Configure IKEv1 IPsec Site-to-Site Tunnels with the ASDM or CLI on the ASAv

Contents

Introduction

This document describes how to configure an IKEv1 IPsec site-to-site tunnel between two Cisco Secure Firewall Virtual (ASAv) running v9.18.3.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- The end-to-end IP connectivity must be established
- These protocols must be allowed:
  1. User Datagram Protocol (UDP) 500 and 4500 for the IPsec control plane
  2. Encapsulating Security Payload (ESP) IP Protocol 50 for the IPsec data plane

Components Used

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

- Cisco Secure Firewall ASA Virtual that runs the software version 9.18.3

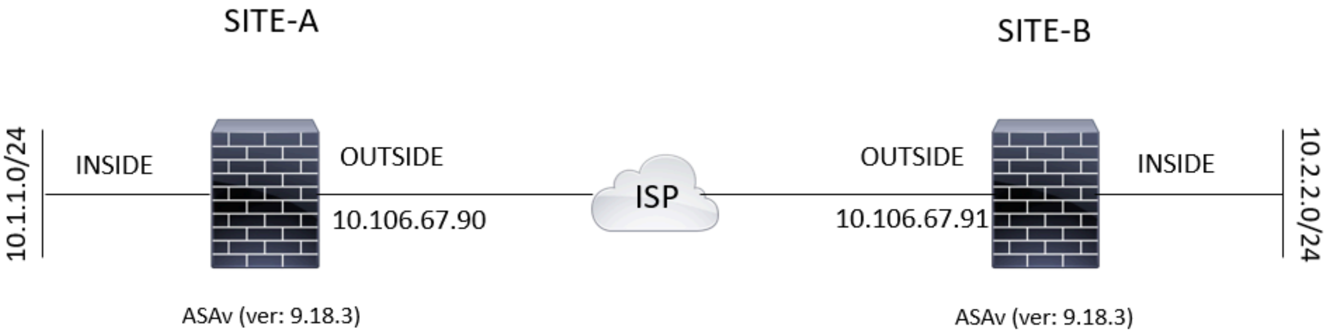
The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Configure

This section describes how to configure the site-to-site VPN tunnel via the Adaptive Security Device Manager (ASDM) VPN wizard or via the CLI.

Network Diagram

This topology is used for the examples throughout this document:

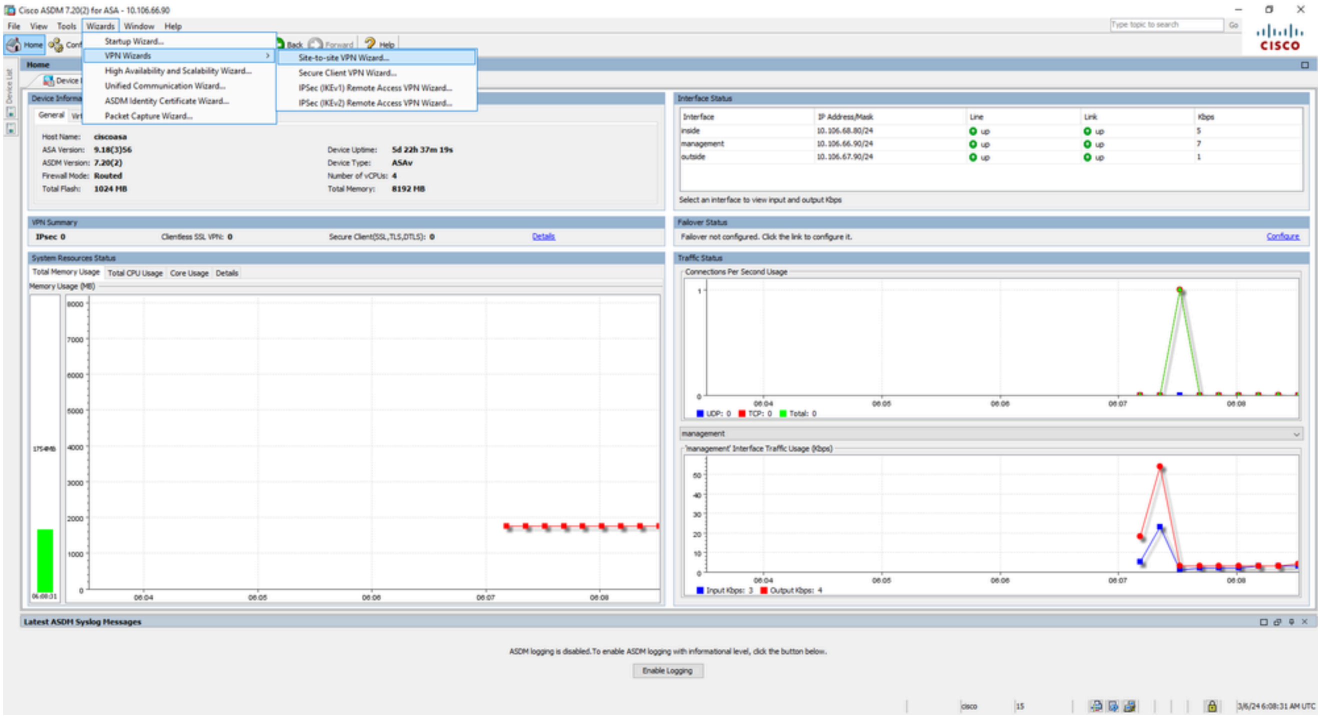


Topology Diagram

Configure Via the ASDM VPN Wizard

Complete these steps in order to set up the site-to-site VPN tunnel via the ASDM wizard:

1. Open the ASDM and navigate to Wizards > VPN Wizards > Site-to-site VPN Wizard.


Cisco ASDM 7.20(2) for ASA - 10.106.66.90
File View Tools Wizards Window Help
Home Conf Back Forward Help
Type topic to search Go
Startup Wizard...
VPN Wizards
High Availability and Scalability Wizard...
Unified Communication Wizard...
ASDM Identity Certificate Wizard...
Packet Capture Wizard...
Site-to-site VPN Wizard...
Secure Client VPN Wizard...
IPSec (IKEv1) Remote Access VPN Wizard...
IPSec (IKEv2) Remote Access VPN Wizard...
Home
Device List
General
Device Information
VPN Summary
System Resources Status
Total Memory Usage
Total CPU Usage
Core Usage
Details
Memory Usage (MB)
Interface Status
Failover Status
Configure
Traffic Status
Connections Per Second Usage
UDP: 0
TCP: 0
Total: 0
management
'management' Interface Traffic Usage (Kbps)
Input Kbps: 3
Output Kbps: 4
Latest ASDM Syslog Messages
Enable Logging

Host Name: ciscoasa
ASA Version: 9.18(3)56
ASDM Version: 7.20(2)
Firewall Mode: Routed
Total Flash: 1024 MB
Device Uptime: 5d 22h 37m 19s
Device Type: ASAv
Number of vCPUs: 4
Total Memory: 8192 MB

IPsec 0 Clientless SSL VPN: 0 Secure Client(SSL,TLS,DTLS): 0 Details

Interface	IP Address/Mask	Line	Link	Kbps
inside	10.106.68.80/24	up	up	5
management	10.106.66.90/24	up	up	7
outside	10.106.67.90/24	up	up	1

