Configuration Example of ASA VPN with Overlapping Scenarios

Contents

Introduction
Prerequisites
Requirements
Components Used
Background Information
Translation on both VPN Endpoints
ASA 1
Create the necessary objects for the subnets in use
Configure the NAT Statement
Configure the crypto ACL with the translated subnets
Relevant crypto configuration
ASA 2
Create the necessary objects for the subnets in use
Configure the NAT Statement
Configure the crypto ACL with the translated subnets
Relevant crypto configuration
Verify
ASA 1
ASA 2
Hub and Spoke Topology with Overlapping Spokes
ASA 1
Create the necessary objects for the subnets in use
Create manual statements to translate:
Configure the crypto ACL with the translated subnets
Relevant crypto configuration
ASA 2 (SPOKE 1)
Configure the crypto ACL going to the translated subnet (10.20.20.0 /24)
Relevant crypto configuration
R1 (SPOKE 2)
Configure the crypto ACL going to the translated subnet (10.30.30.0 /24)
Relevant crypto configuration
Verify
ASA 1
ASA 2 (SPOKE 1)
R1 (SPOKE 2)
Troubleshoot
Clear Security Associations
Review NAT Configuration
Troubleshooting Commands
Introduction

This document describes the steps used to translate the VPN traffic that travels over a LAN-to-LAN (L2L) IPsec tunnel between two Adaptive Security Appliances (ASA) in overlapping scenarios and also Port Address Translation (PAT) the internet traffic.

Prerequisites

Requirements

Make sure you have configured the Cisco Adaptive Security Appliance with IP addresses on the interfaces, and have basic connectivity before you proceed with this configuration example.

Components Used

The information in this document is based on this software version:

- Cisco Adaptive Security Appliance Software version 8.3 and 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, make sure that you understand the potential impact of any command.

Background Information

Each device has a private, protected network behind it. In overlapping scenarios, communication across the VPN never happens because the packets never leave the local subnet since the traffic is sent to an IP address of the same subnet. This can be accomplished with Network Address Translation (NAT) as explained in the following sections.

Translation on both VPN Endpoints

When the VPN protected networks overlap and the configuration can be modified on both endpoints; NAT can be used to translate the local network to a different subnet when going to the remote translated subnet.
ASA 1

Create the necessary objects for the subnets in use

object network LOCAL
    subnet 192.168.1.0 255.255.255.0
object network XLATED-LOCAL
    subnet 192.168.2.0 255.255.255.0
object network XLATED-REMOTE
    subnet 192.168.3.0 255.255.255.0

Configure the NAT Statement

Create a manual statement to translate the local network to a different subnet only when going to the remote subnet (also translated)

nat (inside, outside) source static LOCAL XLATED-LOCAL destination static XLATED-REMOTE XLATED-REMOTE

Configure the crypto ACL with the translated subnets

access-list VPN-TRAFFIC extended permit ip object XLATED-LOCAL object XLATED-REMOTE

Relevant crypto configuration

crypto ikev1 enable outside
crypto ikev1 policy 1
    authentication pre-share
    encryption aes-256
    hash sha
    group 2
    lifetime 86400

crypto ipsec ikev1 transform-set AES256-SHA esp-aes-256 esp-sha-hmac
crypto ipsec security-association pmtu-aging infinite
crypto map MYMAP 10 match address VPN-TRAFFIC
crypto map MYMAP 10 set peer 172.16.2.1
crypto map MYMAP 10 set ikev1 transform-set AES256-SHA
crypto map MYMAP interface outside
tunnel-group 172.16.2.1 type ipsec-l2l
tunnel-group 172.16.2.1 ipsec-attributes
    ikev1 pre-shared-key secure_PSK

ASA 2
Create the necessary objects for the subnets in use

object network LOCAL
  subnet 192.168.1.0 255.255.255.0
object network XLATED-LOCAL
  subnet 192.168.3.0 255.255.255.0
object network XLATED-REMOTE
  subnet 192.168.2.0 255.255.255.0

Configure the NAT Statement

Create a manual statement to translate the local network to a different subnet only when going to the remote subnet (also translated)

nat (inside,outside) source static LOCAL XLATED-LOCAL destination static XLATED-REMOTE XLATED-REMOTE

