

Understand IPsec IKEv1 Protocol

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Components Used](#)

[Background Information](#)

[IPsec](#)

[IKE Protocol](#)

[IKE Phases](#)

[IKE Modes \(Phase 1\)](#)

[Main Mode](#)

[Aggressive Mode](#)

[IPsec Mode \(Phase 2\)](#)

[Quick Mode](#)

[IKE Glossary](#)

[Main Mode Packet Exchange](#)

[Main Mode 1 \(MM1\)](#)

[Identify Two Simultaneous Negotiations](#)

[Main Mode 2 \(MM2\)](#)

[Main Mode 3 and 4 \(MM3-MM4\)](#)

[Main Mode 5 and 6 \(MM5-MM6\)](#)

[Quick Mode \(QM1, QM2, and QM3\)](#)

[Aggressive Mode Packet Exchange](#)

[Main Mode vs Aggressive Mode](#)

[IKEv2 vs IKEv1 Packet Exchange](#)

[Policy-Based vs Route-based](#)

[Policy-Based VPN](#)

[Route-Based VPN](#)

[Common Issues for Traffic Does Not Receive through the VPN](#)

[ISP Blocks UDP 500/4500](#)

[ISP Blocks ESP](#)

[Related Information](#)

Introduction

This document describes the Internet Key Exchange (IKEv1) protocol process for a Virtual Private Network (VPN) establishment.

Prerequisites

Requirements

Cisco recommends that you have knowledge of basic security concepts:

- Authentication
- Confidentiality
- Integrity
- IPsec

Components Used

This document is not restricted to specific software and hardware versions.

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.

Background Information

Internet Key Exchange (IKEv1) protocol process for a Virtual Private Network (VPN) establishment is important to understand the packet exchange for simpler troubleshooting any kind of Internet Protocol Security (IPsec) issue with IKEv1.

IPsec

IPsec is a suite of protocols that provides security to Internet communications at the IP layer. The most common current use of IPsec is to provide a Virtual Private Network (VPN), either between two locations (gateway-to-gateway) or between a remote user and an enterprise network (host-to-gateway).

IKE Protocol

IPsec uses the IKE protocol to negotiate and establish secured site-to-site or remote access virtual private network (VPN) tunnels. IKE protocol is also called the Internet Security Association and Key Management Protocol (ISAKMP) (Only in Cisco).

There are two versions of IKE:

- IKEv1: Defined in RFC 2409, The Internet Key Exchange
- IKE version 2 (IKEv2): Defined in RFC 4306, Internet Key Exchange (IKEv2) Protocol

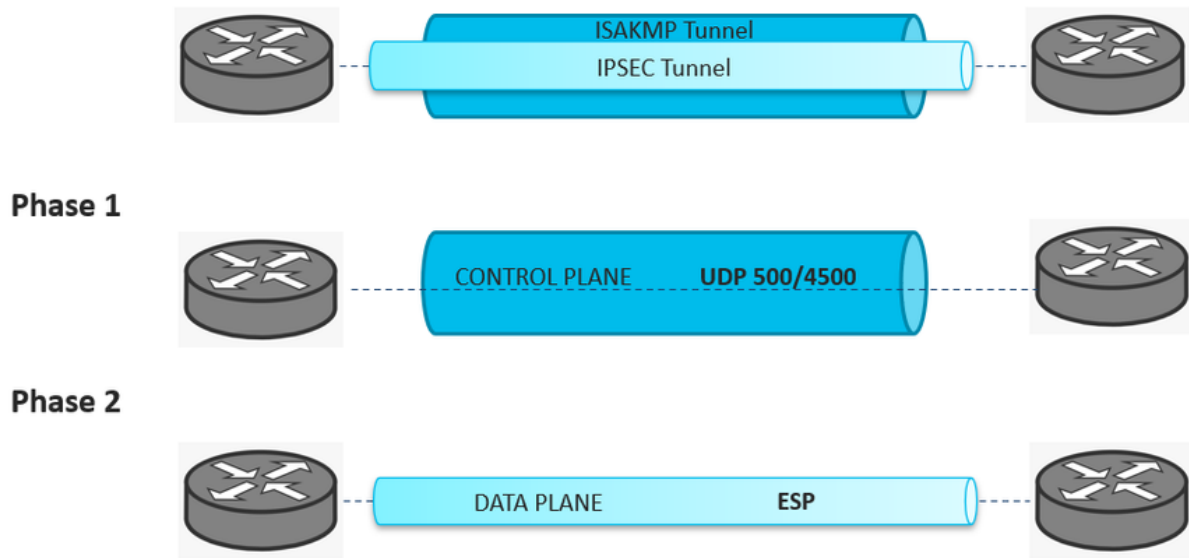
IKE Phases


ISAKMP separates negotiation into two phases:


- Phase 1: The two ISAKMP peers establish a secure and authenticated tunnel, which protects ISAKMP negotiation messages. This tunnel is known as the ISAKMP SA. There are two modes defined by ISAKMP: Main Mode (MM) and Aggressive Mode.
- Phase 2: It negotiates key materials and algorithms for the encryption (SAs) of the data to be transferred over the IPsec tunnel. This phase is called Quick Mode.

To materialize all the abstract concepts, the Phase 1 tunnel is the Parent tunnel and phase 2 is a sub tunnel. This image illustrates the two phases as tunnels:

ISAKMP-IPSEC Tunnel



 **Note:** Phase 1 (ISAKMP) Tunnel protects the Control Plane VPN traffic between the two gateways. Control Plane traffic can be Negotiation packets, information packages, DPD, keepalives, rekey, and so on. ISAKMP negotiation uses the UDP 500 and 4500 ports to establish a secure channel.

