LAB4: IPSec VPN

IPSec modes of operation

IPSec is set of security services defined in RFC 4301, 4302, 4303,. . . which delivers encryption and authentication to IP protocol.

In **IPSec transport mode**, packet is secured by adding ESP/AH (Encapsulating Security Payload/Authentication Header) to IP packet. IP header stays the same, all higher layer data are secured by encryption and authentication (IP header (IP source and destination addresses) is authenticated as well using AH (authentication header)). Transport mode is end to end encryption and authentication (end devices must support IPSec to encrypt traffic)

IPSec in tunnel mode encapsulates whole IP packet in new IP header (encrypted and authenticated by IPSec). Tunneling protocol creates Virtual Private Network (VPN) between networks communicating over unsecured network (Internet).

IPSec operation

IKE/ISAKMP (Internet Security Association and Key Management Protocol) – protocol used for establishing IPSec connection. Key exchange and authentication. Uses UDP port 500.

IPSec – protocols used to encrypt traffic.

Phases of IPSec operation:

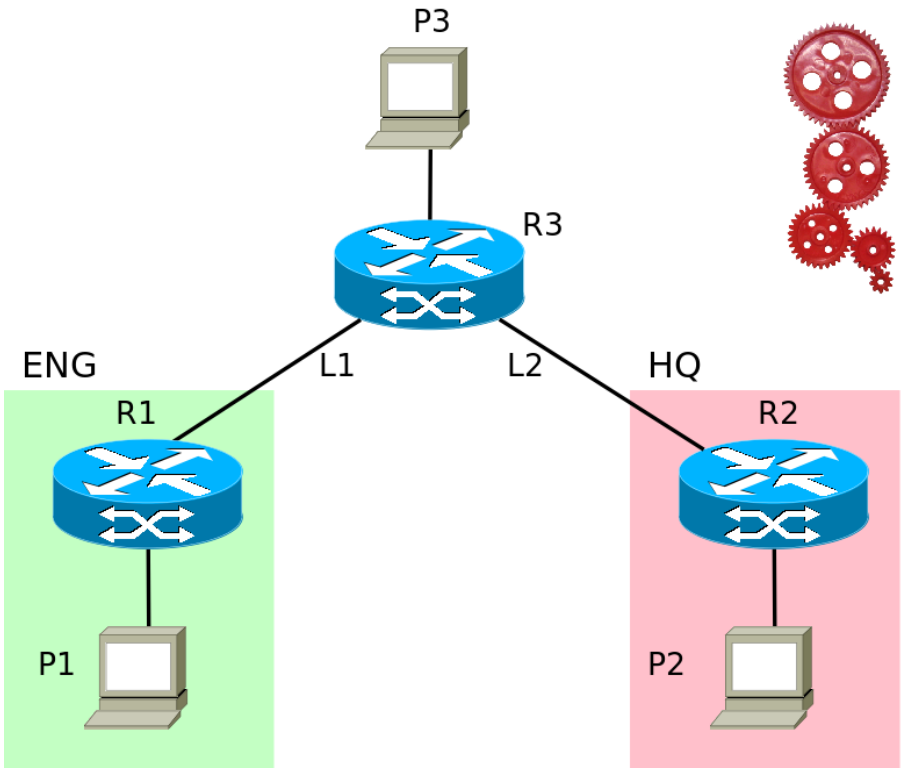
1. *interesting* traffic initiates IKE process (Internet Key Exchange). „interesting traffic“ – traffic which you have configured to be secured.
2. IKE phase 1 – authentication of IPSec peers and ISAKMP SA (security association) creation for key exchange – this phase is not encrypted. Uses Diffie-Hellman algorithm to exchange encryption keys for IKE phase 2.
3. IKE phase 2 – negotiation of IPSec SA parameters (prefered ciphers and authentication algorithms, encryption keys for IPSec communication exchange using Diffie-Hellman algorithm). This part is encrypted.
4. IPSec communication using negotiated protocols and keys.
5. IPSec tunnel termination.

