GETVPN met TrustSec SGT Inline Tagging en SGT-Aware Zone-gebaseerde firewallconfiguratie Voorbeeld

Inhoud

Inleiding

Dit artikel zal tonen hoe te om GETVPN te vormen om beleid te duwen dat het verzenden en ontvangen van de Vraag van de Groep van de Veiligheid (SGT) in gecodeerde pakketten toelaat. Het voorbeeld omvat twee takken die al het verkeer taggen met specifieke SGT-tags en het ZBF-beleid (Zone Based Firewall) toepassen op basis van ontvangen SGT-tags.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

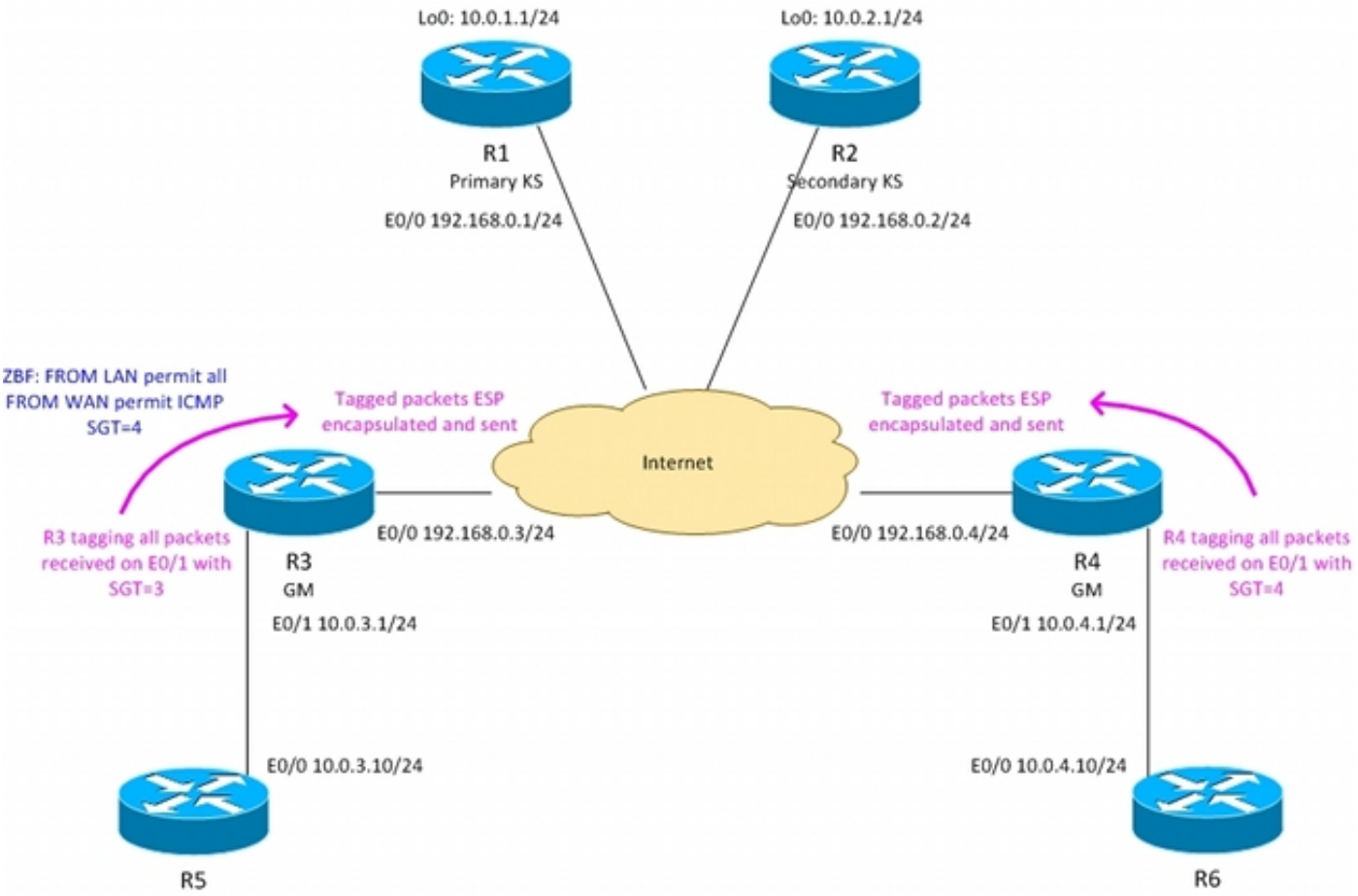
- Basiskennis van IOS commando-line interface (CLI) configuratie en GETVPN-configuratie
- Basiskennis van Trustsec-diensten.
- Basiskennis van de op een zone gebaseerde firewall

