GETVPN com colocação de etiquetas Inline de TrustSec SGT e exemplo Zona-baseado SGT-ciente da configuração de firewall

Índice

Introdução

Este artigo apresentará como configurar GETVPN para empurrar políticas permitindo a emissão e a recepção da etiqueta do grupo de segurança (SGT) introduzida em pacotes criptografado. O exemplo envolverá dois ramos que etiquetam todo o tráfego com as etiquetas específicas SGT e que aplicam as políticas baseadas zona do Firewall (ZBF) baseadas em etiquetas recebidas SGT.

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

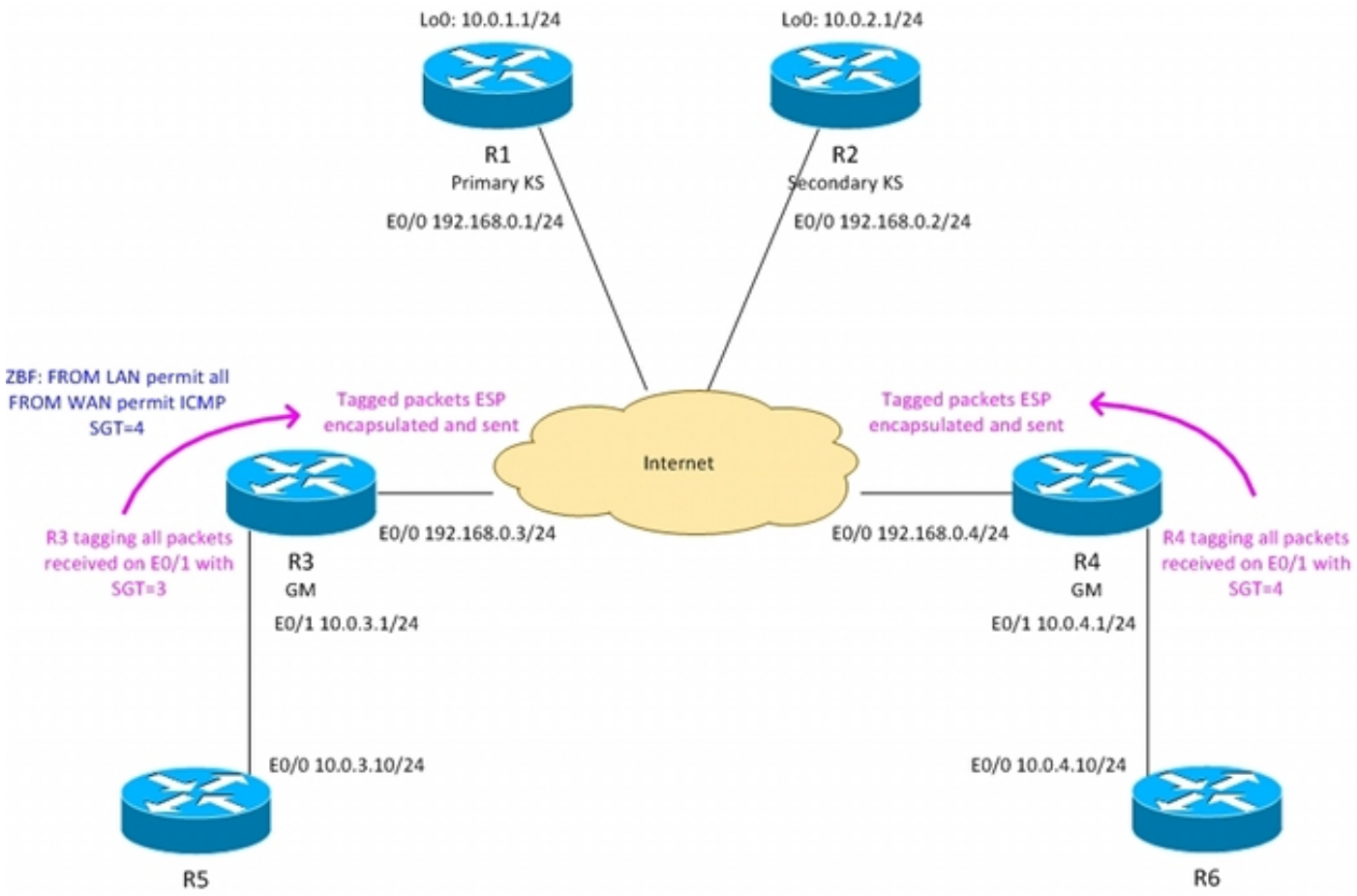
- Conhecimento básico da configuração do comando line interface(cli) IO e da configuração GETVPN
- Conhecimento básico de serviços de Trustsec.
- Conhecimento básico do Firewall Zona-baseado