GNS3 setup

1. import new IOS image to GNS3
   - IP base image doesn't support IPSec
   - an Advanced IP services image available
     - visit `http://caine.ics.muni.cz/PA197`

   .
2. learn how to add a linecard to Cisco router (Configuration → Slots, use NM-1FE-TX card)

LAB 1: network-network IPSec



Basic lab:
A small company called RedGears Ltd. producing red wheels has one department - Engineering (ENG) and headquaters (HQ) located in separated technology parks. Communication between these two locations goes over the Internet and needs to be secured.

Goal: Encrypt communications between network ENG and network HQ. Rest of the traffic goes unencrypted (communication to the Internet,. . .)

LAB 1: IP addresses setup

Host	IP
P1	192.168.1.11/24
P2	192.168.2.11/24
P3	192.168.3.11/24

Line	Network
L1	192.168.0.0/30
L2	192.168.0.4/30
Tunnel 0	192.168.0.8/30

LAB 1: tasks

1. build the whole topology without any IPSec tunnels
   - and test its functionality...
2. build IPSec tunnel between network ENG and network HQ
3. `ping` from P1 to P2
4. `ping` from P1 to P3
5. run packet capture on link L1.
   - 5.1 Is traffic from P1 to P2 encrypted using IPSec?
   - 5.2 Is traffic from P1 to P3 encrypted using IPSec?

Interfaces configuration – router R1

R1

```
interface Vlan1
  ip address 192.168.1.1 255.255.255.0
  no shutdown

interface FastEthernet2/0
  ip address 192.168.0.1 255.255.255.252
  no shutdown

ip route 0.0.0.0 0.0.0.0 192.168.0.2
```

Interfaces configuration – router R2

R2

```
interface Vlan1
  ip address 192.168.2.1 255.255.255.0
  no shutdown

interface FastEthernet2/0
  ip address 192.168.0.6 255.255.255.252
  no shutdown

ip route 0.0.0.0 0.0.0.0 192.168.0.5
```

Interfaces configuration – router R3

R3

```
interface Vlan1
  ip address 192.168.3.1 255.255.255.0
  no shutdown

interface FastEthernet2/0
  ip address 192.168.0.2 255.255.255.252
  no shutdown

interface FastEthernet3/0
  ip address 192.168.0.5 255.255.255.252
  no shutdown

ip route 192.168.1.0 255.255.255.0 192.168.0.1
ip route 192.168.2.0 255.255.255.0 192.168.0.6
```

LAB 1: testing the network setup

Now, test the networking among all the end-nodes P1-P3...

ISAKMP & IPSec setup – router R1

R1

```
crypto isakmp policy 1
  encr aes                          <-- cypher spec. for IKE phase 2
  authentication pre-share          <-- type of authentication
  group 5                           <-- Diffie-Hellman algorithm
  lifetime 600                      <-- lifetime of ISAKMP SA

crypto isakmp key test123 address 192.168.0.6
                                    <-- authentication key for remote host

crypto ipsec transform-set SECURE esp-aes esp-sha-hmac
                                    <-- type of encryption for IPSec

crypto ipsec profile PROTECT-GRE
  set security-association lifetime seconds 600
  set transform-set SECURE
```

ISAKMP & IPSec setup – router R2

R2

```
crypto isakmp policy 1
  encr aes                          <-- cypher specification
  authentication pre-share          <-- type of authentication
  group 5                           <-- Diffie-Hellman algorithm
  lifetime 600                      <-- lifetime of ISAKMP SA

crypto isakmp key test123 address 192.168.0.1
                                    <-- authentication key for remote host

crypto ipsec transform-set SECURE esp-aes esp-sha-hmac
                                    <-- type of encryption for IPSec

crypto ipsec profile PROTECT-GRE
  set security-association lifetime seconds 600
  set transform-set SECURE
```

Adapting the interfaces configuration – router R1

R1

```
interface Tunnel0
  ip address 192.168.0.9 255.255.255.252
  tunnel source 192.168.0.1
  tunnel destination 192.168.0.6
  tunnel protection ipsec profile PROTECT-GRE

ip route 192.168.2.0 255.255.255.0 192.168.0.10
```

