Configure a Site-to-Site IKEv2 Tunnel Between 2 ASAs Using IKEv2 Multiple Key Exchanges

Contents

Prerequisites

- Requirements
- Components Used
- Limitations
- Licensing

Background Information

- Need for Additional Key Exchanges

Configure

- Network Diagram
- ASA Configuration
  - Configure the ASA Interfaces
  - Configure the IKEv2 Policy with Multiple Key Exchange and Enable IKEv2 on the Outside Interface
  - Configure the Tunnel Group
  - Configure Interesting Traffic and Crypto ACL
  - Configure an Identity NAT (Optional)
  - Configure the IKEv2 IPSec Proposal
  - Configure a Crypto Map and Bind it to the Interface
- Local ASA Final Configuration
- Remote ASA Final Configuration

Verify

Troubleshoot

Introduction

This document describes how to configure a Site-To-Site IKEv2 VPN connection between two Cisco ASAs using IKEv2 Multiple Key Exchanges.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Cisco Adaptive Security Appliance (ASA)
- General IKEv2 Concepts

Components Used

The information in this document is based on the Cisco ASAs running 9.20.1.

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.

Limitations

The IKEv2 Multiple Key Exchange has these limitations:

- Supported on the ASA CLI only
- Supported on Multi-Contexted and HA devices
- Not supported on Clustered devices

Licensing

The licensing requirements are the same as for Site-to-Site VPN on the ASAs.

Background Information

Need for Additional Key Exchanges

The arrival of big quantum computers poses a big risk to security systems, especially those using public-key cryptography. Cryptographic methods that were thought to be very hard for regular computers can be broken easily by quantum computers. So, the need arises to switch to new, quantum-resistant methods, also called post-quantum cryptography (PQC) algorithms. The aim is to enhance the security of IPsec communication by using multiple key exchanges. This involves combining a traditional key exchange with a post-quantum one. This approach ensures that the resulting exchange is at least as strong as the traditional key exchange, providing an added layer of security.

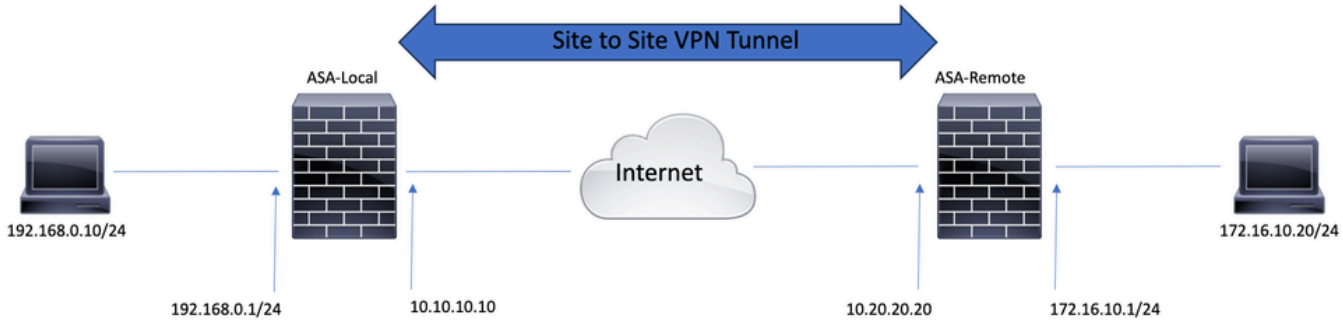
The plan is to improve IKEv2 by adding support for multiple key exchanges. These extra key exchanges can handle algorithms that are safe from quantum threats. To exchange information about these additional keys, a new message type called Intermediate Exchange is introduced. These key exchanges are negotiated using the regular IKEv2 method, through the SA payload.

Configure

This section describes the ASA configurations.