 **Note:** Phase 2 (IPsec) Tunnel protects the Data Plane traffic that passes through the VPN between the two gateways. The algorithms used to protect the data are configured in Phase 2 and are independent of those specified in Phase 1. The protocol used to encapsulate and encrypt these packets is the Encapsulation Security Payload (ESP).

IKE Modes (Phase 1)

Main Mode

An IKE session begins when the initiator sends a proposal or proposal to the responder. The first exchange between nodes establishes the basic security policy; the initiator proposes the encryption and authentication algorithms to be used. The responder chooses the appropriate proposal (assume a proposal is chosen) and sends it to the initiator. The next exchange passes Diffie-Hellman public keys and other data. All further negotiation is encrypted within the IKE SA. The third exchange authenticates the ISAKMP session. Once the IKE SA is established, IPsec negotiation (Quick Mode) begins.

Aggressive Mode

Aggressive Mode squeezes the IKE SA negotiation into three packets, with all data required for the SA passed by the initiator. The responder sends the proposal, key material, and ID, and authenticates the session in the next packet. The initiator replies and authenticates the session. Negotiation is quicker, and the initiator and responder ID pass in the clear.

IPsec Mode (Phase 2)

Quick Mode

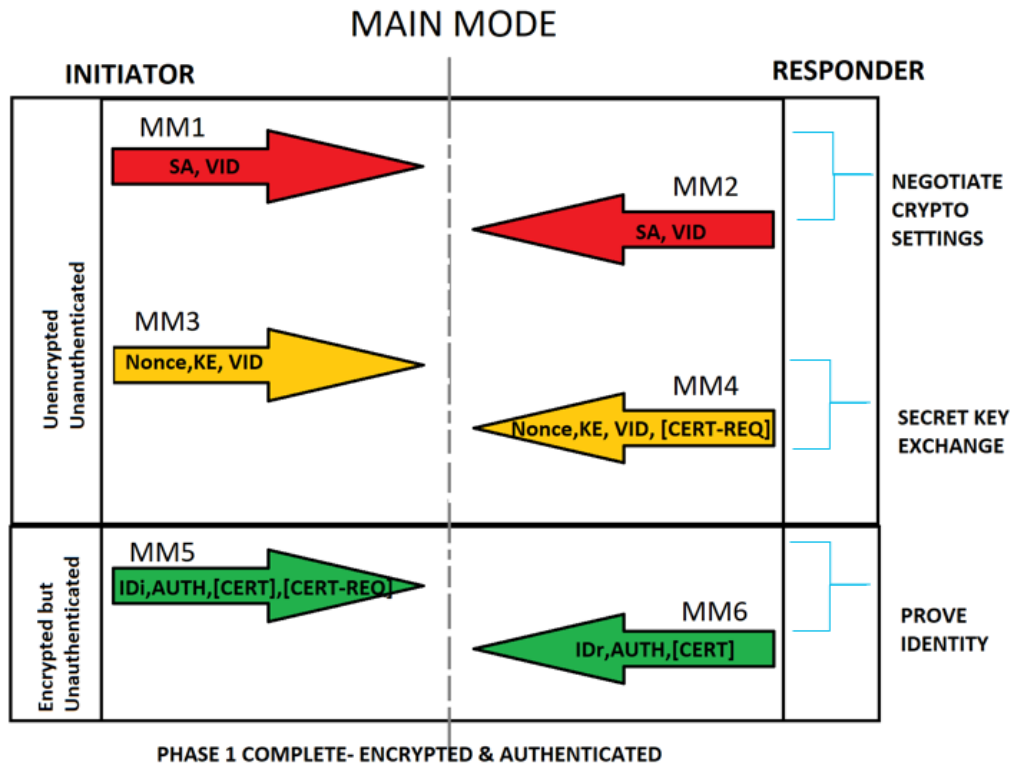
IPSec negotiation, or Quick Mode, is similar to an Aggressive Mode IKE negotiation, except negotiation, must be protected within an IKE SA. Quick Mode negotiates the SA for the data encryption and manages the key exchange for that IPSec SA.

IKE Glossary

- A security association (SA) is the establishment of shared security attributes between two network entities to support secure communication. An SA includes attributes such as cryptographic algorithm and mode; traffic encryption key; and parameters for the network data to be passed over the connection.
- The vendor IDs (VID) are processed to determine whether the peer supports the NAT-Traversal, Dead Peer Detection feature, Fragmentation, and so on.
- Nonce: a randomly generated number that the initiator sends. This nonce is hashed along with the other items with the agreed key used and is sent back. The initiator checks the cookie and the nonce and rejects any messages which do not have the right nonce. This helps prevent replay since no third party can predict what the randomly generated nonce is.
- Key-exchange (KE) information for the Diffie-Hellman (DH) secure key-exchange process.
- Identity Initiator/responder (IDi/IDr) is used to send out authentication information to the peer. This information is transmitted under the protection of the common shared secret.
- Diffie–Hellman (DH) key exchange is a method of securely cryptographic algorithms exchange over a public channel.
- The IPSec shared key can be derived with the DH used again to ensure Perfect Forward Secrecy (PFS) or the original DH exchange refreshed to the shared secret derived previously.

Main Mode Packet Exchange

Each ISAKMP packet contains payload information for the tunnel establishment. The IKE glossary explains the IKE abbreviations as part of the payload content for the packet exchange on Main Mode as shown in this image.

