Migrate Policy Based Crypto Tunnel to Route Based Crypto Tunnel on ASA

Contents

Introduction

This document describes the migration of policy-based tunnels to route-based tunnels on ASA.

Prerequisites

Requirements

Cisco recommends that you know these topics:

- Basic understanding of IKEv2-IPSec VPN concepts.
- Knowledge of IPSec VPN on ASA and its configuration.

Components Used

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

- Cisco ASA: ASA code version 9.8(1) or later.

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.

Configure

Steps for Migration:

1. Remove Existing Policy-Based VPN Configuration

2. Configure IPSec Profile
3. Configure Virtual Tunnel Interface (VTI)
4. Configure Static Routing or Dynamic Routing Protocol

Configurations

Existing Policy-based Tunnel:

1. Interface Configuration:

Egress interface where the crypto map is bound.

```
interface GigabitEthernet0/0
nameif outside
security-level 0
ip address 10.10.10.10 255.255.255.0
```

2. IKEv2 policy:

It defines the parameters for Phase 1 of the IPsec negotiation process.

```
crypto ikev2 policy 10
 encryption aes-256
 integrity sha256
 group 20
 prf sha256
 lifetime seconds 86400
```

3. Tunnel Group:

It defines parameters for VPN connections. Tunnel Groups are essential for configuring site-to-site VPNs, as they contain information about the peer, authentication methods, and various connection parameters.

```
tunnel-group 10.20.20.20 type ipsec-l2l
tunnel-group 10.20.20.20 ipsec-attributes
 ikev2 remote-authentication pre-shared-key *****
 ikev2 local-authentication pre-shared-key *****
```

4. Crypto ACL:

It defines the traffic that has to be encrypted and sent through the tunnel.

```
object-group network local-network
 network-object 192.168.0.0 255.255.255.0
object-group network remote-network
 network-object 172.16.10.0 255.255.255.0

access-list asa-vpn extended permit ip object-group local-network object-group remote-network
```

5. Crypto IPSec Proposal:

It defines the IPsec proposal, which specifies the encryption and integrity algorithms for Phase 2 of the IPsec negotiation.

```
crypto ipsec ikev2 ipsec-proposal IKEV2_TSET
 protocol esp encryption aes-256
 protocol esp integrity sha-256
```

6. Crypto Map Config:

It defines the policy for IPsec VPN connections, including the traffic to be encrypted, the peers, and the ipsec-proposal previously configured. It is also bound to the interface that handles the VPN traffic.

```
crypto map outside_map 10 match address asa-vpn
crypto map outside_map 10 set peer 10.20.20.20
crypto map outside_map 10 set ikev2 ipsec-proposal IKEV2_TSET

crypto map outside_map interface outside
```

Migration of policy-based tunnel to route-based tunnel:

1. **Remove Existing Policy-Based VPN Configuration:**
   First, remove the existing policy-based VPN configuration. This includes the crypto map entries for that peer, ACLs, and any related settings.

   ```
   no crypto map outside_map 10 match address asa-vpn
   no crypto map outside_map 10 set peer 10.20.20.20
   no crypto map outside_map 10 set ikev2 ipsec-proposal IKEV2_TSET
   ```

2. **Configure IPSec Profile:**
   Define an IPsec profile with the existing IKEv2 ipsec-proposal or transform-set.

```
crypto ipsec profile PROPOSAL_IKEV2_TSET
 set ikev2 ipsec-proposal IKEV2_TSET
```

3. **Configure Virtual Tunnel Interface (VTI):**
   Create a Virtual Tunnel Interface (VTI) and apply the IPsec profile to it.

```
interface Tunnel1
 nameif VPN-BRANCH
 ip address 10.1.1.2 255.255.255.252
 tunnel source interface outside
 tunnel destination 10.20.20.20
 tunnel mode ipsec ipv4
 tunnel protection ipsec profile PROPOSAL_IKEV2_TSET
```

4. **Configure Static Routing or Dynamic Routing Protocol:**
   Add static routes or configure a dynamic routing protocol to route traffic through the tunnel interface. In this scenario, we are using static routing.

   Static Routing:

```
route VPN-BRANCH 172.16.10.0 255.255.255.0 10.1.1.10
```

Verify

After migrating from a policy-based VPN to a route-based VPN using Virtual Tunnel Interfaces (VTIs) on a Cisco ASA, it is crucial to verify that the tunnel is up and functioning correctly. Here are several steps and commands you can use to verify the status and troubleshoot if necessary.