Select an interface to view input and output Kbps

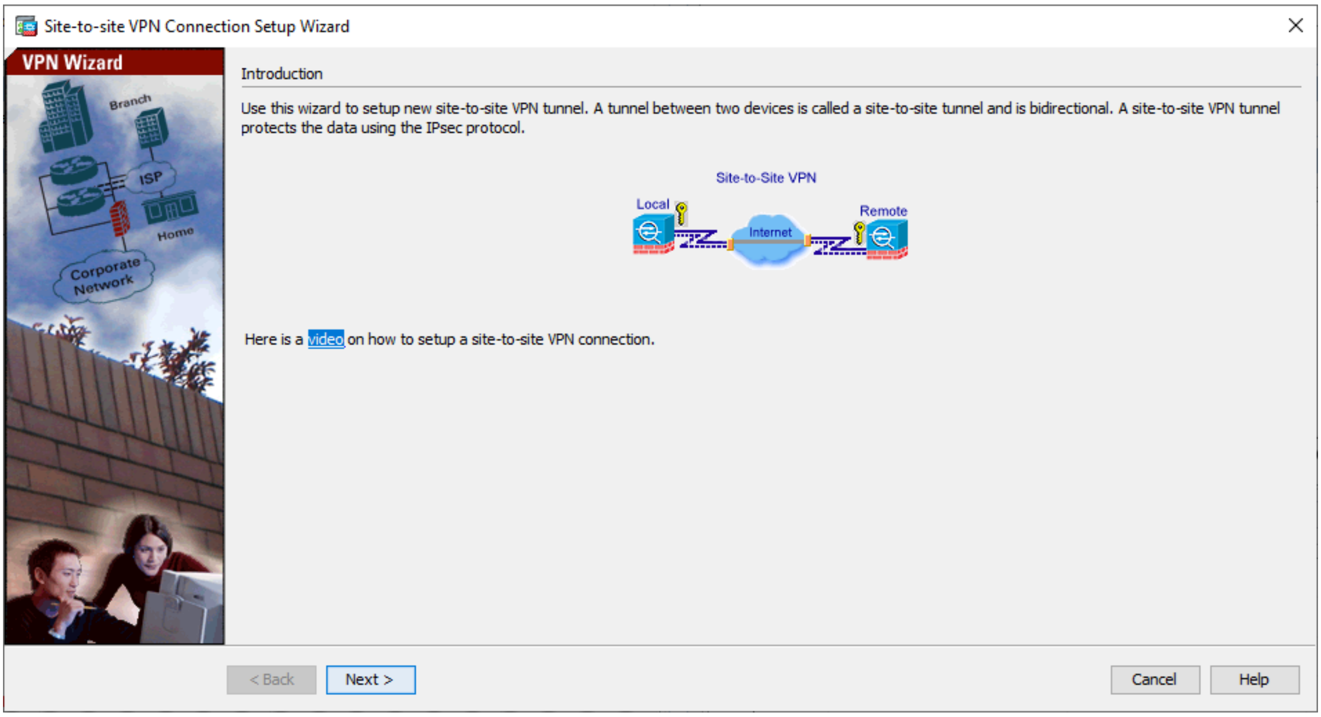
Failover not configured. Click the link to configure it.

ASDM logging is disabled.To enable ASDM logging with informational level, click the button below.

cisco 15 3/6/24 6:08:31 AM UTC

VPN Wizard Navigation

2. Click Next once you reach the wizard home page.



Site-to-site VPN Connection Setup Wizard

Introduction

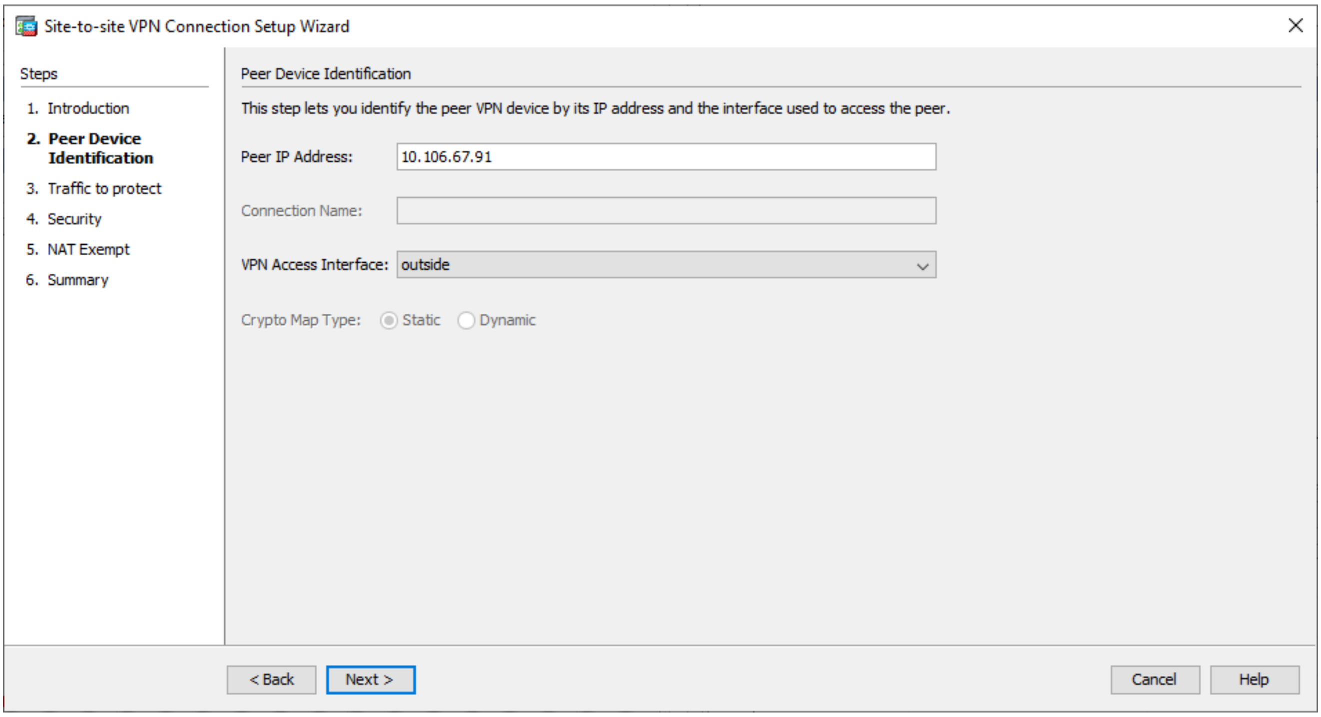
Use this wizard to setup new site-to-site VPN tunnel. A tunnel between two devices is called a site-to-site tunnel and is bidirectional. A site-to-site VPN tunnel protects the data using the IPsec protocol.

Here is a video on how to setup a site-to-site VPN connection.

VPN Wizard Window 1

Note: The most recent ASDM versions provide a link to a video that explains this configuration.

3. Configure the peer IP address. In this example, the peer IP address is set to **10.106.67.91** on Site B. If you configure the peer IP address on Site A, it must be changed to **10.106.67.90**. The interface through which the remote end can be reached is also specified. Click Next once complete.



Site-to-site VPN Connection Setup Wizard

Steps

1. Introduction
2. **Peer Device Identification**
3. Traffic to protect
4. Security
5. NAT Exempt
6. Summary

Peer Device Identification

This step lets you identify the peer VPN device by its IP address and the interface used to access the peer.

Peer IP Address: 10.106.67.91

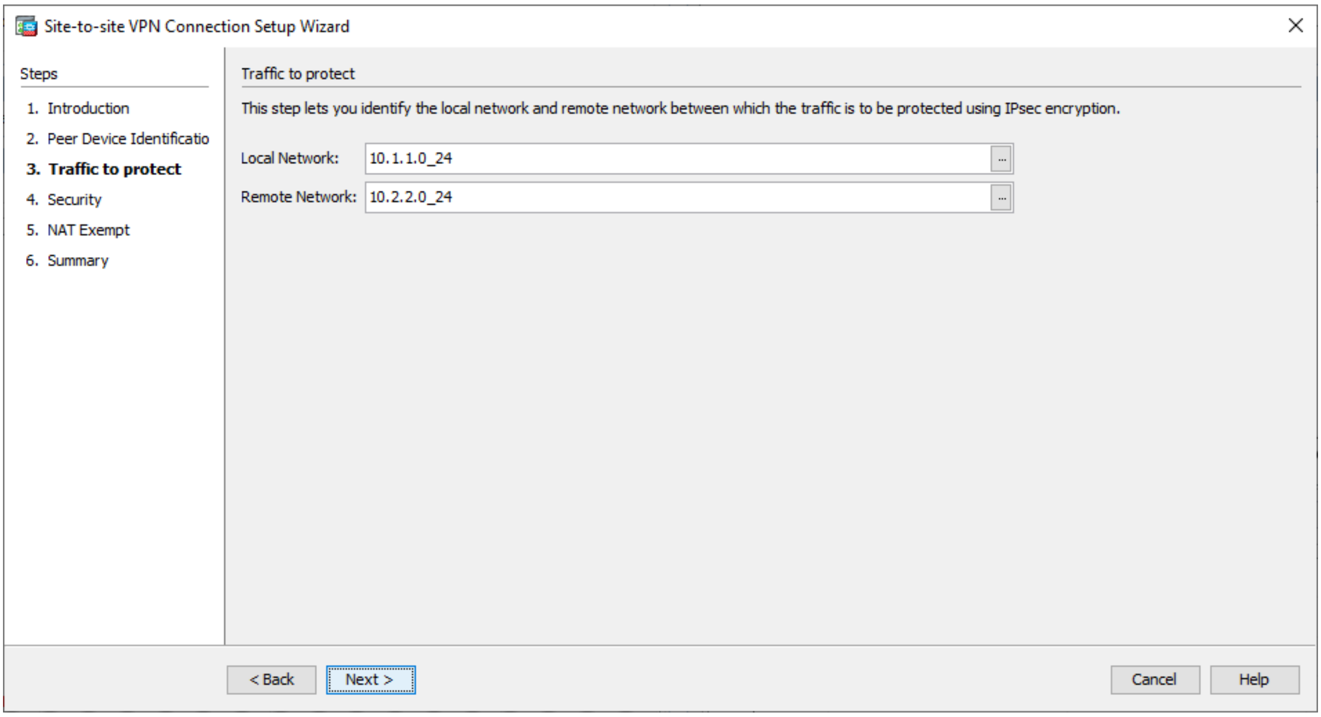
Connection Name:

VPN Access Interface: outside

Crypto Map Type: ● Static ○ Dynamic

VPN Wizard Window 2

4. Configure the local and remote networks (traffic source and destination). This image shows the configuration for Site B (the reverse applies to Site A).