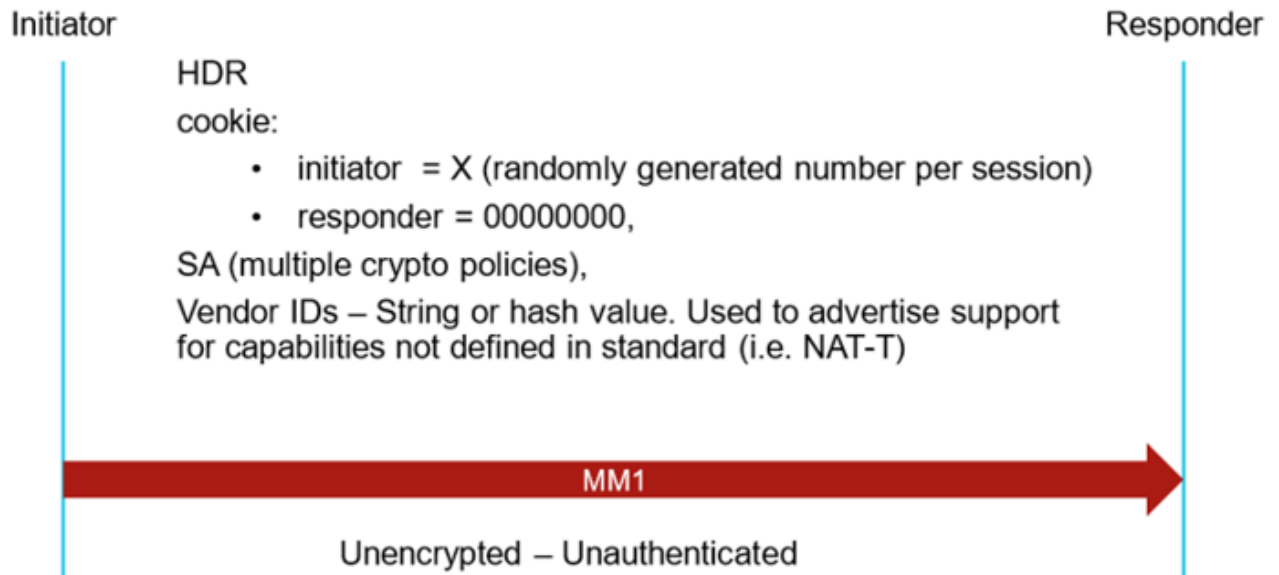


Main Mode 1 (MM1)

To set the terms of the ISAKMP negotiations, you create an ISAKMP policy, which includes:

- An authentication method, to ensure the identity of the peers.
- An encryption method, to protect the data and ensure privacy.
- A Hashed Message Authentication Codes (HMAC) method to ensure the identity of the sender, and to ensure that the message has not been modified in transit.
- A Diffie-Hellman group to determine the strength of the encryption-key-determination algorithm. The security appliance uses this algorithm to derive the encryption and hash keys.
- A limit to the time the security appliance uses an encryption key before it gets replaced.

The first packet is sent by the Initiator of the IKE negotiation as shown in the image:



Note: The Main Mode 1 is the first packet of the IKE negotiation. Therefore, the Initiator SPI is set to a random value while Responder SPI is set to 0. In the second packet (MM2) the Responder SPI must be replied to with a new value and the entire negotiation maintains the same SPIs values.

If the MM1 is captured and a Wireshark network protocol analyzer is used, the SPI value is within the Internet Security Association and Key Management Protocol content as shown in the image:

```
> Ethernet II, Src: 00:00:00_00:00:00 (00:00:00:00:00:00), Dst: 00:00:00_00:00:00 (00:00:00:00:00:00)
> Internet Protocol Version 4, Src: 170.49.116.200, Dst: 209.134.162.150
> User Datagram Protocol, Src Port: 500, Dst Port: 500
v Internet Security Association and Key Management Protocol
  Initiator SPI: 6f80c0380ef6bdfd
  Responder SPI: 0000000000000000
  Next payload: Security Association (33)
```

Note: In the case, the MM1 packet gets lost in the path or there is no MM2 reply, the IKE negotiation keeps the MM1 retransmissions until the maximum number of retransmissions is reached. At this point, the Initiator keeps the same SPI until the next negotiation is triggered again.

Tip: Initiator and Responder SPIs identification is very helpful to identify multiple negotiations for the same VPN and narrow down some negotiation issues.

Identify Two Simultaneous Negotiations

On the Cisco IOS® XE platforms, the debugs can be filtered per tunnel with a conditional for the remote IP address configured. However, the simultaneous negotiations are displayed on the logs, and there is no way to filter them. It is needed to do it manually. As previously mentioned, the whole negotiation keeps the same SPI values for Initiator and responder. In case a packet is received from the same peer IP address but the SPI does not match the previous value tracked before the negotiation reaches the maximum number of retransmission, it is another negotiation for the same peer as shown in the image:


ISR4451

2A8F14E40D648E28

```
*Apr 29 16:57:40.944: IKEv2:(SESSION ID = 27621,SA ID = 1):Sending Packet [To 198.19.252.1:500/From 10.11.6.2:500/VRF i0:f0] |
Initiator SPI : 2A8F14E40D648E28 - Responder SPI : 0000000000000000 Message id: 0
IKEv2 IKE_SA_INIT Exchange REQUEST
Payload contents:
SA KE N VID VID NOTIFY(NAT_DETECTION_SOURCE_IP) NOTIFY(NAT_DETECTION_DESTINATION_IP) NOTIFY(IKEV2_FRAGMENTATION_SUPPORTED) VID
```

