GETVPN avec l'étiquetage d'en ligne de TrustSec SGT et l'exemple basé sur zone SGT-averti de configuration de Pare-feu

Contenu

Introduction

Cet article présentera comment configurer GETVPN pour pousser des stratégies permettant envoyer et recevoir la balise de groupe de sécurité (SGT) insérée dans les paquets chiffrés. L'exemple impliquera deux branchements étiquetant tout le trafic avec des balises de la particularité SGT et appliquant des stratégies du Pare-feu basées par zone (ZBF) basées sur les balises reçues SGT.

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

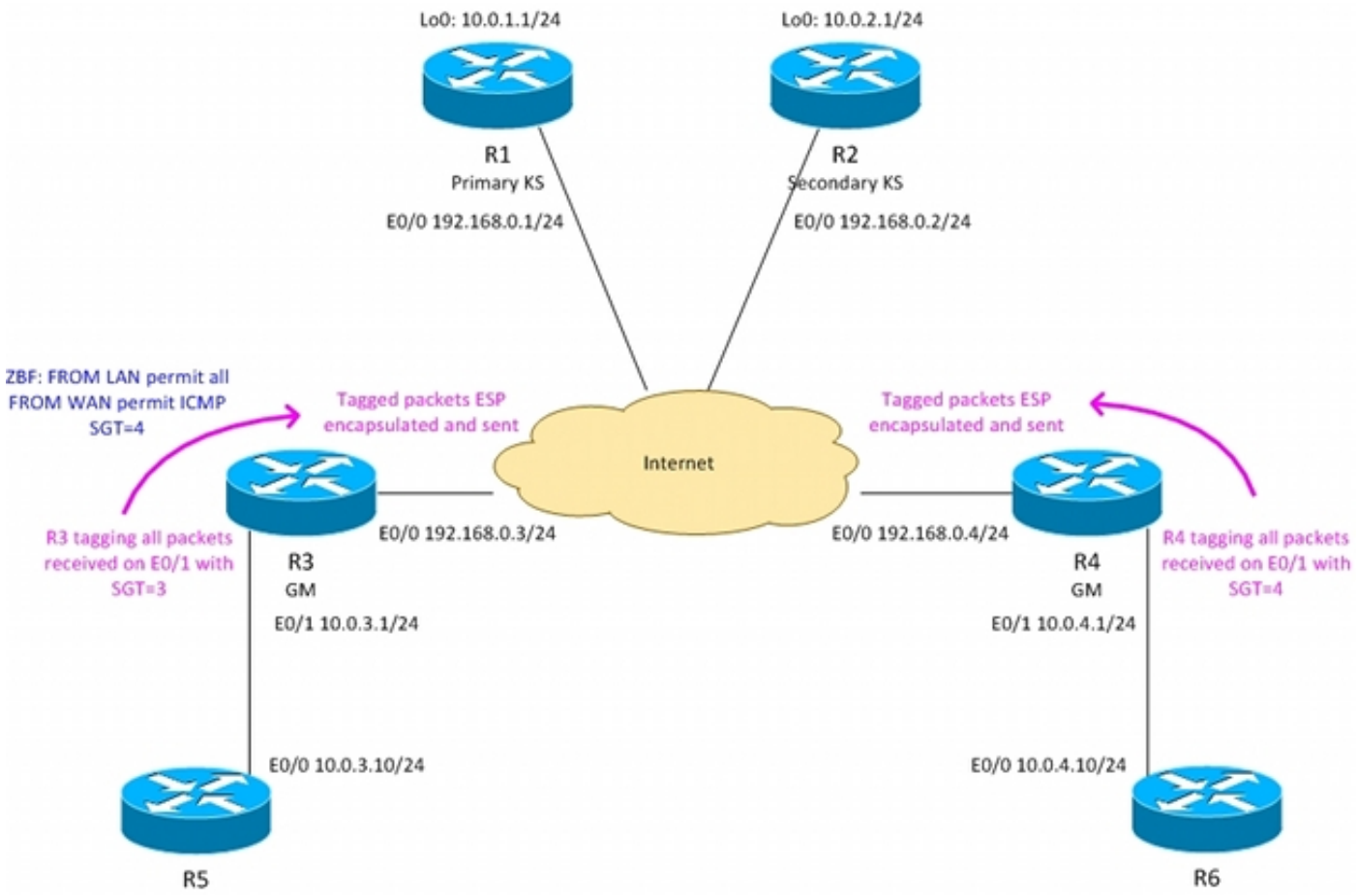
- Connaissance de base de configuration de l'interface de ligne de commande IOS (CLI) et de configuration GETVPN
- Connaissance de base des services de Trustsec.
- Connaissance de base de Pare-feu basé sur zone

