Configure Hairpinning of Traffic Between Two Site-to-Site Tunnels

Contents

Introduction

This document describes how to forward VPN traffic between two VPN tunnels on a single interface.

Prerequisites

Requirements

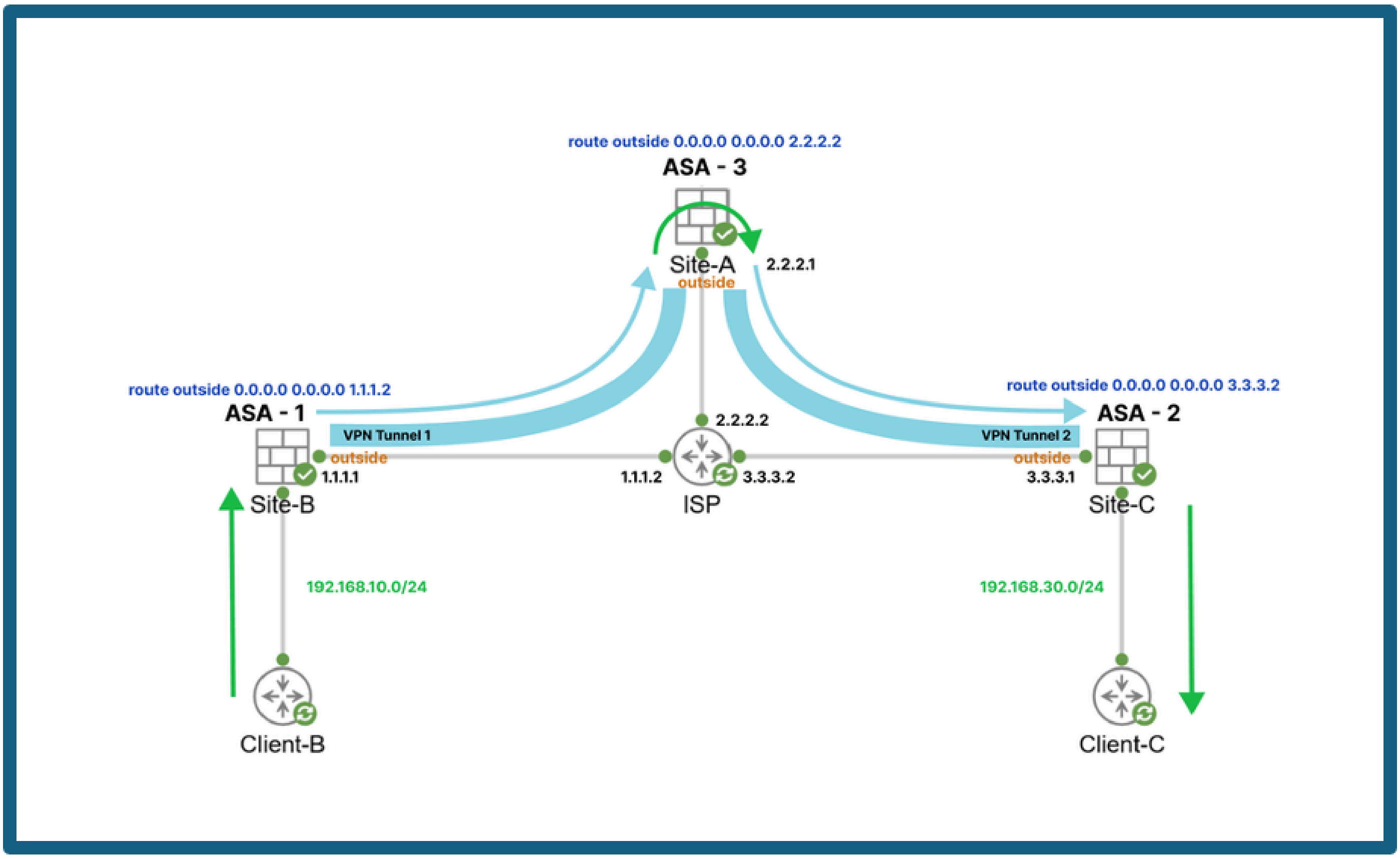
Cisco recommends knowledge of these topics:
• Basic understanding of Policy Based Site to Site VPN
• Experience with ASA command line

Components Used

The information in this document is based on these software and hardware versions:
• Adaptive Security Appliance (ASA) version 9.20
• IKEv1

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.

Topology



Topology

Background Information

This configuration demonstrates how to redirect traffic from one site-to-site tunnel to another on the same device. To illustrate this setup, we have used three ASAs representing Site A, Site B, and Site C.

Configuration

This section outlines the configuration required to allow traffic from ASA-1 (Site B) to ASA-2 (Site C) through ASA-3 (Site A).

