Understand IKEv2 Crypto Map Backup Peers on Secure Firewall

Contents

Introduction

This document describes the functionality of IKEv2 crypto map backup peers during link failover on Cisco Secure Firewall devices.

Prerequisites

â€¢ Adaptive Security Appliance version 9.14(1) or higher

â€¢ Firewall Threat Defense version 6.6 or higher

â€¢ Firewall Management Center version 6.6 or higher

â€¢ Firewall Device Manager version 6.6 - 7.0 (via API) or 7.1+ via GUI

Requirements

Cisco recommends that you have knowledge of these topics:

â€¢ Basic understanding of IKEv2 Site-to-Site Crypto Maps

â€¢ Basic underlay connectivity between VPN Endpoints

â€¢ Basic understanding of IP Service Level Agreement functionality

Components Used

The information in this document is based on these software versions and hardware versions:

â€¢ Two Cisco ASAv devices version 9.16(2)

â€¢ Three Cisco IOS® Routers version 15.9(3)M4

â€¢ Two Ubuntu Hosts version 20.04

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Theory

IKEv2 Peer Traversal is not supported on the Responder side of an IKEv2 multi-peer topology. For example, there are two VPN endpoints in a topology called Peer 1 and Peer 2. Peer 2 has two ISP interfaces, and Peer 1 has 1 ISP interface. In the event of ISP failover, Peer 2 initiates IKE on the secondary ISP interface if the configuration is in place to monitor the path. Peer 1 does not automatically traverse IP addresses to use the backup peer listed for the crypto map to accommodate Peer 2's ISP failover. The connection fails until traffic is initiated from Peer 1. Once Peer 1 initiates traffic based on the crypto ACL, it attempts to communicate via the primary ISP path until the path is declared dead from retransmissions. This process takes approximately 2 minutes. Once the primary peer is declared inactive, Peer 1 initiates a connection with the backup peer listed, and the connection establishes. Once the Primary ISP path is available again and Peer 2 switches to its primary ISP interface, Peer 1 needs to generate interesting traffic. This process allows Peer 1 to initiate a connection with the primary peer listed in the crypto map and establish the IKE connection as normal.

Order of Operations

1. VPN Peer 2 SLA detects path failure.

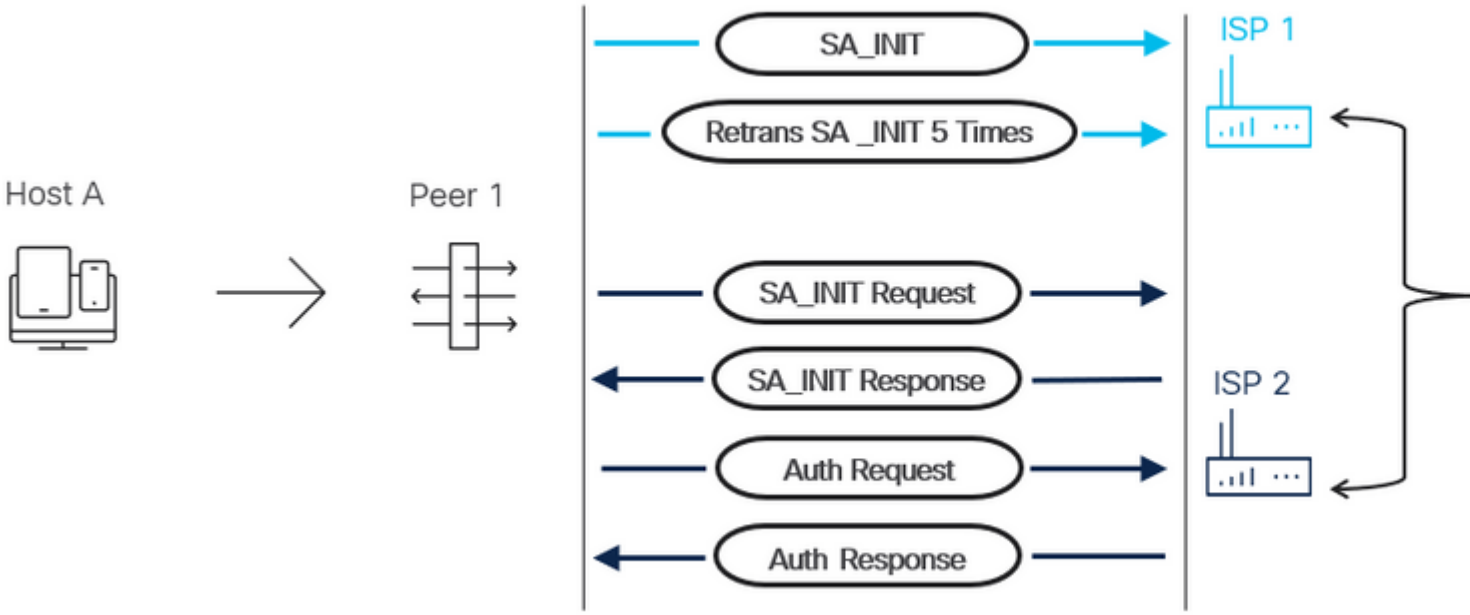
2. VPN Peer 2 has a routing table update to change the path used to reach VPN Peer 1 which changes its IKE identity.