Network Diagram

The information in this document uses this network setup:



ASA Configuration

Configure the ASA Interfaces

If the ASA interfaces are not configured, ensure that you configure at least the IP addresses, interface names, and security levels:

```
interface GigabitEthernet0/0
nameif outside
security-level 0
ip address 10.10.10.10 255.255.255.0
!
interface GigabitEthernet0/1
nameif inside
security-level 100
ip address 192.168.0.1 255.255.255.0
```

Note: Ensure that there is connectivity to both the internal and external networks, especially to the remote peer that is used to establish a site-to-site VPN tunnel. You can use a ping in order to verify basic connectivity.

Configure the IKEv2 Policy with Multiple Key Exchange and Enable IKEv2 on the Outside Interface

In order to configure the IKEv2 policies for these connections, enter these commands:

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

Additional key exchange transforms can be configured under `crypto ikev2 policy` using the `additional-key-exchange` command. A total of seven additional exchange transforms can be configured. In this example, two additional exchange transforms have been configured (using DH groups 21 and 31).

```
 additional-key-exchange 1
  key-exchange-method 21
 additional-key-exchange 2
  key-exchange-method 31
```

The final IKEv2 policy looks like this:

```
crypto ikev2 policy 10
 encryption aes-256
 integrity sha256
 group 20
 prf sha256
 lifetime seconds 86400
 additional-key-exchange 1
  key-exchange-method 21
 additional-key-exchange 2
  key-exchange-method 31
```



Note: An IKEv2 policy match exists when both of the policies from the two peers contain the same authentication, encryption, hash, Diffie-Hellman parameter, and Additional Key Exchange parameter values.

You must enable IKEv2 on the interface that terminates the VPN tunnel. Typically, this is the outside (or internet) interface. In order to enable IKEv2, enter the `crypto ikev2 enable outside` command in global configuration mode.

Configure the Tunnel Group

For a Site-to-Site tunnel, the connection profile type is IPSec-l2l. In order to configure the IKEv2 preshared key, enter these commands:

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

Configure Interesting Traffic and Crypto ACL

The ASA uses Access Control Lists (ACLs) in order to differentiate the traffic that must be protected with IPSec encryption from the traffic that does not require protection. It protects the outbound packets that match a permit Application Control Engine (ACE) and ensures that the inbound packets that match a permit ACE have protection.

```
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
```

Note: The VPN Peer must have the same ACL in a mirrored format.

Configure an Identity NAT (Optional)

Typically, an identity NAT is needed in order to prevent the interesting traffic from hitting the dynamic NAT. The Identity NAT that is configured in this case is:

```
nat (inside,outside) source static local-network local-network destination static remote-network remote-network no-proxy-arp route-lookup
```

Configure the IKEv2 IPSec Proposal

The IKEv2 IPSec Proposal is used to define a set of encryption and integrity algorithms in order to protect

the data traffic. This proposal must match both VPN Peers in order to build an IPSec SA successfully. The commands used in this case are:

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

Configure a Crypto Map and Bind it to the Interface

A crypto map combines all the required configurations and must necessarily contain:

- An access list to match the traffic that must be encrypted (commonly referred to as Crypto ACL)
- Peer Identification
- At least one IKEv2 IPSec Proposal

The configuration used here is:

```
crypto map outside_map 1 match address asa-vpn
crypto map outside_map 1 set peer 10.20.20.20
crypto map outside_map 1 set ikev2 ipsec-proposal IKEV2_TSET
```

The final part is applying this crypto map to the outside (public) interface using the `crypto map outside_map interface outside` command.

