TrustSec SGT 인라인 태깅 및 SGT 인식 영역 기반 방화벽 컨피그레이션의 IKEv2 예

목차

소개

이 문서에서는 VPN 터널로 전송된 패킷에 태그를 지정하기 위해 IKEv2(Internet Key Exchange Version 2) 및 SGT(Security Group Tag)를 사용하는 방법에 대해 설명합니다. 일반적인 구축 및 활용 사례에 대한 설명이 포함되어 있습니다. 또한 SGT 인식 ZBF(Zone-Based Firewall)에 대해 설명하고 두 가지 시나리오를 소개합니다.

- IKEv2 터널에서 수신된 SGT 태그를 기반으로 하는 ZBF

- SXP(SGT eXchange Protocol) 매핑을 기반으로 하는 ZBF

모든 예에는 SGT 태그가 전송되는 방법을 확인하기 위한 패킷 레벨 디버깅이 포함됩니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- TrustSec 구성 요소에 대한 기본 지식
- Cisco Catalyst 스위치의 CLI(Command Line Interface) 구성에 대한 기본 지식
- Cisco ISE(Identity Services Engine) 구성 경험
- 영역 기반 방화벽에 대한 기본 지식
- IKEv2에 대한 기본 지식

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- Microsoft Windows 7 및 Microsoft Windows XP
- Cisco Catalyst 3750-X Software 릴리스 15.0 이상
- Cisco Identity Services Engine Software 릴리스 1.1.4 이상
- Cisco 2901 ISR(Integrated Services Router) with Software Release 15.3(2)T 이상

참고: IKEv2는 ISR G2(Generation 2) 플랫폼에서만 지원됩니다.

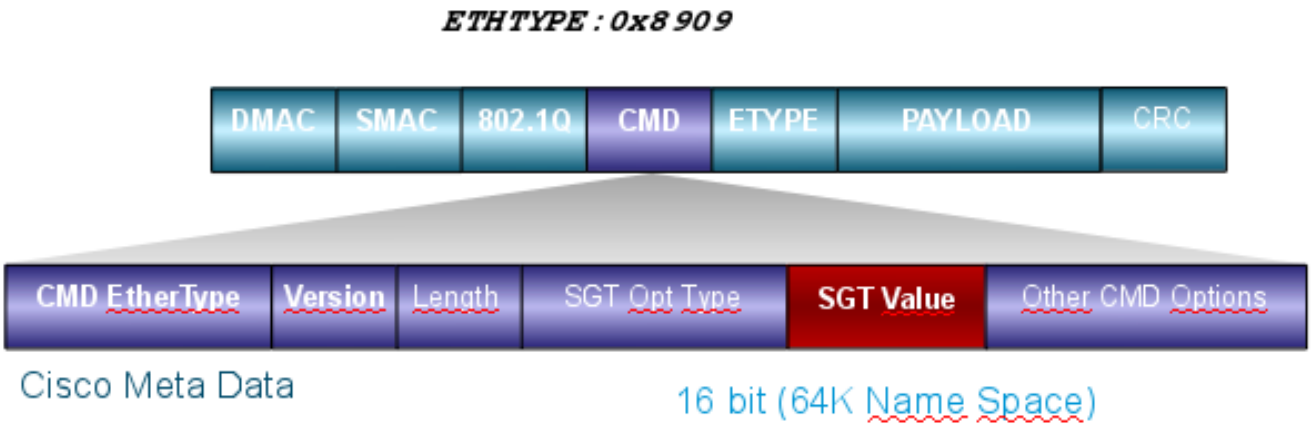
이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우, 모든 명령어의 잠재적인 영향을 미리 숙지하시기 바랍니다.

SGT(보안 그룹 태그)

SGT는 Cisco TrustSec 솔루션 아키텍처의 일부로서, IP 주소를 기반으로 하지 않는 유연한 보안 정책을 사용하도록 설계되었습니다.

TrustSec 클라우드의 트래픽은 분류되고 SGT 태그로 표시됩니다. 해당 태그를 기반으로 트래픽을 필터링하는 보안 정책을 구축할 수 있습니다. 모든 정책은 ISE에서 중앙 집중식으로 관리되며 TrustSec 클라우드의 모든 디바이스에 구축됩니다.

SGT 태그에 대한 정보를 전달하기 위해 Cisco는 802.1q 태그를 수정한 방법과 유사한 이더넷 프레임을 수정했습니다. 수정된 이더넷 프레임은 선택된 Cisco 디바이스에서만 인식할 수 있습니다. 수정된 형식입니다.



CMD(Cisco Meta Data) 필드는 SMAC(Source mac Address) 필드 바로 뒤에 삽입되거나 802.1q 필드가 사용되는 경우(이 예에서처럼) 삽입됩니다.

VPN을 통해 TrustSec 클라우드를 연결하기 위해 IKE 및 IPsec 프로토콜에 대한 확장이 생성되었습니다. IPsec 인라인 태깅이라고 하는 확장을 사용하면 SGT 태그를 ESP(Encapsulating Security Payload) 패킷에서 전송할 수 있습니다. ESP 페이로드는 패킷의 페이로드 바로 앞에 8바이트 CMD 필드를 전달하도록 수정됩니다. 예를 들어 인터넷을 통해 전송되는 암호화된 ICMP(Internet Control Message Protocol) 패킷은 [IP][ESP][CMD][IP][ICMP][DATA]를 포함합니다.

자세한 내용은 기사 뒷부분에 제시되어 있다.

