具有TrustSec SGT內聯標籤和SGT感知區域防火牆的GETVPN配置示例

目錄

[簡介](#)
[必要條件](#)
[需求](#)
[採用元件](#)
[拓撲](#)
[組態](#)
[R1（中心站點中的金鑰伺服器）](#)
[R3（Branch1中的組成員）](#)
[R5、R6配置](#)
[驗證](#)
[測試SGT感知GETVPN](#)
[測試SGT感知ZBF](#)
[參考資料](#)
[相關思科支援社群討論](#)

簡介

本文將介紹如何配置GETVPN以推送策略，從而允許傳送和接收插入到加密資料包的安全組標籤(SGT)。示例將涉及兩個分支，它們使用特定的SGT標籤為所有流量新增標籤，並根據收到的SGT標籤應用基於區域的防火牆(ZBF)策略。

必要條件

需求

思科建議您瞭解以下主題：

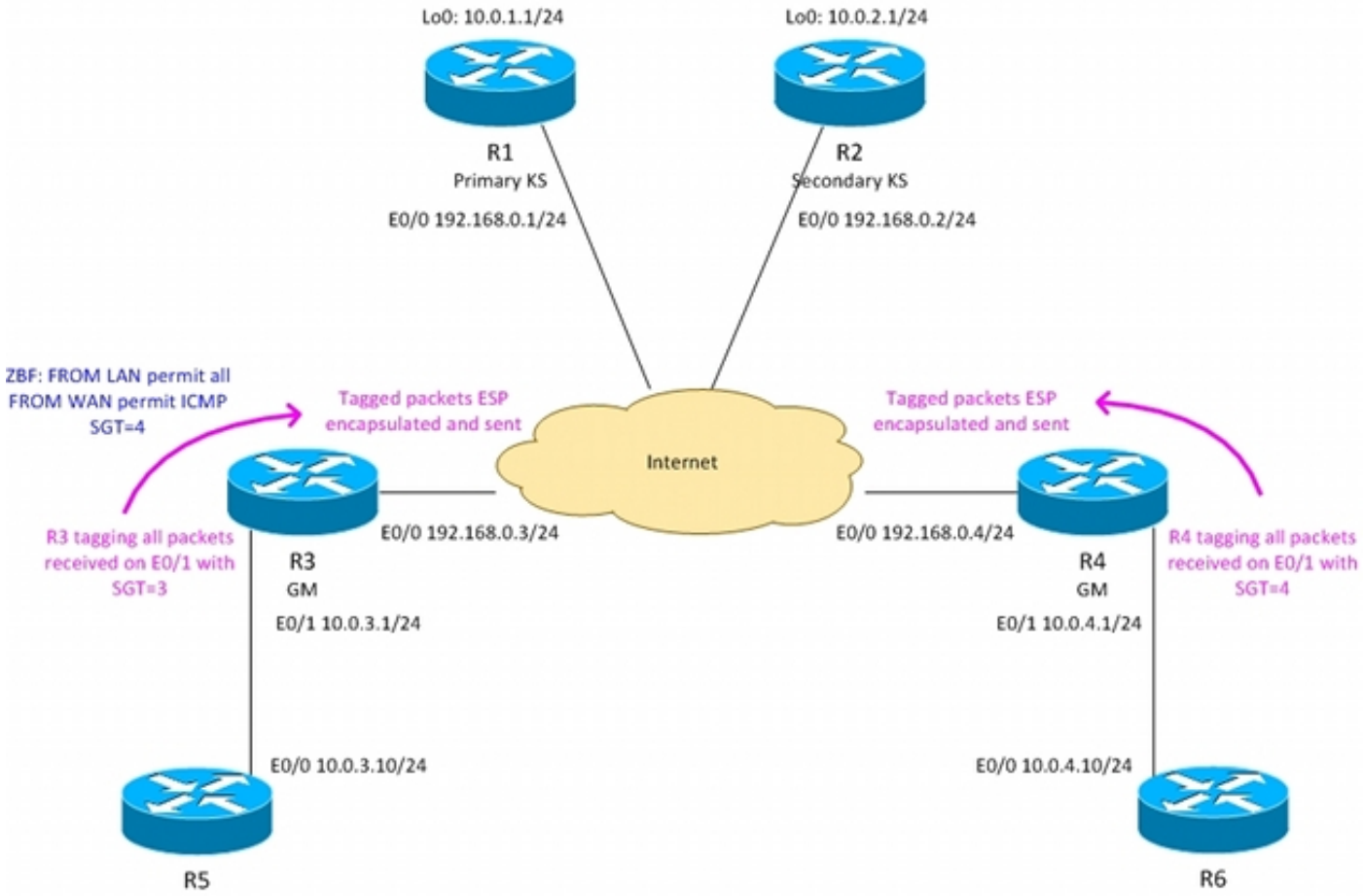
- IOS命令列介面(CLI)配置和GETVPN配置的基本知識
- Trustsec服務基礎知識。
- 基於區域的防火牆的基本知識

