

Configure a Site-to-Site IPSec IKEv1 Tunnel Between ASA and Cisco IOS XE Router

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Components Used](#)

[Configure](#)

[Network Diagram](#)

[ASA Configuration](#)

[Configure the ASA Interfaces](#)

[Configure the IKEv1 Policy and Enable IKEv1 on the Outside Interface](#)

[Configure the Tunnel Group \(LAN-to-LAN Connection Profile\)](#)

[Configure the ACL for the VPN Traffic of Interest](#)

[Configure a NAT Exemption](#)

[Configure the IKEv1 Transform Set](#)

[Configure a Crypto Map and Apply it to an Interface](#)

[ASA Final Configuration](#)

[Cisco IOS XE Router CLI Configuration](#)

[Configure the Interfaces](#)

[Configure the ISAKMP \(IKEv1\) Policy](#)

[Configure a Crypto ISAKMP Key](#)

[Configure an ACL for VPN Traffic of Interest](#)

[Configure a NAT Exemption](#)

[Configure a Transform Set](#)

[Configure a Crypto Map and Apply it to an Interface](#)

[Cisco IOS XE Final Configuration](#)

[Verify](#)

[Phase 1 Verification](#)

[Phase 2 Verification](#)

[Phase 1 and 2 Verification](#)

[Troubleshoot](#)

[IPSec LAN-to-LAN Checker Tool](#)

[ASA Debugs](#)

[Cisco IOS XE Router Debugs](#)

[References](#)

Introduction

This document describes how to configure a site-to-site IKEv1 tunnel via the CLI between a Cisco ASA and

a router that runs Cisco IOS XE software.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Cisco IOS XE
- Cisco Adaptive Security Appliance (ASA)
- General IPsec concepts

Components Used

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

- Cisco ASA running ciscosoft Version 9.20(2)2
- Cisco CSR running Cisco IOS XE software Version 17.03.03

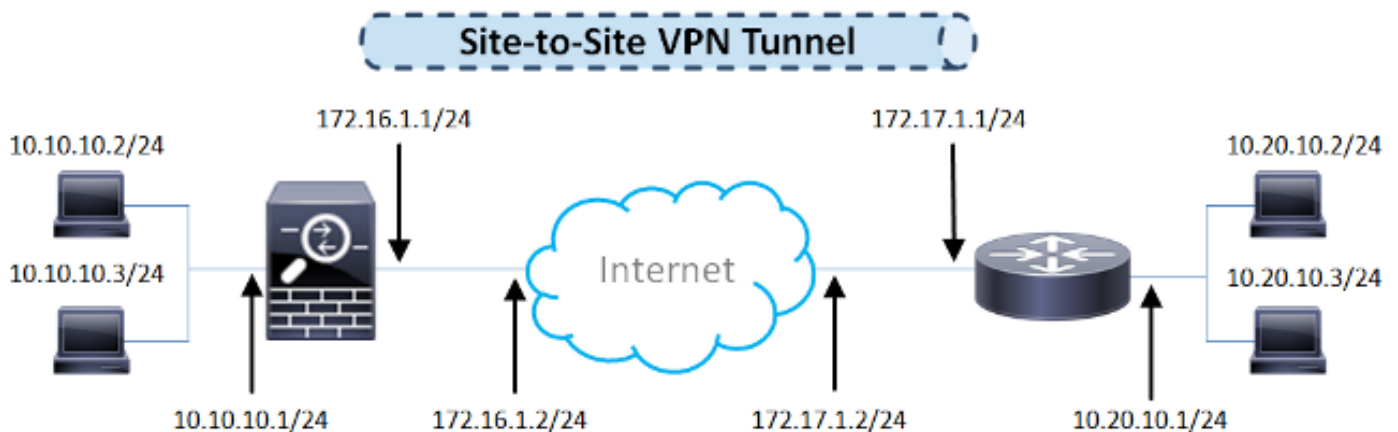
The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Configure

This section describes how to complete the ASA and Cisco IOS XE router CLI 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 the security-levels:

```
interface GigabitEthernet0/0
 nameif outside
 security-level 0
 ip address 172.16.1.1 255.255.255.0
!
interface GigabitEthernet0/1
 nameif inside
 security-level 100
 ip address 10.10.10.1 255.255.255.0
```