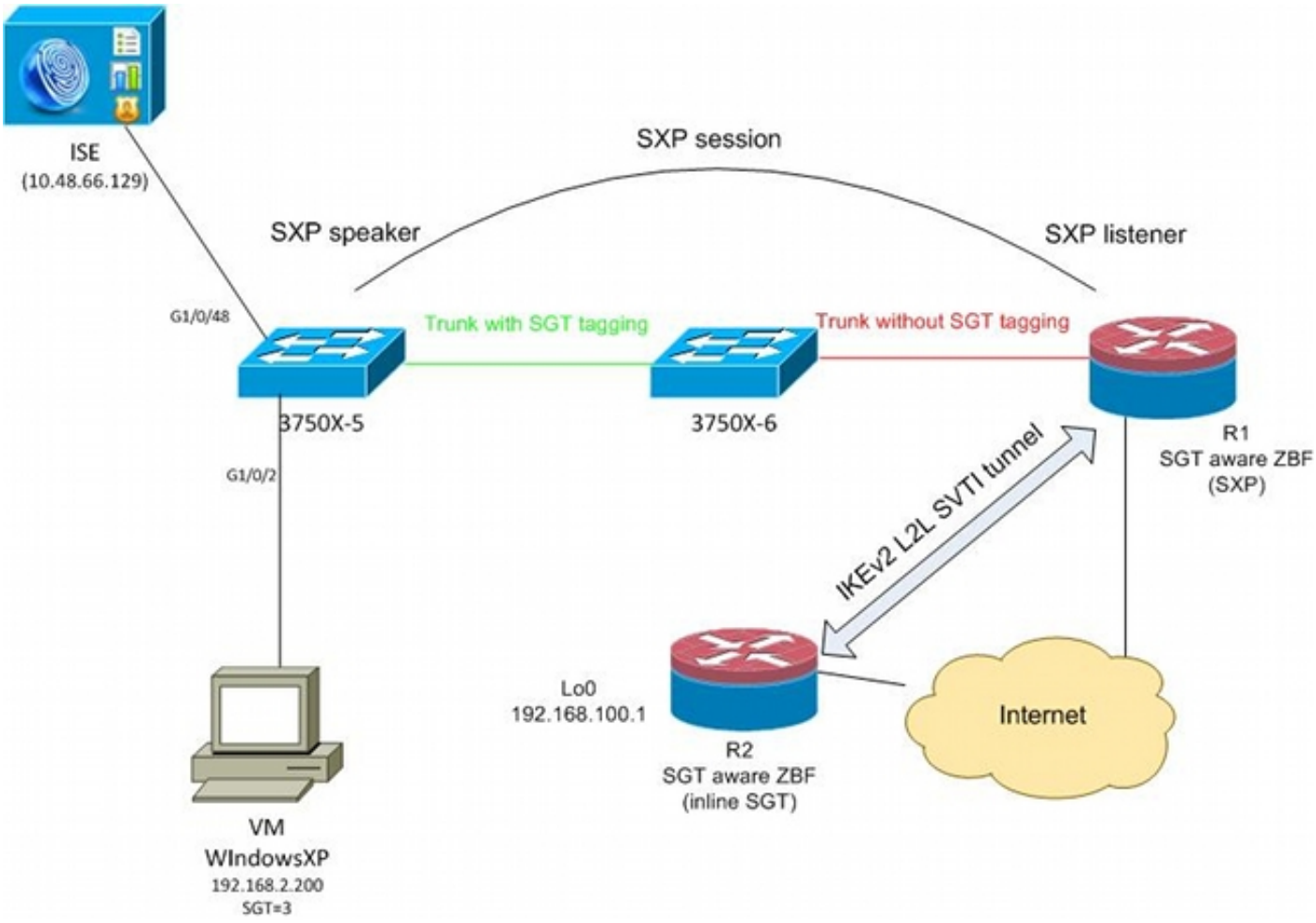
구성

참고:

아웃풋 인터프리터 툴(등록 고객 전용)은 특정 **show** 명령을 지원합니다. **show** 명령 출력의 분석을 보려면 아웃풋 인터프리터 툴을 사용합니다.

debug 명령을 사용하기 전에 debug 명령에 대한 중요한 정보를 참조하십시오.

네트워크 다이어그램



트래픽 흐름

이 네트워크에서는 3750X-5 및 3750X-6이 TrustSec 클라우드 내의 Catalyst 스위치입니다. 두 스위치 모두 클라우드에 참가하기 위해 자동 PAC(Protected Access Credentials) 프로비저닝을 사용합니다. 3750X-5는 시드로, 3750X-6은 비시드 디바이스로 사용되었습니다. 두 스위치 간 트래픽은 MACsec으로 암호화되며 올바르게 태그가 지정됩니다.

WindowsXP는 네트워크에 액세스하기 위해 802.1x를 사용합니다. 인증에 성공하면 ISE는 해당 세션에 적용할 SGT 태그 특성을 반환합니다. 해당 PC에서 제공된 모든 트래픽에는 SGT=3으로 태그가 지정됩니다.

라우터 1(R1) 및 라우터 2(R2)는 2901 ISR입니다. ISR G2는 현재 SGT 태깅을 지원하지 않으므로 R1 및 R2는 TrustSec 클라우드 외부에 있으며 SGT 태그를 전달하기 위해 CMD 필드로 수정된 이더넷 프레임을 인식하지 못합니다. 따라서 3750X-5에서 R1로 IP/SGT 매핑에 대한 정보를 전달하기 위해 SXP가 사용됩니다.

R1에는 원격 위치(192.168.100.1)로 향하는 트래픽을 보호하도록 구성되고 인라인 태깅이 활성화된 IKEv2 터널이 있습니다. IKEv2 협상 후 R1은 R2로 전송된 ESP 패킷에 태그를 지정하기 시작합니다. 태깅은 3750X-5에서 수신된 SXP 데이터를 기반으로 합니다.

R2는 해당 트래픽을 수신할 수 있으며 수신된 SGT 태그에 따라 ZBF에 의해 정의된 특정 작업을 수행할 수 있습니다.

R1도 마찬가지입니다. SXP 매핑을 사용하면 SGT 프레임이 지원되지 않는 경우에도 R1이 SGT 태그를 기반으로 LAN에서 수신한 패킷을 삭제할 수 있습니다.

TrustSec 클라우드 컨피그레이션

컨피그레이션의 첫 번째 단계는 TrustSec 클라우드를 구축하는 것입니다. 두 3750 스위치의 요구 사항:

- TrustSec 클라우드(ISE)에 대한 인증에 사용되는 PAC를 가져옵니다.
- NDAC(Network Device Admission Control) 프로세스를 인증하고 전달합니다.
- 링크에서 MACsec 협상에 SAP(Security Association Protocol)를 사용합니다.