Site-to-site VPN Connection Setup Wizard

Traffic to protect

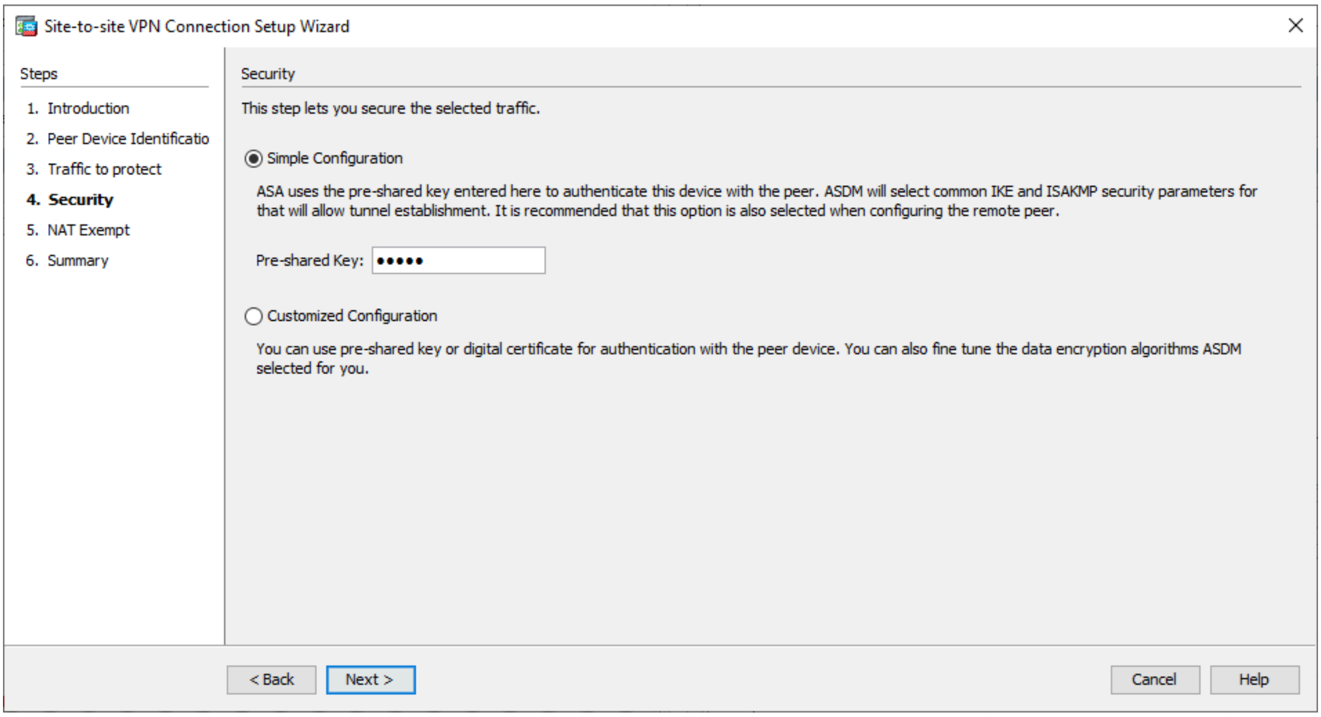
This step lets you identify the local network and remote network between which the traffic is to be protected using IPsec encryption.

Local Network: 10.1.1.0_24

Remote Network: 10.2.2.0_24

VPN Wizard Window 3

5. On the Security page, configure the pre-shared key (it must match on both ends). Click `Next` once complete.



Site-to-site VPN Connection Setup Wizard

Security

This step lets you secure the selected traffic.

● Simple Configuration

ASA uses the pre-shared key entered here to authenticate this device with the peer. ASDM will select common IKE and ISAKMP security parameters for that will allow tunnel establishment. It is recommended that this option is also selected when configuring the remote peer.

Pre-shared Key: •••••

○ Customized Configuration

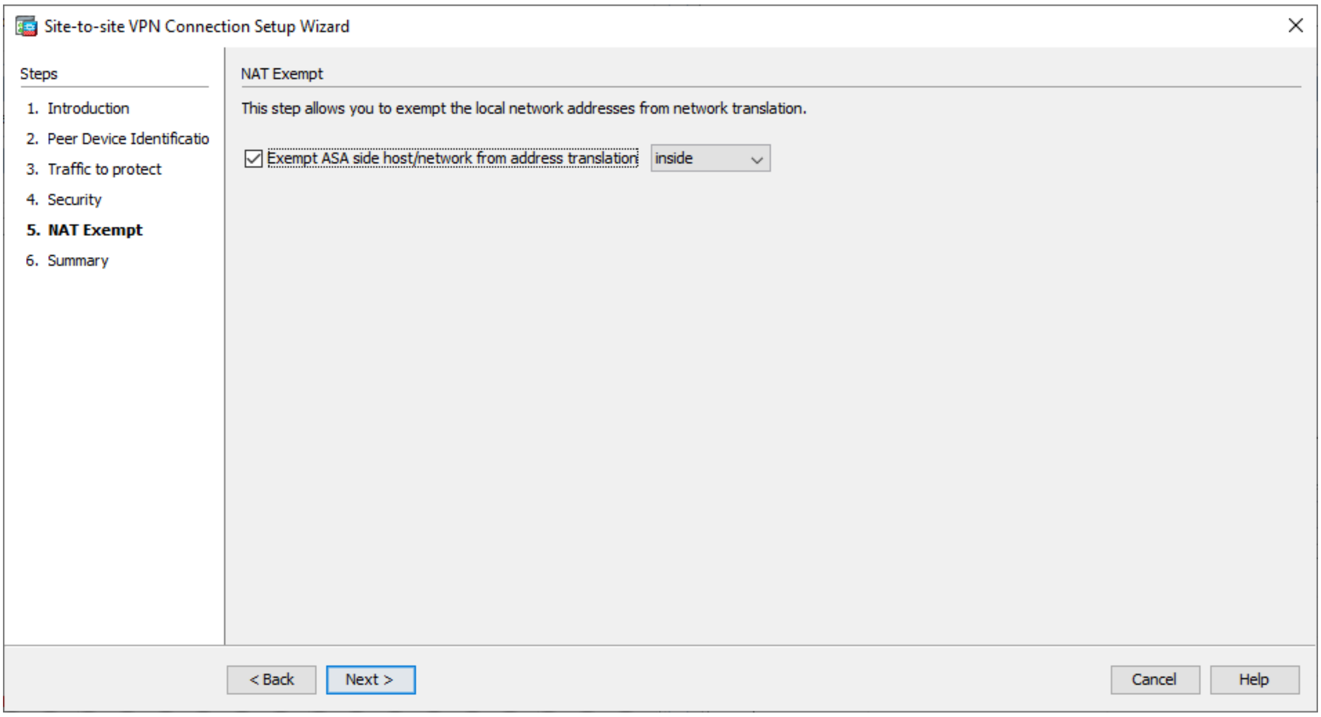
You can use pre-shared key or digital certificate for authentication with the peer device. You can also fine tune the data encryption algorithms ASDM selected for you.

VPN Wizard Window 4

6. Configure the source interface for the traffic on the ASA. The ASDM automatically creates the Network Address Translation (NAT) rule based on the ASA version and pushes it with the rest of the

configuration in the final step.

Note: For the example that is used in this document, 'inside' is the source of the traffic.