Gebruikte componenten

De informatie in dit document is gebaseerd op deze softwareversies:

- Cisco 2921 router met software 15.3(2)T en nieuwer

Topologie



R3 - grensrouter in Branch1, GETVPN-groepslid

R4 - grensrouter in Branch2, GETVPN-groepslid

R1,R2 - GETVPN-sleutelservers in Central Site

OSPF-beperking op alle routers

ACL geduwd van KS dwingend encryptie voor verkeer tussen 10.0.0.0/16 <-> 10.0.0.0/16

R3-router tagt al verkeer dat vanuit Branch1 wordt verzonden met SGT-tag = 3

R4-router is het taggen van al het verkeer dat vanuit Branch2 wordt verzonden met SGT-tag = 4

R3 verwijdert SGT-tags bij het verzenden van verkeer naar LAN (veronderstelling dat R5 inline tagging niet ondersteunt)

R4 verwijdert SGT-tags bij het verzenden van verkeer naar LAN (veronderstelling dat R6 geen inline tagging ondersteunt)

R4 heeft geen firewall (alle pakketten accepteren)

R3 wordt ingesteld met ZBF met het volgende beleid:

- al het verkeer via LAN naar WAN accepteren

- alleen ICMP accepteren dat is gelabeld met SGT=4 van WAN naar LAN

Configuratie

R1 (sleutelserver op centrale locatie)

Om beleid te verzenden en ontvangen, moet de opdracht "tac cts sgt" aanwezig zijn:

```
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
```

De configuratie voor R2 lijkt sterk op die voor C2.

R3 (groepslid in afdeling 1)

De configuratie van GETVPN is hetzelfde als voor scenario zonder SGT-tags. LAN-interface is ingesteld met handmatige vertrouwen:

- "Policy statische sgt 3 vertrouwd" - tags die alle pakketten ontvangen zijn van LAN met behulp van SGT=3
- "geen doorgifte van SST" - verwijdert alle SGT-tags bij het verzenden van de pakketten naar 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
```

ZBF-configuratie op R3:

Alle pakketten van LAN worden geaccepteerd. Van WAN worden alleen ICMP-pakketten die gelabeld zijn met SGT=4 geaccepteerd:

```
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 in Branch2 configuratie is zeer vergelijkbaar, behalve ZBF dat daar niet is geconfigureerd.

R5, R6-configuratie

R5 en R6 simuleren lokaal LAN in beide takken. Voorbeeld configuratie voor R5:

```
interface Ethernet0/0
 ip address 10.0.3.10 255.255.255.0
router ospf 1
 network 10.0.0.0 0.0.255.255 area 0
```

Verificatie

TesSGT-bewuste GETVPN

Controle of SGT-markering op groepslid in Branch1 (R3) wordt ondersteund:

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

Controle of het TEK beleid dat naar groepslid in Vestiging1 (R3) wordt geduwd SGT gebruikt:

```
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
```

Verzenden van ICMP-verkeer van R6 naar 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
```

Controleer of R3 een SGT-tag aan versleutelde pakketten hecht:

```
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...>
```

Controle van dataplanetellers voor GETVPN op groepslid in 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
```

Afhankelijk van het platform kunnen meer details worden onthuld met behulp van debugs. Bijvoorbeeld op R3:

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

Packets die R3 van LAN ontvangt, moeten SGT zijn gelabeld:

```
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]
```

Tevens worden versleutelde pakketten die via de tunnel worden verzonden, getagd:

```
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
```

Testen SGT-bewuste ZBF

R3 zal alleen ICMP-pakketten accepteren die zijn gelabeld met SGT=4 en die van WAN afkomstig zijn. Bij het verzenden van ICMP-pakketten van R6 naar 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 ontvangt gelabeld ESP-pakket en decrypteert het. Dan accepteert ZBF het verkeer:

```
*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
```

Ook zal de politiek-kaart de tellers met de aantallen geaccepteerde pakje presenteren:

```
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
```

Wanneer men probeert te tellen van R6 naar R5 - dat komt neer op R3 omdat telnet niet is toegestaan:

```
*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
```

Referenties

- Cisco TrustSec-switchconfiguratie-gids: De betekenis van Cisco TrustSec
- Een externe server configureren voor security applicatie, gebruikersautorisatie
- Cisco ASA Series 5000 Series VPN CLI-configuratiegids, 9.1

- Gebruikershandleiding voor Cisco Identity Services Engine, release 1.2
- Technische ondersteuning en documentatie – Cisco Systems