이 단계는 이 활용 사례에 필요하지만 SXP 프로토콜이 올바르게 작동하기 위해서는 필요하지 않습니다. R1은 SXP 매핑 및 IKEv2 인라인 태깅을 수행하기 위해 ISE에서 PAC 또는 환경 데이터를 가져올 필요가 없습니다.

확인

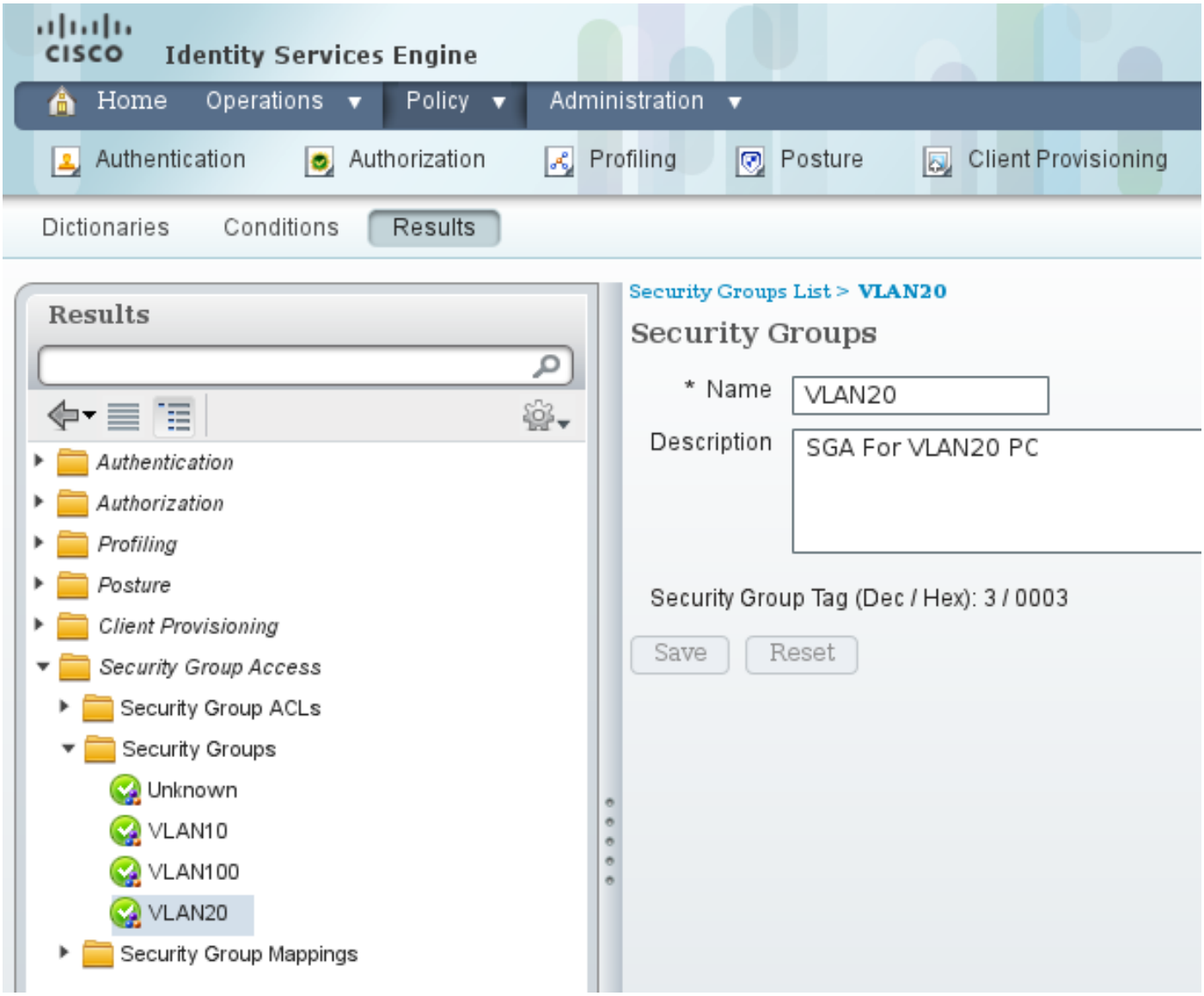
3750X-5와 3750X-6 간의 링크에서는 802.1x에서 협상한 MACsec 암호화를 사용합니다. 두 스위치 모두 피어에서 수신한 SGT 태그를 신뢰하고 수락합니다.

```
bsns-3750-5#show cts interface
Global Dot1x feature is Enabled
Interface GigabitEthernet1/0/20:
   CTS is enabled, mode:    DOT1X
   IFC state:               OPEN
   Authentication Status:   SUCCEEDED
       Peer identity:       "3750X6"
       Peer's advertised capabilities: "sap"
       802.1X role:         Supplicant
       Reauth period applied to link:  Not applicable to Supplicant role
    Authorization Status:    SUCCEEDED
       Peer SGT:            0:Unknown
       Peer SGT assignment: Trusted
   SAP Status:              SUCCEEDED
       Version:             2
        Configured pairwise ciphers:
            gcm-encrypt

       Replay protection:      enabled
       Replay protection mode: STRICT

       Selected cipher:        gcm-encrypt

   Propagate SGT:           Enabled
   Cache Info:
       Cache applied to link : NONE

   Statistics:
       authc success:              32
       authc reject:               1543
       authc failure:              0
       authc no response:          0
       authc logoff:               2
       sap success:                32
       sap fail:                   0
       authz success:              50
       authz fail:                 0
       port auth fail:             0
```

스위치에서 RBACL(Role-Based Access Control List)을 직접 적용할 수는 없습니다. 이러한 정책은 ISE에서 구성되며 스위치에서 자동으로 다운로드됩니다.

클라이언트 컨피그레이션

클라이언트는 802.1x, MAB(MAC 인증 우회) 또는 웹 인증을 사용할 수 있습니다. 권한 부여 규칙에 대한 올바른 보안 그룹이 반환되도록 ISE를 구성해야 합니다.