Configure the crypto ACL with the translated subnets

access-list VPN-TRAFFIC extended permit ip object XLATED-LOCAL object XLATED-REMOTE

Relevant crypto configuration

crypto ikev1 enable outside
crypto ikev1 policy 1
  authentication pre-share
  encryption aes-256
  hash sha
  group 2
  lifetime 86400

crypto ipsec ikev1 transform-set AES256-SHA esp-aes-256 esp-sha-hmac
crypto ipsec security-association pmtu-aging infinite
crypto map MYMAP 10 match address VPN-TRAFFIC
crypto map MYMAP 10 set peer 172.16.1.1
crypto map MYMAP 10 set ikev1 transform-set AES256-SHA
crypto map MYMAP interface outside
tunnel-group 172.16.1.1 type ipsec-l2l
tunnel-group 172.16.1.1 ipsec-attributes
  ikev1 pre-shared-key secure_PSK

Verify

Use this section to confirm that your configuration works properly.

ASA 1

ASA1(config)# sh cry isa sa

IKEv1 SAs:

  Active SA: 1
    Rekey SA: 0 (A tunnel will report 1 Active and 1 Rekey SA during rekey)
Total IKE SA: 1

  1   IKE Peer: 172.16.2.1
      Type : L2L   Role : initiator
      Rekey : no   State : MM_ACTIVE

There are no IKEv2 SAsASA1(config)# show crypto ipsec sa
ASA 2

ASA2(config)# show crypto isa sa

IKEv1 SAs:

Active SA: 1
Rekey SA: 0 (A tunnel will report 1 Active and 1 Rekey SA during rekey)
Total IKE SA: 1

1 IKE Peer: 172.16.1.1
  Type : L2L  Role : responder
  Rekey : no  State : MM_ACTIVE

There are no IKEv2 SAs ASA2(config)# show crypto ipsec sa
interface: outside

ASA 2
Hub and Spoke Topology with Overlapping Spokes

In the following topology, both spokes have the same subnet that needs to be protected over the IPsec tunnel towards the Hub. To facilitate the management on the spokes the NAT configuration to workaround the overlapping problem is performed on the Hub only.
Create the necessary objects for the subnets in use

object network LOCAL
   subnet 10.10.10.0 255.255.255.0
object network SPOKES-NETWORK
   subnet 192.168.2.0 255.255.255.0
object network LOCAL-XLATE-TO-SPOKE1
   subnet 10.20.20.0 255.255.255.0
object network LOCAL-XLATE-TO-SPOKE2
   subnet 10.30.30.0 255.255.255.0
object network REMOTE-XLATE-SPOKE1
   subnet 192.168.3.0 255.255.255.0
object network REMOTE-XLATE-SPOKE2
   subnet 192.168.4.0 255.255.255.0

Create manual statements to translate:

- The local network 10.10.10.0 /24 to 10.20.20.0 /24 when going to the SPOKE1 (192.168.2.0 /24).
- The SPOKE1 network 192.168.2.0 /24 to 192.168.3.0 /24 when coming to 10.20.20.0 /24.
- The local network 10.10.10.0 /24 to 10.30.30.0 /24 when going to the SPOKE3 (192.168.2.0 /24).
- The SPOKE2 network 192.168.2.0 /24 to 192.168.4.0 /24 when coming to 10.30.30.0 /24.

nat (inside, outside) source static LOCAL LOCAL-XLATE-SPOKE1 destination static REMOTE-XLATE-SPOKE1 SPOKES-NETWORK
nat (inside, outside) source static LOCAL LOCAL-XLATE-SPOKE2 destination static REMOTE-XLATE-SPOKE2 SPOKES-NETWORK

Configure the crypto ACL with the translated subnets
access-list VPN-to-SPOKE1 extended permit ip object LOCAL-XLATE-SPOKE1 object SPOKES-NETWORKS
access-list VPN-to-SPOKE2 extended permit ip object LOCAL-XLATE-SPOKE2 object SPOKES-NETWORKS

