Содержание

Введение

Эта статья представит, как настроить GETVPN для продвижения разрешения политики передающий и получающий тег группы безопасности (SGT), вставленный в зашифрованные пакеты. Пример включит два ответвления, помечающие весь трафик с определенными метками SGT и применяющие политику Зонального базирующегося межсетевого экрана (ZBF) на основе полученных меток SGT.

Предварительные условия

Требования

Компания Cisco рекомендует предварительно ознакомиться со следующими предметами:

- Базовые знания о конфигурации интерфейса командной строки (CLI) IOS и конфигурации GETVPN
- Базовые знания о сервисах Trustsec.
- Базовые знания о зональном Межсетевом экране

Используемые компоненты

Сведения, содержащиеся в этом документе, касаются следующих версий программного обеспечения:

- Маршрутизатор Cisco 2921 с программным обеспечением 15.3 (2) T и более новый

Топология

R3 - граничный маршрутизатор в Branch1, элементе группы GETVPN

R4 - граничный маршрутизатор в Branch2, элементе группы GETVPN

R1, R2 - Серверы ключей GETVPN в Центральном узле

OSPF, работающий на всех маршрутизаторах

ACL выдвинул от KS принуждение шифрования для трафика между 10.0.0.0/16 <-> 10.0.0.0/16

Маршрутизатор R3 помечает весь трафик, передаваемый от Branch1 с меткой SGT = 3

Маршрутизатор R4 помечает весь трафик, передаваемый от Branch2 с меткой SGT = 4

R3 удаляет метки SGT при передаче трафика к LAN (предположение, что R5 не поддерживает встроенную маркировку),

R4 удаляет метки SGT при передаче трафика к LAN (предположение, что R6 не поддерживает встроенную маркировку),

R4 не имеет никакого межсетевого экрана (принимающий все пакеты)

R3 настроен с ZBF со следующей политикой:

- принятие всего трафика от LAN к глобальной сети (WAN)

- принятие только ICMP помечено с SGT=4 от глобальной сети (WAN) к LAN

!--- конфигурацию

R1 (Сервер ключей в центральном узле)

Для передачи политики, обеспечивающей передачу и получение маркированных тегами пакетов, ", команда" cts sgt tac должна присутствовать:

```
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
```

Конфигурация для R2 подобна.

R3 (Элемент группы в Branch1)

Конфигурация GETVPN совпадает с для сценария без меток SGT. Интерфейс LAN (локальной сети) был настроен с руководством trustsec:

- "политика, которой статический сержант 3 доверял" - помечает все пакеты, полученные от LAN с помощью SGT=3
- "нет распространитесь, сержант" - удаляет все метки SGT при передаче пакетов к 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
```

Конфигурация ZBF на R3:

Все пакеты от LAN будут приняты. От глобальной сети (WAN) только будут приняты пакеты ICMP, помеченные с 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 в конфигурации Branch2 подобен кроме ZBF, который не настроен там.

R5, конфигурация R6

R5 и R6 моделируют локальную сеть в обоих ответвлениях. Пример конфигурации для 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
```

Проверка

Tesing SGT осведомленный GETVPN

Проверка, поддерживается ли маркировка SGT на элементе группы в Branch1 (R3):

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

Проверка, используют ли Policy Pushed TEK к элементу группы в Branch1 (R3) 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
```

Передача трафика ICMP от R6 до 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
```

Проверка, если R3 подключает метку SGT к зашифрованным пакетам:

```
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...>
```

Проверка dataplane противостоит для GETVPN на элементе группы в 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
```

В зависимости от платформы больше подробных данных может быть показано с помощью отладок. Например, на R3:

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

Пакетами, полученными R3 от LAN, должен быть теговый 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]
```

Также зашифрованные пакеты передают через туннель, будет помечен:

```
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
```

Тестирование SGT осведомленный ZBF

R3 примет только пакеты ICMP, помеченные с SGT=4, прибывающим из глобальной сети (WAN). При передаче пакетов ICMP от R6 до 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 получит теговый пакет ESP, дешифрует его. Затем ZBF примет трафик:

```
*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
```

Также policy-map предоставит счетчикам количество принятого пакета:

```
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
```

При попытке к telnet от R6 до R5 - который будет отброшен R3, потому что не была позволена 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
```

Ссылки

- Руководство конфигурации коммутатора Cisco TrustSec: понимание Cisco TrustSec
- Настройка внешний сервер для авторизации пользователя на устройстве безопасности
- Руководство конфигурации интерфейса командой строки VPN серии Cisco ASA, 9.1
- Руководство пользователя платформы Cisco Identity Services Engine, выпуск 1.2
- Cisco Systems – техническая поддержка и документация