확인

클라이언트 컨피그레이션을 확인합니다.

```
bsns-3750-5#show authentication sessions interface g1/0/2
           Interface:  GigabitEthernet1/0/2
         MAC Address:  0050.5699.4ea1
           IP Address:  192.168.2.200
           User-Name:  cisco
```

```
              Status:  Authz Success
              Domain:  DATA
     Security Policy:  Should Secure
     Security Status:  Unsecure
      Oper host mode:  multi-auth
    Oper control dir:  both
       Authorized By:  Authentication Server
         Vlan Policy:  20
                 SGT:  0003-0
     Session timeout:  N/A
        Idle timeout:  N/A
   Common Session ID:  C0A80001000006367BE96D54
     Acct Session ID:  0x00000998
              Handle:  0x8B000637

Runnable methods list:
      Method   State
      dot1x    Authc Success
      mab      Not run
```

이 시점부터 3750X-5에서 TrustSec 클라우드 내의 다른 스위치로 전송되는 클라이언트 트래픽에는 SGT=3으로 태그가 지정됩니다.

권한 부여 규칙의 예는 ASA 및 Catalyst 3750X Series Switch TrustSec 컨피그레이션 예 및 트러블슈팅 가이드를 참조하십시오.

3750X-5와 R1 사이의 SGT 교환 프로토콜

R1은 CMD 필드가 있는 이더넷 프레임을 인식하지 못하는 2901 ISR G2 라우터이므로 TrustSec 클라우드에 가입할 수 없습니다. 따라서 SXP는 3750X-5에서 구성됩니다.

```
bsns-3750-5#show run | i sxp
cts sxp enable
cts sxp default source-ip 192.168.1.10
cts sxp default password cisco
cts sxp connection peer 192.168.1.20 password default mode local
```

SXP는 R1에도 구성됩니다.

```
BSNS-2901-1#show run | i sxp
cts sxp enable
cts sxp default source-ip 192.168.1.20
cts sxp default password cisco
cts sxp connection peer 192.168.1.10 password default mode local listener
hold-time 0 0
```

확인

R1이 IP/SGT 매핑 정보를 수신하는지 확인합니다.

```
BSNS-2901-1#show cts sxp sgt-map
SXP Node ID(generated):0xC0A80214(192.168.2.20)
IP-SGT Mappings as follows:
IPv4,SGT: <192.168.2.200 , 3>
source  : SXP;
Peer IP : 192.168.1.10;
```

```
Ins Num : 1;
Status  : Active;
Seq Num : 1
Peer Seq: 0
```

이제 R1은 192.168.2.200에서 수신된 모든 트래픽을 SGT=3으로 태그가 지정된 것처럼 처리해야 한다는 것을 알고 있습니다.

R1과 R2 간의 IKEv2 컨피그레이션

이는 IKEv2 스마트 기본값을 사용하는 간단한 SVTI(Static Virtual Tunnel Interfaces) 기반 시나리오입니다. 사전 공유 키는 인증에 사용되며, Null 암호화는 ESP 패킷 분석의 용이성을 위해 사용됩니다. 192.168.100.0/24에 대한 모든 트래픽은 Tunnel1 인터페이스를 통해 전송됩니다.

R1의 설정:

```
crypto ikev2 keyring ikev2-keyring
 peer 192.168.1.21
 address 192.168.1.21
 pre-shared-key cisco
 !
crypto ikev2 profile ikev2-profile
 match identity remote address 192.168.1.21 255.255.255.255
 authentication remote pre-share
 authentication local pre-share
 keyring local ikev2-keyring

crypto ipsec transform-set tset esp-null esp-sha-hmac
 mode tunnel
!
crypto ipsec profile ipsec-profile
 set transform-set tset
 set ikev2-profile ikev2-profile

interface Tunnel1
 ip address 172.16.1.1 255.255.255.0
 tunnel source GigabitEthernet0/1.10
 tunnel mode ipsec ipv4
 tunnel destination 192.168.1.21
 tunnel protection ipsec profile ipsec-profile

interface GigabitEthernet0/1.10
 encapsulation dot1Q 10
 ip address 192.168.1.20 255.255.255.0

ip route 192.168.100.0 255.255.255.0 172.16.1.2
```

R2에서 네트워크 192.168.2.0/24에 대한 모든 반환 트래픽은 Tunnel1 인터페이스를 통해 전송됩니다.

