Security of Networks
Nicolas Fischer
Yanis Chamson

LAB 1

Part 1: Configure IPsecParameters on R1

Step 1:

ping from PC-A to PC-C

```
C:\>ping 192.168.3.3

Pinging 192.168.3.3 with 32 bytes of data:

Reply from 192.168.3.3: bytes=32 time=20ms TTL=125
Reply from 192.168.3.3: bytes=32 time=12ms TTL=125
Reply from 192.168.3.3: bytes=32 time=12ms TTL=125
Reply from 192.168.3.3: bytes=32 time=9ms TTL=125

Ping statistics for 192.168.3.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 9ms, Maximum = 20ms, Average = 13ms
```

Step 2:

'show version' command on R1

```
License Info:

License UDI:

-------------------------------------------------
Device#    PID                 SN
-------------------------------------------------
*0         CISCO1941/K9        FTX1524F8G8


Technology Package License Information for Module:'c1900'

-----------------------------------------------------------------
Technology    Technology-package          Technology-package
              Current       Type          Next reboot
-----------------------------------------------------------------
ipbase        ipbasek9      Permanent     ipbasek9
security      disable       None          None
data          disable       None          None

Configuration register is 0x2102
```

Security of Networks
Nicolas Fischer
Yanis Chamson

enabling the Security Technology Package

```
R1(config)#license boot module c1900 technology-package securityk9
PLEASE READ THE FOLLOWING TERMS CAREFULLY. INSTALLING THE LICENSE OR
LICENSE KEY PROVIDED FOR ANY CISCO PRODUCT FEATURE OR USING SUCH
PRODUCT FEATURE CONSTITUTES YOUR FULL ACCEPTANCE OF THE FOLLOWING
TERMS. YOU MUST NOT PROCEED FURTHER IF YOU ARE NOT WILLING TO BE BOUND
BY ALL THE TERMS SET FORTH HEREIN.

Use of this product feature requires an additional license from Cisco,
together with an additional payment. You may use this product feature
on an evaluation basis, without payment to Cisco, for 60 days. Your use
of the product, including during the 60 day evaluation period, is
subject to the Cisco end user license agreement
http://www.cisco.com/en/US/docs/general/warranty/English/EU1KEN_.html
If you use the product feature beyond the 60 day evaluation period, you
must submit the appropriate payment to Cisco for the license. After the
60 day evaluation period, your use of the product feature will be
governed solely by the Cisco end user license agreement (link above),
together with any supplements relating to such product feature. The
above applies even if the evaluation license is not automatically
terminated and you do not receive any notice of the expiration of the
evaluation period. It is your responsibility to determine when the
evaluation period is complete and you are required to make payment to
Cisco for your use of the product feature beyond the evaluation period.

Your acceptance of this agreement for the software features on one
product shall be deemed your acceptance with respect to all such
software on all Cisco products you purchase which includes the same
software. (The foregoing notwithstanding, you must purchase a license
for each software feature you use past the 60 days evaluation period,
so that if you enable a software feature on 1000 devices, you must
purchase 1000 licenses for use past the 60 day evaluation period.)

Activation of the software command line interface will be evidence of
your acceptance of this agreement.


ACCEPT? [yes/no]: yes
% use 'write' command to make license boot config take effect on next boot
```

‘show version’ command on R1 after reloading

```
License Info:

License UDI:

-------------------------------------------------
Device#    PID                 SN
-------------------------------------------------
*0         CISCO1941/K9        FTX1524F8G8


Technology Package License Information for Module:'c1900'

-----------------------------------------------------------------
Technology    Technology-package          Technology-package
              Current       Type          Next reboot
-----------------------------------------------------------------
ipbase        ipbasek9      Permanent     ipbasek9
security      securityk9    Evaluation    securityk9
data          disable       None          None

Configuration register is 0x2102
```

Security of Networks
Nicolas Fischer
Yanis Chamson

Step 5:

```
R1(config)#access-list 110 permit ip 192.168.1.0 0.0.0.255 192.168.3.0 0.0.0.255
R1(config)#crypto isakmp policy 10
R1(config-isakmp)#encryption aes 256
R1(config-isakmp)#authentication pre-share
R1(config-isakmp)#group 5
R1(config-isakmp)#exit
R1(config)#crypto isakmp key vpnpa55 address 10.2.2.2
R1(config)#crypto map VPN-M
R1(config)#crypto map VPN-MAP 10 ipsec-isakmp
% NOTE: This new crypto map will remain disabled until a peer
        and a valid access list have been configured.
R1(config)#crypto ipsec transform-set VPN-SET esp-aes esp-sha-hmac
R1(config)#crypto map VPN-MAP 10 ipsec-isakmp
R1(config-crypto-map)#description VPN connection to R3
R1(config-crypto-map)#set peer 10.2.2.2
R1(config-crypto-map)#set transform-set VPN-SET
R1(config-crypto-map)#match address 110
R1(config-crypto-map)#exit
```