1. Verify the Tunnel Interface
Check the status of the tunnel interface to ensure it is up.

<#root>

```
ciscoasa# show interface Tunnel1
```

Interface Tunnel1 "VPN-BRANCH", is up, line protocol is up

```
Hardware is Virtual Tunnel Interface
Description: IPsec VPN Tunnel to Remote Site
Internet address is
```

10.1.1.2/24

```
MTU 1500 bytes, BW 10000 Kbit/sec, DLY 500000 usec
65535 packets input, 4553623 bytes, 0 no buffer
Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
```

```
65535 packets output, 4553623 bytes, 0 underruns
0 output errors, 0 collisions, 0 interface resets
0 late collisions, 0 deferred
0 input reset drops, 0 output reset drops
```

Tunnel source 10.10.10.10, destination 10.20.20.20

```
Tunnel protocol/transport IPSEC/IP
Tunnel protection
```

IPsec profile PROPOSAL_IKEV2_TSET

This command provides details about the Tunnel interface, including its operational status, IP address, and tunnel source/destination. Look for these indicators:
• The interface status is up.
• The line protocol status is up.

2. Verify IPsec Security Associations (SAs)

Check the status of the IPsec SAs to ensure that the tunnel has been successfully negotiated.

<#root>

```
ciscoasa# show crypto ipsec sa

interface: Tunnel1
Crypto map tag: Tunnel1-head-0, seq num: 1, local addr:
```

10.10.10.10

```
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:
```

10.20.20.20

#pkts encaps: 1000, #pkts encrypt: 1000, #pkts digest: 1000

#pkts decaps: 1000, #pkts decrypt: 1000, #pkts verify: 1000

```
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 1000, #pkts compr. failed: 0, #pkts decompress failed: 0

local crypto endpt.:
```

10.10.10.10

```
/500, remote crypto endpt.:
```

10.20.20.20

```
/500
path mtu 1500, ipsec overhead 74, media mtu 1500
current outbound spi: 0xC0A80101(3232235777)
current inbound spi : 0xC0A80102(3232235778)
```

inbound esp sas:

spi: 0xC0A80102(3232235778)

```
transform: esp-aes-256 esp-sha-256-hmac no compression
in use settings ={Tunnel, }
slot: 0, conn id: 2001, flow_id: CSR:1, crypto map: Tunnel1-head-0
sa timing: remaining key lifetime (kB/sec): (4608000/3540)
IV size: 16 bytes
replay detection support: Y
```

Status: ACTIVE

outbound esp sas:

spi: 0xC0A80101(3232235777)

```
transform: esp-aes-256 esp-sha-256-hmac no compression
in use settings ={Tunnel, }
slot: 0, conn id: 2002, flow_id: CSR:2, crypto map: Tunnel1-head-0
sa timing: remaining key lifetime (kB/sec): (4608000/3540)
IV size: 16 bytes
replay detection support: Y
```

Status: ACTIVE

This command displays the status of the IPsec SAs, including counters for encapsulated and decapsulated packets. Ensure that:
• There are active SAs for the tunnel.
• The encapsulation and decapsulation counters are incrementing, indicating traffic flow.

For more detailed information, you can use:

<#root>

```
ciscoasa# show crypto ikev2 sa

IKEv2 SAs:
```

Session-id:2, Status:UP-ACTIVE

```
, IKE count:1, CHILD count:1

Tunnel-id Local Remote Status Role
3363898555
```

```
10.10.10.10/500 10.20.20.20/500 READY INITIATOR


Encr: AES-CBC, keysize: 256, PRF: SHA256, Hash: SHA256, DH Grp:20, Auth sign: PSK, Auth verify: PSK
Life/Active Time: 86400/259 sec
```

This command shows the status of the IKEv2 SAs, which is in the READY state.

3. Verify Routing
Check the routing table to ensure that routes are correctly pointing through the tunnel interface.

<#root>

```
ciscoasa# show route

Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF Intra, IA - OSPF Inter, E1 - OSPF External Type 1
E2 - OSPF External Type 2, N1 - OSPF NSSA External Type 1, N2 - OSPF NSSA External Type 2
i - IS-IS, su - IS-IS summary null, 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, H - NHRP, l - LISP
+ - replicated route, % - next hop override

S 0.0.0.0 0.0.0.0 [1/0] via 203.0.113.2, outside

C 10.1.1.0 255.255.255.0 is directly connected, Tunnel1


S 172.16.10.0 255.255.255.0 [1/0] via 10.1.1.10, Tunnel1
```

Look for routes that are routed through the tunnel interface.

Troubleshoot

This section provides information you can use to troubleshoot your configuration.

1. Verify the route-based tunnel configuration of the ASA.

2. To troubleshoot the IKEv2 tunnel, you can use these debugs:

```
debug crypto condition peer <peer IP address>
debug crypto ikev2 platform 255
debug crypto ikev2 protocol 255
debug crypto ipsec 255
```

3. To troubleshoot the traffic issue on the ASA take packet capture and check configuration.