Relevant crypto configuration

crypto ikev1 enable outside
crypto ikev1 policy 1
   authentication pre-share
   encryption aes-256
   hash sha
group 2
   lifetime 86400

crypto ipsec ikev1 transform-set AES256-SHA esp-aes-256 esp-sha-hmac
crypto ipsec security-association pmtu-aging infinite
crypto map MYMAP 10 match address VPN-to-SPOKE1
crypto map MYMAP 10 set peer 172.16.2.1
crypto map MYMAP 10 set ikev1 transform-set AES256-SHA
crypto map MYMAP 20 match address VPN-to-SPOKE2
crypto map MYMAP 20 set peer 172.16.3.1
crypto map MYMAP 20 set ikev1 transform-set AES256-SHA
crypto map MYMAP interface outside
tunnel-group 172.16.2.1 type ipsec-l2l
tunnel-group 172.16.2.1 ipsec-attributes
   ikev1 pre-shared-key secure_PSK
tunnel-group 172.16.3.1 type ipsec-l2l
tunnel-group 172.16.3.1 ipsec-attributes
   ikev1 pre-shared-key secure_PSK

ASA2 (SPOKE1)

Configure the crypto ACL going to the translated subnet (10.20.20.0 /24)

access-list VPN-TRAFFIC extended permit ip 192.168.2.0 255.255.255.0 10.20.20.0 255.255.255.0

Relevant crypto configuration

crypto ikev1 enable outside
crypto ikev1 policy 1
   authentication pre-share
   encryption aes-256
   hash sha
group 2
   lifetime 86400

crypto ipsec ikev1 transform-set esp-aes-256 esp-sha-hmac
crypto ipsec security-association pmtu-aging infinite
crypto map MYMAP 10 match address VPN-TRAFFIC
crypto map MYMAP 10 set peer 172.16.1.1
crypto map MYMAP 10 set ikev1 transform-set AES256-SHA
crypto map MYMAP interface outside
tunnel-group 172.16.1.1 type ipsec-l2l
tunnel-group 172.16.1.1 ipsec-attributes
   ikev1 pre-shared-key secure_PSK

R1 (SPOKE2)

Configure the crypto ACL going to the translated subnet (10.30.30.0 /24)

ip access-list extended VPN-TRAFFIC
permit ip 192.168.2.0 0.0.0.255 10.30.30.0 0.0.0.255

**Relevant crypto configuration**

crypto isakmp policy 1
  encr aes 256
  authentication pre-share
group 2
crypto isakmp key secure_PSK address 172.16.1.1
crypto ipsec transform-set AES256-SHA esp-aes 256 esp-sha-hmac
  mode tunnel
crypto map MYMAP 10 ipsec-isakmp
  set peer 172.16.1.1
  set transform-set AES256-SHA
  match address VPN-TRAFFIC
interface GigabitEthernet0/1
  ip address 172.16.3.1 255.255.255.0
duplex auto
  speed auto
  media-type rj45
crypto map MYMAP

**Verify**

**ASA 1**

ASA1(config)# show crypto isakmp sa

IKEv1 SAs:

Active SA: 2
  Rekey SA: 0 (A tunnel will report 1 Active and 1 Rekey SA during rekey)
Total IKE SA: 2

1  IKE Peer: 172.16.3.1
   Type : L2L  Role : responder
   Rekey : no  State : MM_ACTIVE
2  IKE Peer: 172.16.2.1
   Type : L2L  Role : responder
   Rekey : no  State : MM_ACTIVE

There are no IKEv2 SAsASA1(config)# show crypto ipsec sa
interface: outside
  Crypto map tag: MYMAP, seq num: 10, local addr: 172.16.1.1
  access-list VPN-to-SPOKE1 extended permit ip 10.20.20.0 255.255.255.0 192.168.2.0 255.255.255.0
  local ident (addr/mask/prot/port): (10.20.20.0/255.255.255.0/0/0)
  remote ident (addr/mask/prot/port): (192.168.2.0/255.255.255.0/0/0)
  current_peer: 172.16.2.1