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

Configure the IKEv1 Policy and Enable IKEv1 on the Outside Interface


In order to configure the Internet Security Association and Key Management Protocol (ISAKMP) policies for the IPsec Internet Key Exchange Version 1 (IKEv1) connections, enter the `crypto ikev1 policy`

`<priority>` command:

```
<#root>
```

```
crypto ikev1 policy 10
```

```
 authentication pre-share
 encryption aes-256
 hash sha
 group 14
 lifetime 86400
```

 **Note:** An IKEv1 policy match exists when both of the policies from the two peers contain the same authentication, encryption, hash, and Diffie-Hellman parameter values. For IKEv1, the remote peer policy must also specify a lifetime less than or equal to the lifetime in the policy that the initiator sends. If the lifetimes are not identical, then the ASA uses the shorter lifetime.

 **Note:** If you do not specify a value for a given policy parameter, the default value is applied.

You must enable IKEv1 on the interface that terminates the VPN tunnel. Typically, this is the outside (or public) interface. In order to enable IKEv1, enter the `crypto ikev1 enable <interface-name>` command in global configuration mode:

```
<#root>
```

```
crypto ikev1 enable outside
```

Configure the Tunnel Group (LAN-to-LAN Connection Profile)

For a LAN-to-LAN tunnel, the connection profile type is `ipsec-l2l` . In order to configure the IKEv1 pre-shared key, enter the `tunnel-group ipsec-attributes` configuration mode:

```
tunnel-group 172.17.1.1 type ipsec-l2l
tunnel-group 172.17.1.1 ipsec-attributes
 ikev1 pre-shared-key cisco123
```

Configure the ACL for the VPN Traffic of Interest

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.


```
<#root>
object-group network
local-network


network-object 10.10.10.0 255.255.255.0
object-group network
remote-network


network-object 10.20.10.0 255.255.255.0

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


object-group
remote-network
```

 **Note:** An ACL for VPN traffic uses the source and destination IP addresses after Network Address Translation (NAT).

 **Note:** An ACL for VPN traffic must be mirrored on both of the VPN peers.

 **Note:** If there is a need to add a new subnet to the protected traffic, simply add a subnet/host to the respective object group and complete a mirror change on the remote VPN peer.

Configure a NAT Exemption

 **Note:** The configuration that is described in this section is optional.

Typically, there must be no NAT performed on the VPN traffic. In order to exempt that traffic, you must create an identity NAT rule. The identity NAT rule simply translates an address to the same address.

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

Configure the IKEv1 Transform Set

An IKEv1 transform set is a combination of security protocols and algorithms that define the way that the ASA protects data. During IPsec Security Association (SA) negotiations, the peers must identify a transform set or proposal that is the same for both of the peers. The ASA then applies the matched transform set or proposal in order to create an SA that protects data flows in the access list for that crypto map.

In order to configure the IKEv1 transform set, enter the `crypto ipsec ikev1 transform-set` command:

```
<#root>
crypto ipsec ikev1 transform-set ESP-AES256-SHA esp-aes-256 esp-sha-hmac
```

Configure a Crypto Map and Apply it to an Interface

A crypto map defines an IPsec policy to be negotiated in the IPsec SA and includes:

- An access list in order to identify the packets that the IPsec connection permits and protects
- Peer identification
- A local address for the IPsec traffic

- The IKEv1 transform sets
- Perfect Forward Secrecy (Optional)

Here is an example:

```
crypto map outside_map 10 match address asa-router-vpn
crypto map outside_map 10 set peer 172.17.1.1
crypto map outside_map 10 set ikev1 transform-set ESP-AES256-SHA
```

You can then apply the crypto map to the interface:

```
<#root>
crypto map outside_map interface outside
```

ASA Final Configuration

Here is the final configuration of the ASA:

```
interface GigabitEthernet0/0
 nameif outside
 security-level 0
 ip address 172.16.1.1 255.255.255.0
!
interface GigabitEthernet0/1
 nameif inside
 security-level 100
 ip address 10.10.10.1 255.255.255.0
!
object-group network local-network
 network-object 10.10.10.0 255.255.255.0
object-group network remote-network
 network-object 10.20.10.0 255.255.255.0
!
access-list asa-router-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 ikev1 policy 10
 authentication pre-share
 encryption aes-256
 hash sha
 group 14
```

```

lifetime 86400
!
crypto ikev1 enable outside
!
crypto ipsec ikev1 transform-set ESP-AES256-SHA esp-aes-256 esp-sha-hmac
!
crypto map outside_map 10 match address asa-router-vpn
crypto map outside_map 10 set peer 172.17.1.1
crypto map outside_map 10 set ikev1 transform-set ESP-AES256-SHA
crypto map outside_map interface outside
!
tunnel-group 172.17.1.1 type ipsec-l2l
tunnel-group 172.17.1.1 ipsec-attributes
 ikev1 pre-shared-key cisco123
!

