**Phase 1 configuration**

Phase 1 configuration primarily defines the parameters used in IKE (Internet Key Exchange) negotiation between the ends of the IPsec tunnel. The local end is the FortiGate interface that initiates the IKE negotiations. The remote end is the remote gateway that responds and exchanges messages with the initiator. Hence, they are sometimes referred to as the initiator and responder. The purpose of phase 1 is to secure a tunnel with one bi-directional IKE SA (security association) for negotiating IKE phase 2 parameters.

The auto-negotiate and negotiation-timeout commands control how the IKE negotiation is processed when there is no traffic, and the length of time that the FortiGate waits for negotiations to occur.

IPsec tunnels can be configured in the GUI using the *VPN Creation Wizard*. Go to *VPN > IPsec Wizard*. The wizard includes several templates (site-to-site, hub and spoke, remote access), but a custom tunnel can be configured with the following settings.

|  |  |
| --- | --- |
| Note | The IPsec phase 1 interface type cannot be changed after it is configured. This is due to the tunnel ID parameter (tun\_id), which is used to match routes to IPsec tunnels to forward traffic. If the IPsec phase 1 interface type needs to be changed, a new interface must be configured. |

|  |  |  |
| --- | --- | --- |
| **Name** | | Phase 1 definition name.  The maximum length is 15 characters for an interface mode VPN and 35 characters for a policy-based VPN.  For a policy-based VPN, the name normally reflects where the remote connection originates. For a route-based tunnel, the FortiGate also uses the name for the virtual IPsec interface that it creates automatically. |
| **Network** | |  |
|  | **IP Version** | Protocol, either IPv4 or IPv6. |
|  | **Remote Gateway** | Category of the remote connection:   * *Static IP Address*: the remote peer has a static IP address. * *Dialup User*: one or more FortiClient or FortiGate dialup clients with dynamic IP addresses will connect to the FortiGate. * *Dynamic DNS*: a remote peer that has a domain name and subscribes to a dynamic DNS service will connect to the FortiGate. |
|  | **IP Address** | The IP address of the remote peer. This option is only available when the *Remote Gateway* is *Static IP Address*. |
|  | **Dynamic DNS** | The domain name of the remote peer. This option is only available when the *Remote Gateway* is *Dynamic DNS*. |
|  | **Interface** | The interface through which remote peers or dialup clients connect to the FortiGate. This option is only available in NAT mode.  By default, the local VPN gateway IP address is the IP address of the interface that was selected (*Primary IP* in the *Local Gateway* field). |
|  | **Local Gateway** | IP address for the local end of the VPN tunnel (*Primary IP* is used by default):   * *Secondary IP*: secondary address of the interface selected in the *Interface* field. * *Specify*: manually enter an address.   Interface mode cannot be configured in a transparent mode VDOM. |
|  | **Mode Config** | This option is only available when the *Remote Gateway* is *Dialup User*.  Configure the client IP address range, subnet mask/prefix length, DNS server, and split tunnel capability to automate remote client addressing. |
|  | **NAT Traversal** | This option is only available when the *Remote Gateway* is *Static IP Address* or *Dynamic DNS*.  ESP (encapsulating security payload), the protocol for encrypting data in the VPN session, uses IP protocol 50 by default. However, it does not use any port numbers so when traversing a NAT device, the packets cannot be demultiplexed. Enabling NAT traversal encapsulates the ESP packet inside a UDP packet, thereby adding a unique source port to the packet. This allows the NAT device to map the packets to the correct session.   * *Enable*: a NAT device exists between the local FortiGate and the VPN peer or client. Outbound encrypted packets are wrapped inside a UDP IP header that contains a port number. The local FortiGate and the VPN peer or client must have the same NAT traversal setting (both selected or both cleared) to connect reliably. When in doubt, enable NAT traversal. * *Disable*: disable the NAT traversal setting. * *Forced*: the FortiGate will use a port value of zero when constructing the NAT discovery hash for the peer. This causes the peer to think it is behind a NAT device, and it will use UDP encapsulation for IPsec, even if no NAT is present. This approach maintains interoperability with any IPsec implementation that supports the NAT-T RFC. |
|  | **Keepalive Frequency** | Keepalive frequency setting. This option is only available when *NAT Traversal* is set to *Enable* or *Forced*. The NAT device between the VPN peers may remove the session when the VPN connection remains idle for too long.  The value represents an interval in seconds where the connection will be maintained with periodic keepalive packets. The keepalive interval must be smaller than the session lifetime value used by the NAT device.  The keepalive packet is a 138-byte ISAKMP exchange. |