Site-to-site VPN Connection Setup Wizard

Steps

1. Introduction
2. Peer Device Identificatio
3. Traffic to protect
4. Security
5. **NAT Exempt**
6. Summary

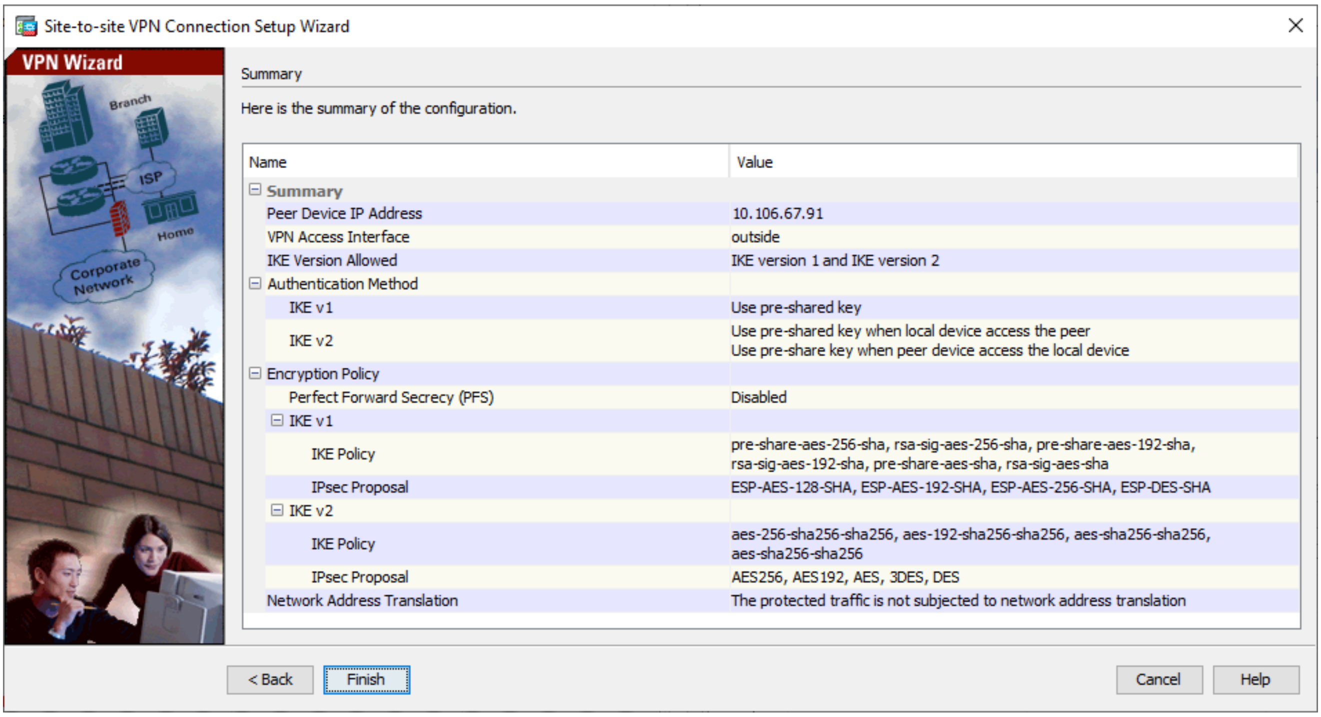
NAT Exempt

This step allows you to exempt the local network addresses from network translation.

☑ Exempt ASA side host/network from address translation: inside

VPN Wizard Window 5

7. The wizard now provides a summary of the configuration that is pushed to the ASA. Review and verify the configuration settings, and then click Finish.



Site-to-site VPN Connection Setup Wizard

Summary

Here is the summary of the configuration.

Name	Value
⊟ Summary	
Peer Device IP Address	10.106.67.91
VPN Access Interface	outside
IKE Version Allowed	IKE version 1 and IKE version 2
⊟ Authentication Method	
IKE v1	Use pre-shared key
IKE v2	Use pre-shared key when local device access the peer Use pre-share key when peer device access the local device
⊟ Encryption Policy	
Perfect Forward Secrecy (PFS)	Disabled
⊟ IKE v1	
IKE Policy	pre-share-aes-256-sha, rsa-sig-aes-256-sha, pre-share-aes-192-sha, rsa-sig-aes-192-sha, pre-share-aes-sha, rsa-sig-aes-sha
IPsec Proposal	ESP-AES-128-SHA, ESP-AES-192-SHA, ESP-AES-256-SHA, ESP-DES-SHA
⊟ IKE v2	
IKE Policy	aes-256-sha256-sha256, aes-192-sha256-sha256, aes-sha256-sha256, aes-sha256-sha256
IPsec Proposal	AES256, AES192, AES, 3DES, DES
Network Address Translation	The protected traffic is not subjected to network address translation

VPN Wizard Window 6

Configure Via the CLI

This section describes how to configure the IKEv1 IPsec site-to-site tunnel via the CLI.

Configure Site B

Tip: For an IKEv2 configuration example with the ASA, take a look at the Site-to-Site IKEv2 Tunnel between ASA and Router Configuration Examples Cisco document.

Phase 1 (IKEv1)

Complete these steps for the Phase 1 configuration:

1. Enter this command into the CLI in order to enable IKEv1 on the outside interface:

```
crypto ikev1 enable outside
```

2. Create an IKEv1 policy that defines the algorithms/methods to be used for hashing, authentication, Diffie-Hellman group, lifetime, and encryption:

```
crypto ikev1 policy 1
! The 1 in the above command refers to the Policy suite priority (1 highest, 65535 lowest)
  authentication pre-share
  encryption aes-256
  hash sha
  group 14
  lifetime 86400
```

3. Create a tunnel group under the IPsec attributes and configure the peer IP address and the tunnel pre-shared key:

```
tunnel-group 10.106.67.90 type ipsec-l2l
tunnel-group 10.106.67.90 ipsec-attributes
 ikev1 pre-shared-key cisco
 ! Note the IKEv1 keyword at the beginning of the pre-shared-key command.
```

Phase 2 (IPsec)

Complete these steps for the Phase 2 configuration:

1. Create an access list that defines the traffic to be encrypted and tunneled. In this example, the traffic of interest is the traffic from the tunnel that is sourced from the **10.2.2.0** subnet to **10.1.1.0**. It can contain multiple entries if there are multiple subnets involved between the sites.

```
object network 10.2.2.0_24
 subnet 10.2.2.0 255.255.255.0
object network 10.1.1.0_24
```

```
 subnet 10.1.1.0 255.255.255.0

access-list 100 extended permit ip object 10.2.2.0_24 object 10.1.1.0_24
```

2. Configure the Transform Set (TS), which must involve the keyword IKEv1. An identical TS must be created on the remote end as well.

```
crypto ipsec ikev1 transform-set myset esp-aes-256 esp-sha-hmac
```

3. Configure the crypto map, which contains these components:
    - The peer IP address
    - The defined access list that contains the traffic of interest
    - The TS
    - An optional Perfect Forward Secrecy (PFS) setting, which creates a new pair of Diffie-Hellman keys that are used in order to protect the data (both sides must be PFS-enabled before Phase 2 comes up)

4. Apply the crypto map on the outside interface:

```
crypto map outside_map 20 match address 100
crypto map outside_map 20 set peer 10.106.67.90
crypto map outside_map 20 set ikev1 transform-set myset
crypto map outside_map 20 set pfs
crypto map outside_map interface outside
```

NAT Exemption

Ensure that the VPN traffic is not subjected to any other NAT rule. This is the NAT rule that is used:

```
nat (inside,outside) 1 source static 10.2.2.0_24 10.2.2.0_24 destination static 10.1.1.0_24 10.1.1.0_24
```

Note: When multiple subnets are used, you must create object groups with all of the source and destination subnets and use them in the NAT rule.

```
object-group  network 10.x.x.x_SOURCE
 network-object  10.4.4.0 255.255.255.0
 network-object  10.2.2.0 255.255.255.0

object network 10.x.x.x_DESTINATION
 network-object  10.3.3.0 255.255.255.0
 network-object  10.1.1.0 255.255.255.0
```

```
nat (inside,outside) 1 source static 10.x.x.x_SOURCE 10.x.x.x_SOURCE destination static 10.x.x.x_DESTIN
```

Complete Sample Configuration

Here is the complete configuration for Site B:

```
crypto ikev1 enable outside

crypto ikev1 policy 10
 authentication pre-share
 encryption aes-256
 hash sha
 group 14
 lifetime 86400

tunnel-group 10.106.67.90 type ipsec-l2l
tunnel-group 10.106.67.90 ipsec-attributes
 ikev1 pre-shared-key cisco
 !Note the IKEv1 keyword at the beginning of the pre-shared-key command.

object network 10.2.2.0_24
 subnet 10.2.2.0 255.255.255.0
object network 10.1.1.0_24
 subnet 10.1.1.0 255.255.255.0

access-list 100 extended permit ip object 10.2.2.0_24 object 10.1.1.0_24

crypto ipsec ikev1 transform-set myset esp-aes esp-sha-hmac

crypto map outside_map 20 match address 100
crypto map outside_map 20 set peer 10.106.67.90
crypto map outside_map 20 set ikev1 transform-set myset
crypto map outside_map 20 set pfs
crypto map outside_map interface outside

nat (inside,outside) 1 source static 10.2.2.0_24 10.2.2.0_24 destination static 10.1.1.0_24 10.1.1.0_24
```

Group Policy

Group policies are used in order to define specific settings that apply to the tunnel. These policies are used in conjunction with the tunnel group.