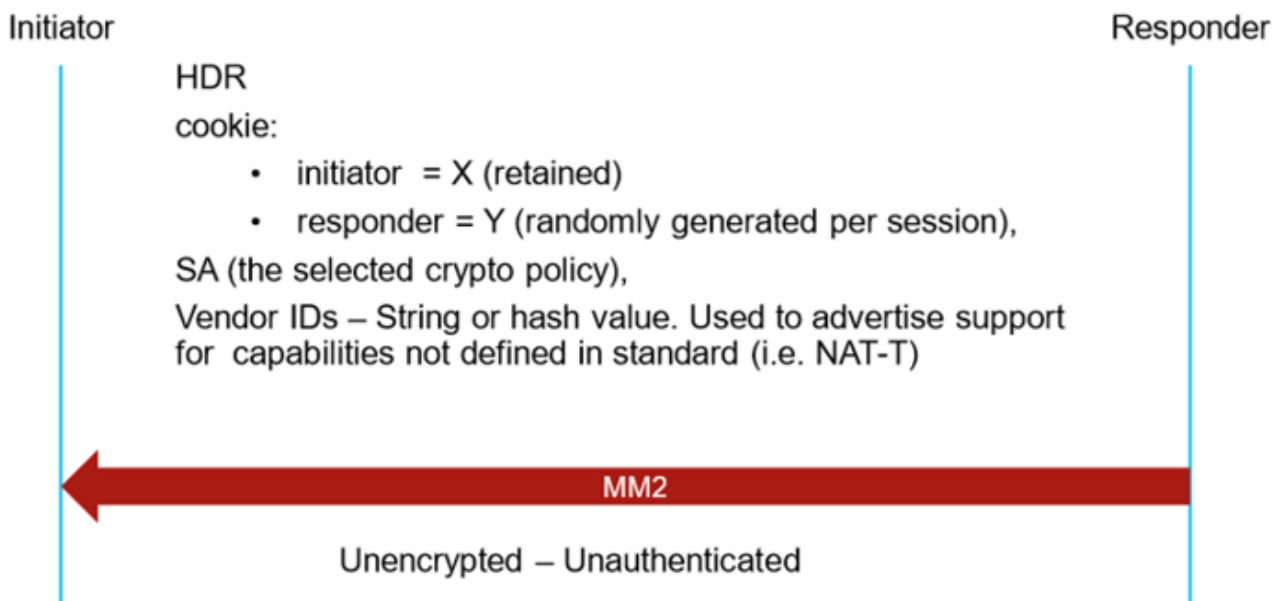
```
*Apr 29 16:57:42.200: IPSEC:(SESSION ID = 27621) (key_engine) request timer fired: count = 1,
(identity) local= 10.11.6.2:0, remote= 198.19.252.1:0,
local_proxy= 0.0.0.0/0.0.0.0/256/0,
remote_proxy= 0.0.0.0/0.0.0.0/256/0
*Apr 29 16:57:42.200: IPSEC(sa_request): ,
(key eng. msg.) OUTBOUND local= 10.11.6.2:500, remote= 198.19.252.1:500,
local_proxy= 0.0.0.0/0.0.0.0/256/0,
remote_proxy= 0.0.0.0/0.0.0.0/256/0,
protocol= ESP, transform= esp-aes 256 esp-sha-hmac (Tunnel),
lifedur= 28800s and 4294967295kb,
spi= 0x0(0), conn_id= 0, keysize= 256, flags= 0x0
omr2-site1# 5638222923EA3C5A
```

```
*Apr 29 16:57:53.763: IKEv2:Received Packet [From 198.19.252.1:500/To 10.11.6.2:500/VRF i0:f0]
Initiator SPI : 5638222923EA3C5A - Responder SPI : 0000000000000000 Message id: 0
IKEv2 IKE_SA_INIT Exchange REQUEST
Payload contents:
SA KE N NOTIFY(NAT_DETECTION_SOURCE_IP) NOTIFY(NAT_DETECTION_DESTINATION_IP) NOTIFY(IKEV2_FRAGMENTATION_SUPPORTED) NOTIFY(Unknown - 16431) NOTIFY(REDIRECT_SUPPORTED)
```

 **Note:** The example shows simultaneous negotiation for the first packet in the negotiation (MM1). However, this can occur at whatever negotiation point. All the subsequent packets must include a value different from 0 on responder SPI.

Main Mode 2 (MM2)

In the Main Mode 2 packet, the responder sends the selected policy for the proposals matched, and the responder SPI is set to a random value. The entire negotiation maintains the same SPIs values. The MM2 replies to MM1 and the SPI responder is set to a different value from 0 as shown in the image:



If the MM2 is captured and a Wireshark network protocol analyzer is used, the Initiator SPI and Responder SPI values are within the Internet Security Association and Key Management Protocol content as shown in

the image:

```
> Ethernet II, Src: 00:00:00_00:00:00 (00:00:00:00:00:00), Dst: 00:00:00_00:00:00 (00:00:00:00:00:00)
> Internet Protocol Version 4, Src: 209.134.162.150, Dst: 170.49.116.200
> User Datagram Protocol, Src Port: 500, Dst Port: 500
v Internet Security Association and Key Management Protocol
  Initiator SPI: 6f80c0380ef6bdfd
  Responder SPI: 2bc06438c94e88dc
  Next payload: Security Association (33)
```

