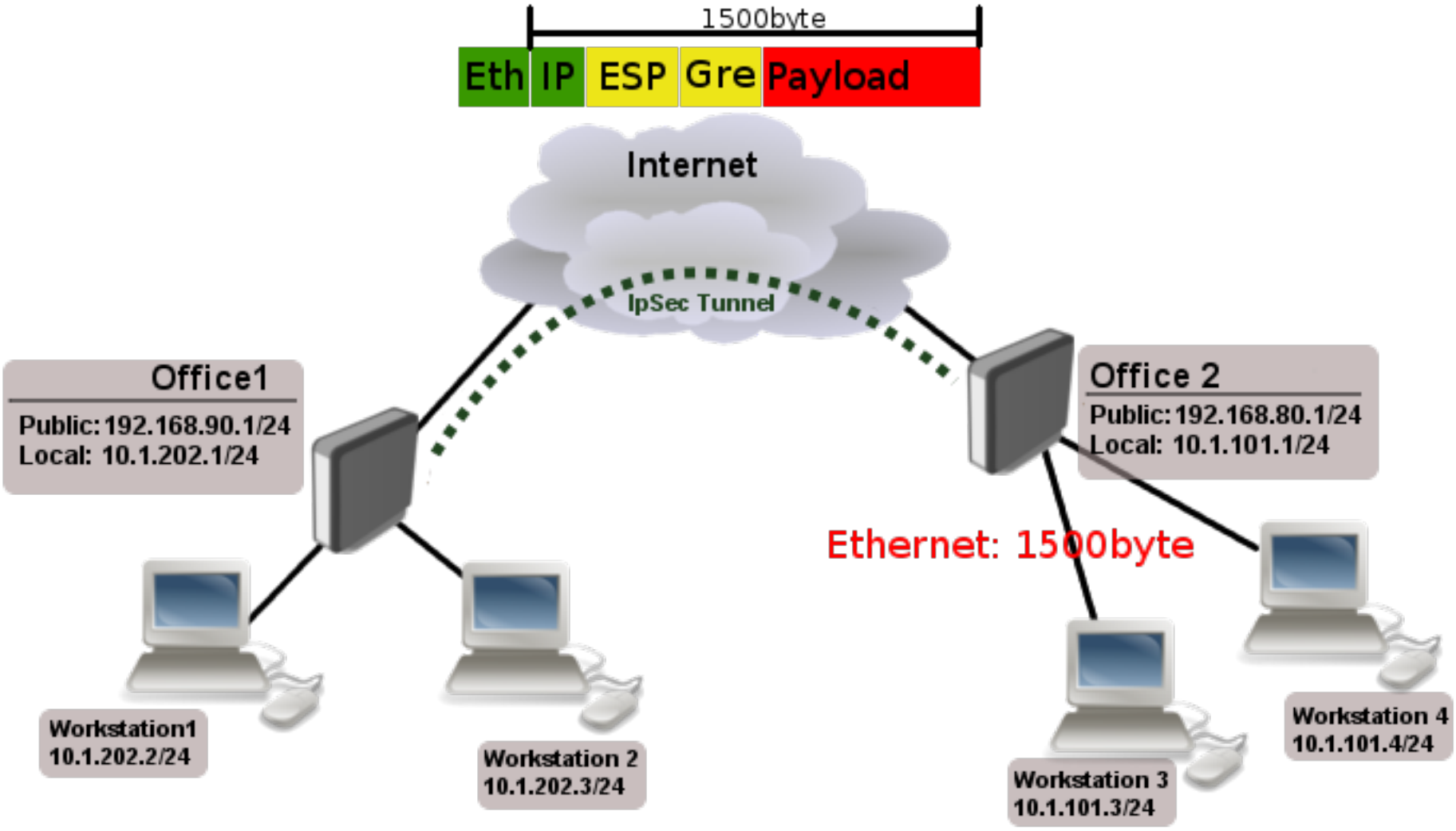
Аппаратное ускорение

CCR серии (с 2.4Gbps до 12Gbps)

Советы по эффективности



Советы по эффективности



Советы по эффективности

- Избегайте фрагментации (если один фрагмент потерян, другие фрагменты отбрасываются)
- Пакеты не более 1400 байт
- ставить change-mss 1400-40 (для TCP)
- Отрегулируйте MTU инкапсулированного туннеля вручную (GRE, IPIP ...)
- RouterOS может автоматически настраивать MTU (actual-mtu)
- Может не работать, если удаленный не является RouterOS

Советы по эффективности

- Оптимизация Firewall с fasttrak-om:
  - RAW Таблица уменьшает нагрузку на 30%

```
/ip firewall raw
add action=notrack chain=prerouting src-address=192.168.90.0/24 dst-address=192.168.80.0/24
add action=notrack chain=prerouting src-address=192.168.80.0/24 dst-address=192.168.90.0/24
```

Советы по использованию оборудования

- Использовать only-hardware-queue
- RB1100 ставить ether11 на собственном ядре процессора
- CCR1009 Избегайте использования портов коммутатора (ether 1-4), Классификатор не оптимален
- На маршрутизаторах серии CCR, чтобы использовать весь потенциал, разделить трафик потоками – 1 поток = 1SA пара

Советы по безопасности

Разрешить только шифрование:

- firewall policy matcher
- policy action=discard
- Новый вариант для l2tp use-ipsec=require

- Использовать aes-256/sha256
- Рассмотрите использование аутентификации RSA
- Переключить на IKEv2

Спасибо!