Contenido

Introducción

Este artículo presentará cómo configurar GETVPN para avanzar las directivas permitiendo el envío y la recepción de la etiqueta del grupo de seguridad (SGT) insertada en los paquetes encriptados. El ejemplo implicará dos bifurcaciones que marcan todo el tráfico con etiqueta con las etiquetas específicas SGT y que aplican las directivas basadas zona del Firewall (ZBF) basadas en las etiquetas recibidas SGT.

Prerrequisitos

Requisitos

Cisco recomienda que tenga conocimiento sobre estos temas:

- Conocimiento básico de la configuración del comando line interface(cli) IOS y de la configuración GETVPN
- Conocimiento básico de los servicios de Trustsec.
- Conocimiento básico del Firewall Zona-basado

Componentes Utilizados

La información que contiene este documento se basa en estas versiones de software:

- Cisco 2921 Router con el software 15.3(2)T y más nuevo

Topología

Router del borde R3- en Branch1, miembro del grupo GETVPN

Router del borde R4- en Branch2, miembro del grupo GETVPN

R1,R2 - Servidores de la clave GETVPN en el sitio central

OSPF que se ejecuta en todo el Routers

ACL avanzado de KS que fuerza el cifrado para el tráfico entre 10.0.0.0/16 el <-> 10.0.0.0/16

El router R3 está marcando todo el tráfico con etiqueta enviado de Branch1 con la etiqueta SGT = 3

El router R4 está marcando todo el tráfico con etiqueta enviado de Branch2 con la etiqueta SGT = 4

El R3 está quitando las etiquetas SGT al enviar el tráfico hacia LAN (suposición que el R5 no está soportando en línea marcar con etiqueta)

El R4 está quitando las etiquetas SGT al enviar el tráfico hacia LAN (suposición que el R6 no está soportando en línea marcar con etiqueta)

El R4 no está teniendo ningún Firewall (que valida todos los paquetes)

El R3 se configura con ZBF con las directivas siguientes:

- validar todo el tráfico del LAN hacia WAN

- validando solamente el ICMP marcado con etiqueta con SGT=4 de WAN hacia el LAN

Configuración

R1 (servidor dominante en el sitio central)

Para enviar las directivas teniendo en cuenta enviar y recibir los paquetes con Tag “comando del sgt de los cts tac” necesita estar presente:

```
interface Loopback0
 ip address 10.0.1.1 255.255.255.0
!
interface Ethernet0/0
 ip address 192.168.0.1 255.255.255.0

crypto ipsec transform-set TS esp-aes esp-sha256-hmac
 mode tunnel
!
crypto ipsec profile prof1
 set transform-set TS
!
crypto gdoi group group1
 identity number 1
 server local
 rekey authentication mypubkey rsa GETKEY
 rekey transport unicast
 sa ipsec 1
```

```
  profile prof1
  match address ipv4 GET-IPV4
  replay counter window-size 64
   tag cts sgt
 address ipv4 192.168.0.1
 redundancy
  local priority 100
  peer address ipv4 192.168.0.2

router ospf 1
 network 10.0.0.0 0.0.255.255 area 0
 network 192.168.0.0 0.0.0.255 area 0

ip access-list extended GET-IPV4
 permit icmp 10.0.0.0 0.0.255.255 10.0.0.0 0.0.255.255
```

La configuración para el r2 es muy similar.

R3 (miembro del grupo en Branch1)

La configuración GETVPN es lo mismo que para el escenario sin las etiquetas SGT. La interfaz LAN se ha configurado con el trustsec manual:

- el “sgt estático 3 de la directiva confiado en” - marca todos los paquetes con etiqueta recibidos del LAN usando SGT=3
- “ningún sgt de la propagación” - quita todas las etiquetas SGT al transmitir los paquetes hacia el LAN

```
crypto gdoi group group1
 identity number 1
 server address ipv4 192.168.0.1
 server address ipv4 192.168.0.2
!
!
crypto map cmap 10 gdoi
 set group group1

interface Ethernet0/0
 ip address 192.168.0.3 255.255.255.0
 crypto map cmap
!
interface Ethernet0/1
 ip address 10.0.3.1 255.255.255.0
cts manual
   no propagate sgt
   policy static sgt 3 trusted

router ospf 1
 network 10.0.0.0 0.0.255.255 area 0
 network 192.168.0.0 0.0.0.255 area 0
```

Configuración ZBF en el R3:

Todos los paquetes del LAN serán validados. De los paquetes icmp de WAN solamente marcados con etiqueta con SGT=4 será validado:

```
class-map type inspect match-all TAG_4_ICMP
match security-group source tag 4
 match protocol icmp
!
policy-map type inspect FROM_LAN
```

```
 class class-default
 pass log
policy-map type inspect FROM_WAN
 class type inspect TAG_4_ICMP
 pass log
 class class-default
 drop log
!
zone security lan
zone security wan
zone-pair security WAN-LAN source wan destination lan
 service-policy type inspect FROM_WAN
zone-pair security LAN-WAN source lan destination wan
 service-policy type inspect FROM_LAN

interface Ethernet0/0
 zone-member security wan
!
interface Ethernet0/1
 zone-member security lan
```

El R4 en configuración Branch2 es muy similar excepto ZBF que no se configure allí.

R5, configuración R6

El R5 y el R6 simula el LAN local en ambas bifurcaciones. Ejemplo de configuración para el R5:

```
class-map type inspect match-all TAG_4_ICMP
match security-group source tag 4
 match protocol icmp
!
policy-map type inspect FROM_LAN
 class class-default
 pass log
policy-map type inspect FROM_WAN
 class type inspect TAG_4_ICMP
 pass log
 class class-default
 drop log
!
zone security lan
zone security wan
zone-pair security WAN-LAN source wan destination lan
 service-policy type inspect FROM_WAN
zone-pair security LAN-WAN source lan destination wan
 service-policy type inspect FROM_LAN

interface Ethernet0/0
 zone-member security wan
!
interface Ethernet0/1
 zone-member security lan
```

Verificación

Tesing SGT GETVPN enterado

El marcar si el marcar con etiqueta SGT se soporta en el miembro del grupo en Branch1 (R3):

```
R3#show crypto gdoi feature cts-sgt
      Version    Feature Supported
       1.0.8           Yes
```

El marcar si las directivas TEK avanzadas para agrupar al miembro en Branch1 (R3) están utilizando SGT:

```
R3#show crypto gdoi
GROUP INFORMATION

<...some output ommited for clarity...>

TEK POLICY for the current KS-Policy ACEs Downloaded:
 Ethernet0/0:
   IPsec SA:
       spi: 0xD100D58E(3506492814)
       transform: esp-aes esp-sha256-hmac
       sa timing:remaining key lifetime (sec): expired
       Anti-Replay(Counter Based) : 64
        tag method : cts sgt
       alg key size: 16 (bytes)
       sig key size: 32 (bytes)
       encaps: ENCAPS_TUNNEL

   IPsec SA:
       spi: 0x52B3CA86(1387514502)
       transform: esp-aes esp-sha256-hmac
       sa timing:remaining key lifetime (sec): (1537)
       Anti-Replay(Counter Based) : 64
        tag method : cts sgt
       alg key size: 16 (bytes)
       sig key size: 32 (bytes)
       encaps: ENCAPS_TUNNEL
```

Envío del tráfico ICMP del R6 al R5:

```
R6#ping 10.0.3.10 repeat 10
Type escape sequence to abort.
Sending 10, 100-byte ICMP Echos to 10.0.3.10, timeout is 2 seconds:
!!!!!!!!!!
Success rate is 100 percent (10/10), round-trip min/avg/max = 1/1/6 ms
```

El marcar si el R3 está asociando la etiqueta SGT a los paquetes encriptados:

```
R3#show crypto ipsec sa detail

interface: Ethernet0/0
   Crypto map tag: cmap, local addr 192.168.0.3

  protected vrf: (none)
  local  ident (addr/mask/prot/port): (10.0.0.0/255.255.0.0/1/0)
  remote ident (addr/mask/prot/port): (10.0.0.0/255.255.0.0/1/0)
  Group: group1
  current_peer 0.0.0.0 port 848
    PERMIT, flags={}
   #pkts encaps: 39, #pkts encrypt: 39, #pkts digest: 39
   #pkts decaps: 39, #pkts decrypt: 39, #pkts verify: 39
   #pkts compressed: 0, #pkts decompressed: 0
   #pkts not compressed: 0, #pkts compr. failed: 0
   #pkts not decompressed: 0, #pkts decompress failed: 0
   #pkts no sa (send) 0, #pkts invalid sa (rcv) 0
   #pkts encaps failed (send) 0, #pkts decaps failed (rcv) 0
   #pkts invalid prot (recv) 0, #pkts verify failed: 0
   #pkts invalid identity (recv) 0, #pkts invalid len (rcv) 0
   #pkts replay rollover (send): 0, #pkts replay rollover (rcv) 0
```

```
   ##pkts replay failed (rcv): 0
    #pkts tagged (send): 39, #pkts untagged (rcv): 39

<...some output ommited for clarity...>
```