|  | **Dead Peer Detection** | Reestablishes VPN tunnels on idle connections and cleans up dead IKE peers if required. This feature minimizes the traffic required to check if a VPN peer is available or unavailable (dead). The available options are:   * *Disable*: disable dead peer detection (DPD). * *On Idle*: triggers DPD when IPsec is idle. * *On Demand*: Passively sends DPD to reduce load on the firewall. Only triggers DPD when IPsec outbound packets are sent, but no reply is received from the peer. When there is no traffic and the last DPD-ACK has been received, IKE will not send DPDs periodically.   Notifications are received whenever a tunnel goes up or down, or to keep the tunnel connection open when no traffic is being generated inside the tunnel. For example, in scenarios where a dialup client or dynamic DNS peer connects from an IP address that changes periodically, traffic may be suspended while the IP address changes.  When *Dead Peer Detection* is selected, optionally specify a retry count and a retry interval using dpd-retrycount and dpd-retryinterval. See [Dead peer detection](https://docs.fortinet.com/document/fortigate/7.4.0/administration-guide/790613/phase-1-configuration#DPD). |
|  | **Forward Error Correction** | Enable on both ends of the tunnel to correct errors in data transmission by sending redundant data across the VPN. |
|  | **Device creation** | Advanced option. When enabled, a dynamic interface (network device) is created for each dialup tunnel. |
|  | **Aggregate member** | Advanced option. When enabled, the tunnel can be used as an aggregate member candidate. |
| **Authentication** | |  |  |
|  | **Method** | Either *Pre-shared Key* or *Signature*. |  |
|  | **Pre-shared Key** | The pre-shared key that the FortiGate will use to authenticate itself to the remote peer or dialup client during phase 1 negotiations. The same key must be defined at the remote peer or client. See [Pre-shared key](https://docs.fortinet.com/document/fortigate/7.4.0/administration-guide/560886/pre-shared-key-vs-digital-certificates#key). |  |
|  | **Certificate Name** | The server certificate that the FortiGate will use to authenticate itself to the remote peer or dialup client during phase 1 negotiations. See [Digital certificates](https://docs.fortinet.com/document/fortigate/7.4.0/administration-guide/560886/pre-shared-key-vs-digital-certificates#cert). |  |
|  | **IKE Version** | Either *1* or *2*. See [Choosing IKE version 1 and 2](https://docs.fortinet.com/document/fortigate/7.4.0/administration-guide/167137/choosing-ike-version-1-and-2). |  |
|  | **Mode** | This option is only available when IKEv1 is selected. The two available options are:   * *Aggressive*: the phase 1 parameters are exchanged in a single message with unencrypted authentication information. * *Main (ID protection)*: the phase 1 parameters are exchanged in multiple rounds with encrypted authentication information.   When the remote VPN peer has a dynamic IP address and is authenticated by a pre-shared key, you must select *Aggressive* mode if there is more than one dialup phase 1 configuration for the interface IP address.  When the remote VPN peer has a dynamic IP address and is authenticated by a certificate, you must select *Aggressive* mode if there is more than one phase 1 configuration for the interface IP address and these phase 1 configurations use different proposals. |  |
|  | **Peer Options** | Options to authenticate VPN peers or clients depending on the *Remote Gateway* and *Authentication Method* settings. |  |
|  | **Any peer ID** | Accepts the local ID of any remote VPN peer or client. The FortiGate does not check identifiers (local IDs). *Mode* can be set to *Aggressive* or *Main*.  This option can be used with digital certificate authentication, but for higher security, use *Peer certificate*. |  |
|  | **Specific peer ID** | This option is only available when *Aggressive Mode* is enabled. Enter the identifier that is used to authenticate the remote peer. The identifier must match the local ID configured by the remote peer’s administrator.  If the remote peer is a FortiGate, the identifier is specified in the *Local ID* field of the *Phase 1 Proposal* settings.  If the remote peer is a FortiClient user, the identifier is specified in the *Local ID* field.  In circumstances where multiple remote dialup VPN tunnels exist, each tunnel must have a peer ID set. |  |
|  | **Peer certificate** | Define the CA certificate used to authenticate the remote peer when the authentication mode is *Signature*.  If the FortiGate will act as a VPN client, and you are using security certificates for authentication, set the *Local ID* to the distinguished name (DN) of the local server certificate that the FortiGate unit will use for authentication purposes. |  |