Step 6:

Binding the crypto map

```
R1(config)#interface S0/0/0
R1(config-if)#crypto map VPN-MAP
*Jan  3 07:16:26.785: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON
```

Part 2: Configure IPsecParameters on R1

Step 1:

'show version' command on R3

```
License Info:

License UDI:

-------------------------------------------------
Device#   PID                 SN
-------------------------------------------------
*0        CISCO1941/K9        FTX1524I27D


Technology Package License Information for Module:'c1900'

-----------------------------------------------------------------
Technology    Technology-package          Technology-package
              Current       Type          Next reboot
-----------------------------------------------------------------
ipbase        ipbasek9      Permanent     ipbasek9
security      securityk9    Evaluation    securityk9
data          disable       None          None

Configuration register is 0x2102
```

Security of Networks
Nicolas Fischer
Yanis Chamson

‘show version’ command on R3 after reloading

```
License Info:

License UDI:

-------------------------------------------------
Device#   PID                 SN
-------------------------------------------------
*0        CISCO1941/K9        FTX1524I27D


Technology Package License Information for Module:'c1900'

-----------------------------------------------------------------
Technology    Technology-package          Technology-package
              Current       Type          Next reboot
-----------------------------------------------------------------
ipbase        ipbasek9      Permanent     ipbasek9
security      securityk9    Evaluation    securityk9
data          disable       None          None

Configuration register is 0x2102
```

Step 3:

```
R3(config)#access-list 110 permit ip 192.168.3.0 0.0.0.255 192.168.1.0 0.0.0.255
R3(config)#crypto isakmp policy 10
R3(config-isakmp)#encryption aes 256
R3(config-isakmp)#authentication pre-share
R3(config-isakmp)#group 5
R3(config-isakmp)#exit
R3(config)#crypto isakmp key vnpna55 address 10.1.1.2
R3(config)#crypto ipsec transform-set VPN-SET esp-aes esp-sha-hmac
```

Step 4 & 5 :

```
R3#config t
Enter configuration commands, one per line.  End with CNTL/Z.
R3(config)#crypto map VPN-MAP 10 ipsec-isakmp
R3(config-crypto-map)#description VPN connection to R1
R3(config-crypto-map)#set peer 10.1.1.2
R3(config-crypto-map)#set transform-set VPN-SET
R3(config-crypto-map)#match address 10.1.1.2
R3(config-crypto-map)#exit
R3(config)#interface s0/0/1
R3(config-if)#crypto map VP?
WORD
R3(config-if)#crypto map VPN-MAP
*Jan  3 07:16:26.785: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON
```

Security of Networks
Nicolas Fischer
Yanis Chamson

Part 3: Verify the IPsec VPN

Step 1:

```
R1#show crypto ipsec sa

interface: Serial0/0/0
    Crypto map tag: VPN-MAP, local addr 10.1.1.2

   protected vrf: (none)
   local  ident (addr/mask/prot/port): (192.168.1.0/255.255.255.0/0/0)
   remote  ident (addr/mask/prot/port): (192.168.3.0/255.255.255.0/0/0)
   current_peer 10.2.2.2 port 500
    PERMIT, flags={origin_is_acl,}
   #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
   #pkts decaps: 0, #pkts decrypt: 0, #pkts verify: 0
   #pkts compressed: 0, #pkts decompressed: 0
   #pkts not compressed: 0, #pkts compr. failed: 0
   #pkts not decompressed: 0, #pkts decompress failed: 0
   #send errors 0, #recv errors 0

     local crypto endpt.: 10.1.1.2, remote crypto endpt.:10.2.2.2
     path mtu 1500, ip mtu 1500, ip mtu idb Serial0/0/0
     current outbound spi: 0x0(0)

     inbound esp sas:

     inbound ah sas:

     inbound pcp sas:

     outbound esp sas:

     outbound ah sas:

     outbound pcp sas:
```

Step 2:

Ping from PC-C to PC-A

```
C:\>ping 192.168.1.3

Pinging 192.168.1.3 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.1.3:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

Security of Networks
Nicolas Fischer
Yanis Chamson

Step 3:

```
interface: Serial0/0/0
    Crypto map tag: VPN-MAP, local addr 10.1.1.2

   protected vrf: (none)
   local  ident (addr/mask/prot/port): (192.168.1.0/255.255.255.0/0/0)
   remote  ident (addr/mask/prot/port): (192.168.3.0/255.255.255.0/0/0)
   current_peer 10.2.2.2 port 500
    PERMIT, flags={origin_is_acl,}
   #pkts encaps: 7, #pkts encrypt: 7, #pkts digest: 0
   #pkts decaps: 6, #pkts decrypt: 6, #pkts verify: 0
   #pkts compressed: 0, #pkts decompressed: 0
   #pkts not compressed: 0, #pkts compr. failed: 0
   #pkts not decompressed: 0, #pkts decompress failed: 0
   #send errors 1, #recv errors 0

     local crypto endpt.: 10.1.1.2, remote crypto endpt.:10.2.2.2
     path mtu 1500, ip mtu 1500, ip mtu idb Serial0/0/0
     current outbound spi: 0x4BC266F1(1271031537)

     inbound esp sas:
      spi: 0x1FF52F37(536162103)
        transform: esp-aes esp-sha-hmac ,
        in use settings ={Tunnel, }
        conn id: 2007, flow_id: FPGA:1, crypto map: VPN-MAP
        sa timing: remaining key lifetime (k/sec): (4525504/3558)
        IV size: 16 bytes
        replay detection support: N
        Status: ACTIVE

     inbound ah sas:

     inbound pcp sas:

     outbound esp sas:
      spi: 0x4BC266F1(1271031537)
        transform: esp-aes esp-sha-hmac ,
        in use settings ={Tunnel, }
        conn id: 2008, flow_id: FPGA:1, crypto map: VPN-MAP
        sa timing: remaining key lifetime (k/sec): (4525504/3558)
        IV size: 16 bytes
        replay detection support: N
        Status: ACTIVE

     outbound ah sas:

     outbound pcp sas:
```

We have ping PC-C twice because the first one for some reason was entirely timed out.

Step 4:

Ping from PC-A to PC-B

```
C:\>ping 192.168.2.3

Pinging 192.168.2.3 with 32 bytes of data:

Reply from 192.168.2.3: bytes=32 time=25ms TTL=126
Reply from 192.168.2.3: bytes=32 time=1ms TTL=126
Reply from 192.168.2.3: bytes=32 time=22ms TTL=126
Reply from 192.168.2.3: bytes=32 time=20ms TTL=126

Ping statistics for 192.168.2.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 25ms, Average = 17ms
```

Security of Networks
Nicolas Fischer
Yanis Chamson

Step 5:

```
interface: Serial0/0/0
    Crypto map tag: VPN-MAP, local addr 10.1.1.2

   protected vrf: (none)
   local  ident (addr/mask/prot/port): (192.168.1.0/255.255.255.0/0/0)
   remote  ident (addr/mask/prot/port): (192.168.3.0/255.255.255.0/0/0)
   current_peer 10.2.2.2 port 500
    PERMIT, flags={origin_is_acl,}
   #pkts encaps: 7, #pkts encrypt: 7, #pkts digest: 0
   #pkts decaps: 6, #pkts decrypt: 6, #pkts verify: 0
   #pkts compressed: 0, #pkts decompressed: 0
   #pkts not compressed: 0, #pkts compr. failed: 0
   #pkts not decompressed: 0, #pkts decompress failed: 0
   #send errors 1, #recv errors 0

     local crypto endpt.: 10.1.1.2, remote crypto endpt.:10.2.2.2
     path mtu 1500, ip mtu 1500, ip mtu idb Serial0/0/0
     current outbound spi: 0x4BC266F1(1271031537)

     inbound esp sas:
      spi: 0x1FF52F37(536162103)
        transform: esp-aes esp-sha-hmac ,
        in use settings ={Tunnel, }
        conn id: 2007, flow_id: FPGA:1, crypto map: VPN-MAP
        sa timing: remaining key lifetime (k/sec): (4525504/2157)
        IV size: 16 bytes
        replay detection support: N
        Status: ACTIVE

     inbound ah sas:

     inbound pcp sas:

     outbound esp sas:
      spi: 0x4BC266F1(1271031537)
        transform: esp-aes esp-sha-hmac ,
        in use settings ={Tunnel, }
        conn id: 2008, flow_id: FPGA:1, crypto map: VPN-MAP
        sa timing: remaining key lifetime (k/sec): (4525504/2157)
        IV size: 16 bytes
        replay detection support: N
        Status: ACTIVE

     outbound ah sas:

     outbound pcp sas:
```

The number of packets has not increased because the data didn’t go through the IPSec VPN Tunnel and therefore is not encrypted.

Step 6:

Completed.