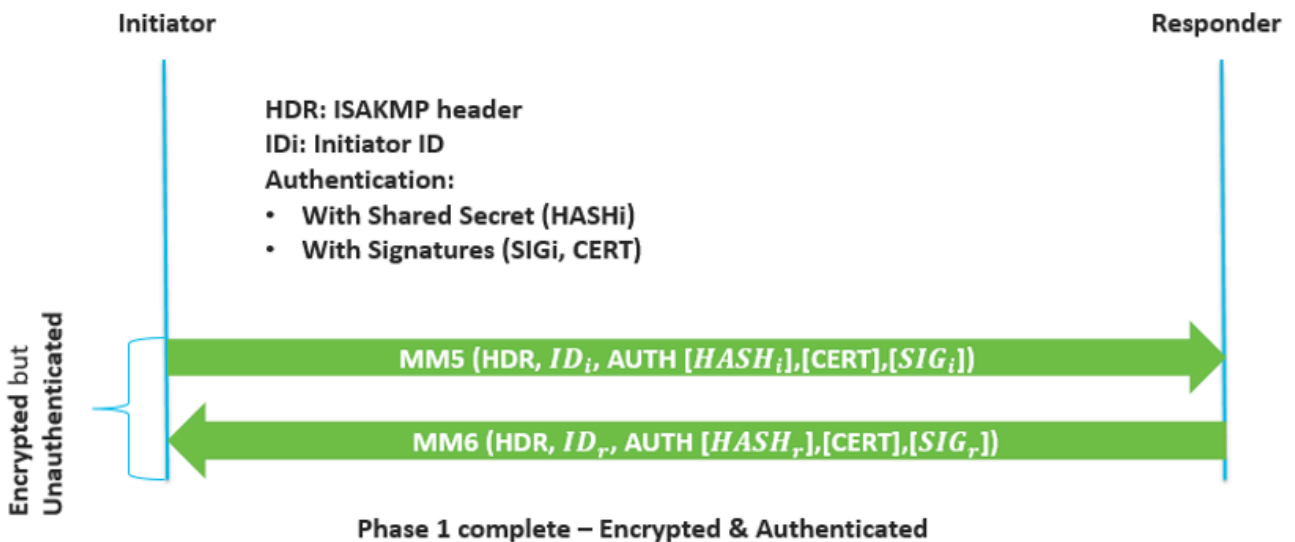
Main Mode 3 and 4 (MM3-MM4)

The MM3 and MM4 packets are still unencrypted and unauthenticated and the Secret key exchange takes place. MM3 and MM4 are shown in the image:



Main Mode 5 and 6 (MM5-MM6)

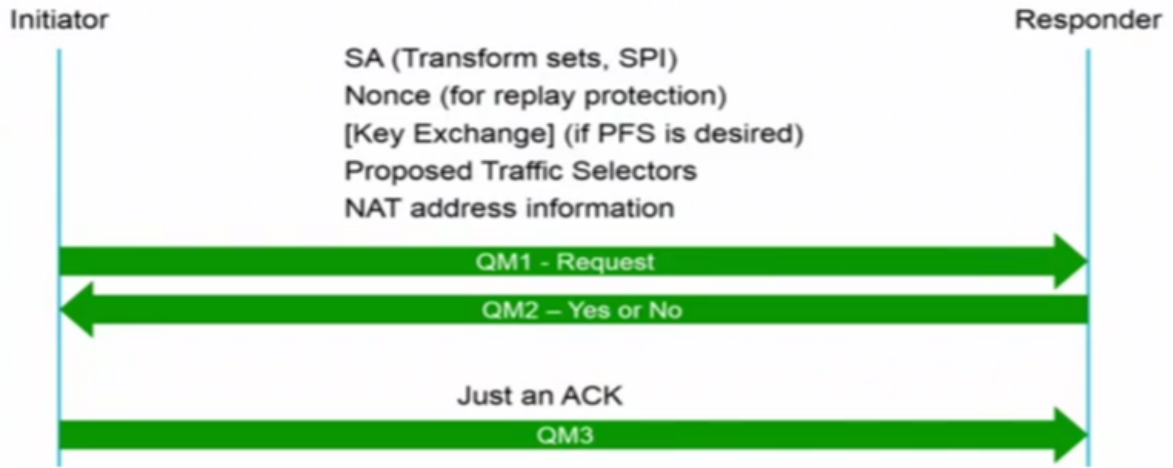
The MM5 and MM6 packets are already encrypted but still unauthenticated. On these packets, the authentication takes place as shown in the image:



Quick Mode (QM1, QM2, and QM3)

Quick mode occurs after the Main mode and the IKE has established the secure tunnel in phase 1. Quick Mode negotiates the shared IPSec policy, for the IPSec security algorithms and manages the key exchange for the IPSec SA establishment. The nonces are used to generate new shared secret key material and prevent replay attacks from bogus SAs generated.

Three packets are exchanged in this phase as shown in the image:

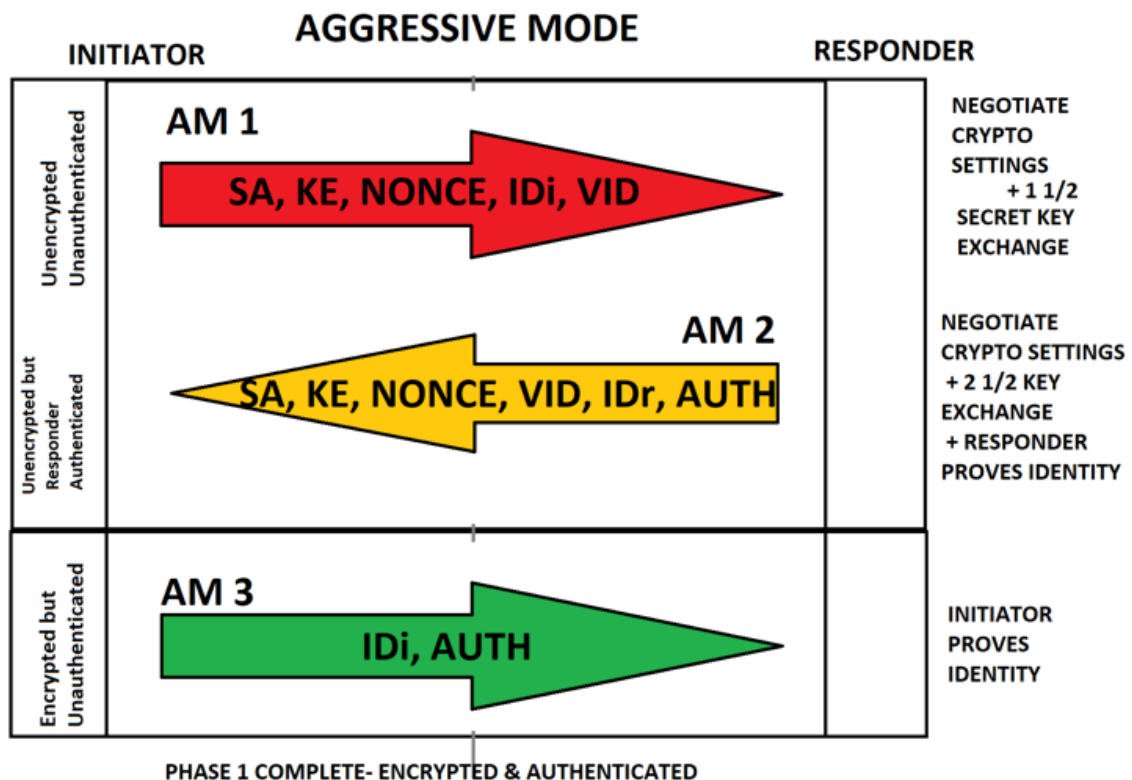


Aggressive Mode Packet Exchange

The Aggressive Mode squeezes the IKE SA negotiation into three packets, with all data required for the SA passed by the initiator.

- The responder sends the proposal, key material, and ID, and authenticates the session in the next packet.
- The initiator replies and authenticates the session.
- Negotiation is quicker, and the initiator and responder ID pass in the clear.

The image shows the payload content for the three packets exchanged on Aggressive mode:

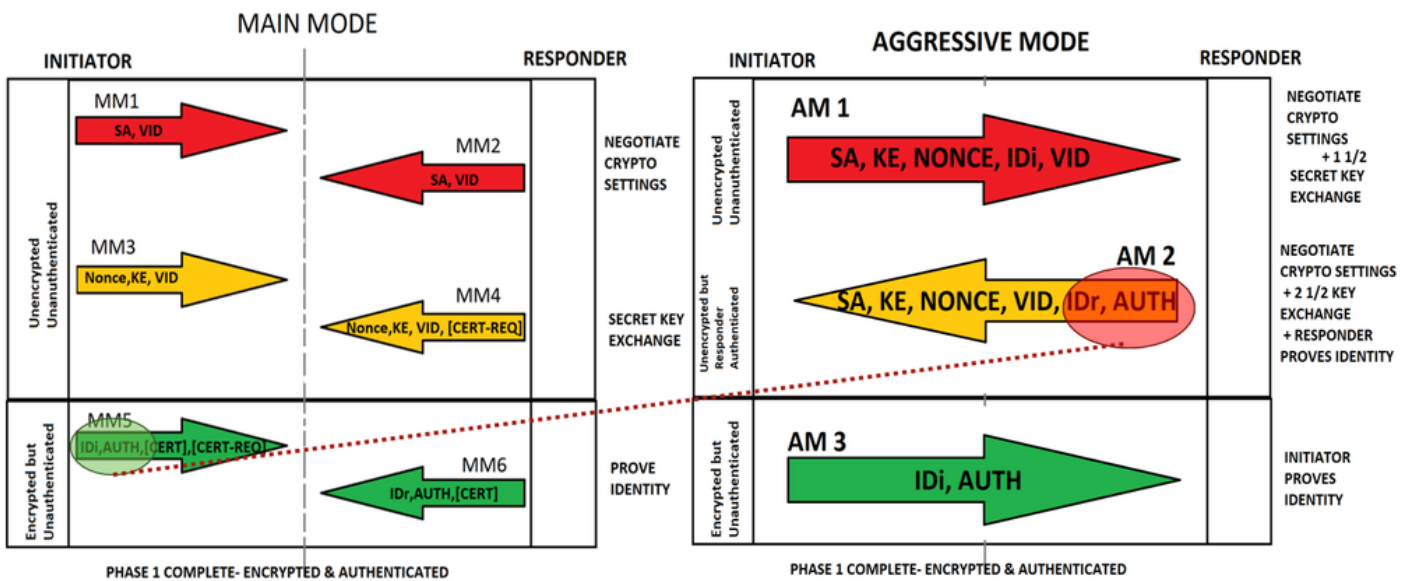


Main Mode vs Aggressive Mode

Compared to the Main Mode, Aggressive Mode comes down to three packages:

- AM 1 absorbs MM1 and MM3.
- AM 2 absorbs MM2, MM4, and part of the MM6. This is where the vulnerability of Aggressive Mode comes from. The AM 2 makes up the IDr and Authentication unencrypted. Unlike the Main Mode, this information is encrypted.
- AM 3 provides the IDi and the Authentication. Those values are encrypted.