#pkts encaps: 10, #pkts encrypt: 9, #pkts digest: 10
#pkts decaps: 10, #pkts decrypt: 9, #pkts verify: 10
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 9, #pkts comp failed: 0, #pkts decomp failed: 0
#pre-frag successes: 0, #pre-frag failures: 0, #fragments created: 0
#PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
#TFC rcvd: 0, #TFC sent: 0
local crypto endpt.: 172.16.1.1/0, remote crypto endpt.: 172.16.2.1/0
path mtu 1500, ipsec overhead 74(44), media mtu 1500
PMTU time remaining (sec): 0, DF policy: copy-df
ICMP error validation: disabled, TFC packets: disabled
current outbound spi: 79384296
current inbound spi: 2189BF7A

inbound esp sas:
spi: 0x2189BF7A (562675578)
  transform: esp-aes-256 esp-sha-hmac no compression
  in use settings = (L2L, Tunnel, IKEv1, )
  slot: 0, conn_id: 12288, crypto-map: MYMAP
  sa timing: remaining key lifetime (kB/sec): (3914999/28618)
  IV size: 16 bytes
  replay detection support: Y
  Anti replay bitmap:
    0x00000000 0x00000001

outbound esp sas:
spi: 0x79384296 (2033730198)
  transform: esp-aes-256 esp-sha-hmac no compression
  in use settings = (L2L, Tunnel, IKEv1, )
  slot: 0, conn_id: 12288, crypto-map: MYMAP
  sa timing: remaining key lifetime (kB/sec): (3914999/28618)
  IV size: 16 bytes
  replay detection support: Y
  Anti replay bitmap:
    0x00000000 0x00000001

access-list VPN-to-SPOKE2 extended permit ip 10.30.30.0 255.255.255.0 192.168.2.0 255.255.255.0
local ident (addr/mask/prot/port): (10.30.30.0/255.255.255.0/0/0)
remote ident (addr/mask/prot/port): (192.168.2.0/255.255.255.0/0/0)
current peer: 172.16.3.1

inbound esp sas:
spi: 0x05B7155D (95884637)
  transform: esp-aes-256 esp-sha-hmac no compression
  in use settings = (L2L, Tunnel, IKEv1, )
  slot: 0, conn_id: 8192, crypto-map: MYMAP
  sa timing: remaining key lifetime (kB/sec): (3914999/28618)
  IV size: 16 bytes
replay detection support: Y
Anti replay bitmap:
0x00000000 0x0000001F
outbound esp sas:
spi: 0x65DF4F5 (1711142133)
transform: esp-aes-256 esp-sha-hmac no compression
in use settings ={L2L, Tunnel, IKEv1, }
slot: 0, conn_id: 8192, crypto-map: MYMAP
sa timing: remaining key lifetime (kB/sec): (3914999/2883)
IV size: 16 bytes
replay detection support: Y
Anti replay bitmap:
0x00000000 0x00000001

ASA2 (SPOKE1)

ASA2(config)# show crypto isakmp sa

IKEv1 SAs:

Active SA: 1
Rekey SA: 0 (A tunnel will report 1 Active and 1 Rekey SA during rekey)
Total IKE SA: 1

1 IKE Peer: 172.16.1.1
Type : L2L Role : initiator
Rekey : no State : MM_ACTIVE

There are no IKEv2 SAs

ASA2(config)# show crypto ipsec sa

interface: outside
Crypto map tag: MYMAP, seq num: 10, local addr: 172.16.2.1

access-list VPN-TRAFFIC extended permit ip 192.168.2.0 255.255.255.0 10.20.20.0 255.255.255.0
local ident (addr/mask/prot/port): (192.168.2.0/255.255.255.0/0/0)
remote ident (addr/mask/prot/port): (10.20.20.0/255.255.255.0/0/0)
current_peer: 172.16.1.1

#pkts encaps: 10, #pkts encrypt: 10, #pkts digest: 10
#pkts decaps: 10, #pkts decrypt: 10, #pkts verify: 10
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 9, #pkts comp failed: 0, #pkts decomp failed: 0
#pre-frag successes: 0, #pre-frag failures: 0, #fragments created: 0
#PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
#TFC rcvd: 0, #TFC sent: 0
#Valid ICMP Errors rcvd: 0, #Invalid ICMP Errors rcvd: 0
#send errors: 0, #recv errors: 0

local crypto endpt.: 172.16.2.1/0, remote crypto endpt.: 172.16.1.1/0
path mtu 1500, ipsec overhead 74(44), media mtu 1500
PMTU time remaining (sec): 0, DF policy: copy-df
ICMP error validation: disabled, TFC packets: disabled
current outbound spi: 2189BF7A
current inbound spi : 79384296