3. Host A continuously initiates traffic destined for Host B.

4. VPN Peer 1 attempts to form an IKE connection with VPN Peer 2's Primary-ISP interface until 5 retransmissions occur.

5. VPN Peer 1 then declares that peer dead and moves to the secondary peer in the crypto map which is VPN Peer 2's secondary ISP interface. This connection establishes successfully.

Network Diagram



Configuration Example

VPN Peer 2

<#root>

Interfaces:

```
interface GigabitEthernet0/0
nameif PRIMARY-ISP
security-level 0
ip address 203.0.113.1 255.255.255.0

interface GigabitEthernet0/1
nameif BACKUP-ISP
security-level 0
ip address 198.51.100.1 255.255.255.0

interface GigabitEthernet0/2
nameif inside
security-level 100
ip address 192.168.10.2 255.255.255.00
```

SLA and Routing:

```
sla monitor 500
type echo protocol ipIcmpEcho 209.165.200.226 interface PRIMARY-ISP
num-packets 3
frequency 5
```

```
sla monitor schedule 500 life forever start-time now


track 1 rtr 500 reachability


route PRIMARY-ISP 0.0.0.0 0.0.0.0 203.0.113.2 1 track 1
route BACKUP-ISP 0.0.0.0 0.0.0.0 198.51.100.2 254
```

Crypto:

```
crypto ikev2 policy 1
encryption aes-256
integrity sha256
group 21
prf sha256
lifetime seconds 86400

crypto ikev2 enable PRIMARY-ISP
crypto ikev2 enable BACKUP-ISP

crypto ipsec ikev2 ipsec-proposal PROPOSAL
protocol esp encryption aes-256
protocol esp integrity sha-256

crypto map MAP 1 match address CRYPTO
crypto map MAP 1 set peer 192.0.2.1
crypto map MAP 1 set ikev2 ipsec-proposal PROPOSAL
crypto map MAP interface PRIMARY-ISP
crypto map MAP interface BACKUP-ISP
```

Tunnel-group:

```
tunnel-group 192.0.2.1 type ipsec-l2l
tunnel-group 192.0.2.1 ipsec-attributes
ikev2 remote-authentication pre-shared-key cisco
ikev2 local-authentication pre-shared-key cisco
```

Access-list:

```
access-list CRYPTO line 1 extended permit ip 192.168.10.0 255.255.255.0 10.10.10.0 255.255.255.0
```