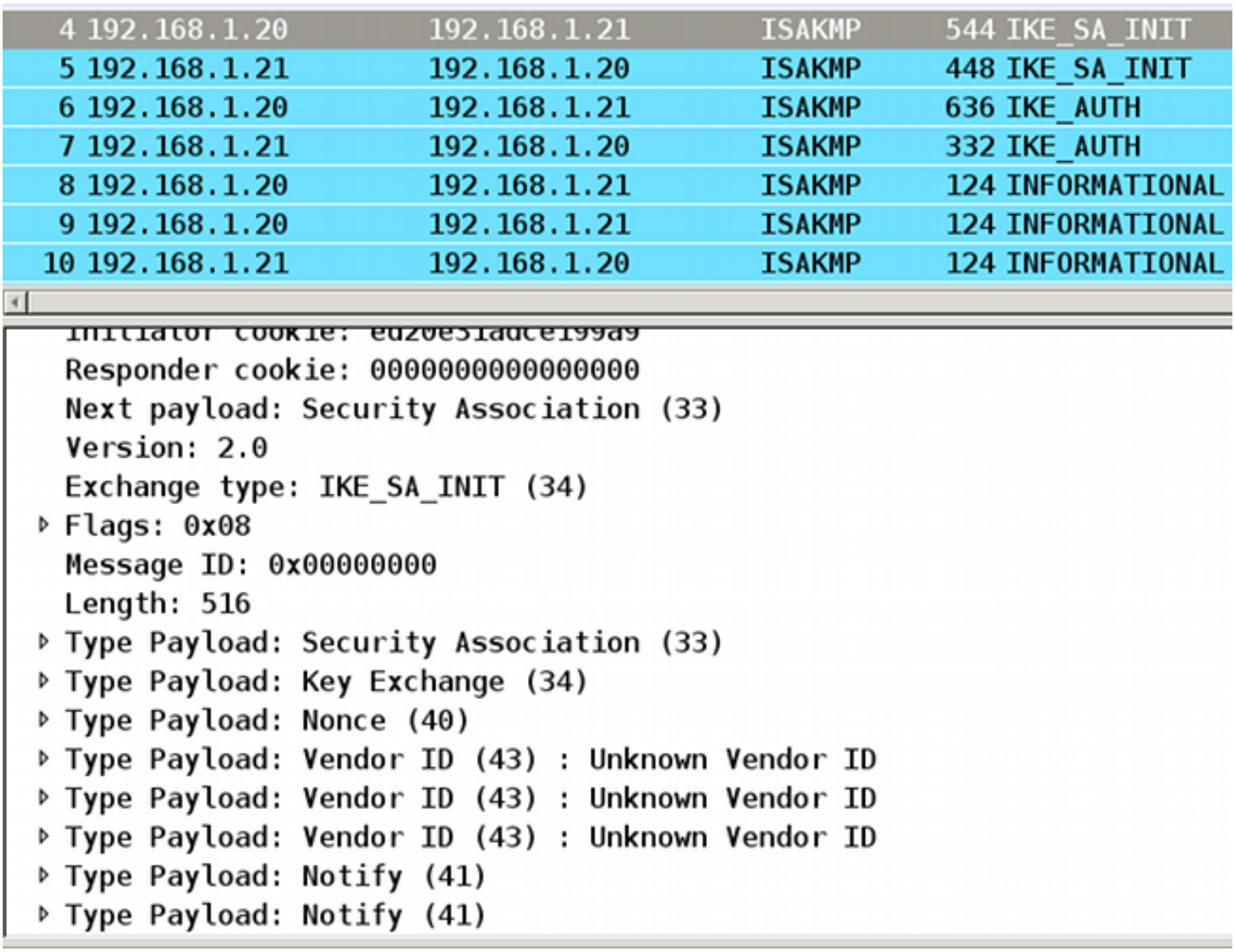
```
crypto ikev2 keyring ikev2-keyring
 peer 192.168.1.20
 address 192.168.1.20
 pre-shared-key cisco

crypto ikev2 profile ikev2-profile
 match identity remote address 192.168.1.20 255.255.255.255
 authentication remote pre-share
 authentication local pre-share
```

```
 keyring local ikev2-keyring

crypto ipsec transform-set tset esp-null esp-sha-hmac
 mode tunnel

crypto ipsec profile ipsec-profile
 set transform-set tset
 set ikev2-profile ikev2-profile

interface Loopback0
description Protected Network
 ip address 192.168.100.1 255.255.255.0

interface Tunnel1
 ip address 172.16.1.2 255.255.255.0
 tunnel source GigabitEthernet0/1.10
 tunnel mode ipsec ipv4
 tunnel destination 192.168.1.20
 tunnel protection ipsec profile ipsec-profile

interface GigabitEthernet0/1.10
 encapsulation dot1Q 10
 ip address 192.168.1.21 255.255.255.0

ip route 192.168.2.0 255.255.255.0 172.16.1.1
```

인라인 태깅을 활성화하려면 두 라우터에서 모두 하나의 명령, 즉 crypto ikev2 cts sgt 명령만 필요합니다.

확인

인라인 태깅을 협상해야 합니다. 첫 번째 및 두 번째 IKEv2 패킷에서는 특정 벤더 ID가 전송됩니다.



Wireshark에서 알 수 없는 3개의 벤더 ID(VID)가 있습니다. 관련 항목:

- DELETE-REASON, Cisco 지원
- FlexVPN, Cisco에서 지원
- SGT 인라인 태깅

디버그가 이를 확인합니다. IKEv2 개시자인 R1은 다음을 전송합니다.

```
debug crypto ikev2 internal

*Jul 25 07:58:10.633: IKEv2:Construct Vendor Specific Payload: DELETE-REASON
*Jul 25 07:58:10.633: IKEv2:(1): Sending custom vendor id : CISCO-CTS-SGT

*Jul 25 07:58:10.633: IKEv2:Construct Vendor Specific Payload: (CUSTOM)
*Jul 25 07:58:10.633: IKEv2:Construct Vendor Specific Payload: (CUSTOM)
```

R1은 두 번째 IKEv2 패킷과 동일한 VID를 수신합니다.

```
*Jul 25 07:58:10.721: IKEv2:Parse Vendor Specific Payload: CISCO-DELETE-REASON VID
*Jul 25 07:58:10.721: IKEv2:Parse Vendor Specific Payload: (CUSTOM) VID
*Jul 25 07:58:10.721: IKEv2:Parse Vendor Specific Payload: (CUSTOM) VID
*Jul 25 07:58:10.721: IKEv2:Parse Notify Payload: NAT_DETECTION_SOURCE_IP
NOTIFY(NAT_DETECTION_SOURCE_IP)
*Jul 25 07:58:10.725: IKEv2:Parse Notify Payload: NAT_DETECTION_DESTINATION_IP
NOTIFY(NAT_DETECTION_DESTINATION_IP)
```

```
*Jul 25 07:58:10.725: IKEv2:(1): Received custom vendor id : CISCO-CTS-SGT
```

따라서 양측은 CMD 데이터를 ESP 페이로드의 시작 부분에 넣는 것에 동의한다.