|  | **Peer ID from dialup group** | Authenticate multiple FortiGate or FortiClient dialup clients that use unique identifiers and unique pre-shared keys (or unique pre‑shared keys only) through the same VPN tunnel.  You must create a dialup user group for authentication purposes. Select the group from the list next to the *Peer ID from dialup group* option.  You must set *Mode* to *Aggressive* when the dialup clients use unique identifiers and unique pre-shared keys. If the dialup clients use unique pre-shared keys only, you can set *Mode* to *Main* if there is only one dialup Phase 1 configuration for this interface IP address. |  |
| **Phase 1 Proposal** | | The encryption and authentication algorithms used to generate keys for the IKE SA.  There must be a minimum of one combination. The remote peer or client must be configured to use at least one of the proposals that you define. |  |
|  | **Encryption** | The following symmetric-key encryption algorithms are available:   * *DES*: Digital Encryption Standard, a 64-bit block algorithm that uses a 56-bit key. * *3DES*: triple-DES; plain text is encrypted three times by three keys. * *AES128*: Advanced Encryption Standard, a 128-bit block algorithm that uses a 128-bit key. * *AES128GCM*: AES in Galois/Counter Mode, a 128-bit block algorithm that uses a 128-bit key. Only available for IKEv2. * *AES192*: a 128-bit block algorithm that uses a 192-bit key. * *AES256*: a 128-bit block algorithm that uses a 256-bit key. * *AES256GCM*: AES in Galois/Counter Mode, a 128-bit block algorithm that uses a 256-bit key. Only available for IKEv2. * *CHACHA20POLY1305*: a 128-bit block algorithm that uses a 128-bit key and a symmetric cipher. Only available for IKEv2. See also [HMAC settings](https://docs.fortinet.com/document/fortigate/7.4.0/administration-guide/790613/phase-1-configuration#HMAC). |  |
|  | **Authentication** | The following message digests that check the message authenticity during an encrypted session are available:   * *MD5*: message digest 5. * *SHA1*: secure hash algorithm 1; a 160-bit message digest. * *SHA256*: a 256-bit message digest. * *SHA384*: a 384-bit message digest. * *SHA512*: a 512-bit message digest.   In IKEv2, encryption algorithms include authentication, but a PRF (pseudo random function) is still required (*PRFSHA1*, *PRFSHA256*, *PRFSHA384*, *PRFSHA512*). See also [HMAC settings](https://docs.fortinet.com/document/fortigate/7.4.0/administration-guide/790613/phase-1-configuration#HMAC). |  |
|  | **Diffie-Hellman Groups** | Asymmetric key algorithms used for public key cryptography.  Select one or more from groups 1, 2, 5, and 14 through 32. At least one of the *Diffie-Hellman Groups* (DH) settings on the remote peer or client must match one the selections on the FortiGate. Failure to match one or more DH groups will result in failed negotiations. |  |
|  | **Key Lifetime** | The time (in seconds) that must pass before the IKE encryption key expires. When the key expires, a new key is generated without interrupting service. The keylife can be from 120 to 172 800 seconds. |  |
|  | **Local ID** | Optional setting. This value must match the peer ID value given for the remote VPN peer’s *Peer Options*.   * If the FortiGate will act as a VPN client and you are using peer IDs for authentication purposes, enter the identifier that the FortiGate will supply to the VPN server during the phase 1 exchange. * If the FortiGate will act as a VPN client and you are using security certificates for authentication, select the distinguished name (DN) of the local server certificate that the FortiGate will use for authentication purposes. |  |
| **XAUTH** | | This option supports the authentication of dialup clients. It is only available for IKE version 1.   * *Disable*: do not use XAuth. * *Client*: available only if the *Remote Gateway* is set to *Static IP Address* or *Dynamic DNS*. If the FortiGate is a dialup client, enter the user name and password for the FortiGate to authenticate itself to the remote XAuth server. * *PAP Server*, *CHAP Server*, *Auto Server*: available only if *Remote Gateway* is set to *Dialup User*. Dialup clients authenticate as members of a dialup user group. A user group must be created first for the dialup clients that need access to the network behind the FortiGate.   The FortiGate must be configured to forward authentication requests to an external RADIUS or LDAP authentication server.  Select the server type based on the encryption method used between the FortiGate, the XAuth client, and the external authentication server. Then select the user group (*Inherit from policy* or *Choose*). See [Using XAuth authentication](https://docs.fortinet.com/document/fortigate/7.4.0/administration-guide/277729/using-xauth-authentication). |  |
|  | **Username** | User name used for authentication. |  |
|  | **Password** | Password used for authentication. |  |