The group policy can be defined as either internal, which means that the attributes are pulled from that which is defined on the ASA, or it can be defined as external, where the attributes are queried from an external server. This is the command that is used in order to define the group policy:

```
group-policy SITE_A internal
```

Note: You can define multiple attributes in the group policy. For a list of all possible attributes, refer to the Configuring Group Policies section.

Group Policy Optional Attributes

The vpn-tunnel-protocol attribute determines the tunnel type to which these settings must be applied. In this example, IPsec is used:

```
vpn-tunnel-protocol ?
  group-policy mode commands/options:
  IPSec        IP Security Protocol
  l2tp-ipsec   L2TP using IPSec for security
  svc          SSL VPN Client
  webvpn       WebVPN

vpn-tunnel-protocol ikev1 - Version 8.4 and later
```

You have the option to configure the tunnel so that it stays idle (no traffic) and does not go down. In order to configure this option, the vpn-idle-timeout attribute value must use minutes, or you can set the value to none, which means that the tunnel never goes down.

Here is an example:

```
group-policy SITE_A attributes
  vpn-idle-timeout ?

group-policy mode commands/options:
  <1-35791394>    Number of minutes
  alert-interval  Specify timeout alert interval in minutes
  none            Site-to-Site (IKEv1, IKEv2) and IKEv1 remote-access: Disable
                  timeout and allow an unlimited idle period; AnyConnect (SSL,
                  IPSec/IKEv2): Use value of default-idle-timeout
```

The default-group-policy command under the general attributes of the tunnel group defines the group policy that is used in order to push certain policy settings for the tunnel that is established. The default settings for the options that you did not define in the group policy are taken from a global default group policy:

```
tunnel-group 10.106.67.91 general-attributes
 default-group-policy SITE_A
```

Verify

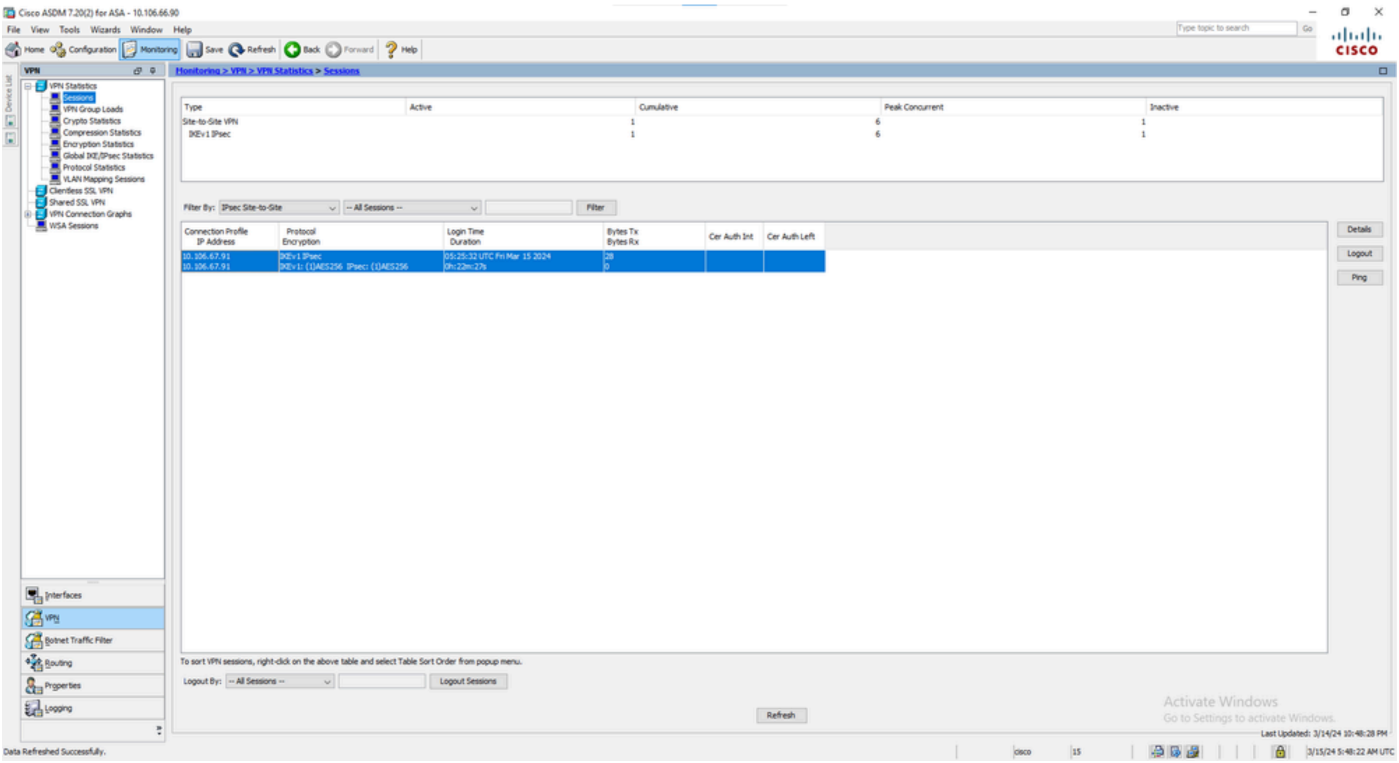
Use the information that is provided in this section in order to verify that your configuration works properly.

ASDM

In order to view the tunnel status from the ASDM, navigate to Monitoring > VPN. This information is provided:

- The peer IP address
- The protocol that is used in order to build the tunnel
- The encryption algorithm that is used
- The time at which the tunnel came up and the up-time
- The number of packets that are received and transferred

Tip: Click Refresh in order to view the latest values, as the data does not update in real time.



Cisco ASDM 7.20(2) for ASA - 10.106.66.90

Monitoring > VPN > VPN Statistics > Sessions

Type	Active	Cumulative	Peak Concurrent	Inactive
Site-to-Site VPN	1	6	1	
IKEv1 IPsec	1	6	1	

Filter By: IPsec Site-to-Site | -- All Sessions --

Connection Profile IP Address	Protocol Encryption	Login Time Duration	Bytes Tx Bytes Rx	Cer Auth Int	Cer Auth Left
10.106.67.91 10.106.67.91	IKEv1 IPsec IKEv1: (1)AES256 IPsec: (1)AES256	05:25:32 UTC Fri Mar 15 2024 0h:22m:27s	28 0		

To sort VPN sessions, right-click on the above table and select Table Sort Order from popup menu.

Logout By: -- All Sessions --

Last Updated: 3/14/24 10:48:28 PM

Data Refreshed Successfully.

cisco 15 3/15/24 5:48:22 AM UTC

VPN Monitoring Window

CLI

This section describes how to verify your configuration via the CLI.

Phase 1

Enter this command into the CLI in order to verify the Phase 1 configuration on the Site B side:

<#root>

```
show crypto ikev1 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:

10.106.67.91


    Type    : L2L             Role    :

initiator


    Rekey   : no              State   :

MM_ACTIVE
```

Phase 2

The show crypto ipsec sa command shows the IPsec SAs that are built between the peers. The encrypted tunnel is built between IP addresses 10.106.67.90 and 10.106.67.91 for the traffic that flows between the networks 10.1.1.0 and 10.2.2.0. You can see the two ESP SAs built for the inbound and outbound traffic. The Authentication Header (AH) is not used because there are no AH SAs.