이 계약을 확인하려면 IKEv2 SA(Security Association)를 확인합니다.

```
BSNS-2901-1#show crypto ikev2 sa detailed
 IPv4 Crypto IKEv2  SA

Tunnel-id Local                 Remote                fvrf/ivrf            Status
1         192.168.1.20/500      192.168.1.21/500      none/none            READY
     Encr: AES-CBC, keysize: 256, Hash: SHA512, DH Grp:5, Auth sign: PSK, Auth
verify: PSK
     Life/Active Time: 86400/225 sec
     CE id: 1019, Session-id: 13
     Status Description: Negotiation done
     Local spi: 1A4E0F7D5093D2B8       Remote spi: 08756042603C42F9
     Local id: 192.168.1.20
     Remote id: 192.168.1.21
     Local req msg id:  2              Remote req msg id:  0
     Local next msg id: 2              Remote next msg id: 0
     Local req queued:  2              Remote req queued:  0
     Local window:      5              Remote window:      5
     DPD configured for 0 seconds, retry 0
     Fragmentation not configured.
     Extended Authentication not configured.
     NAT-T is not detected
     Cisco Trust Security SGT is enabled
     Initiator of SA : Yes

 IPv6 Crypto IKEv2 SA
```

Windows 클라이언트에서 192.168.100.1로 트래픽을 전송하면 R1에 다음이 표시됩니다.

```
BSNS-2901-1#sh crypto session detail
Crypto session current status

Code: C - IKE Configuration mode, D - Dead Peer Detection
K - Keepalives, N - NAT-traversal, T - cTCP encapsulation
X - IKE Extended Authentication, F - IKE Fragmentation

Interface: Tunnel1
Uptime: 00:01:17
Session status: UP-ACTIVE
Peer: 192.168.1.21 port 500 fvrf: (none) ivrf: (none)
     Phase1_id: 192.168.1.21
     Desc: (none)
 IKEv2 SA: local 192.168.1.20/500 remote 192.168.1.21/500 Active
         Capabilities:(none) connid:1 lifetime:23:58:43
 IPSEC FLOW: permit ip 0.0.0.0/0.0.0.0 0.0.0.0/0.0.0.0
       Active SAs: 2, origin: crypto map
       Inbound:  #pkts dec'ed 4 drop 0 life (KB/Sec) 4227036/3522
       Outbound: #pkts enc'ed 9 drop 0 life (KB/Sec) 4227035/3522


BSNS-2901-1#show crypto ipsec sa detail

interface: Tunnel1
   Crypto map tag: Tunnel1-head-0, local addr 192.168.1.20

  protected vrf: (none)
  local  ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
```

```
  remote ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
  current_peer 192.168.1.21 port 500
    PERMIT, flags={origin_is_acl,}
   #pkts encaps: 9, #pkts encrypt: 9, #pkts digest: 9
   #pkts decaps: 4, #pkts decrypt: 4, #pkts verify: 4
   #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): 9, #pkts untagged (rcv): 4
    #pkts not tagged (send): 0, #pkts not untagged (rcv): 0
   #pkts internal err (send): 0, #pkts internal err (recv) 0
   #send dummy packets 9, #recv dummy packets 0

    local crypto endpt.: 192.168.1.20, remote crypto endpt.: 192.168.1.21
    plaintext mtu 1454, path mtu 1500, ip mtu 1500, ip mtu idb
GigabitEthernet0/1.10
    current outbound spi: 0x9D788FE1(2641924065)
    PFS (Y/N): N, DH group: none

    inbound esp sas:
     spi: 0xDE3D2D21(3728551201)
       transform: esp-null esp-sha-hmac ,
       in use settings ={Tunnel, }
       conn id: 2020, flow_id: Onboard VPN:20, sibling_flags 80000040,
crypto map: Tunnel1-head-0
       sa timing: remaining key lifetime (k/sec): (4227036/3515)
       IV size: 0 bytes
       replay detection support: Y
       Status: ACTIVE(ACTIVE)

    inbound ah sas:

    inbound pcp sas:

    outbound esp sas:
     spi: 0x9D788FE1(2641924065)
       transform: esp-null esp-sha-hmac ,
       in use settings ={Tunnel, }
       conn id: 2019, flow_id: Onboard VPN:19, sibling_flags 80000040,
crypto map: Tunnel1-head-0
       sa timing: remaining key lifetime (k/sec): (4227035/3515)
       IV size: 0 bytes
       replay detection support: Y
       Status: ACTIVE(ACTIVE)

    outbound ah sas:

    outbound pcp sas:
BSNS-2901-1#
```

태그가 지정된 패킷이 전송되었습니다.

트랜짓 트래픽의 경우, R1이 Windows 클라이언트에서 R2로 보낸 트래픽에 태그를 지정해야 할 경우, ESP 패킷에 SGT=3으로 올바르게 태그가 지정되었는지 확인합니다.

debug crypto ipsc metadata sgt

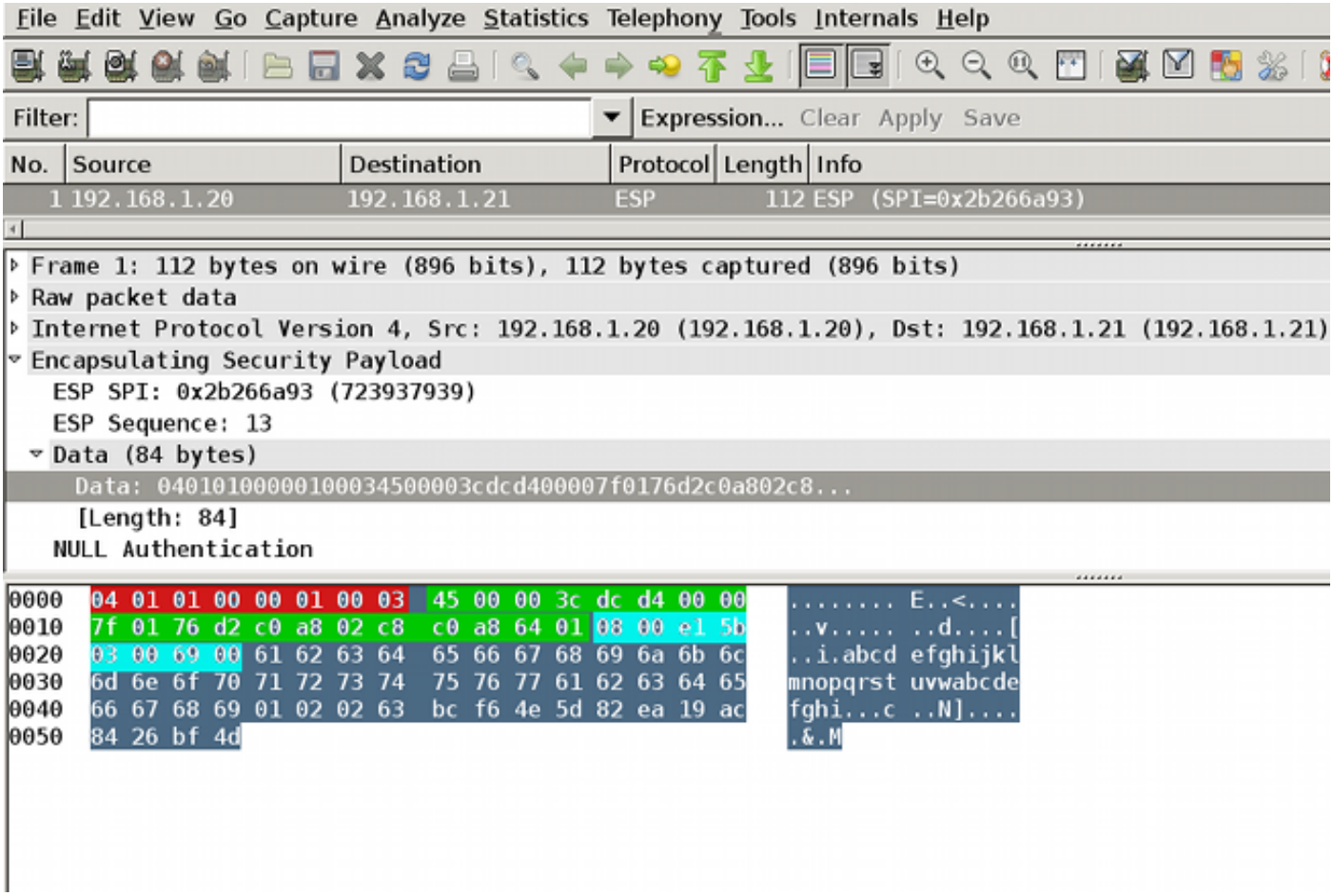
```
*Jul 23 19:01:08.590: IPsec SGT:: inserted SGT = 3 for src ip 192.168.2.200
```