Marcar los contadores del dataplane para GETVPN en el miembro del grupo en Branch2 (R3):

```
R3#show crypto gdoi gm dataplane counters

Data-plane statistics for group group1:
   #pkts encrypt           : 53       #pkts decrypt           : 53
   #pkts tagged (send)     : 53       #pkts untagged (rcv)    : 53
   #pkts no sa (send)      : 0        #pkts invalid sa (rcv)  : 0
   #pkts encaps fail (send) : 0       #pkts decap fail (rcv)  : 0
   #pkts invalid prot (rcv) : 0       #pkts verify fail (rcv)  : 0
   #pkts not tagged (send)  : 0       #pkts not untagged (rcv) : 0
   #pkts internal err (send): 0       #pkts internal err (rcv) : 0
```

Dependiendo de la plataforma más detalles se pueden revelar usando los debugs. Por ejemplo en el R3:

```
R3#debug cts platform l2-sgt rx
R3#debug cts platform l2-sgt tx
```

Los paquetes recibidos por el R3 del LAN deben ser SGT marcado con etiqueta:

```
01:48:08: cts-l2sgt_rx:l2cts-policysgt:[in=Ethernet0/1 src=0100.5e00.0005 dst=aabb.cc00.6800]
Policy SGT Assign [pak=F1B00E00:flag=0x1:psgt=3]
```

También los paquetes encriptados envían vía el túnel serán marcados con etiqueta:

```
01:49:28: cts_ether_cmd_handle_post_encap_feature:pak[36BF868]:size=106 in=Ethernet0/1
out=Ethernet0/0 enctype=1 encsize=0 sgt_offset=18 [adj]:idb=Ethernet0/0 is_dot1q=0 linktype=7
mac_length=22 SGT=3
```

SGT de prueba ZBF enterado

El R3 validará solamente los paquetes icmp marcados con etiqueta con SGT=4 que viene de WAN. Al enviar los paquetes icmp del R6 al R5:

```
R6#ping 10.0.3.10 repeat 11
Type escape sequence to abort.
Sending 1, 100-byte ICMP Echos to 10.0.3.10, timeout is 2 seconds:
!
Success rate is 100 percent (1/1), round-trip min/avg/max = 1/1/6 ms
```

El R3 recibirá el paquete ESP marcado con etiqueta, lo desencripta. Entonces ZBF validará el tráfico:

```
*Mar 17 12:45:28.039: %FW-6-PASS_PKT: (target:class)-(WAN-LAN:TAG_4_ICMP) Passing icmp pkt
10.0.4.10:0 => 10.0.3.10:0 with ip ident 57
```

También el directiva-mapa presentará los contadores con los números de paquete validados:

```
R3#show policy-firewall stats all
Global Stats:
       Session creations since subsystem startup or last reset 0
       Current session counts (estab/half-open/terminating) [0:0:0]
       Maxever session counts (estab/half-open/terminating) [0:0:0]
       Last session created never
       Last statistic reset never
       Last session creation rate 0
       Maxever session creation rate 0
       Last half-open session total 0
```

```
policy exists on zp WAN-LAN
 Zone-pair: WAN-LAN

 Service-policy inspect : FROM_WAN

   Class-map: TAG_4_ICMP (match-all)
      Match: security-group source tag 4
      Match: protocol icmp
     Pass
        18 packets, 1440 bytes

   Class-map: class-default (match-any)
     Match: any
     Drop
       3 packets, 72 bytes

policy exists on zp LAN-WAN
 Zone-pair: LAN-WAN

 Service-policy inspect : FROM_LAN

   Class-map: class-default (match-any)
     Match: any
     Pass
       18 packets, 1440 bytes
```

Al intentar al telnet del R6 al R5- que será caído por el R3 porque el telnet no fue permitido:

```
*Mar 17 12:49:30.475: %FW-6-DROP_PKT: Dropping tcp session 10.0.4.10:37500 10.0.3.10:23 on zone-pair WAN-LAN class class-default due to  DROP action found in policy-map with ip ident 36123
```

Referencias

- Guía de configuración del switch de Cisco TrustSec: Comprensión de Cisco TrustSec
- Configurar a un servidor externo para la autorización de usuario del dispositivo de seguridad
- Guía de configuración CLI de la serie VPN de Cisco ASA, 9.1
- Guía del usuario del Cisco Identity Services Engine, versión 1.2
- Soporte Técnico y Documentación - Cisco Systems