Main Mode vs Aggressive Mode

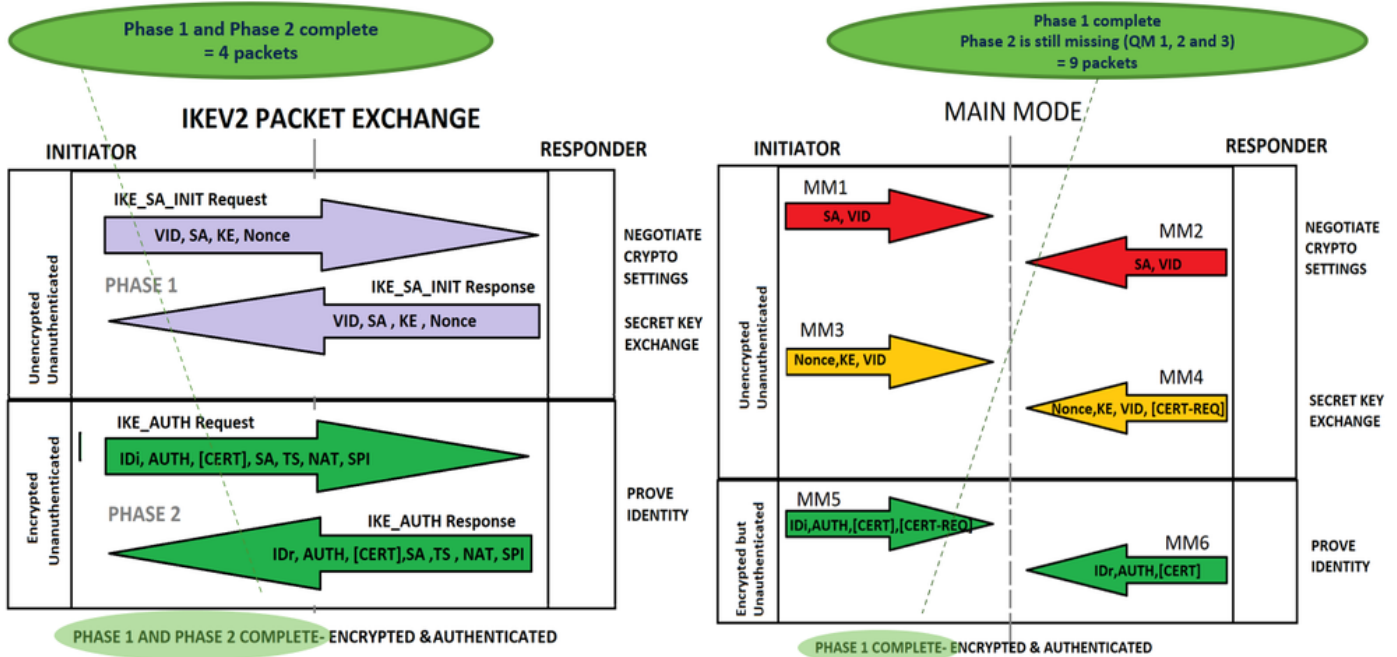



IKEv2 vs IKEv1 Packet Exchange

In the IKEv2 negotiation, fewer messages are exchanged to establish a tunnel. IKEv2 uses four messages; IKEv1 uses either six messages (in the main mode) or three messages (in aggressive mode).

The IKEv2 message types are defined as Request and Response pairs. The image shows the packets comparison and payload content of IKEv2 versus IKEv1:

IKEv2 vs IKEv1 (MM)



 **Note:** This document does not delve deeper into the IKEv2 Packet exchange. For more references, navigate to [IKEv2 Packet Exchange and Protocol Level Debugging](#).

Policy-Based vs Route-based

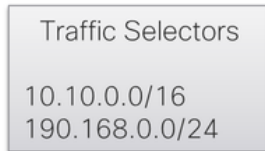
Policy-Based VPN

As the name states, a policy-based VPN is an IPsec VPN tunnel with a policy action for the transit traffic that meets the policy's match criteria. In the case of Cisco devices, an Access List (ACL) is configured and attached to a crypto map to specify the traffic to be redirected to the VPN and encrypted.

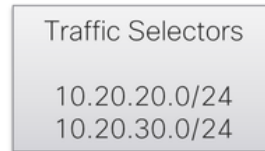
The traffic selectors are the subnets or hosts specified on the policy as shown in the image:

POLICY BASED VPN

- Crypto maps



```
ip access-list extended TS
permit ip 10.10.0.0.0.0.255.255 10.20.20.0.0.0.255
permit ip 10.10.0.0.0.255.255 10.20.30.0.0.0.255
permit ip 192.168.0.0.0.0.255 10.20.20.0.0.0.255
permit ip 192.168.0.0.0.0.255 10.20.30.0.0.0.255
exit
```



```
ip access-list extended TS
permit ip 10.20.20.0.0.0.255 10.10.0.0.0.255.255
permit ip 10.20.30.0.0.0.255 10.10.0.0.0.255.255
permit ip 10.20.20.0.0.0.255 192.168.0.0.0.255
permit ip 10.20.30.0.0.0.255 192.168.0.0.0.255
exit
```

Route-Based VPN

A Policy is not needed. The traffic is redirected toward the tunnels with routes, and it supports dynamic routing over the tunnel interface. The traffic selectors (traffic encrypted through the VPN) are from 0.0.0.0 to 0.0.0.0 by default as shown in the image:


ROUTE BASED VPN


- Supports dynamic routing over the tunnel interface.



```
interface: Tunnel100001
Crypto map tag: Tunnel100001-head-0, local addr 10.0.21.17

protected vrf: 1
local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
remote ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
```

 **Note:** Due to the Traffic selectors are 0.0.0.0, any host or subnet is included within. Therefore, only one SA is created. There is an exception for Dynamic tunnel. This document does not describe

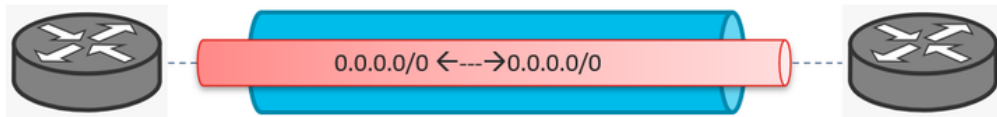
 dynamic tunnels.

The Policy and Route-based VPN can be materialized as shown in the image:

ISAKMP-IPSEC Tunnel

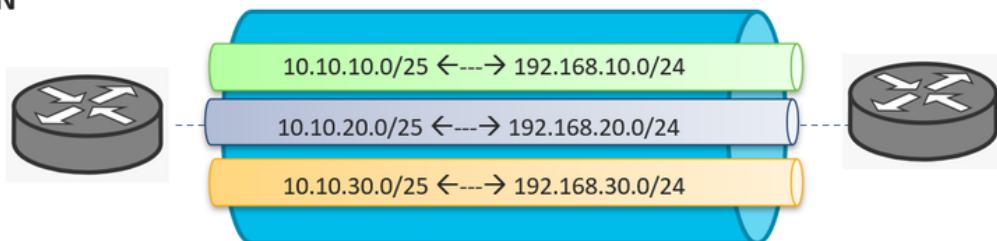
Route based VPN


*** Edges only support this.



Policy based VPN

- IOS - XE
- ASA
- FTD
- 3rd party devices



 **Note:** Unlike Route-based VPN with only one SA created, the Policy-based VPN can create multiples SA. As an ACL is configured, each statement on the ACL (if they are different between them) creates a sub-tunnel.