스위치에서 소싱되는 동일한 VLAN의 다른 트래픽은 SGT=0으로 기본 설정됩니다.

```
*Jul 23 19:43:08.590: IPsec SGT:: inserted SGT = 0 for src ip 192.168.2.10
```

ESP 패킷 레벨 확인

다음 그림과 같이 EPC(Embedded Packet Capture)를 사용하여 R1에서 R2로의 ESP 트래픽을 검토합니다.



Wireshark는 SPI(보안 매개 변수 인덱스)에 대한 Null 암호화를 디코딩하는 데 사용되었습니다. IPv4 헤더에서 소스 및 대상 IP는 라우터의 인터넷 IP 주소입니다(터널 소스 및 대상으로 사용됨).

ESP 페이로드는 8바이트 CMD 필드를 포함하며, 빨간색으로 강조 표시됩니다.

- 0x04 - 다음 헤더(IP)
- 0x01 - 길이(헤더 뒤 4바이트, 헤더 뒤 8바이트)
- 0x01 - 버전 01
- 0x00 - 예약됨
- 0x00 - SGT 길이(총 4바이트)
- 0x01 - SGT 유형
- 0x0003 - SGT 태그(마지막 두 옥텟은 00 03입니다. SGT는 Windows 클라이언트에 사용됩니다.)

IPsec IPv4 모드가 터널 인터페이스에 사용되었으므로 다음 헤더는 IP이며 녹색으로 강조 표시됩니다. 소스 IP는 c0 a8 02 c8(192.168.2.200)이고, 목적지 IP는 c0 a8 64 01(192.168.100.1)입니다. 프

로토콜 번호는 1이며 ICMP입니다.

마지막 헤더는 ICMP이며 파란색으로 강조 표시되어 Type 08 및 Code 8(Echo Request)입니다.

ICMP 페이로드는 그 다음이며 32바이트 길이입니다(즉, a에서 i로의 문자). 그림의 페이로드는 Windows 클라이언트의 일반적인 페이로드입니다.

나머지 ESP 헤더는 ICMP 페이로드를 따릅니다.

- 0x01 0x02 - 안쪽 여백
- 0x02 - 안쪽 여백 길이.
- 0x63 - 프로토콜 0x63을 가리키는 다음 헤더로서 '모든 비공개 암호화 체계'입니다. 이는 다음 필드(ESP 데이터의 첫 번째 필드)가 SGT 태그임을 나타냅니다.
- 무결성 검사 값 12바이트.

CMD 필드는 일반적으로 암호화되는 ESP 페이로드 내부에 있습니다.

IKEv2 위험: GRE 또는 IPsec 모드

지금까지 이러한 예에서는 터널 모드 IPsec IPv4를 사용했습니다. GRE(Generic Routing Encapsulation) 모드를 사용할 경우 어떻게 됩니까?

라우터가 트랜짓 IP 패킷을 GRE에 캡슐화하면 TrustSec은 패킷을 로컬에서 시작된 것으로 봅니다. 즉, GRE 패킷의 소스는 Windows 클라이언트가 아니라 라우터입니다. CMD 필드를 추가하면 항상 특정 태그 대신 기본 태그(SGT=0)가 사용됩니다.

모드 IPsec IPv4에서 Windows 클라이언트(192.168.2.200)에서 트래픽이 전송되는 경우 SGT=3이 표시됩니다.

```
debug crypto ipsc metadata sgt
*Jul 23 19:01:08.590: IPsec SGT:: inserted SGT = 3 for src ip 192.168.2.200
```

그러나 동일한 트래픽에 대해 터널 모드가 GRE로 변경된 후 SGT=0이 표시됩니다. 이 예에서 192.168.1.20은 터널 소스 IP입니다.

```
*Jul 25 20:34:08.577: IPsec SGT:: inserted SGT = 0 for src ip 192.168.1.20
```

> **참고**: 따라서 GRE를 **사용하지 않는 것이** 매우 **중요합니다**.