VPN Peer 1

<#root>

Interfaces

:

```
interface GigabitEthernet0/0
nameif OUTSIDE
security-level 0
ip address 192.0.2.1 255.255.255.0

interface GigabitEthernet0/1
nameif INSIDE
security-level 100
ip address 10.10.10.2 255.255.255.0
```

Routing:

```
route OUTSIDE 0.0.0.0 0.0.0.0 192.0.2.2
```

Crypto:

```
crypto ikev2 policy 1
encryption aes-256
integrity sha256
group 21
prf sha256
lifetime seconds 86400

crypto ikev2 enable OUTSIDE

crypto ipsec ikev2 ipsec-proposal PROPOSAL
protocol esp encryption aes-256
protocol esp integrity sha-256

crypto map MAP-2 1 match address CRYPTO-2
crypto map MAP-2 1 set peer 203.0.113.1 198.51.100.1
crypto map MAP-2 1 set ikev2 ipsec-proposal PROPOSAL
crypto map MAP-2 interface OUTSIDE
```

Tunnel-group:

```
tunnel-group 203.0.113.1 type ipsec-l2l
tunnel-group 203.0.113.1 ipsec-attributes
ikev2 remote-authentication pre-shared-key cisco
ikev2 local-authentication pre-shared-key cisco


tunnel-group 198.51.100.1 type ipsec-l2l
tunnel-group 198.51.100.1 ipsec-attributes
ikev2 remote-authentication pre-shared-key cisco
ikev2 local-authentication pre-shared-key cisco
```

Access-List:

```
access-list CRYPTO-2 line 1 extended permit ip 10.10.10.0 255.255.255.0 192.168.10.0 255.255.255.0
```

Primary ISP

Interfaces:

```
GigabitEthernet0/0 203.0.113.2 255.255.255.0
GigabitEthernet0/1 209.165.200.225 255.255.255.224
```

Backup ISP

Interfaces:

```
GigabitEthernet0/0 198.51.100.2  255.255.255.0
GigabitEthernet0/1 209.165.202.130 255.255.255.224
```

ISP

Interfaces:

```
GigabitEthernet0/0 209.165.202.129 255.255.255.224
GigabitEthernet0/1 209.165.200.226 255.255.255.224
```

Hosts

Host 2:

```
192.168.10.1 255.255.255.0 dev ens2
```

Host 1:

```
10.10.10.1 255.255.255.0 dev ens2
```

Configuration Objectives

In this lab, VPN Peer 2 queries the reachability of the G0/1 interface for the primary ISP. This query is done with ICMP via SLA monitoring. The SLA configuration is tied to a track which is then tied to the Primary-ISP route. If this route becomes unavailable due to SLA reachability failure, the Backup-ISP route automatically becomes active. This means that the IKE negotiation from VPN Peer 2 is now initiated from the BACKUP-ISP interface with the IP address of 198.51.100.1. On the VPN Peer 1 side, the 198.51.100.1 address is listed as the secondary peer in the crypto map. VPN Peer 1 needs to initiate crypto ACL traffic to the primary peer in the crypto map. Then declare that peer inactive via retransmissions before the secondary peer in the crypto map is used.

Verify

Use this section to confirm the configuration functions as intended

Before SLA detects failure:

<#root>

```
VPN-PEER-2#
```

show track

```
Track 1
   Response Time Reporter 500 reachability
   Reachability is Up
   12 changes, last change 05:51:34
   Latest operation return code: OK
   Latest RTT (millisecs) 7
   Tracked by:
      STATIC-IP-ROUTING 0

VPN-PEER-2#
```