採用元件

本檔案中的資訊是根據以下軟體版本：

- Cisco 2921路由器，帶15.3(2)T及更高版本的軟體

拓撲



R3 - Branch1中的邊界路由器，GETVPN組成員

R4 - Branch2中的邊界路由器，GETVPN組成員

R1、R2 — 中央站點中的GETVPN金鑰伺服器

OSPF在所有路由器上運行

從KS推送的ACL強制對10.0.0.0/16 <-> 10.0.0.0/16之間的流量進行加密

R3路由器使用SGT標籤= 3標籤從Branch1傳送的所有流量

R4路由器使用SGT標籤= 4標籤從Branch2傳送的所有流量

R3在向LAN傳送流量時刪除SGT標籤（假設R5不支援內聯標籤）

R4在向LAN傳送流量時刪除SGT標籤（假設R6不支援內聯標籤）

R4沒有防火牆（接受所有資料包）

R3配置了具有以下策略的ZBF:

— 接受從LAN到WAN的所有流量

— 僅接受從WAN到LAN的ICMP標籤SGT=4

組態

R1（中心站點中的金鑰伺服器）

要傳送允許傳送和接收標籤資料包「tac cts sgt」命令的策略，需要存在：

```
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
```

R2的配置非常相似。

R3（Branch1中的組成員）

GETVPN配置與不帶SGT標籤的方案相同。已使用手動trustsec配置LAN介面：

- "policy static sgt 3 trusted" — 使用SGT=3標籤從LAN接收的所有資料包
- "no propagate sgt" — 在將資料包傳輸到LAN時刪除所有SGT標籤

```
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
```

R3上的ZBF配置：

將接受來自LAN的所有資料包。在WAN中，僅接受標籤為SGT=4的ICMP資料包：

```
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
```

Branch2配置中的R4非常相似，但此處未配置ZBF。

R5、R6配置

R5和R6模擬兩個分支中的本地LAN。R5的配置示例：

```
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
```

驗證

測試SGT感知GETVPN

檢查Branch1(R3)中的組成員是否支援SGT標籤：

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

檢查推入到Branch1(R3)組成員的TEK策略是否使用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
```

從R6向R5傳送ICMP流量：

```
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
```

檢查R3是否將SGT標籤附加到加密資料包：

```
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...>
```

檢查Branch2(R3)中組成員上的GETVPN的資料平面計數器：

```
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
```

根據平台的不同，可使用debug顯示更多詳細資訊。例如，在R3上：

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

R3從LAN接收的資料包應進行SGT標籤：

```
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]
```

此外，透過通道傳送的加密封包也會被標籤：

```
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
```

測試SGT感知ZBF

R3將僅接受來自WAN且標籤有SGT=4的ICMP資料包。從R6向R5傳送ICMP資料包時：

```
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將接收已標籤的ESP資料包，對其進行解密。然後ZBF將接受流量：

```
*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
```

此外，策略對映將顯示接受的資料包數量的計數器：

```
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
```

當嘗試從R6 telnet到R5時，由於不允許telnet，R3將丟棄該消息：

```
*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
```

參考資料

- Cisco TrustSec交換機配置指南：瞭解Cisco TrustSec
- 配置外部伺服器以進行安全裝置使用者授權
- Cisco ASA系列VPN CLI配置指南9.1
- 思科身份服務引擎使用手冊，版本1.2
- 技術支援與文件 - Cisco Systems