IPSEC VPN

PRACTICA 1.4

HECHO POR: IZAN NAVARRO

IES SERRA PERENXISA

INDICE

Parte 1: Habilitar las características de seguridad

Paso 1: Activar el módulo securityk9.

Se debe activar la licencia del paquete de tecnología de seguridad para completar esta actividad.
Nota: la contraseña de los modos EXEC del usuario y EXEC privilegiado es cisco. a.

a. Emita el comando show version en el modo EXEC del usuario o EXEC privilegiado para verificar si se activó la licencia del paquete de tecnología de seguridad.

Emitimos el comando "Show versión" y se nos muestra algo así:

```
If you require further assistance please contact us by sending email to
export@cisco.com.
Cisco CISCO1941/K9 (revision 1.0) with 491520K/32768K bytes of memory.
Processor board ID FTX152400KS
2 Gigabit Ethernet interfaces
2 Low-speed serial(sync/async) network interface(s)
DRAM configuration is 64 bits wide with parity disabled.
255K bytes of non-volatile configuration memory.
249856K bytes of ATA System CompactFlash 0 (Read/Write)

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
```

No tendremos nada en security activado

b. De lo contrario, active el módulo securityk9 para el siguiente arranque del router, acepte la licencia, guarde la configuración y reinicie.

R1(config)# **license boot module c2900 technology-package securityk9**
R1(config)# **end**
R1# **copy running-config startup-config**
R1# **reload**

Estos comandos activan la licencia y activa el security

c. Una vez finalizada la recarga, vuelva a emitir el comando show version para verificar si se activó la licencia del paquete de tecnología de seguridad.

```
If you require further assistance please contact us by sending email to
export@cisco.com.
Cisco CISCO1941/K9 (revision 1.0) with 491520K/32768K bytes of memory.
Processor board ID FTX152400KS
2 Gigabit Ethernet interfaces
2 Low-speed serial(sync/async) network interface(s)
DRAM configuration is 64 bits wide with parity disabled.
255K bytes of non-volatile configuration memory.
249856K bytes of ATA System CompactFlash 0 (Read/Write)

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


R1#
```

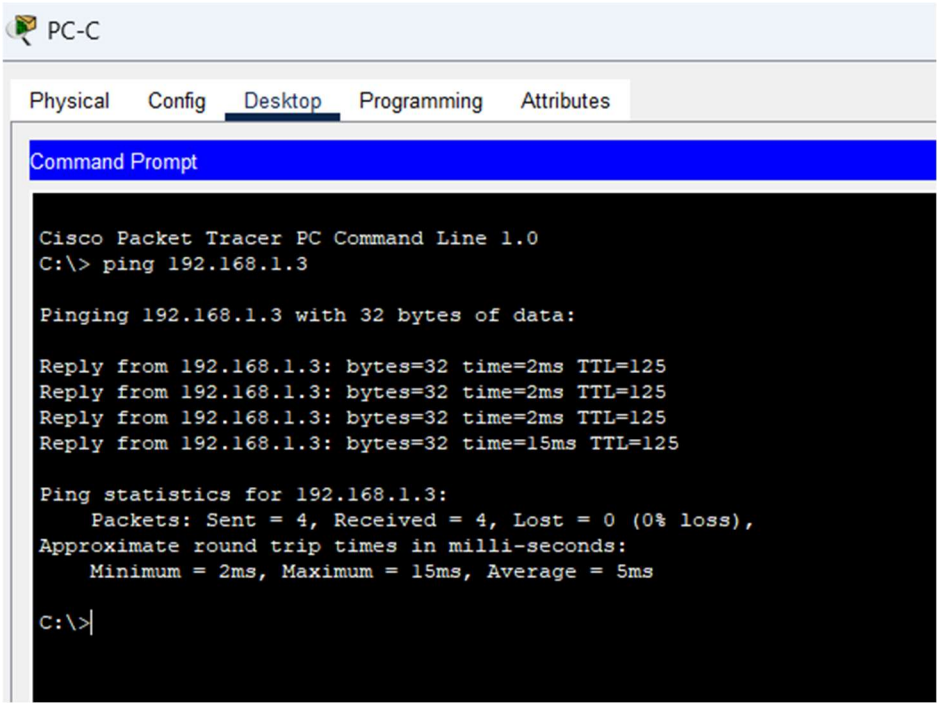
d. Repita los pasos 1 a 1 con el R3.

```
If you require further assistance please contact us by sending email t
export@cisco.com.
Cisco CISCO1941/K9 (revision 1.0) with 491520K/32768K bytes of memory.
Processor board ID FTX152400KS
2 Gigabit Ethernet interfaces
2 Low-speed serial(sync/async) network interface(s)
DRAM configuration is 64 bits wide with parity disabled.
255K bytes of non-volatile configuration memory.
249856K bytes of ATA System CompactFlash 0 (Read/Write)

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


R3#
```

Parte 2: Configurar los parámetros de IPsec en el R1

Paso 1: Probar la conectividad.

Haga ping de la PC-A a la PC-C.