inbound esp sas:
spi: 0x79384296 (2033730198)
transform: esp-aes-256 esp-sha-hmac no compression
in use settings ={L2L, Tunnel, IKEv1, }
slot: 0, conn_id: 8192, crypto-map: MYMAP
sa timing: remaining key lifetime (kB/sec): (4373999/28494)
IV size: 16 bytes
replay detection support: Y
Anti replay bitmap:
0x00000000 0x000003FF

outbound esp sas:
spi: 0x2189BF7A (562675578)
transform: esp-aes-256 esp-sha-hmac no compression
in use settings ={L2L, Tunnel, IKEv1, }
slot: 0, conn_id: 8192, crypto-map: MYMAP
sa timing: remaining key lifetime (kB/sec): (4373999/28494)
IV size: 16 bytes
replay detection support: Y
Anti replay bitmap:
0x00000000 0x00000001

R1 (SPOKE2)

R31show crypto isakmp sa
IPv4 Crypto ISAKMP SA

<table>
<thead>
<tr>
<th>dst</th>
<th>src</th>
<th>state</th>
<th>conn-id</th>
<th>status</th>
</tr>
</thead>
<tbody>
<tr>
<td>172.16.1.1</td>
<td>172.16.3.1</td>
<td>QM_IDLE</td>
<td>1001</td>
<td>ACTIVE</td>
</tr>
</tbody>
</table>

IPv6 Crypto ISAKMP SAR1#show crypto ipsec sa

interface: GigabitEthernet0/1
Crypto map tag: MYMAP, local addr 172.16.3.1

protected vrf: (none)
local ident (addr/mask/prot/port): (192.168.2.0/255.255.255.0/0/0)
remote ident (addr/mask/prot/port): (10.30.30.0/255.255.255.0/0/0)
current_peer 172.16.1.1 port 500

PERMIT, flags=(origin_is_acl,)
#pkts encaps: 10, #pkts encrypt: 10, #pkts digest: 10
#pkts decaps: 10, #pkts decrypt: 10, #pkts verify: 10
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 0, #pkts compr. failed: 0
#pkts not decompressed: 0, #pkts decompress failed: 0
#send errors 0, #recv errors 0

local crypto endpt.: 172.16.3.1, remote crypto endpt.: 172.16.1.1
plaintext mtu 1438, path mtu 1500, ip mtu 1500, ip mtu idb GigabitEthernet0/1
current outbound spi: 0x5B7155D(95884637)
PFS (Y/N): N, DH group: none

inbound esp sas:
spi: 0x65FDF4F5(1711142133)
transform: esp-256-aes esp-sha-hmac ,
in use settings ={Tunnel, }
conn id: 1, flow_id: SW:1, sibling_flags 80004040, crypto map: MYMAP
sa timing: remaining key lifetime (k/sec): (4188495/2652)
IV size: 16 bytes
replay detection support: Y
Status: ACTIVE(ACTIVE)

inbound ah sas:

inbound pcp sas:

outbound esp sas:
spi: 0x5B7155D(95884637)
transform: esp-256-aes esp-sha-hmac ,
in use settings ={Tunnel, }
conn id: 2, flow_id: SW:2, sibling_flags 80004040, crypto map: MYMAP
sa timing: remaining key lifetime (k/sec): (4188495/2652)
IV size: 16 bytes
replay detection support: Y
Troubleshoot

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

Clear Security Associations

When you troubleshoot, be sure to clear existing SAs after you make a change. In the privileged mode of the PIX, use these commands:

- `clear crypto ipsec sa` - Deletes the active IPsec SAs.
- `clear crypto isakmp sa` - Deletes the active IKE SAs.

Review NAT Configuration

- `show nat detail` - Displays the NAT configuration with the object(s) / object-group(s) expanded

Troubleshooting Commands

Use this section to confirm that your configuration works properly.

The Cisco CLI Analyzer (registered customers only) supports certain `show` commands. Use the Cisco CLI Analyzer in order to view an analysis of `show` command output.

- `debug crypto ipsec` - Displays the IPsec negotiations of Phase 2.
- `debug crypto isakmp` - Displays the ISAKMP negotiations of Phase 1.

Related Information

- [NAT Configuration Guide](#)
- [Most Common L2L and Remote Access IPsec VPN Troubleshooting Solutions](#)
- [IPsec Negotiation/IKE Protocols](#)
- [Technical Support & Documentation - Cisco Systems](#)