Enter this command into the CLI in order to verify the Phase 2 configuration on the Site A side:

<#root>

```
interface: outside
     Crypto map tag:

outside_map

, seq num: 20, local addr: 10.106.67.90


      access-list 100 extended permit ip 10.1.1.0 255.255.255.0 10.2.2.0 255.255.255.0


      local ident (addr/mask/prot/port): (10.1.1.0/255.255.255.0/0/0)


      remote ident (addr/mask/prot/port): (10.2.2.0/255.255.255.0/0/0)


      current_peer: 10.106.67.91




      #pkts encaps: 20, #pkts encrypt: 20, #pkts digest: 20
```

```
#pkts decaps: 20, #pkts decrypt: 20, #pkts verify: 20


#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 20, #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.: 10.106.67.90/0, remote crypto endpt.: 10.106.67.91/0


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: F8951DA2



current inbound spi : 662C7ABE



inbound esp sas:
  spi: 0x662C7ABE (1714191038)
    SA State: active

    transform: esp-aes-256 esp-sha-hmac no compression


    in use settings ={L2L, Tunnel, PFS Group 14, IKEv1, }
    slot: 0, conn_id: 1, crypto-map: outside_map
    sa timing: remaining key lifetime (kB/sec): (3914998/28074)
    IV size: 16 bytes
    replay detection support: Y
    Anti replay bitmap:
      0x00000000 0x001FFFFF
outbound esp sas:
  spi: 0xF8951DA2 (4170522018)
    SA State: active

    transform: esp-aes-256 esp-sha-hmac no compression


    in use settings ={L2L, Tunnel, PFS Group 14, IKEv1, }
    slot: 0, conn_id: 1, crypto-map: outside_map
    sa timing: remaining key lifetime (kB/sec): (3914998/28073)
    IV size: 16 bytes
    replay detection support: Y
    Anti replay bitmap:
      0x00000000 0x00000001
```

Enter this command into the CLI in order to verify the Phase 2 configuration on the Site B side:

<#root>

```
interface: outside
```

```
    Crypto map tag:

outside_map

, seq num: 20, local addr: 10.106.67.91

      access-list 100 extended permit ip 10.2.2.0 255.255.255.0 10.1.1.0 255.255.255.0

      local ident (addr/mask/prot/port): (10.2.2.0/255.255.255.0/0/0)

      remote ident (addr/mask/prot/port): (10.1.1.0/255.255.255.0/0/0)

      current_peer: 10.106.67.90

      #pkts encaps: 20, #pkts encrypt: 20, #pkts digest: 20

      #pkts decaps: 20, #pkts decrypt: 20, #pkts verify: 20

      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 20, #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.: 10.106.67.91/0, remote crypto endpt.: 10.106.67.90/0

      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: 662C7ABE

      current inbound spi : F8951DA2

      inbound esp sas:
        spi: 0xF8951DA2 (4170522018)
        SA State: active

        transform: esp-aes-256 esp-sha-hmac no compression

        in use settings ={L2L, Tunnel, PFS Group 14, IKEv1, }
        slot: 0, conn_id: 1, crypto-map: outside_map
        sa timing: remaining key lifetime (kB/sec): (4373998/27737)
        IV size: 16 bytes
        replay detection support: Y
```

```
         Anti replay bitmap:
           0x00000000 0x001FFFFF
      outbound esp sas:
        spi: 0x662C7ABE (1714191038)
        SA State: active
```

```
        transform: esp-aes-256 esp-sha-hmac no compression
```

```
        in use settings ={L2L, Tunnel, PFS Group 14, IKEv1, }
        slot: 0, conn_id: 1, crypto-map: outside_map
        sa timing: remaining key lifetime (kB/sec): (4373998/27737)
        IV size: 16 bytes
        replay detection support: Y
        Anti replay bitmap:
          0x00000000 0x00000001
```

Troubleshoot

Use the information that is provided in this section in order to troubleshoot configuration issues.

Enter these debug commands in order to determine the location of the tunnel failure:

- debug crypto ikev1 127 (Phase 1)
- debug crypto ipsec 127 (Phase 2)

Here is a complete example of debug output:

<#root>

```
IPSEC(crypto_map_check)-3: Looking for crypto map matching 5-tuple: Prot=1, saddr=10.1.1.10, sport=2304
IPSEC(crypto_map_check)-3: Checking crypto map outside_map 20: matched.
Mar 15 05:41:39 [IKEv1 DEBUG]Pitcher: received a key acquire message, spi 0x0
IPSEC(crypto_map_check)-3: Looking for crypto map matching 5-tuple: Prot=1, saddr=10.1.1.10, sport=2304
```

```
IPSEC(crypto_map_check)-3: Checking crypto map outside_map 20: matched.
```

```
Mar 15 05:41:39 [IKEv1]IP = 10.106.67.91, IKE Initiator: New Phase 1, Intf inside, IKE Peer 10.106.67.9
Mar 15 05:41:39 [IKEv1 DEBUG]IP = 10.106.67.91, constructing ISAKMP SA payload
Mar 15 05:41:39 [IKEv1 DEBUG]IP = 10.106.67.91, constructing NAT-Traversal VID ver 02 payload
Mar 15 05:41:39 [IKEv1 DEBUG]IP = 10.106.67.91, constructing NAT-Traversal VID ver 03 payload
Mar 15 05:41:39 [IKEv1 DEBUG]IP = 10.106.67.91, constructing NAT-Traversal VID ver RFC payload
Mar 15 05:41:39 [IKEv1 DEBUG]IP = 10.106.67.91, constructing Fragmentation VID + extended capabilities p
Mar 15 05:41:39 [IKEv1]IP = 10.106.67.91, IKE_DECODE SENDING Message (msgid=0) with payloads : HDR + SA
Mar 15 05:41:39 [IKEv1]IKE Receiver: Packet received on 10.106.67.90:500 from 10.106.67.91:500
Mar 15 05:41:39 [IKEv1]IP = 10.106.67.91, IKE_DECODE RECEIVED Message (msgid=0) with payloads : HDR + SA
Mar 15 05:41:39 [IKEv1 DEBUG]IP = 10.106.67.91, processing SA payload
Mar 15 05:41:39 [IKEv1 DEBUG]IP = 10.106.67.91, Oakley proposal is acceptable
Mar 15 05:41:39 [IKEv1 DEBUG]IP = 10.106.67.91, processing VID payload
Mar 15 05:41:39 [IKEv1 DEBUG]IP = 10.106.67.91, Received NAT-Traversal RFC VID
Mar 15 05:41:39 [IKEv1 DEBUG]IP = 10.106.67.91, processing VID payload
Mar 15 05:41:39 [IKEv1 DEBUG]IP = 10.106.67.91, Received Fragmentation VID
Mar 15 05:41:39 [IKEv1 DEBUG]IP = 10.106.67.91, IKE Peer included IKE fragmentation capability flags: M
Mar 15 05:41:39 [IKEv1 DEBUG]IP = 10.106.67.91, constructing ke payload
Mar 15 05:41:39 [IKEv1 DEBUG]IP = 10.106.67.91, constructing nonce payload
Mar 15 05:41:39 [IKEv1 DEBUG]IP = 10.106.67.91, constructing Cisco Unity VID payload
Mar 15 05:41:39 [IKEv1 DEBUG]IP = 10.106.67.91, constructing xauth V6 VID payload
Mar 15 05:41:39 [IKEv1 DEBUG]IP = 10.106.67.91, Send IOS VID
Mar 15 05:41:39 [IKEv1 DEBUG]IP = 10.106.67.91, Constructing ASA spoofing IOS Vendor ID payload (versio
Mar 15 05:41:39 [IKEv1 DEBUG]IP = 10.106.67.91, constructing VID payload
Mar 15 05:41:39 [IKEv1 DEBUG]IP = 10.106.67.91, Send Altiga/Cisco VPN3000/Cisco ASA GW VID
Mar 15 05:41:39 [IKEv1 DEBUG]IP = 10.106.67.91, constructing NAT-Discovery payload
Mar 15 05:41:39 [IKEv1 DEBUG]IP = 10.106.67.91, computing NAT Discovery hash
Mar 15 05:41:39 [IKEv1 DEBUG]IP = 10.106.67.91, constructing NAT-Discovery payload
Mar 15 05:41:39 [IKEv1 DEBUG]IP = 10.106.67.91, computing NAT Discovery hash
Mar 15 05:41:39 [IKEv1]IP = 10.106.67.91, IKE_DECODE SENDING Message (msgid=0) with payloads : HDR + KE
Mar 15 05:41:39 [IKEv1]IKE Receiver: Packet received on 10.106.67.90:500 from 10.106.67.91:500
Mar 15 05:41:39 [IKEv1]IP = 10.106.67.91, IKE_DECODE RECEIVED Message (msgid=0) with payloads : HDR + K
Mar 15 05:41:39 [IKEv1 DEBUG]IP = 10.106.67.91, processing ke payload
Mar 15 05:41:39 [IKEv1 DEBUG]IP = 10.106.67.91, processing ISA_KE payload
Mar 15 05:41:39 [IKEv1 DEBUG]IP = 10.106.67.91, processing nonce payload
Mar 15 05:41:39 [IKEv1 DEBUG]IP = 10.106.67.91, processing VID payload
Mar 15 05:41:39 [IKEv1 DEBUG]IP = 10.106.67.91, Received Cisco Unity client VID
Mar 15 05:41:39 [IKEv1 DEBUG]IP = 10.106.67.91, processing VID payload
Mar 15 05:41:39 [IKEv1 DEBUG]IP = 10.106.67.91, Received xauth V6 VID
Mar 15 05:41:39 [IKEv1 DEBUG]IP = 10.106.67.91, processing VID payload
Mar 15 05:41:39 [IKEv1 DEBUG]IP = 10.106.67.91, Processing VPN3000/ASA spoofing IOS Vendor ID payload (
Mar 15 05:41:39 [IKEv1 DEBUG]IP = 10.106.67.91, processing VID payload
Mar 15 05:41:39 [IKEv1 DEBUG]IP = 10.106.67.91, Received Altiga/Cisco VPN3000/Cisco ASA GW VID
Mar 15 05:41:39 [IKEv1 DEBUG]IP = 10.106.67.91, processing NAT-Discovery payload
Mar 15 05:41:39 [IKEv1 DEBUG]IP = 10.106.67.91, computing NAT Discovery hash
Mar 15 05:41:39 [IKEv1 DEBUG]IP = 10.106.67.91, processing NAT-Discovery payload
Mar 15 05:41:39 [IKEv1 DEBUG]IP = 10.106.67.91, computing NAT Discovery hash
Mar 15 05:41:39 [IKEv1]IP = 10.106.67.91, Connection landed on tunnel_group 10.106.67.91
Mar 15 05:41:39 [IKEv1 DEBUG]Group = 10.106.67.91, IP = 10.106.67.91, Generating keys for Initiator...
Mar 15 05:41:39 [IKEv1 DEBUG]Group = 10.106.67.91, IP = 10.106.67.91, constructing ID payload
Mar 15 05:41:39 [IKEv1 DEBUG]Group = 10.106.67.91, IP = 10.106.67.91, constructing hash payload
Mar 15 05:41:39 [IKEv1 DEBUG]Group = 10.106.67.91, IP = 10.106.67.91, Computing hash for ISAKMP
Mar 15 05:41:39 [IKEv1 DEBUG]IP = 10.106.67.91, Constructing IOS keep alive payload: proposal=32767/327
Mar 15 05:41:39 [IKEv1 DEBUG]Group = 10.106.67.91, IP = 10.106.67.91, constructing dpd vid payload
Mar 15 05:41:39 [IKEv1]IP = 10.106.67.91, IKE_DECODE SENDING Message (msgid=0) with payloads : HDR + ID
Mar 15 05:41:39 [IKEv1]Group = 10.106.67.91, IP = 10.106.67.91, Automatic NAT Detection Status: Remote
Mar 15 05:41:39 [IKEv1]IKE Receiver: Packet received on 10.106.67.90:500 from 10.106.67.91:500
Mar 15 05:41:39 [IKEv1]IP = 10.106.67.91, IKE_DECODE RECEIVED Message (msgid=0) with payloads : HDR + I
Mar 15 05:41:39 [IKEv1 DEBUG]Group = 10.106.67.91, IP = 10.106.67.91, processing ID payload
Mar 15 05:41:39 [IKEv1 DECODE]Group = 10.106.67.91, IP = 10.106.67.91, ID_IPV4_ADDR ID received 10.106.
Mar 15 05:41:39 [IKEv1 DEBUG]Group = 10.106.67.91, IP = 10.106.67.91, processing hash payload
Mar 15 05:41:39 [IKEv1 DEBUG]Group = 10.106.67.91, IP = 10.106.67.91, Computing hash for ISAKMP
Mar 15 05:41:39 [IKEv1 DEBUG]IP = 10.106.67.91, Processing IOS keep alive payload: proposal=32767/32767
Mar 15 05:41:39 [IKEv1 DEBUG]Group = 10.106.67.91, IP = 10.106.67.91, processing VID payload
Mar 15 05:41:39 [IKEv1 DEBUG]Group = 10.106.67.91, IP = 10.106.67.91, Received DPD VID
Mar 15 05:41:39 [IKEv1]IP = 10.106.67.91, Connection landed on tunnel_group 10.106.67.91
Mar 15 05:41:39 [IKEv1 DEBUG]Group = 10.106.67.91, IP = 10.106.67.91, Oakley begin quick mode
Mar 15 05:41:39 [IKEv1 DECODE]Group = 10.106.67.91, IP = 10.106.67.91, IKE Initiator starting QM: msg i
```

