TrustSec SGT 인라인 태깅 및 SGT 인식 영역 기반 방화벽 컨피그레이션이 포함된 GETVPN 예

목차

소개

이 문서에서는 암호화된 패킷에 삽입된 SGT(Security Group Tag)를 보내고 받을 수 있는 정책을 푸시하도록 GETVPN을 구성하는 방법을 설명합니다.예를 들어, 특정 SGT 태그로 모든 트래픽에 태그를 지정하고 수신된 SGT 태그를 기반으로 ZBF(Zone Based Firewall) 정책을 적용하는 2개의 브랜치가 포함됩니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

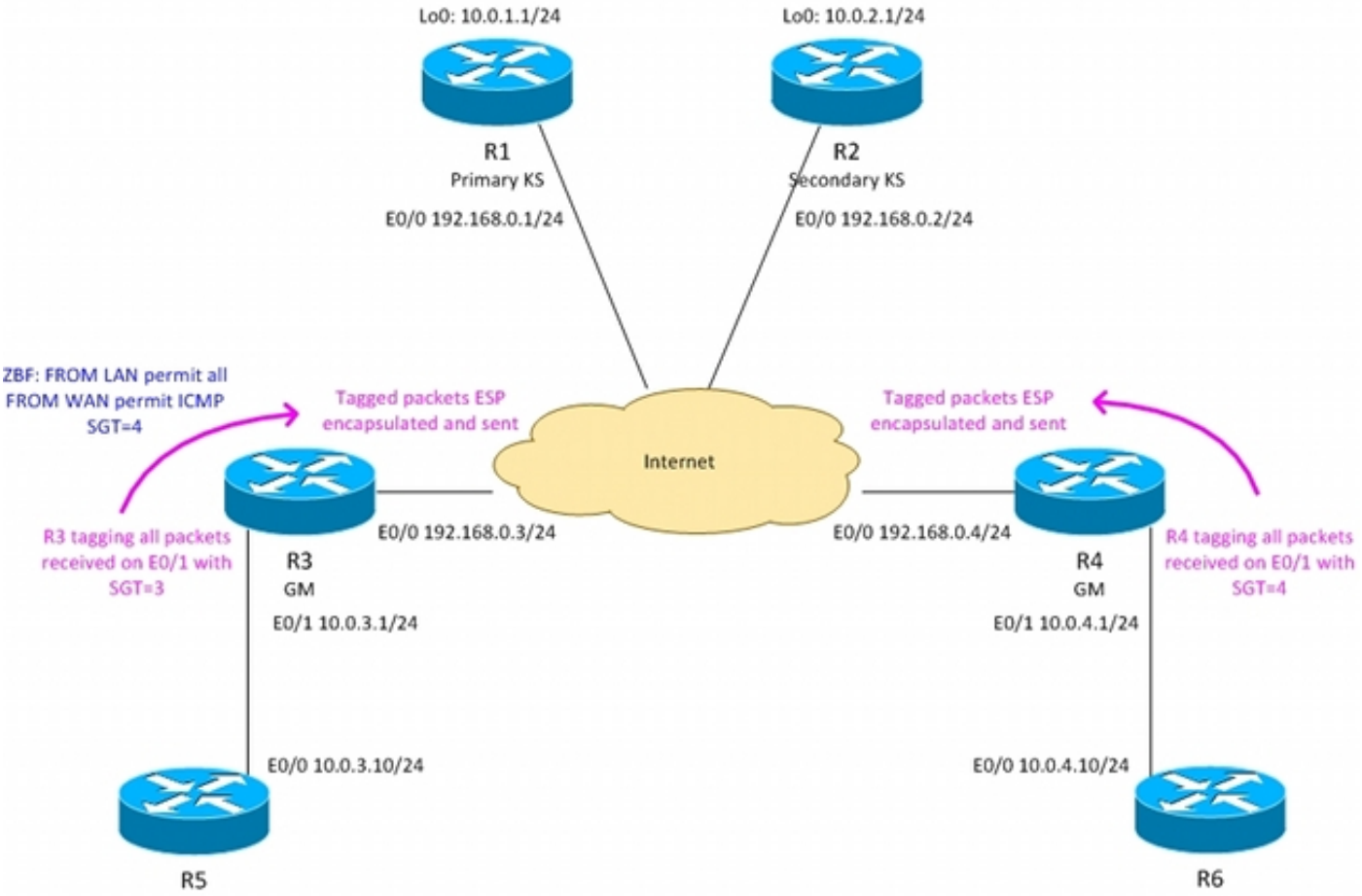
- IOS CLI(Command-Line Interface) 컨피그레이션 및 GETVPN 컨피그레이션에 대한 기본적인 지식
- Trustsec 서비스에 대한 기본 지식
- 영역 기반 방화벽에 대한 기본 지식

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 버전을 기반으로 합니다.