```

Cisco IOS XE Router CLI Configuration

Configure the Interfaces

If the Cisco IOS XE router interfaces are not yet configured, then at least the LAN and WAN interfaces must be configured. Here is an example:

```

interface GigabitEthernet0/0
 ip address 172.17.1.1 255.255.255.0
 no shutdown
!
interface GigabitEthernet0/1
 ip address 10.20.10.1 255.255.255.0
 no shutdown

```

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

Configure the ISAKMP (IKEv1) Policy

In order to configure the ISAKMP policies for the IKEv1 connections, enter the `crypto isakmp policy <priority>` command in global configuration mode. Here is an example:

```


<#root>

crypto isakmp policy 10

 encryption aes 256
 hash sha

```

```
authentication pre-share
group 14
```

 **Note:** You can configure multiple IKE policies on each peer that participates in IPsec. When the IKE negotiation begins, it attempts to find a common policy that is configured on both of the peers, and it starts with the highest priority policies that are specified on the remote peer.

Configure a Crypto ISAKMP Key


In order to configure a preshared authentication key, enter the `crypto isakmp key` command in global configuration mode:


```
<#root>
crypto isakmp key cisco123 address 172.16.1.1
```

Configure an ACL for VPN Traffic of Interest


Use the extended or named access list in order to specify the traffic that must be protected by encryption. Here is an example:

```
access-list 110 remark Interesting traffic access-list
access-list 110 permit ip 10.20.10.0 0.0.0.255 10.10.10.0 0.0.0.255
```

 **Note:** An ACL for VPN traffic uses the source and destination IP addresses after NAT.

 **Note:** An ACL for VPN traffic must be mirrored on both of the VPN peers.

Configure a NAT Exemption

 **Note:** The configuration that is described in this section is optional.

Typically, there must be no NAT performed on the VPN traffic. If the NAT overload is used, then a route-map must be used in order to exempt the VPN traffic of interest from translation. Notice that in the access-list that is used in the route-map, the VPN traffic of interest must be denied.

```
access-list 111 remark NAT exemption access-list
```



```
access-list 111 deny ip 10.20.10.0 0.0.0.255 10.10.10.0 0.0.0.255
access-list 111 permit ip 10.20.10.0 0.0.0.255 any

route-map nonat permit 10
 match ip address 111

ip nat inside source route-map nonat interface GigabitEthernet0/0 overload
```

Configure a Transform Set

In order to define an IPsec transform set (an acceptable combination of security protocols and algorithms), enter the `crypto ipsec transform-set` command in global configuration mode. Here is an example:

```
<#root>

crypto ipsec transform-set ESP-AES256-SHA esp-aes 256 esp-sha-hmac

mode tunnel
```

Configure a Crypto Map and Apply it to an Interface

In order to create or modify a crypto map entry and enter the crypto map configuration mode, enter the **crypto map** global configuration command. In order for the crypto map entry to be complete, there are some aspects that must be defined at a minimum:

- The IPsec peers to which the protected traffic can be forwarded must be defined. These are the peers with which an SA can be established. In order to specify an IPsec peer in a crypto map entry, enter the `set peer` command.
- The transform sets that are acceptable for use with the protected traffic must be defined. In order to specify the transform sets that can be used with the crypto map entry, enter the `set transform-set` command.
- The traffic that must be protected must be defined. In order to specify an extended access list for a crypto map entry, enter the `match address` command.