Local ASA Final Configuration

```
interface GigabitEthernet0/0
 nameif outside
 security-level 0
 ip address 10.10.10.10 255.255.255.0
!
interface GigabitEthernet0/1
 nameif inside
 security-level 100
 ip address 192.168.0.1 255.255.255.0
!
crypto ikev2 policy 10
 encryption aes-256
 integrity sha256
 group 20
 prf sha256
 lifetime seconds 86400
 additional-key-exchange 1
  key-exchange-method 21
```

```
 additional-key-exchange 2
  key-exchange-method 31
!
crypto ikev2 enable outside
!
tunnel-group 10.20.20.20 type ipsec-l2l
tunnel-group 10.20.20.20 ipsec-attributes
 ikev2 remote-authentication pre-shared-key cisco
 ikev2 local-authentication pre-shared-key cisco
!
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
!
nat (inside,outside) source static local-network local-network destination static remote-network remote-network no-proxy-arp route-lookup
!
crypto ipsec ikev2 ipsec-proposal IKEV2_TSET
 protocol esp encryption aes-256
 protocol esp integrity sha-256
!
crypto map outside_map 1 match address asa-vpn
crypto map outside_map 1 set peer 10.20.20.20
crypto map outside_map 1 set ikev2 ipsec-proposal IKEV2_TSET
!
crypto map outside_map interface outside
```

Remote ASA Final Configuration

```
interface GigabitEthernet0/0
nameif outside
security-level 0
ip address 10.20.20.20 255.255.255.0
!
interface GigabitEthernet0/1
nameif inside
security-level 100
ip address 172.16.10.1 255.255.255.0
!
crypto ikev2 policy 10
encryption aes-256
integrity sha256
group 20
prf sha256
lifetime seconds 86400
additional-key-exchange 1
key-exchange-method 21
additional-key-exchange 2
key-exchange-method 31
!
crypto ikev2 enable outside
!
```

```
tunnel-group 10.10.10.10 type ipsec-l2l
tunnel-group 10.10.10.10 ipsec-attributes
ikev2 remote-authentication pre-shared-key cisco
ikev2 local-authentication pre-shared-key cisco
!
object-group network local-network
network-object 172.16.10.0 255.255.255.0
!
object-group network remote-network
network-object 192.168.0.0 255.255.255.0
!
access-list asa-vpn extended permit ip object-group local-network object-group remote-network
!
nat (inside,outside) source static local-network local-network destination static remote-network remote-network no-proxy-arp route-lookup
!
crypto ipsec ikev2 ipsec-proposal IKEV2_TSET
protocol esp encryption aes-256
protocol esp integrity sha-256
!
crypto map outside_map 1 match address asa-vpn
crypto map outside_map 1 set peer 10.10.10.10
crypto map outside_map 1 set ikev2 ipsec-proposal IKEV2_TSET
!
crypto map outside_map interface outside
```



Note: The ACL is in the mirrored format and the pre-shared keys are the same at both ends.

Verify

Before you verify if the tunnel is up and that it is passing the traffic, you must ensure that interesting traffic is being sent to the ASAs.



Note: The packet tracer was used in order to simulate the traffic flow. It can be done using the packet-tracer command; packet-tracer input inside icmp 192.168.0.11 8 0 172.16.10.11 detailed on the Local-ASA.

In order to validate the additional key exchanges, you can use the show crypto ikev2 sa command. As seen in the output, you can check the AKE parameters in order to validate the selected exchange algorithms.

<#root>

Local-ASA# show crypto ikev2 sa

IKEv2 SAs:

Session-id:2, Status:UP-ACTIVE, IKE count:1, CHILD count:1

Tunnel-id Local Remote fvrf/ivrf Status Role
246015 10.10.10.10/500 10.20.20.20/500 READY INITIATOR
Encr: AES-CBC, keysize: 256, Hash: SHA256, DH Grp:20, Auth sign: PSK, Auth verify: PSK
Additional Key Exchange Group:

AKE1: 21 AKE2: 31

```
      Life/Active Time: 86400/7 sec
Child sa: local selector  192.168.0.0/0 - 192.168.0.255/65535
          remote selector 172.16.10.0/0 - 172.16.10.255/65535
          ESP spi in/out: 0xf41ca3b5/0xda0e693b
```

Troubleshoot

The mentioned debugs can be used to troubleshoot the IKEv2 tunnel:

debug crypto ikev2 protocol 127
debug crypto ikev2 platform 127



Note: If you wish to troubleshoot only one tunnel (which must be the case if the device is in production), you must enable debugs conditionally using the debug crypto condition peer X.X.X.X command.