Cisco 버그 ID CSCuj25890, GRE 모드의 IOS IPSec 인라인 태깅: 라우터 SGT 삽입을 참조하십시오. 이 버그는 GRE를 사용할 때 적절한 SGT 전파를 허용하기 위해 생성되었습니다. DMVPN을 통한 SGT는 Cisco IOS® XE 3.13S에서 지원됩니다

IKEv2의 SGT 태그 기반 ZBF

R2의 ZBF에 대한 예제 컨피그레이션입니다. IKEv2 터널에서 수신된 모든 패킷에 태그가 지정되므로(즉, CMD 필드가 포함되어 있음) SGT=3의 VPN 트래픽을 식별할 수 있습니다. 따라서 VPN 트래픽을 삭제하고 기록할 수 있습니다.

```
class-map type inspect match-all TAG_3
 match security-group source tag 3
class-map type inspect match-all TAG_ANY
 match security-group source tag 0
!
policy-map type inspect FROM_VPN
 class type inspect TAG_3
 drop log
 class type inspect TAG_ANY
 pass log
 class class-default
 drop
!
zone security vpn
zone security inside
zone-pair security ZP source vpn destination self
 service-policy type inspect FROM_VPN

interface Tunnel1
 ip address 172.16.1.2 255.255.255.0
 zone-member security vpn
```

확인

Windows 클라이언트에서 192.168.100.1에 대한 ping이 제공된 경우(SGT=3) 디버그는 다음을 보여줍니다.

```
*Jul 23 20:05:18.822: %FW-6-DROP_PKT: Dropping icmp session
192.168.2.200:0 192.168.100.1:0 on zone-pair ZP class TAG_3 due to
DROP action found in policy-map with ip ident 0
```

스위치에서 소싱된 ping(SGT=0)의 경우 디버그에 다음 내용이 표시됩니다.

```
*Jul 23 20:05:39.486: %FW-6-PASS_PKT: (target:class)-(ZP:TAG_ANY)
Passing icmp pkt 192.168.2.10:0 => 192.168.100.1:0 with ip ident 0
```

R2의 방화벽 통계는 다음과 같습니다.

```
BSNS-2901-2#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 ZP
 Zone-pair: ZP

 Service-policy inspect : FROM_VPN

   Class-map: TAG_3 (match-all)
     Match: security-group source tag 3
     Drop
        4 packets, 160 bytes
```

```
   Class-map: TAG_ANY (match-all)
     Match: security-group source tag 0
      Pass
        5 packets, 400 bytes

   Class-map: class-default (match-any)
     Match: any
     Drop
       0 packets, 0 bytes
```

4개의 삭제(Windows에서 보낸 ICMP 에코의 기본 개수)와 5개의 수락(스위치의 기본 개수)이 있습니다.

SXP를 통한 SGT 매핑 기반 ZBF

R1에서 SGT 인식 ZBF를 실행하고 LAN에서 수신된 트래픽을 필터링할 수 있습니다. 해당 트래픽은 SGT 태그가 지정되지 않았지만 R1은 SXP 매핑 정보를 가지고 있으며 해당 트래픽을 태그로 처리할 수 있습니다.

이 예에서는 LAN과 VPN 영역 간에 정책이 사용됩니다.

```
class-map type inspect match-all TAG_3
 match security-group source tag 3
class-map type inspect match-all TAG_ANY
 match security-group source tag 0
!
policy-map type inspect FROM_LAN
 class type inspect TAG_3
  drop log
 class type inspect TAG_ANY
  pass log
 class class-default
 drop
!
zone security lan
zone security vpn
zone-pair security ZP source lan destination vpn
 service-policy type inspect FROM_LAN

interface Tunnel1
 zone-member security vpn

interface GigabitEthernet0/1.20
 zone-member security lan
```

확인

Windows 클라이언트에서 ICMP Echo를 전송하면 다음과 같은 삭제를 볼 수 있습니다.

```
*Jul 25 09:22:07.380: %FW-6-DROP_PKT: Dropping icmp session 192.168.2.200:0
192.168.100.1:0 on zone-pair ZP class TAG_3 due to  DROP action found in
policy-map with ip ident 0

BSNS-2901-1#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 ZP
 Zone-pair: ZP

 Service-policy inspect : FROM_LAN

   Class-map: TAG_3 (match-all)
     Match: security-group source tag 3
      Drop
        4 packets, 160 bytes

   Class-map: TAG_ANY (match-all)
     Match: security-group source tag 0
      Pass
        5 packets, 400 bytes

   Class-map: class-default (match-any)
     Match: any
     Drop
       0 packets, 0 bytes
```

SXP 세션은 TCP를 기반으로 하므로 3750X-5와 R2 사이의 IKEv2 터널을 통해 SXP 세션을 구축하고 인라인 태깅 없이 R2의 태그를 기반으로 ZBF 정책을 적용할 수도 있습니다.

로드맵

GET VPN 인라인 태깅은 ISR G2 및 Cisco ASR 1000 Series Aggregation Services Router에서도 지원됩니다. ESP 패킷에는 CMD 필드에 대해 8바이트가 추가로 포함됩니다.

DMVPN(Dynamic Multipoint VPN)도 지원됩니다.

자세한 내용은 Cisco TrustSec 지원 인프라 로드맵을 참조하십시오.

다음을 확인합니다.

컨피그레이션 예에는 확인 절차가 포함되어 있습니다.

문제 해결

현재 이 설정에 사용할 수 있는 특정 문제 해결 정보가 없습니다.

관련 정보

- Cisco TrustSec 스위치 컨피그레이션 가이드: Cisco TrustSec 이해
- 책 1: Cisco ASA Series 일반 운영 CLI 컨피그레이션 가이드, 9.1: Cisco TrustSec과 통합되도

룩 ASA 구성

- Cisco TrustSec General Availability Releases(Cisco TrustSec 일반 가용성 릴리스 정보): Cisco TrustSec 3.0 General Deployability 2013 Release Notes(Cisco TrustSec 3.0 일반 구축 릴리스 정보)
- TrustSec에 대한 IPsec 인라인 태깅 구성
- Cisco Group Encrypted Transport VPN Configuration Guide, Cisco IOS XE Release 3S: GET VPN Support of IPsec Inline Tagging for Cisco TrustSec
- 기술 지원 및 문서 – Cisco Systems

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.