Here is an example:

```
<#root>

crypto map outside_map 10 ipsec-isakmp

set peer 172.16.1.1
set transform-set ESP-AES256-SHA
match address 110
```

The final step is to apply the previously defined crypto map set to an interface. In order to apply this, enter the `crypto map` interface configuration command:

```
<#root>
interface GigabitEthernet0/0

crypto map outside_map
```

Cisco IOS XE Final Configuration


Here is the final Cisco IOS XE router CLI configuration:

```
crypto isakmp policy 10
  encryption aes 256
  authentication pre-share
  group 14
crypto isakmp key cisco123 address 172.16.1.1
!
crypto ipsec transform-set ESP-AES256-SHA esp-aes 256 esp-sha-hmac
mode tunnel
!
crypto map outside_map 10 ipsec-isakmp
  set peer 172.16.1.1
  set transform-set ESP-AES256-SHA
  match address 110
!
interface GigabitEthernet0/0
  ip address 172.17.1.1 255.255.255.0
  ip nat outside
  ip virtual-reassembly in
  duplex auto
  speed auto
  crypto map outside_map
!
interface GigabitEthernet0/1
  ip address 10.20.10.1 255.255.255.0
  ip nat inside
  ip virtual-reassembly in
  duplex auto
  speed auto
!
ip nat inside source route-map nonat interface GigabitEthernet0/0 overload
!
route-map nonat permit 10
  match ip address 111
!
access-list 110 remark Interesting traffic access-list
access-list 110 permit ip 10.20.10.0 0.0.0.255 10.10.10.0 0.0.0.255
access-list 111 remark NAT exemption access-list
```

```
access-list 111 deny ip 10.20.10.0 0.0.0.255 10.10.10.0 0.0.0.255
access-list 111 permit ip 10.20.10.0 0.0.0.255 any
```

Verify

Before you verify whether the tunnel is up and that it passes the traffic, you must ensure that the traffic of interest is sent toward either the ASA or the Cisco IOS XE router.

 **Note:** On the ASA, the packet-tracer tool that matches the traffic of interest can be used in order to initiate the IPsec tunnel (such as `packet-tracer input inside tcp 10.10.10.10 12345 10.20.10.10 80` detailed for example).

Phase 1 Verification

In order to verify whether IKEv1 Phase 1 is up on the ASA, enter the **show crypto isakmp sa** command. The expected output is to see the MM_ACTIVE state:

```
<#root>
```

```
ciscoasa#
```

```
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: 172.17.1.1
```

```
Type : L2L
```

```
Role : responder
```

```
Rekey : no
```

```
State : MM_ACTIVE
```

```
There are no IKEv2 SAs
```

```
ciscoasa#
```

In order to verify whether the IKEv1 Phase 1 is up on the Cisco IOS XE, enter the `show crypto isakmp sa` command. The expected output is to see the ACTIVE state:

```
<#root>
```

```
Router#
```

```
show crypto isakmp sa
```


```
IPv4 Crypto ISAKMP SA
dst          src          state          conn-id status
172.16.1.1   172.17.1.1   QM_IDLE       2003 ACTIVE
```

```
IPv6 Crypto ISAKMP SA
```

```
Router#
```

Phase 2 Verification

In order to verify whether IKEv1 Phase 2 is up on the ASA, enter the `show crypto ipsec sa` command. The expected output is to see both the inbound and outbound Security Parameter Index (SPI). If the traffic passes through the tunnel, you must see the encaps/decaps counters increment.

 **Note:** For each ACL entry, a separate inbound/outbound SA is created, which can result in a long `show crypto ipsec sa` command output (dependent upon the number of ACE entries in the crypto ACL).

Here is an example:

```
<#root>
ciscoasa#
show crypto ipsec sa peer 172.17.1.1

peer address: 172.17.1.1
  Crypto map tag: outside_map, seq num: 10, local addr: 172.16.1.1

access-list asa-router-vpn extended permit ip 10.10.10.0 255.255.255.0
  10.20.10.0 255.255.255.0
    local ident (addr/mask/prot/port): (10.10.10.0/255.255.255.0/0/0)
    remote ident (addr/mask/prot/port): (10.20.10.0/255.255.255.0/0/0)
    current_peer: 172.17.1.1

#pkts encaps: 989, #pkts encrypt: 989, #pkts digest: 989
#pkts decaps: 989, #pkts decrypt: 989, #pkts verify: 989
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 989, #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.: 172.16.1.1/0, remote crypto endpt.: 172.17.1.1/0
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: 5397114D
current inbound spi : 9B592959

inbound esp sas:
spi: 0x9B592959 (2606311769)
```

```
SA State: active
transform: esp-aes-256 esp-sha-hmac no compression
in use settings ={L2L, Tunnel, IKEv1, }
slot: 0, conn_id: 2, crypto-map: outside_map
sa timing: remaining key lifetime (kB/sec): (4373903/3357)
IV size: 16 bytes
replay detection support: Y
Anti replay bitmap:
0xFFFFFFFF 0xFFFFD7FF
```

```
outbound esp sas:
spi: 0x5397114D (1402409293)
SA State: active
transform: esp-aes-256 esp-sha-hmac no compression
in use settings ={L2L, Tunnel, IKEv1, }
slot: 0, conn_id: 2, crypto-map: outside_map
sa timing: remaining key lifetime (kB/sec): (4373903/3357)
IV size: 16 bytes
replay detection support: Y
Anti replay bitmap:
0x00000000 0x00000001
```

```
ciscoasa#
```