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de logiciel suivantes :

- Routeur de Cisco 2921 avec le logiciel 15.3(2)T et plus nouveau

Topologie



R3 - routeur de cadre dans Branch1, membre du groupe GETVPN

R4 - routeur de cadre dans Branch2, membre du groupe GETVPN

R1,R2 - Serveurs de clé GETVPN dans le lieu d'exploitation principal

Exécution OSPF sur tous les Routeurs

L'ACL a poussé de KS forçant le cryptage pour le trafic entre 10.0.0.0/16 le <-> 10.0.0.0/16

Le routeur R3 étiquette tout le trafic envoyé de Branch1 avec la balise SGT = 3

Le routeur R4 étiquette tout le trafic envoyé de Branch2 avec la balise SGT = 4

R3 retire des balises SGT en envoyant le trafic vers le RÉSEAU LOCAL (supposition que R5 ne prend en charge pas l'étiquetage d'en ligne)

R4 retire des balises SGT en envoyant le trafic vers le RÉSEAU LOCAL (supposition que R6 ne prend en charge pas l'étiquetage d'en ligne)

R4 n'a aucun Pare-feu (recevant tous les paquets)

R3 est configuré avec ZBF avec les stratégies suivantes :

- recevant tous le trafic du RÉSEAU LOCAL vers le WAN

- recevant seulement l'ICMP étiqueté avec SGT=4 de WAN vers le RÉSEAU LOCAL

Configuration

R1 (serveur principal dans le lieu d'exploitation principal)

Pour envoyer des stratégies tenant compte d'envoyer et de recevoir des paquets balisés commande « de cts sgt tac » doit être présent :

```
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 configuration pour R2 est très semblable.

R3 (membre du groupe dans Branch1)

La configuration GETVPN est identique que pour le scénario sans balises SGT. L'interface de RÉSEAU LOCAL a été configurée avec le trustsec manuel :

- « le sgt statique 3 de stratégie fait confiance » - étiquette tous les paquets reçus du RÉSEAU LOCAL utilisant SGT=3
- « aucun sgt de propagation » - retire toutes les balises SGT en transmettant les paquets vers le RÉSEAU LOCAL

```
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
```

Configuration ZBF sur R3 :

Tous les paquets de RÉSEAU LOCAL seront reçus. Des paquets d'ICMP de WAN seulement étiquetés avec SGT=4 sera reçu :

```
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
```

R4 dans la configuration Branch2 est très semblable excepté ZBF qui n'est pas configuré là.

R5, configuration R6

R5 et R6 simule le réseau local dans les deux branchements. Exemple de configuration pour 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
```

Vérification

Tesing SGT GETVPN averti

Vérifier si l'étiquetage SGT est pris en charge sur le membre du groupe dans Branch1 (R3) :

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

Vérifier si les stratégies TEK poussées au membre du groupe dans Branch1 (R3) utilisent 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
```

Envoi du trafic d'ICMP de R6 à 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
```

Vérifier si R3 relie la balise SGT aux paquets chiffrés :

```
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...>
```

Vérifier le dataplane pare pour GETVPN sur le membre du groupe dans 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
```

Selon la plate-forme que plus de détails peuvent être indiqués utilisant met au point. Par exemple sur R3 :

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

Les paquets reçus par R3 du RÉSEAU LOCAL devraient être SGT étiqueté :

```
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]
```

Les paquets également chiffrés envoient par l'intermédiaire du tunnel seront étiquetés :

```
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 test ZBF averti

R3 recevra seulement des paquets d'ICMP étiquetés avec SGT=4 provenant le WAN. En envoyant des paquets d'ICMP de R6 à 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
```

R3 recevra le paquet étiqueté de l'ESP, le déchiffre. Alors ZBF recevra le trafic :

```
*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
```

Également le policy-map présentera les compteurs avec les nombres de paquet reçus :

```
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
```

En essayant au telnet de R6 à R5 - qui sera relâché par R3 parce que le telnet n'a pas été permis :

```
*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
```

Références

- Guide de configuration de commutateur de Cisco TrustSec : Compréhension du Cisco TrustSec
- Configurer un serveur externe pour l'autorisation d'utilisateur de dispositifs de sécurité
- Guide de configuration de la gamme VPN CLI de Cisco ASA, 9.1
- Guide de l'utilisateur de Logiciel Cisco Identity Services Engine, version 1.2
- Support et documentation techniques - Cisco Systems