Esempio di configurazione del firewall basato su zona GETVPN con TrustSec SGT Inline Tagging e con riconoscimento SGT

Sommario

Introduzione

In questo articolo viene illustrato come configurare GETVPN per il push dei criteri che consentono l'invio e la ricezione di tag SGT (Security Group Tag) inseriti nei pacchetti crittografati. L'esempio prevede due diramazioni che etichettano tutto il traffico con tag SGT specifici e applicano policy ZBF (Zone Based Firewall) in base ai tag SGT ricevuti.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

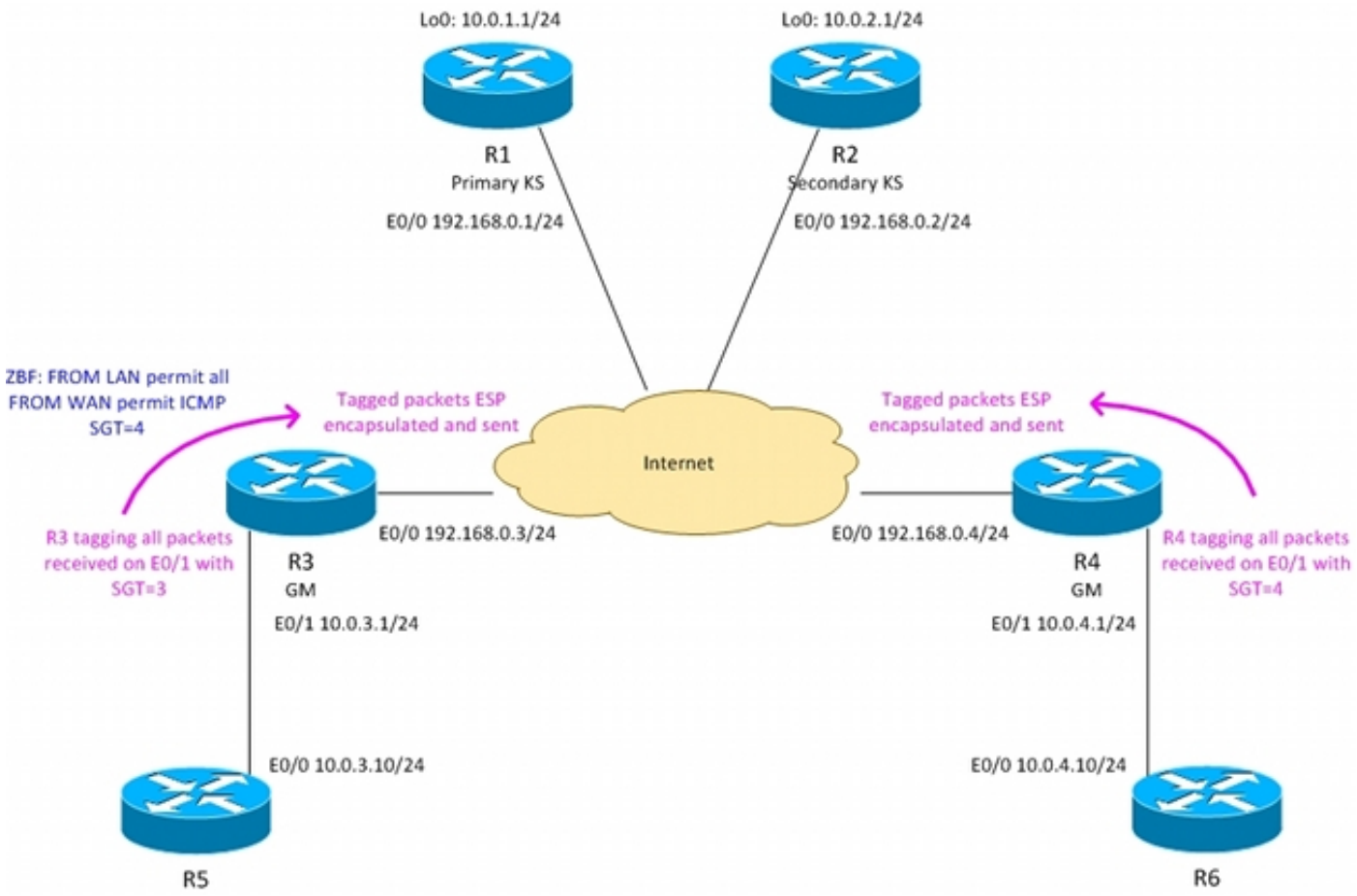
- Conoscenze base di configurazione dell'interfaccia della riga di comando (CLI) di IOS e di configurazione di GETVPN
- Conoscenze base dei servizi Trustsec.
- Conoscenze base di Zone-Based Firewall