**Additional CLI configurations**

The following phase 1 settings can be configured in the CLI:

|  |  |
| --- | --- |
| **VXLAN over IPsec** | Packets with a VXLAN header are encapsulated within IPsec tunnel mode.  **To configure VXLAN over IPsec:**  config vpn ipsec phase1-interface/phase1  edit ipsec  set interface <name>  set encapsulation vxlan/gre  set encapsulation-address ike/ipv4/ipv6  set encap-local-gw4 xxx.xxx.xxx.xxx  set encap-remote-gw xxx.xxx.xxx.xxx  next  end |
| **IPsec tunnel idle timer** | Define an idle timer for IPsec tunnels. When no traffic has passed through the tunnel for the configured idle-timeout value, the IPsec tunnel will be flushed.  **To configure IPsec tunnel idle timeout:**  config vpn ipsec phase1-interface  edit p1  set idle-timeout [enable | disable]  set idle-timeoutinterval <integer> *IPsec tunnel idle timeout in minutes (10 - 43200).*  next  end |
| **Monitor tunnel for failover** | Monitor a site-to-site tunnel to guarantee operational continuity if the primary tunnel fails. Configure the secondary phase 1 interface to monitor the primary interface.  **To configure the monitor:**  config vpn ipsec phase1-interface  edit <secondary phase1-interface>  set monitor <primary phase1-interface>  next  end |
| **Passive mode** | Passive mode turns one side of the tunnel to be a responder only. It does not initiate VPN tunnels either by auto-negotiation, rekey, or traffic initiated behind the FortiGate.  **To configure passive mode:**  config vpn ipsec phase1-interface  edit <example>  set rekey {enable | disable}  set passive-mode {enable | disable}  set passive-tunnel-interface {enable | disable}  next  end |
| **Network ID** | The network ID is a Fortinet-proprietary attribute that is used to select the correct phase 1 between IPsec peers, so that multiple IKEv2 tunnels can be established between the same local/remote gateway pairs.  In a dial-up VPN, network-id is in the first initiator message of an IKEv2 phase 1 negotiation. The responder (Hub) uses the network-id to match a phase 1 configuration with a matching network-id. The Hub can then differentiate multiple dial-up phase 1s that are bound to the same underlay interface and IP address. Without a network-id, the Hub cannot have multiple phase 1 dialup tunnels on the same interface.  In static phase 1 configurations, network-id is used with the pair of gateway IPs to negotiate the correct tunnel with a matching network-id. This allows IPsec peers to use the same pair of underlay IPs to establish multiple IPsec tunnels. Without it, only a single tunnel can be established over the same pair of underlay IPs.  **To configure the network ID:**  config vpn ipsec phase1-interface  edit <example>  set ike-version 2  set network-overlay enable  set network-id <integer>  next  end |