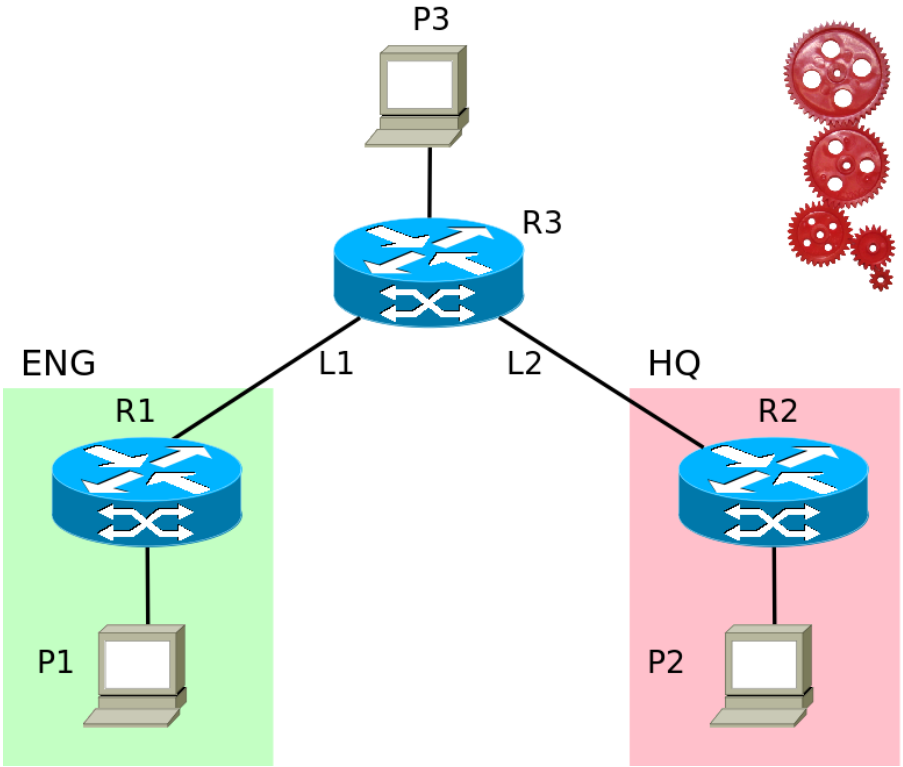
Adapting the interfaces configuration – router R2

R2

```
interface Tunnel0
  ip address 192.168.0.10 255.255.255.252
  tunnel source 192.168.0.6
  tunnel destination 192.168.0.1
  tunnel protection ipsec profile PROTECT-GRE

ip route 192.168.1.0 255.255.255.0 192.168.0.9
```

LAB 2: Hub and spoke topology



Hub and Spoke
Hub and spoke topology gives better control on traffic leaving company network. All traffic has to go through hub of the enterprise network (usually headquarters). Firewall, IPSs and other security equipments are located here.

LAB 2: tasks

1. change the logical topology of previous lab (LAB 1) to hub and spoke topology: make R2 hub - that means that all traffic from network ENG goes through IPSec tunnel to HQ and then to the neighboring networks (this means, that traffic from P1 to P3 goes through the tunnel to R2 and then to R3 and P3)
   - **Hint:** there is no need to change IPSec tunnel. All you have to do is changing IP routing tables on R1 and R3.
2. test this topology:
   - 2.1 `ping` from P1 to P3
   - 2.2 Capture packets on link L1. Is there unencrypted traffic from P1 to P3?
   - 2.3 Capture packets on link L2. Is there unencrypted traffic from P1 to P3?

LAB 2: config

Use LAB 1 config, then:

Router R1:

1. *delete* `ip route 0.0.0.0 0.0.0.0 192.168.0.2`
2. *add* `ip route 192.168.0.6 255.255.255.255 192.168.0.2`
3. *add* `ip route 0.0.0.0 0.0.0.0 192.168.0.10`

Router R3:

1. *delete* `ip route 192.168.1.0 255.255.255.0 192.168.0.1`
2. *add* `ip route 192.168.1.0 255.255.255.0 192.168.0.6`

References

- Cisco IOS Security Configuration Guide, Release 12.4, http://www.cisco.com/c/en/us/td/docs/ios/security/configuration/guide/12_4/sec_12_4_book.html