Componenti usati

Le informazioni di questo documento si basano sulle seguenti versioni software:

- Cisco 2921 Router con software versione 15.3(2)T e successive

Topologia



R3 - router di confine in Branch1, membro gruppo GETVPN

R4 - router di confine in Branch2, membro gruppo GETVPN

R1,R2 - GETVPN Server chiavi nel sito centrale

OSPF in esecuzione su tutti i router

Push di ACL da KS con crittografia forzata per il traffico tra 10.0.0.0/16 <-> 10.0.0.0/16

Il router R3 sta taggando tutto il traffico inviato da Branch1 con tag SGT = 3

Il router R4 sta taggando tutto il traffico inviato dal branch2 con tag SGT = 4

R3 sta rimuovendo i tag SGT durante l'invio del traffico verso la LAN (si presume che R5 non supporti i tag in linea)

R4 sta rimuovendo i tag SGT durante l'invio del traffico verso la LAN (si presume che R6 non supporti i tag in linea)

R4 non dispone di firewall (accetta tutti i pacchetti)

R3 è configurato con ZBF con i seguenti criteri:

- accettazione di tutto il traffico dalla LAN alla WAN

- accettare solo ICMP con tag SGT=4 da WAN verso LAN

Configurazione

R1 (server chiave nel sito centrale)

Per inviare criteri che consentano l'invio e la ricezione di pacchetti con tag, è necessario che sia presente il comando "tac cts sgt":

```
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 configurazione di R2 è molto simile.

R3 (membro del gruppo in Branch1)

La configurazione di GETVPN è identica a quella dello scenario senza tag SGT. L'interfaccia LAN è stata configurata con trustsec manuale:

- "policy static sgt 3 trusted" - contrassegna tutti i pacchetti ricevuti da LAN utilizzando SGT=3
- "no propagate sgt" - rimuove tutte le etichette SGT quando trasmette i pacchetti verso una 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
```

Configurazione ZBF su R3:

Verranno accettati tutti i pacchetti provenienti da LAN. Dalla WAN vengono accettati solo i pacchetti ICMP contrassegnati con SGT=4:

```
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 nella configurazione Branch2 è molto simile, ad eccezione di ZBF che non è configurato lì.

Configurazione R5, R6

R5 e R6 simulano LAN locali in entrambe le filiali. Esempio di configurazione per 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
```

Verifica

Test di GETVPN con supporto SGT

Verifica del supporto del tagging SGT per il membro del gruppo in Branch1 (R3):

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

Verifica dell'utilizzo di SGT da parte dei criteri TEK inviati al membro del gruppo in Branch1 (R3):

```
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
```

Invio del traffico ICMP da R6 a 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
```

Verifica se R3 sta collegando il tag SGT ai pacchetti crittografati:

```
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...>
```

Controllo dei contatori del piano dati per GETVPN sul membro del gruppo 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
```

A seconda della piattaforma è possibile visualizzare ulteriori dettagli utilizzando i debug. Ad esempio su R3:

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

I pacchetti ricevuti da R3 da LAN devono essere contrassegnati con SGT:

```
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]
```

Anche i pacchetti crittografati inviati tramite il tunnel saranno contrassegnati:

```
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
```

Test ZBF compatibile SGT

R3 accetta solo pacchetti ICMP con tag SGT=4 provenienti da WAN. Quando si inviano pacchetti ICMP da R6 a 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 riceverà il pacchetto ESP con tag, lo decripterà. Quindi ZBF accetterà il traffico:

```
*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
```

Anche la mappa dei criteri presenterà i contatori con il numero di pacchetti accettati:

```
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
```

Quando si tenta di eseguire una connessione telnet da R6 a R5, questa verrà eliminata da R3 perché non è consentito utilizzare la connessione telnet:

```
*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
```

Riferimenti

- Guida alla configurazione dello switch Cisco TrustSec: Informazioni su Cisco TrustSec

- Configurazione di un server esterno per l'autorizzazione utente di Security Appliance
- Guida alla configurazione di Cisco ASA VPN CLI, 9.1
- Guida dell'utente di Cisco Identity Services Engine, versione 1.2
- Documentazione e supporto tecnico – Cisco Systems