

目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[拓扑](#)

[配置](#)

[R1 \(关键服务器在中心站点\)](#)

[R3 \(Branch1的组成员\)](#)

[R5 , R6配置](#)

[验证](#)

[Testing SGT意识GETVPN](#)

[测试SGT意识ZBF](#)

[参考](#)

[相关的思科支持社区讨论](#)

简介

此条款将提交如何配置GETVPN推送允许发送和接收的策略安全组标记(SGT)插入到加密的信息包。示例将介入标记所有流量用特定SGT标记和应用区域基于防火墙(ZBF)策略的两个分组根据已接收SGT标记。

先决条件

要求

Cisco 建议您了解以下主题：

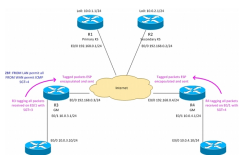
- IOS命令行界面(CLI)配置和GETVPN配置基础知识
- Trustsec服务基础知识。
- 基于区域的防火墙基础知识

使用的组件

本文档中的信息基于以下软件版本：

- 有软件的15.3(2)T思科2921路由器和更新

拓扑



R3 - Branch1的边界路由器， GETVPN组成员

R4 - Branch2的边界路由器， GETVPN组成员

R1,R2 - GETVPN密钥服务器在中心站点

运行在所有路由器的OSPF

从KS推送的ACL强制流量的加密10.0.0.0/16 <-> 10.0.0.0/16之间

R3路由器用SGT标记标记从Branch1发送的所有流量= 3

R4路由器用SGT标记标记从Branch2发送的所有流量= 4

R3删除SGT标记，当发送往LAN时(假定的流量R5不支持轴向标记)

R4删除SGT标记，当发送往LAN时(假定的流量R6不支持轴向标记)

R4没有防火墙(接受所有信息包)

R3配置与以下策略的ZBF：

-接受从LAN的所有流量往广域网

-接受用从广域网的SGT=4标记的仅ICMP往LAN

配置

R1 (关键服务器在中心站点)

要发送允许发送和接收的策略标记信息包“TAC cts sgt”命令需要存在：

```
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的配置是非常类似的。

R3 (Branch1的组成员)

没有SGT标记，GETVPN配置是相同的象为方案。LAN接口配置与手工的trustsec：

- “策略静态sgt 3委托” -标记从LAN接收的所有信息包使用SGT=3
- 当传送给LAN时的数据包“没有繁殖sgt” -删除所有SGT标记

```

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

```

在R3的ZBF配置：

从LAN的所有信息包将接受。仅从用SGT=4标记的广域网ICMP数据包将接受：

```

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在Branch2配置方面是非常类似的除了没有配置那里的ZBF。

R5 , R6配置

R5和R6模拟在两个分组的本地LAN。R5的配置示例：

```

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

```

验证

Testing SGT意识GETVPN

检查是否Branch1的(R3)组成员支持SGT标记：

```

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

```

检查推送的TEK策略分组Branch1的(R3)成员是否使用SGT：

```

R3#show crypto gdoi
GROUP INFORMATION

```

<...some output omitted 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

发送ICMP流量从R6到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

检查R3是否附加SGT标记到加密的信息包 :

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 (rcv) 0, #pkts verify failed: 0

#pkts invalid identity (rcv) 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 omitted for clarity...>

检查dataplane计数器在组成员的GETVPN Branch2的(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
```

使用调试，根据平台更多详细信息可以被透露。例如在R3：

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

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

从LAN的R3接收的数据包应该是被标记的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]
```

并且加密的信息包通过通道发送将是标记为的：

```
01:49:28: cts_ether_cmd_handle_post_encap_feature:pak[36BF868]:size=106 in=Ethernet0/1
out=Ethernet0/0 encypte=1 encsize=0 sgt_offset=18 [adj]:idb=Ethernet0/0 is_dot1q=0 linktype=7
mac_length=22 SGT=3
```

测试SGT意识ZBF

R3将接受用SGT=4标记的仅ICMP数据包来自广域网。当发送ICMP数据包从R6到R5时：

```
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将收到标记为的ESP数据包，解密它。然后ZBF将接收流量：

```
*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
```

并且策略映射将提交计数器用接受的数据包编号：

```
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
```

当尝试从R6远程登录到将由R3丢弃的R5时-，因为telnet未允许：

```
*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
```

参考

- [思科TrustSec交换机配置指南：了解思科TrustSec](#)
- [配置安全工具用户授权的一个外部服务器](#)
- [思科ASA系列VPN CLI配置指南，9.1](#)
- [思科身份服务引擎用户指南，版本1.2](#)
- [技术支持和文档 - Cisco Systems](#)