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software:

- Cisco 2921 Router com software 15.3(2)T e mais novo

Topologia



Roteador de borda R3- em Branch1, membro do grupo GETVPN

Roteador de borda R4- em Branch2, membro do grupo GETVPN

R1,R2 - Server da chave GETVPN na instalação central

OSPF que é executado em todo o Roteadores

ACL empurrado de KS que força a criptografia para um tráfego entre 10.0.0.0/16 o <-> 10.0.0.0/16

O roteador R3 está etiquetando todo o tráfego enviado de Branch1 com a etiqueta SGT = 3

O roteador R4 está etiquetando todo o tráfego enviado de Branch2 com a etiqueta SGT = 4

O R3 está removendo as etiquetas SGT ao enviar o tráfego para LAN (suposição que o R5 não está apoiando inline a colocação de etiquetas)

O R4 está removendo as etiquetas SGT ao enviar o tráfego para LAN (suposição que o R6 não está apoiando inline a colocação de etiquetas)

O R4 não está tendo nenhum Firewall (que aceita todos os pacotes)

O R3 é configurado com o ZBF com as seguintes políticas:

- aceitando todo o tráfego do LAN para WAN

- aceitando somente o ICMP etiquetado com o SGT=4 de WAN para o LAN

Configuração

R1 (server chave na instalação central)

Para enviar políticas permitindo enviar e receber o comando do sgt dos pacotes rotulados “os cts que tac” precisa estam 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
```

A configuração para o R2 é muito similar.

R3 (membro do grupo em Branch1)

A configuração GETVPN é a mesma que para a encenação sem etiquetas SGT. A interface de LAN foi configurada com o trustsec manual:

- da “o sgt estático 3 política confiado” - etiqueta todos os pacotes recebidos do LAN usando SGT=3

- “nenhum sgt da propagação” - remove todas as etiquetas SGT ao transmitir os pacotes para o 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
```

Configuração ZBF no R3:

Todos os pacotes do LAN serão aceitados. Dos pacotes ICMP de WAN somente etiquetados com o SGT=4 será aceitado:

```
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
```

O R4 na configuração Branch2 é muito similar exceto ZBF que não é configurado lá.

R5, configuração R6

O R5 e o R6 simulam o LAN local em ambos os ramos. Exemplo de configuração para o 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
```

Verificação

Tesing SGT GETVPN ciente

Verificando se a colocação de etiquetas SGT é apoiada no membro do grupo em Branch1 (R3):

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

Verificando se as políticas TEK empurradas para agrupar o membro em Branch1 (R3) estão usando 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
```

Enviando o tráfego ICMP do R6 ao 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
```

Verificando se o R3 está anexando a etiqueta SGT aos pacotes criptografado:

```
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...>
```

Verificando contadores do dataplane para ver se há GETVPN no membro do grupo em 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
```

Segundo a plataforma que mais detalhes podem ser utilização revelada debuga. Por exemplo no R3:

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

Os pacotes recebidos pelo R3 do LAN devem ser SGT etiquetado:

```
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]
```

Igualmente os pacotes criptografado enviam através do túnel serão etiquetados:

```
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 teste ZBF ciente

O R3 aceitará somente os pacotes ICMP etiquetados com o SGT=4 que vem de WAN. Ao enviar pacotes ICMP do R6 ao 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
```

O R3 receberá o pacote ESP etiquetado, decifra-o. Então ZBF aceitará o tráfego:

```
*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
```

Igualmente o mapa de política apresentará os contadores com os números de pacote aceitados:

```
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
```

Ao tentar ao telnet do R6 ao R5- que será deixado cair pelo R3 porque o telnet não foi 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
```

Referências

- Guia de configuração de switch de Cisco TrustSec: Compreendendo Cisco TrustSec
- Configurando um servidor interno para a autorização de usuário da ferramenta de segurança
- Guia de configuração de CLI da série VPN de Cisco ASA, 9.1
- Guia do Usuário do Cisco Identity Services Engine, liberação 1.2
- Suporte Técnico e Documentação - Cisco Systems