**Dead peer detection**

By default, dead peer detection (DPD) sends probe messages every five seconds. If you are experiencing high network traffic, you can experiment with increasing the ping interval. However, longer intervals will require more traffic to detect dead peers, which will result in more traffic.

|  |  |
| --- | --- |
| Note | In a dynamic (dialup) connection, the *On Idle* option encourages dialup server configurations to more proactively delete tunnels if the peer is unavailable. |

In the GUI, the dead peer detection option can be configured when defining phase 1 options. The following CLI commands support additional options for specifying a retry count and a retry interval.

For example, enter the following to configure DPD on the existing IPsec phase 1 configuration to use 15-second intervals and to wait for three missed attempts before declaring the peer dead and taking action.

**To configure DPD:**

config vpn ipsec phase1-interface

edit <value>

set dpd [disable | on-idle | on-demand]

set dpd-retryinveral 15

set dpd-retrycount 3

next

end

**DPD scalability**

On a dialup server, if many VPN connections are idle, the increased DPD exchange could negatively impact the performance/load of the daemon. The on-demand option in the CLI triggers DPD when IPsec traffic is sent, but no reply is received from the peer.

When there is no traffic and the last DPD-ACK had been received, IKE will not send DPDs periodically. IKE will only send out DPDs if there are outgoing packets to send, but no inbound packets have since been received.

**HMAC settings**

The FortiGate uses the HMAC based on the authentication proposal that is chosen in phase 1 or phase 2 of the IPsec configuration. Each proposal consists of the encryption-hash pair (such as 3des-sha256). The FortiGate matches the most secure proposal to negotiate with the peer.

**To view the chosen proposal and the HMAC hash used:**

# diagnose vpn ike gateway list

vd: root/0

name: MPLS

version: 1

interface: port1 3

addr: 192.168.2.5:500 -> 10.10.10.1:500

tun\_id: 10.10.10.1

virtual-interface-addr: 172.31.0.2 -> 172.31.0.1

created: 1015820s ago

IKE SA: created 1/13 established 1/13 time 10/1626/21010 ms

IPsec SA: created 1/24 established 1/24 time 0/11/30 ms

id/spi: 124 43b087dae99f7733/6a8473e58cd8990a

direction: responder

status: established 68693-68693s ago = 10ms

**proposal: 3des-sha256**

key: e0fa6ab8dc509b33-aa2cc549999b1823-c3cb9c337432646e

lifetime/rekey: 86400/17436

DPD sent/recv: 000001e1/00000000

**Choosing IKE version 1 and 2**

If you create a route-based VPN, you have the option of selecting IKE version 2. Otherwise, IKE version 1 is used.

IKEv2, defined in [RFC 4306](http://tools.ietf.org/html/rfc4306), simplifies the negotiation process that creates the security association (SA).

If you select IKEv2:

* There is no choice in phase 1 of aggressive or main mode.
* Extended authentication (XAUTH) is not available.
* You can utilize EAP and MOBIKE.

**Repeated authentication in IKEv2**

This feature provides the option to control whether a device requires its peer to re-authenticate or whether re-key is sufficient. It does not influence the re-authentication or re-key behavior of the device itself, which is controlled by the peer (the default being to re-key). This solution is in response to [RFC 4478](https://tools.ietf.org/html/rfc4478). As described by the IETF, "the purpose of this is to limit the time that security associations (SAs) can be used by a third party who has gained control of the IPsec peer".