Mar 15 05:41:39 [IKEv1]Group = 10.106.67.91, IP = 10.106.67.91, PHASE 1 COMPLETED

```
Mar 15 05:41:39 [IKEv1]IP = 10.106.67.91, Keep-alive type for this connection: DPD
Mar 15 05:41:39 [IKEv1 DEBUG]Group = 10.106.67.91, IP = 10.106.67.91, Starting P1 rekey timer: 73440 se
Mar 15 05:41:39 [IKEv1]Group = 10.106.67.91, IP = 10.106.67.91, Add to IKEv1 Tunnel Table succeeded for
Mar 15 05:41:39 [IKEv1]Group = 10.106.67.91, IP = 10.106.67.91, Add to IKEv1 MIB Table succeeded for SA
IPSEC INFO: Setting an IPSec timer of type SA Purge Timer for 30 seconds with a jitter value of 0
IPSEC INFO: IPSec SA PURGE timer started SPI 0x0001B739
IPSEC: New embryonic SA created @ 0x00007f05294f4620,
  SCB          : 0x294CFE60,
  Direction    : inbound
  SPI          : 0x50EF49AD
  Session ID   : 0x00002000
  VPIF num     : 0x00000002
  Tunnel type  : l2l
  Protocol     : esp
  Lifetime     : 240 seconds
  SA handle    : 0x0001B739
Mar 15 05:41:39 [IKEv1 DEBUG]Group = 10.106.67.91, IP = 10.106.67.91, IKE got SPI from key engine: SPI =
Mar 15 05:41:39 [IKEv1 DEBUG]Group = 10.106.67.91, IP = 10.106.67.91, oakley constructing quick mode
Mar 15 05:41:39 [IKEv1 DEBUG]Group = 10.106.67.91, IP = 10.106.67.91, constructing blank hash payload
Mar 15 05:41:39 [IKEv1 DEBUG]Group = 10.106.67.91, IP = 10.106.67.91, constructing IPSec SA payload
Mar 15 05:41:39 [IKEv1 DEBUG]Group = 10.106.67.91, IP = 10.106.67.91, constructing IPSec nonce payload
Mar 15 05:41:39 [IKEv1 DEBUG]Group = 10.106.67.91, IP = 10.106.67.91, constructing pfs ke payload
Mar 15 05:41:39 [IKEv1 DEBUG]Group = 10.106.67.91, IP = 10.106.67.91, constructing proxy ID
Mar 15 05:41:39 [IKEv1 DEBUG]Group = 10.106.67.91, IP = 10.106.67.91, Transmitting Proxy Id:
  Local subnet: 10.1.1.0 mask 255.255.255.0 Protocol 0 Port 0
  Remote subnet: 10.2.2.0 Mask 255.255.255.0 Protocol 0 Port 0
Mar 15 05:41:39 [IKEv1 DECODE]Group = 10.106.67.91, IP = 10.106.67.91, IKE Initiator sending Initial Co
Mar 15 05:41:39 [IKEv1 DEBUG]Group = 10.106.67.91, IP = 10.106.67.91, constructing qm hash payload
Mar 15 05:41:39 [IKEv1 DECODE]Group = 10.106.67.91, IP = 10.106.67.91, IKE Initiator sending 1st QM pkt
Mar 15 05:41:39 [IKEv1]IP = 10.106.67.91, IKE_DECODE SENDING Message (msgid=ad712fa9) with payloads : H
Mar 15 05:41:39 [IKEv1]IKE Receiver: Packet received on 10.106.67.90:500 from 10.106.67.91:500
Mar 15 05:41:39 [IKEv1]IP = 10.106.67.91, IKE_DECODE RECEIVED Message (msgid=ad712fa9) with payloads :
Mar 15 05:41:39 [IKEv1 DEBUG]Group = 10.106.67.91, IP = 10.106.67.91, processing hash payload
Mar 15 05:41:39 [IKEv1 DEBUG]Group = 10.106.67.91, IP = 10.106.67.91, processing SA payload
Mar 15 05:41:39 [IKEv1 DEBUG]Group = 10.106.67.91, IP = 10.106.67.91, processing nonce payload
Mar 15 05:41:39 [IKEv1 DEBUG]Group = 10.106.67.91, IP = 10.106.67.91, processing ke payload
Mar 15 05:41:39 [IKEv1 DEBUG]Group = 10.106.67.91, IP = 10.106.67.91, processing ISA_KE for PFS in phas
Mar 15 05:41:39 [IKEv1 DEBUG]Group = 10.106.67.91, IP = 10.106.67.91, processing ID payload
Mar 15 05:41:39 [IKEv1 DECODE]Group = 10.106.67.91, IP = 10.106.67.91, ID_IPV4_ADDR_SUBNET ID received-
Mar 15 05:41:39 [IKEv1 DEBUG]Group = 10.106.67.91, IP = 10.106.67.91, processing ID payload
Mar 15 05:41:39 [IKEv1 DECODE]Group = 10.106.67.91, IP = 10.106.67.91, ID_IPV4_ADDR_SUBNET ID received-
Mar 15 05:41:39 [IKEv1 DEBUG]Group = 10.106.67.91, IP = 10.106.67.91, loading all IPSEC SAs
Mar 15 05:41:39 [IKEv1 DEBUG]Group = 10.106.67.91, IP = 10.106.67.91, Generating Quick Mode Key!
Mar 15 05:41:39 [IKEv1 DEBUG]Group = 10.106.67.91, IP = 10.106.67.91, Generating Quick Mode Key!
Mar 15 05:41:39 [IKEv1]Group = 10.106.67.91, IP = 10.106.67.91, Security negotiation complete for LAN-t
Mar 15 05:41:39 [IKEv1 DEBUG]Group = 10.106.67.91, IP = 10.106.67.91, oakley constructing final quick m
Mar 15 05:41:39 [IKEv1 DECODE]Group = 10.106.67.91, IP = 10.106.67.91, IKE Initiator sending 3rd QM pkt
Mar 15 05:41:39 [IKEv1]IP = 10.106.67.91, IKE_DECODE SENDING Message (msgid=ad712fa9) with payloads : H
IPSEC INFO: Setting an IPSec timer of type SA Purge Timer for 30 seconds with a jitter value of 0
IPSEC INFO: IPSec SA PURGE timer started SPI 0x00024311
IPSEC: New embryonic SA created @ 0x00007f05294fd920,
  SCB         : 0x294CCDB0,
  Direction   : outbound
  SPI         : 0xEA689811
  Session ID  : 0x00002000
  VPIF num    : 0x00000002
  Tunnel type : l2l
  Protocol    : esp
  Lifetime    : 240 seconds
  SA handle   : 0x00024311
```