We have two VPN tunnels configured:

- VPN Tunnel 1 : VPN tunnel between Site-B and Site-A
- VPN Tunnel 2 : VPN tunnel between Site-C and Site-A

For detailed guidance on how to create Policy based VPN tunnel on ASA, refer to the ASA Configuration section in the Cisco documentation: Configure a Site-to-Site IPSec IKEv1 Tunnel Between ASA and Cisco IOS XE Router

ASA (Site B) Configuration

We need to allow the traffic from Site-B network to Site-C network in the crypto access-list of VPN Tunnel 1 on outside interface of ASA 1.
In this scenario, it is from 192.168.10.0/24 to 192.168.30.0/24

Crypto Access-list:

```
object network 192.168.10.0_24
subnet 192.168.10.0 255.255.255.0

object network 192.168.30.0_24
subnet 192.168.30.0 255.255.255.0

access-list 110 extended permit ip object 192.168.10.0_24 object 192.168.30.0_24
```

Nat exception:

```
nat (inside,outside) source static192.168.10.0_24192.168.10.0_24 destination static192.168.30.0_24192.1
```

Crypto map for VPN Tunnel 1:

```
crypto map outside_map 10 match address 110
crypto map outside_map 10 set pfs
crypto map outside_map 10 set peer 2.2.2.1
crypto map outside_map 10 set ikev1 transform-set myset

crypto map outside_map interface outside
```

ASA (Site C) Crypto Configuration

Allow the traffic from Site-C network to Site-B network in the crypto access-list of VPN Tunnel 2 on outside interface of ASA 2.
In this scenario, it is from 192.168.30.0/24 to 192.168.10.0/24

Crypto Access-list:

```
object network 192.168.10.0_24
subnet 192.168.10.0 255.255.255.0

object network 192.168.30.0_24
subnet 192.168.30.0 255.255.255.0

access-list 110 extended permit ip object 192.168.30.0_24 object 192.168.10.0_24
```

Nat exception:

```
nat (inside,outside) source static 192.168.30.0_24 192.168.30.0_24 destination static 192.168.10.0_24 1
```

Crypto map for VPN Tunnel 2:

```
crypto map outside_map 20 match address 120
crypto map outside_map 20 set pfs
crypto map outside_map 20 set peer 2.2.2.1
crypto map outside_map 20 set ikev1 transform-set myset

crypto map outside_map interface outside
```

ASA (Site A) Crypto Configuration

Allow the traffic from Site-C network to Site-B network in the crypto access-list of VPN Tunnel 1 and traffic from Site-B network to Site-C network in the crypto access-list of VPN Tunnel 2 on outside interfae of ASA at Site-A which is in reverse direction to what we configured on _ ASAs.

In this scenario, it is from 192.168.30.0/24 to 192.168.10.0/24 for VPN tunnel 1 and from 192.168.10.0/24 to 192.168.30.0/24 for VPN tunnel 2

Crypto Access-list:

```
object network 192.168.30.0_24
subnet 192.168.30.0 255.255.255.0

object network 192.168.10.0_24
subnet 192.168.10.0 255.255.255.0

access-list 110 extended permit ip object 192.168.30.0_24 object 192.168.10.0_24
access-list 120 extended permit ip object 192.168.10.0_24 object 192.168.30.0_24
```

Crypto map configuration for VPN Tunnel 1 and 2:

```
crypto map outside_map 10 match address 110
crypto map outside_map 10 set pfs
crypto map outside_map 10 set peer 1.1.1.1
crypto map outside_map 10 set ikev1 transform-set myset

crypto map outside_map 20 match address 120
crypto map outside_map 20 set pfs
crypto map outside_map 20 set peer 3.3.3.1
crypto map outside_map 20 set ikev1 transform-set myset

crypto map outside_map interface outside
```

In addition to this as we need to route the traffic from outside to outside which is same interface with same security level, we need to configure the command:

```
same-security-traffic permit intra-interface
```

Traffic Flow from Site-B to Site-C

Lets consider the traffic is initiated from Site-B to Site-c that is from 192.168.10.0/24 to 192.168.30.0/24.

Site-B (Source)

1. Traffic initiated from the 192.168.10.0/24 network (Site-B) and destined for the 192.168.30.0/24 network (Site-C) is routed to the outside interface of ASA-1 based on the configured routing table.

2. Once the traffic reaches ASA-1, it matches the crypto access-list 110 configured on ASA-1. This triggers encryption of the traffic using VPN Tunnel 1, which securely sends the data toward Site-A.

Site-A (Intermediate)

1. The encrypted traffic from 192.168.10.0/24 to 192.168.30.0/24 arrives at the outside interface of the ASA at Site-A.
2. At Site-A, the traffic is decrypted by VPN Tunnel 1 to restore the original payload.
3. The decrypted traffic is then re-encrypted using VPN Tunnel 2 at the outside interface of the ASA at Site-A.

Site-C (Destination)

1. The encrypted traffic from 192.168.10.0/24 to 192.168.30.0/24 reaches the outside interface of ASA-2 at Site-C.
2. ASA-2 decrypts the traffic using VPN Tunnel 2 and forwards the packets to the LAN side of Site-C, delivering them to the intended destination within the 192.168.30.0/24 network.

Reverse Traffic Flow from Site-C to Site-B

The reverse traffic flow, originating from Site-C (192.168.30.0/24) and destined for Site-B (192.168.10.0/24), results in the same process but in the reverse direction:
1. At Site-C, the traffic is encrypted by VPN Tunnel 2 before being sent to Site-A.
2. At Site-A, the traffic is decrypted by VPN Tunnel 2, then re-encrypted using VPN Tunnel 1 before being forwarded to Site-B.
3. At Site-B, the traffic is decrypted by VPN Tunnel 1 and delivered to the 192.168.10.0/24 network.