To configure IKE SA re-authentication:

config vpn ipsec phase1-interface

edit p1

set reauth [enable | disable]

next

end

**IKEv2 quick crash detection**

There is support for IKEv2 quick crash detection (QCD) as described in [RFC 6290](https://tools.ietf.org/html/rfc6290).

RFC 6290 describes a method in which an IKE peer can quickly detect that the gateway peer it has and established an IKE session with has rebooted, crashed, or otherwise lost IKE state. When the gateway receives IKE messages or ESP packets with unknown IKE or IPsec SPIs, the IKEv2 protocol allows the gateway to send the peer an unprotected IKE message containing INVALID\_IKE\_SPI or INVALID\_SPI notification payloads.

RFC 6290 introduces the concept of a QCD token, which is generated from the IKE SPIs and a private QCD secret, and exchanged between peers during the protected IKE AUTH exchange.

**To configure QCD:**

config system settings

set ike-quick-crash-detect [enable | disable]

end

**IKEv1 quick crash detection**

Based on the IKEv2 QCD feature previously described, IKEv1 QCD is implemented using a new IKE vendor ID (Fortinet Quick Crash Detection) so both endpoints must be FortiGates. The QCD token is sent in the phase 1 exchange and must be encrypted, so this is only implemented for IKEv1 in main mode (aggressive mode is not supported as there is no available AUTH message to include the token). Otherwise, the feature works the same as in IKEv2 (RFC 6290).

**IKEv1 fragmentation**

UDP fragmentation can cause issues in IPsec when either the ISP or perimeter firewall(s) cannot pass or fragment the oversized UDP packets that occur when using a very large public security key (PSK). The result is that IPsec tunnels do not come up. The solution is IKE fragmentation.

For most configurations, enabling IKE fragmentation allows connections to automatically establish when they otherwise might have failed due to intermediate nodes dropping IKE messages containing large certificates, which typically push the packet size over 1500 bytes.

FortiOS will fragment a packet on sending if only all the following are true:

* Phase 1 contains set fragmentation enable.
* The packet is larger than the minimum MTU (576 for IPv4, 1280 for IPv6).
* The packet is being re-transmitted.

By default, IKE fragmentation is enabled.

**To configure IKEv1 fragmentation:**

config vpn ipsec phase1-interface

edit 1

set fragmentation [enable | disable]

next

end

**IKEv2 fragmentation**

[RFC 7383](http://tools.ietf.org/html/rfc7383) requires each fragment to be individually encrypted and authenticated. With IKEv2, a copy of the unencrypted payloads around for each outgoing packet would need to be kept in case the original single packet was never answered and would retry with fragments. With the following implementation, if the IKE payloads are greater than a configured threshold, the IKE packets are preemptively fragmented and encrypted.

**To configure IKEv2 fragmentation:**

config vpn ipsec phase1-interface

edit ike

set ike-version 2

set fragmentation [enable|disable]

set fragmentation-mtu <500-16000>

next

end

**IPsec global IKE embryonic limit**

When trying to establish thousands of tunnels simultaneously, a situation can arise where new negotiations starve other SAs from progressing to an established state in IKEv2. The IKE daemon can prioritize established SAs, offload groups 20 and 21 to CP9, and optimize the default embryonic limits for mid- and high-end platforms. The IKE embryonic limit can be configured in the CLI.

config system ike

set embryonic-limit <integer>

end

|  |  |
| --- | --- |
| embryonic-limit <integer> | Set the maximum number of IPsec tunnels to negotiate simultaneously (50 - 20000, default = 1000). |

**To configure an IKE embryonic limit of 50:**

config system ike

set embryonic-limit 50

end

**Pre-shared key vs digital certificates**

A FortiGate can authenticate itself to remote peers or dialup clients using either a pre-shared key or a digital certificate.

**Pre-shared key**

Using a pre-shared key is less secure than using certificates, especially if it is used alone, without requiring peer IDs or extended authentication (XAuth). There also needs to be a secure way to distribute the pre-shared key to the peers.