Como podemos ver, se reciben perfectamente sin problemas!

Paso 2: Identificar el tráfico interesante en el R1. Configure la ACL 110 para identificar como interesante el tráfico proveniente de la LAN en el R1 a la LAN en el R3. Este tráfico interesante activa la VPN con IPsec para que se implemente cada vez que haya tráfico entre las LAN de los routers R1 y R3. El resto del tráfico que se origina en las LAN no se cifra. Recuerde que debido a la instrucción implícita deny any, no hay necesidad de agregar dicha instrucción a la lista.

```
R1(config)#access-list 11
R1(config)#access-list 110 pe
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)#
```

CONFIGURAR ISAKMP (FASE 1)

Los valores cambian ya que no reconoce “aes” ni “group 2” ya que el fichero preconfigurado de packetracer tiene unos comandos diferentes. Asignamos “aes 256” y “group 5”.

```
R1(config-if)#crypto isakmp policy 10
R1(config-isakmp)#encry
R1(config-isakmp)#encryption aes
R1(config-isakmp)#encryption aes 2
R1(config-isakmp)#encryption aes 256
R1(config-isakmp)#authe
R1(config-isakmp)#authentication pre-s
R1(config-isakmp)#authentication pre-share
R1(config-isakmp)#group 5
R1(config-isakmp)#group 5
R1(config-isakmp)#exit
R1(config)#cry
R1(config)#crypto is
R1(config)#crypto isakmp key vpnp
R1(config)#crypto isakmp key vpnpa55 add
R1(config)#crypto isakmp key vpnpa55 address 10.2.2.2
R1(config)#
```

CONFIGURAR ISAKMP (FASE 2)

```
R1(config)#crypto ipsec transform-set VPN-SET esp-3des esp-sha-hmac
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-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
R1(config)#
```

```
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
R1(config-if)#
```

Parte 3: Configurar los parámetros de IPsec en el R3

Paso 1:

Entramos en el Router 3 y seguimos los mismos pasos que hemos realizado con el Router 1.

```
R3(config)#access-list 110 permit ip 192.168.3.0 0.0.0.255 192.168.1.0 0.0.0.255
```

Paso 2:

Igual que antes, añadimos “aes 256” y “group 5”.

```
R3(config)#crypto isakmp policy 10
R3(config-isakmp)#encry
R3(config-isakmp)#encryption aes 2
R3(config-isakmp)#encryption aes 256
R3(config-isakmp)#authen
R3(config-isakmp)#authentication pre
R3(config-isakmp)#authentication pre-share
R3(config-isakmp)#group 5
R3(config-isakmp)#exit
R3(config)#cry
R3(config)#crypto isak
R3(config)#crypto isakmp ke
R3(config)#crypto isakmp key c
R3(config)#crypto isakmp key cisc
R3(config)#crypto isakmp key cisco add
R3(config)#crypto isakmp key cisco address 10.1.1.2
R3(config)#
```

Paso 3:

```
R3(config)#crypto ipsec transform-set VPN-SET esp-3des esp-sha-hmac
R3(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.
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 110
R3(config-crypto-map)#exit
```

Paso 4:

```
R3(config)#interface s0/0/1
R3(config-if)#crypto map VPN-MAP
*Jan  3 07:16:26.785: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON
R3(config-if)#
```

Parte 4: Verificar la VPN con Ipsec

Paso 1:

Verificar el túnel antes del tráfico interesante.

```
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:

 --More--
```

Paso 2:

```
C:\>ping 192.168.3.3

Pinging 192.168.3.3 with 32 bytes of data:

Request timed out.
Request timed out.
Reply from 192.168.3.3: bytes=32 time=2ms TTL=126
Reply from 192.168.3.3: bytes=32 time=2ms TTL=126

Ping statistics for 192.168.3.3:
    Packets: Sent = 4, Received = 2, Lost = 2 (50% loss),
Approximate round trip times in milli-seconds:
    Minimum = 2ms, Maximum = 2ms, Average = 2ms
```

Paso 3:

```
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: 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: 0xE58E72C8(3851317960)

     inbound esp sas:
      spi: 0x6BF76DD0(1811377616)
 --More--
```

¡Podremos observar que después de hacer ping al pc3 nos ha subido el número de encrypt y eso quiere decir que se está pasando de forma correcta!

Paso 4:

```
C:\>ping 192.168.2.3

Pinging 192.168.2.3 with 32 bytes of data:

Request timed out.
Reply from 192.168.2.3: bytes=32 time=1ms TTL=126
Reply from 192.168.2.3: bytes=32 time=1ms TTL=126
Reply from 192.168.2.3: bytes=32 time=1ms TTL=126

Ping statistics for 192.168.2.3:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 1ms, Average = 1ms

C:\>
```

Paso 5:

```
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: 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: 0xE58E72C8(3851317960)

     inbound esp sas:
      spi: 0x6BF76DD0(1811377616)
 --More--
```

Hacemos el mismo proceso desde la PC3 a la PC1 y podremos observar también que el contador de encrypt sube y quiere decir que los valores que se reciben del ping van encriptados.