- Cisco 2921 Router, 소프트웨어 15.3(2)T 이상

토폴로지



R3 - Branch1의 보더 라우터, GETVPN 그룹 멤버

R4 - Branch2의 보더 라우터, GETVPN 그룹 멤버

R1,R2 - 중앙 사이트의 GETVPN 키 서버

모든 라우터에서 실행되는 OSPF

KS에서 푸시된 ACL은 10.0.0.0/16 <-> 10.0.0.0/16 사이의 트래픽에 대해 암호화를 적용합니다.

R3 라우터가 Branch1에서 전송된 모든 트래픽에 SGT 태그 = 3을 태깅합니다.

R4 라우터가 Branch2에서 전송된 모든 트래픽에 SGT 태그 = 4를 태깅합니다.

R3는 LAN으로 트래픽을 보낼 때 SGT 태그를 제거합니다(R5가 인라인 태깅을 지원하지 않는다고 가정).

R4는 LAN으로 트래픽을 보낼 때 SGT 태그를 제거합니다(R6이 인라인 태깅을 지원하지 않는다고 가정).

R4에 방화벽이 없습니다(모든 패킷 수락).

R3은 다음 정책으로 ZBF로 구성됩니다.

- LAN에서 WAN으로 향하는 모든 트래픽 수락

- WAN에서 LAN으로 SGT=4로 태그가 지정된 ICMP만 수락

구성

R1(중앙 사이트의 주요 서버)

태그 있는 패킷 "tac cts sgt" 명령을 보내고 받을 수 있는 정책을 보내려면 다음을 수행합니다.

```
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
```

R2의 구성은 매우 유사합니다.

R3(Branch1의 그룹 멤버)

GETVPN 컨피그레이션은 SGT 태그가 없는 시나리오와 동일합니다.LAN 인터페이스가 수동 trustsec으로 구성되었습니다.

- "policy static sgt 3 trusted" - SGT=3을 사용하여 LAN에서 수신된 모든 패킷에 태그 지정
- "no propagate sgt" - 패킷을 LAN에 전송할 때 모든 SGT 태그를 제거합니다.

```
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
```

R3의 ZBF 구성:

LAN의 모든 패킷이 수락됩니다.WAN에서 SGT=4로 태그가 지정된 ICMP 패킷만 수락됩니다.

```
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 컨피그레이션의 R4는 ZBF가 구성되어 있지 않은 경우를 제외하고 매우 유사합니다.

R5, R6 구성

R5 및 R6은 두 브랜치 모두에서 로컬 LAN을 시뮬레이션합니다.R5에 대한 컨피그레이션의 예:

```
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
```

확인

SGT 인식 GETVPN 테스트

Branch1(R3)의 그룹 멤버에 SGT 태깅이 지원되는지 확인:

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

Branch1(R3)의 그룹 멤버에 푸시된 TEK 정책이 SGT를 사용하는지 확인:

```
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
```

R6에서 R5로 ICMP 트래픽 전송:

```
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
```

R3에서 암호화된 패킷에 SGT 태그를 첨부하는지 확인:

```
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...>
```

Branch2(R3)의 그룹 멤버에 대한 GETVPN에 대한 데이터 플레인 카운터를 확인하는 중:

```
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
```

플랫폼에 따라 디버그를 사용하여 자세한 내용을 확인할 수 있습니다.예: R3:

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

LAN에서 R3에 의해 수신된 패킷은 SGT 태그여야 합니다.

```
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]
```

터널을 통해 전송되는 암호화된 패킷도 태그됩니다.

```
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 인식 ZBF 테스트

R3에서는 SGT=4로 태그가 지정된 ICMP 패킷만 WAN에서 수신합니다.R6에서 R5로 ICMP 패킷을 전송하는 경우:

```
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
```

R3는 태그가 지정된 ESP 패킷을 수신하여 해독합니다.그러면 ZBF는 트래픽을 수락합니다.

```
*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
```

또한 policy-map은 수락된 패킷 수와 함께 카운터를 표시합니다.

```
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
```

R6에서 R5로 텔넷을 시도하는 경우 텔넷이 허용되지 않아 R3에서 삭제됩니다.

```
*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
```

참조

- Cisco TrustSec 스위치 구성 가이드:Cisco TrustSec 이해
- 보안 어플라이언스 사용자 권한 부여를 위한 외부 서버 구성
- Cisco ASA Series VPN CLI 컨피그레이션 가이드, 9.1
- Cisco Identity Services Engine 사용 설명서, 릴리스 1.2
- 기술 지원 및 문서 – Cisco Systems