In order to verify whether IKEv1 Phase 2 is up on the Cisco IOS XE, enter the `show crypto ipsec sa` command. The expected output is to see both the inbound and outbound SPI. If the traffic passes through the tunnel, you must see the encaps/decaps counters increment.

Here is an example:

```
<#root>
```

```
Router#
```

```
show crypto ipsec sa peer 172.16.1.1
```

```
interface: GigabitEthernet0/0
  Crypto map tag: outside_map, local addr 172.17.1.1

  protected vrf: (none)
local ident (addr/mask/prot/port): (10.20.10.0/255.255.255.0/0/0)
remote ident (addr/mask/prot/port): (10.10.10.0/255.255.255.0/0/0)
current_peer 172.16.1.1 port 500
  PERMIT, flags={origin_is_acl,}
#pkts encaps: 989, #pkts encrypt: 989, #pkts digest: 989
#pkts decaps: 989, #pkts decrypt: 989, #pkts verify: 989
#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.: 172.17.1.1, remote crypto endpt.: 172.16.1.1
plaintext mtu 1438, path mtu 1500, ip mtu 1500, ip mtu idb GigabitEthernet3
current outbound spi: 0x9B592959(2606311769)
PFS (Y/N): N, DH group: none
```

```
inbound esp sas:
spi: 0x5397114D(1402409293)
transform: esp-256-aes esp-sha-hmac ,
in use settings ={Tunnel, }
conn id: 2003, flow_id: CSR:3, sibling_flags FFFFFFFF80004048, crypto map: outside_map
sa timing: remaining key lifetime (k/sec): (4607857/3385)
IV size: 16 bytes
replay detection support: Y
Status: ACTIVE(ACTIVE)
```

inbound ah sas:

inbound pcg sas:

```
outbound esp sas:
spi: 0x9B592959(2606311769)
transform: esp-256-aes esp-sha-hmac ,
in use settings ={Tunnel, }
conn id: 2004, flow_id: CSR:4, sibling_flags FFFFFFFF80004048, crypto map: outside_map
sa timing: remaining key lifetime (k/sec): (4607901/3385)
IV size: 16 bytes
replay detection support: Y
Status: ACTIVE(ACTIVE)
```

outbound ah sas:

outbound pcg sas:

Router#

Phase 1 and 2 Verification

This section describes the commands that you can use on the ASA or Cisco IOS XE in order to verify the details for both Phases 1 and 2.

Enter the `show vpn-sessiondb` command on the ASA for verification:

<#root>

ciscoasa#

```
show vpn-sessiondb detail l2l filter ipaddress 172.17.1.1
```

Session Type: LAN-to-LAN Detailed

```
Connection   : 172.17.1.1
Index        : 2                               IP Addr      : 172.17.1.1
Protocol     : IKEv1 IPsec
Encryption   : IKEv1: (1)AES256 IPsec: (1)AES256
Hashing      : IKEv1: (1)SHA1 IPsec: (1)SHA1
Bytes Tx     : 98900                            Bytes Rx     : 134504
Login Time   : 06:15:52 UTC Fri Sep 6 2024
```

Duration : 0h:15m:07s

IKEv1 Tunnels: 1

IPsec Tunnels: 1

IKEv1:

Tunnel ID : 2.1

UDP Src Port : 500

IKE Neg Mode : Main

Encryption : AES256

Rekey Int (T): 86400 Seconds

D/H Group : 14

Filter Name :

UDP Dst Port : 500

Auth Mode : preSharedKeys

Hashing : SHA1

Rekey Left(T): 84093 Seconds

IPsec:

Tunnel ID : 2.2

Local Addr : 10.10.10.0/255.255.255.0/0/0

Remote Addr : 10.20.10.0/255.255.255.0/0/0

Encryption : AES256

Encapsulation: Tunnel

Rekey Int (T): 3600 Seconds

Rekey Int (D): 4608000 K-Bytes

Idle Time Out: 30 Minutes

Bytes Tx : 98900

Pkts Tx : 989

Hashing : SHA1

Rekey Left(T): 3293 Seconds

Rekey Left(D): 4607901 K-Bytes

Idle TO Left : 26 Minutes

Bytes Rx : 134504

Pkts Rx : 989

NAC:

Reval Int (T): 0 Seconds

SQ Int (T) : 0 Seconds

Hold Left (T): 0 Seconds

Redirect URL :

Reval Left(T): 0 Seconds

EoU Age(T) : 309 Seconds

Posture Token:

ciscoasa#

Enter the show crypto session command on the Cisco IOS XE for verification:

<#root>

Router#

show crypto session remote 172.16.1.1 detail

Crypto session current status

Code: C - IKE Configuration mode, D - Dead Peer Detection

K - Keepalives, N - NAT-traversal, T - cTCP encapsulation

X - IKE Extended Authentication, F - IKE Fragmentation

Interface: GigabitEthernet0/0

Uptime: 00:03:36

Session status: UP-ACTIVE

Peer: 172.16.1.1 port 500 fvrf: (none) ivrf: (none)

Phase1_id: 172.16.1.1

Desc: (none)

IKE SA: local 172.17.1.1/500 remote 172.16.1.1/500 Active

Capabilities:(none) connid:1005 lifetime:23:56:23

IPSEC FLOW: permit ip 10.20.10.0/255.255.255.0 10.10.10.0/255.255.255.0

```
Active SAs: 2, origin: crypto map
Inbound: #pkts dec'ed 989 drop 0 life (KB/Sec) 4449870/3383
Outbound: #pkts enc'ed 989 drop 0 life (KB/Sec) 4449868/3383
```

Router#

Troubleshoot

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

 **Note:** Refer to the [Important Information on Debug Commands](#) and [IP Security Troubleshooting - Understanding and Using debug Commands](#) Cisco documents before you use debug commands.

IPSec LAN-to-LAN Checker Tool


In order to automatically verify whether the IPSec LAN-to-LAN configuration between the ASA and Cisco IOS XE is valid, you can use the [IPSec LAN-to-LANChecker](#) tool. The tool is designed so that it accepts a `show tech` or `show running-config` command from either an ASA or Cisco IOS XE router. It examines the configuration and attempts to detect whether a crypto map-based LAN-to-LAN IPSec tunnel is configured. If configured, it performs a multi-point check of the configuration and highlights any configuration errors and settings for the tunnel that would be negotiated.

ASA Debugs

In order to troubleshoot IPSec IKEv1 tunnel negotiation on an ASA firewall, you can use these debug commands:

```
<#root>
```

```
debug crypto ipsec 127
debug crypto isakmp 127
debug ike-common 10
```

 **Note:** If the number of VPN tunnels on the ASA is significant, the `debug crypto condition peer A.B.C.D` command must be used before you enable the debugs in order to limit the debug outputs to include only the specified peer.

Cisco IOS XE Router Debugs


In order to troubleshoot IPSec IKEv1 tunnel negotiation on a Cisco IOS XE router, you can use these debug commands:

```
<#root>
```



```
debug crypto ipsec
debug crypto isakmp
```

 **Note:** If the number of VPN tunnels on the Cisco IOS XE is significant, the `debug crypto condition peer ipv4 A.B.C.D` must be used before you enable the debugs in order to limit the debug outputs to include only the specified peer.

 **Tip:** Refer to the [Most Common L2L and Remote Access IPsec VPN Troubleshooting Solutions](#) Cisco document for more information about how to troubleshoot a site-to-site VPN.

References

- [Important Information on Debug Commands](#)
- [IP Security Troubleshooting - Understanding and Using debug Commands](#)
- [Most Common L2L and Remote Access IPsec VPN Troubleshooting Solutions](#)
- [IPsec LAN-to-LAN Checker](#)
- [Technical Support & Documentation - Cisco Systems](#)