Contents

Introduction

This article will present how to configure GETVPN to push policies allowing sending and receiving Security Group Tag (SGT) inserted into encrypted packets. Example will involve two branches tagging all the traffic with specific SGT tags and applying Zone Based Firewall (ZBF) policies based on received SGT tags.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Basic knowledge of IOS command-line interface (CLI) configuration and GETVPN configuration
- Basic knowledge of Trustsec services.
- Basic knowledge of Zone-Based Firewall

Components Used

The information in this document is based on these software versions:

- Cisco 2921 Router with software 15.3(2)T and newer

Topology

R3 - border router in Branch1, GETVPN group member

R4 - border router in Branch2, GETVPN group member

R1,R2 - GETVPN Key servers in Central Site

OSPF running on all routers

ACL pushed from KS forcing encryption for traffic between 10.0.0.0/16 <-> 10.0.0.0/16

R3 router is tagging all traffic sent from Branch1 with SGT tag = 3

R4 router is tagging all traffic sent from Branch2 with SGT tag = 4

R3 is removing SGT tags when sending traffic towards LAN (assumption that R5 is not supporting inline tagging)

R4 is removing SGT tags when sending traffic towards LAN (assumption that R6 is not supporting inline tagging)

R4 is having no firewall (accepting all packets)

R3 is configured with ZBF with the following policies:

- accepting all traffic from LAN towards WAN

- accepting only ICMP tagged with SGT=4 from WAN towards LAN

Configuration

R1 (Key Server in Central Site)

To send policies allowing for sending and receiving tagged packets "tac cts sgt" command needs to be present:

```
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
```

Configuration for R2 is very similar.

R3 (Group Member in Branch1)

GETVPN configuration is the same as for scenario without SGT tags. LAN interface has been configured with manual trustsec:

- "policy static sgt 3 trusted" - tags all packets received from LAN using SGT=3
- "no propagate sgt" - removes all the SGT tags when transmitting the packets towards 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 configuration on R3:

All packets from LAN will be accepted. From WAN only ICMP packets tagged with SGT=4 will be accepted:

```
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 configuration is very similar except ZBF which is not configured there.

R5, R6 configuration

R5 and R6 simulates local LAN in both branches. Example configuration for 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
```

Verification

Tesing SGT aware GETVPN

Checking if SGT tagging is supported on group member in Branch1 (R3):

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

Checking if TEK policies pushed to group member in Branch1 (R3) are using 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
```

Sending ICMP traffic from R6 to 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
```

Checking if R3 is attaching SGT tag to encrypted packets:

```
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...>
```

Checking dataplane counters for GETVPN on group member 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
```

Depending on the platform more details can be revealed using debugs. For example on R3:

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

Packets received by R3 from LAN should be SGT tagged:

```
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]
```

Also encrypted packets send via the tunnel will be tagged:

```
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
```

Testing SGT aware ZBF

R3 will accept only ICMP packets tagged with SGT=4 coming from WAN. When sending ICMP packets from R6 to 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 will receive tagged ESP packet, decrypt it. Then ZBF will accept the traffic:

```
*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
```

Also policy-map will present the counters with the numbers of packet accepted:

```
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
```

When trying to telnet from R6 to R5 - that will be dropped by R3 because telnet was not allowed:

```
*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
```

References

- **Cisco TrustSec Switch Configuration Guide: Understanding Cisco TrustSec**
- **Configuring an External Server for Security Appliance User Authorization**
- **Cisco ASA Series VPN CLI Configuration Guide, 9.1**
- **Cisco Identity Services Engine User Guide, Release 1.2**
- **Technical Support & Documentation - Cisco Systems**