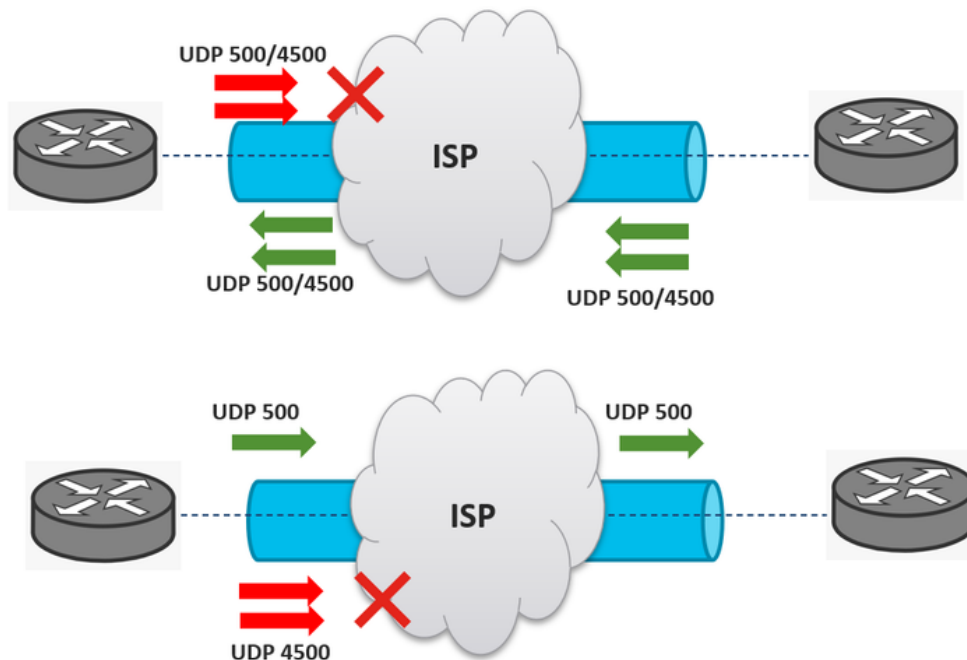
Common Issues for Traffic Does Not Receive through the VPN


ISP Blocks UDP 500/4500


It is a very common issue that the Internet Services Provider (ISP) blocks the UDP 500/4500 ports. For an IPsec tunnel establishment, two different ISPs can be engaged. One of them can block the ports, and the other allows them.

The image shows the two scenarios where an ISP can block the UDP 500/4500 ports in only one direction:

ISP Blocks UDP 500/4500



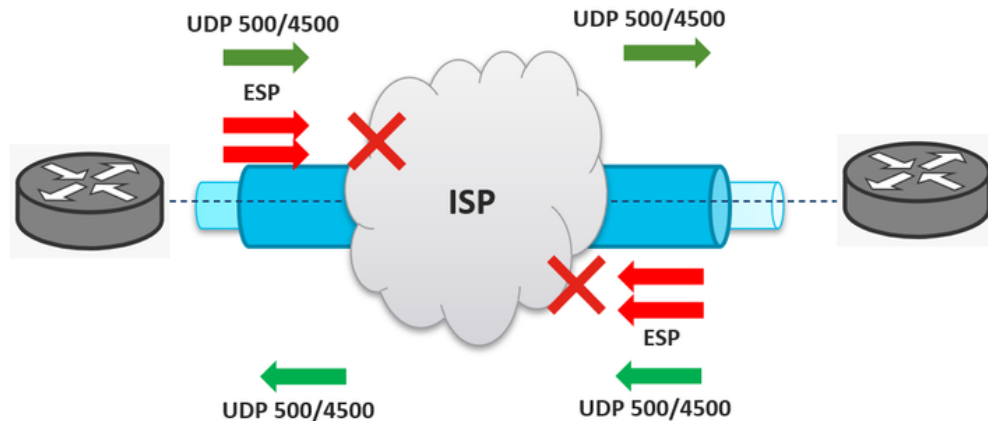
 **Note:** Port UDP 500 is used by the Internet key exchange (IKE) for the establishment of secure VPN tunnels. UDP 4500 is used when NAT is present in one VPN endpoint.


 **Note:** When the ISP Blocks UDP 500/4500, the IPsec tunnel establishment is affected and it does not get up.


ISP Blocks ESP

Another very common issue on IPsec tunnels is the ISP blocks the ESP traffic; however, it allows the UDP 500/4500 ports. For example, the UDP 500/4500 ports are allowed in bidirectional ways. Therefore, the tunnel is successfully established, but the ESP packets are blocked by the ISP or ISPs in both directions. This causes the encrypted traffic through the VPN to fail as shown in the image:

ISP Blocks ESP



 **Note:** When the ISP Blocks ESP packets, the IPsec tunnel establishment is successful, but the traffic encrypted is affected. It can be reflected with the VPN up, but the traffic does not work over it.

 **Tip:** The scenario where the ESP traffic is blocked only in one direction can be present as well. The symptoms are the same, but it can be easily found with the tunnel statistics information, encapsulation, decapsulation counters, or RX and TX counters.

Related Information

- [KEv2 Packet Exchange and Protocol Level Debugging](#)
- [The Internet Key Exchange \(IKE\) - RFC 2409](#)
- [Internet Key Exchange \(IKEv2\) Protocol](#)
- [Technical Support & Documentation - Cisco Systems](#)