show route

```
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2, V - VPN
i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
ia - IS-IS inter area, * - candidate default, U - per-user static route
o - ODR, P - periodic downloaded static route, + - replicated route
SI - Static InterVRF
Gateway of last resort is 203.0.113.2 to network 0.0.0.0

S* 0.0.0.0 0.0.0.0 [1/0] via 203.0.113.2, PRIMARY-ISP
C 192.168.10.0 255.255.255.0 is directly connected, inside
L 192.168.10.2 255.255.255.255 is directly connected, inside
C 198.51.100.0 255.255.255.0 is directly connected, BACKUP-ISP
L 198.51.100.1 255.255.255.255 is directly connected, BACKUP-ISP
C 203.0.113.0 255.255.255.0 is directly connected, PRIMARY-ISP
L 203.0.113.1 255.255.255.255 is directly connected, PRIMARY-ISP
```

```
VPN-PEER-2#
```

show crypto ikev2 sa

```
IKEv2 SAs:

Session-id:75, Status:UP-ACTIVE, IKE count:1, CHILD count:1

Tunnel-id Local                    Remote Status                  Role
160993547 203.0.113.1/500          192.0.2.1/500                  READY INITIATOR
Encr: AES-CBC, keysize: 256, Hash: SHA256, DH Grp:21, Auth sign: PSK, Auth verify: PSK
Life/Active Time: 86400/21202 sec
Child sa: local selector 192.168.10.0/0 - 192.168.10.255/65535
remote selector 10.10.10.0/0 - 10.10.10.255/65535
ESP spi in/out: 0x30138366/0x7405d4a0


VPN-PEER-1#
```

show crypto ikev2 sa

```
IKEv2 SAs:

Session-id:75, Status:UP-ACTIVE, IKE count:1, CHILD count:1

Tunnel-id Local                    Remote Status          Role
168559091 192.0.2.1/500            203.0.113.1/500        READY RESPONDER
Encr: AES-CBC, keysize: 256, Hash: SHA256, DH Grp:21, Auth sign: PSK, Auth verify: PSK
Life/Active Time: 86400/21386 sec
Child sa: local selector 10.10.10.0/0 - 10.10.10.255/65535
remote selector 192.168.10.0/0 - 192.168.10.255/65535
ESP spi in/out: 0x7405d4a0/0x30138366
```

After SLA Detects Failure:

<#root>

```
VPN-PEER-2#
```

show track 1

```
Track 1
Response Time Reporter 500 reachability
Reachability is Down
13 changes, last change 00:05:23
Latest operation return code: Timeout
Tracked by:
STATIC-IP-ROUTING 0


VPN-PEER-2#
```

show route

```
S* 0.0.0.0 0.0.0.0 [254/0] via 198.51.100.2, BACKUP-ISP


VPN-PEER-2#
```

show crypto ikev2 sa

```
There are no IKEv2 SAs
```

> **Caution**: IKE remains down until Host A initiates traffic meant for Host B. VPN Peer 1 then declares the primary peer in crypto map dead, and moves to backup peer IP address.

<#root>

```
VPN-PEER-1#
```

show crypto ikev2 sa

```
IKEv2 SAs:

Session-id:79, Status:UP-ACTIVE, IKE count:1, CHILD count:1

Tunnel-id Local                       Remote Status        Role
178593183 192.0.2.1/500               198.51.100.1/500     READY INITIATOR
Encr: AES-CBC, keysize: 256, Hash: SHA256, DH Grp:21, Auth sign: PSK, Auth verify: PSK
Life/Active Time: 86400/232 sec
Child sa: local selector 10.10.10.0/0 - 10.10.10.255/65535
remote selector 192.168.10.0/0 - 192.168.10.255/65535
ESP spi in/out: 0x695d6bf0/0xbefc13c
```

> **Note**: VPN Peer 1 declares the primary peer in the crypto map dead, and initiates the connection to the backup peer IP address.

Troubleshoot

```
Debug crypto ikev2 platform 255

Debug crypto ikev2 protocol 255

Debug crypto ispec 255

Debug sla monitor error #

Debug sla monitor trace
```

Note: Additional information can be found in the About IKEv2 Multi-Peer Crypto Map section: IKEv2 Multi-Peer Crypto Map Guidelines