Rule Lookup for local 10.1.1.0 to remote 10.2.2.0

Peer matched map outside_map sequence 20

PROXY MATCH on crypto map outside_map seq 20

```
IPSEC DEBUG: Using NP outbound permit rule for SPI 0xEA689811
```

```
IPSEC: Completed host OBSA update, SPI 0xEA689811
IPSEC: Creating outbound VPN context, SPI 0xEA689811
  Flags  : 0x00000005
  SA     : 0x00007f05294fd920
  SPI    : 0xEA689811
  MTU    : 1500 bytes
  VCID   : 0x00000000
  Peer   : 0x00000000
  SCB    : 0x02CEE703
  Channel: 0x00007f0533c4f700
IPSEC: Completed outbound VPN context, SPI 0xEA689811
VPN handle: 0x000000000000763c
IPSEC: New outbound encrypt rule, SPI 0xEA689811
  Src addr: 10.1.1.0
  Src mask: 255.255.255.0
  Dst addr: 10.2.2.0
  Dst mask: 255.255.255.0
  Src ports
    Upper: 0
    Lower: 0
    Op : ignore
  Dst ports
    Upper: 0
    Lower: 0
    Op : ignore
  Protocol: 0
  Use protocol: false
  SPI: 0x00000000
  Use SPI: false
IPSEC: Completed outbound encrypt rule, SPI 0xEA689811
Rule ID: 0x00007f05294f8a60
IPSEC: New outbound permit rule, SPI 0xEA689811
  Src addr: 10.106.67.90
  Src mask: 255.255.255.255
  Dst addr: 10.106.67.91
  Dst mask: 255.255.255.255
  Src ports
    Upper: 0
    Lower: 0
    Op : ignore
  Dst ports
    Upper: 0
    Lower: 0
    Op : ignore
  Protocol: 50
  Use protocol: true
  SPI: 0xEA689811
  Use SPI: true
IPSEC: Completed outbound permit rule, SPI 0xEA689811
Rule ID: 0x00007f05294f9110
Mar 15 05:41:39 [IKEv1 DEBUG]Group = 10.106.67.91, IP = 10.106.67.91, IKE got a KEY_ADD msg for SA: SPI
IPSEC: New embryonic SA created @ 0x00007f05294f4620,
  SCB : 0x294CFE60,
  Direction : inbound
  SPI : 0x50EF49AD
  Session ID : 0x00002000
  VPIF num : 0x00000002
  Tunnel type: l2l
  Protocol : esp
  Lifetime : 240 seconds
  SA handle : 0x0001B739
Rule Lookup for local 10.1.1.0 to remote 10.2.2.0
```

```
Peer matched map outside_map sequence 20
PROXY MATCH on crypto map outside_map seq 20
IPSEC DEBUG: Using NP inbound permit rule for SPI 0x50EF49AD
IPSEC: Completed host IBSA update, SPI 0x50EF49AD
IPSEC: Creating inbound VPN context, SPI 0x50EF49AD
  Flags: 0x00000006
  SA : 0x00007f05294f4620
  SPI : 0x50EF49AD
  MTU : 0 bytes
  VCID : 0x00000000
  Peer : 0x0000763C
  SCB : 0x02CE8BB3
  Channel: 0x00007f0533c4f700
IPSEC: Completed inbound VPN context, SPI 0x50EF49AD
VPN handle: 0x00000000000086bc
IPSEC: Updating outbound VPN context 0x0000763C, SPI 0xEA689811
  Flags: 0x00000005
  SA : 0x00007f05294fd920
  SPI : 0xEA689811
  MTU : 1500 bytes
  VCID : 0x00000000
  Peer : 0x000086BC
  SCB : 0x02CEE703
  Channel: 0x00007f0533c4f700
IPSEC: Completed outbound VPN context, SPI 0xEA689811
VPN handle: 0x000000000000763c
IPSEC: Completed outbound inner rule, SPI 0xEA689811
Rule ID: 0x00007f05294f8a60
IPSEC: Completed outbound outer SPD rule, SPI 0xEA689811
Rule ID: 0x00007f05294f9110
IPSEC: New inbound tunnel flow rule, SPI 0x50EF49AD
  Src addr: 10.2.2.0
  Src mask: 255.255.255.0
  Dst addr: 10.1.1.0
  Dst mask: 255.255.255.0
  Src ports
    Upper: 0
    Lower: 0
    Op : ignore
  Dst ports
    Upper: 0
    Lower: 0
    Op : ignore
    Protocol: 0
  Use protocol: false
  SPI: 0x00000000
  Use SPI: false
IPSEC: Completed inbound tunnel flow rule, SPI 0x50EF49AD
Rule ID: 0x00007f05294f8180
IPSEC: New inbound decrypt rule, SPI 0x50EF49AD
  Src addr: 10.106.67.91
  Src mask: 255.255.255.255
  Dst addr: 10.106.67.90
  Dst mask: 255.255.255.255
  Src ports
    Upper: 0
    Lower: 0
    Op : ignore
  Dst ports
    Upper: 0
    Lower: 0
    Op : ignore
  Protocol: 50
  Use protocol: true
  SPI: 0x50EF49AD
  Use SPI: true
IPSEC: Completed inbound decrypt rule, SPI 0x50EF49AD
Rule ID: 0x00007f05294f7ad0
IPSEC: New inbound permit rule, SPI 0x50EF49AD
  Src addr: 10.106.67.91
  Src mask: 255.255.255.255
  Dst addr: 10.106.67.90
  Dst mask: 255.255.255.255
  Src ports
    Upper: 0
    Lower: 0
    Op : ignore
  Dst ports
    Upper: 0
    Lower: 0
    Op : ignore
  Protocol: 50
  Use protocol: true
  SPI: 0x50EF49AD
  Use SPI: true
IPSEC: Completed inbound permit rule, SPI 0x50EF49AD
Rule ID: 0x00007f05294f4510
IPSEC INFO: Destroying an IPSec timer of type SA Purge Timer
IPSEC INFO: Destroying an IPSec timer of type SA Purge Timer
Mar 15 05:41:39 [IKEv1 DEBUG]Group = 10.106.67.91, IP = 10.106.67.91, Pitcher: received KEY_UPDATE, spi
Mar 15 05:41:39 [IKEv1 DEBUG]Group = 10.106.67.91, IP = 10.106.67.91, Starting P2 rekey timer: 24480 se

Mar 15 05:41:39 [IKEv1]Group = 10.106.67.91, IP = 10.106.67.91, PHASE 2 COMPLETED (msgid=ad712fa9)
```