If you use pre-shared key authentication alone, all remote peers and dialup clients must be configured with the same pre-shared key. Optionally, you can configure remote peers and dialup clients with unique pre-shared keys. On the FortiGate, these are configured in user accounts, not in the phase 1 settings.

The pre-shared key must contain at least six printable characters and should be known by network administrators. For optimum protection against currently known attacks, the key must consist of a minimum of 16 randomly chosen alphanumeric characters. The limit is 128 characters.

If you authenticate the FortiGate using a pre-shared key, you can require remote peers or dialup clients to authenticate using peer IDs, but not client certificates.

**To authenticate the FortiGate using a pre-shared key:**

1. Go to *VPN > IPsec Tunnels* and create a new tunnel, or edit an existing one.
2. Configure or edit the *Network* section as needed.
3. Configure or edit the *Authentication* settings as follows:

|  |  |
| --- | --- |
| **Method** | *Pre-shared Key* |
| **Pre-shared Key** | <string> |
| **IKE Version** | *1* or *2* |
| **Mode** | *Aggressive* or *Main* |
| **Peer Options** | Select an *Accept Type* and the corresponding peer. Options vary based on the *Remote Gateway* and *Authentication Method* settings in the *Network* section.  *Peer Options* are only available in *Aggressive* mode. |

1. For the *Phase 1 Proposal* section, keep the default settings unless changes are needed to meet your requirements.
2. Optionally, for authentication parameters for a dialup user group, define *XAUTH* parameters.
3. Click *OK*.

**Digital certificates**

To authenticate the FortiGate using digital certificates, you must have the required certificates installed on the remote peer and on the FortiGate. The signed server certificate on one peer is validated by the presence of the root certificate installed on the other peer. If you use certificates to authenticate the FortiGate, you can also require the remote peers or dialup clients to authenticate using certificates. See [Site-to-site VPN with digital certificate](https://docs.fortinet.com/document/fortigate/7.4.0/administration-guide/344213/site-to-site-vpn-with-digital-certificate) for a detailed example.

**To authenticate the FortiGate using a digital certificate:**

1. Go to *VPN > IPsec Tunnels* and create a new tunnel, or edit an existing one.
2. Configure or edit the *Network* section as needed.
3. Configure or edit the *Authentication* settings as follows:

|  |  |
| --- | --- |
| **Method** | *Signature* |
| **Certificate Name** | Select the certificate used to identify this FortiGate. If there are no imported certificates, use *Fortinet\_Factory*. |
| **IKE Version** | *1* or *2* |
| **Mode** | *Aggressive* is recommended. |
| **Peer Options** | For *Accept Type*, select *Peer certificate* and select the peer and the CA certificate used to authenticate the peer. If the other end is using the Fortinet\_Factory certificate, then use the *Fortinet\_CA* certificate here. |

1. For the *Phase 1 Proposal* section, keep the default settings unless changes are needed to meet your requirements.
2. Optionally, for authentication parameters for a dialup user group, define *XAUTH* parameters.
3. Click *OK*.

**Using XAuth authentication**

Extended authentication (XAuth) increases security by requiring remote dialup client users to authenticate in a separate exchange at the end of phase 1. XAuth draws on existing FortiGate user group definitions and uses established authentication mechanisms such as PAP, CHAP, RADIUS, and LDAP to authenticate dialup clients. You can configure a FortiGate to function either as an XAuth server or client. If the server or client is attempting a connection using XAuth and the other end is not using XAuth, the failed connection attempts that are logged will not specify XAuth as the reason.

**XAuth server**

A FortiGate can act as an XAuth server for dialup clients. When the phase 1 negotiation completes, the FortiGate challenges the user for a user name and password. It then forwards the user’s credentials to an external RADIUS or LDAP server for verification.

If the user records on the RADIUS server have suitably configured Framed‑IP‑Address fields, you can assign client virtual IP addresses by XAuth instead of from a DHCP address range.

The authentication protocol you use for XAuth depends on the capabilities of the authentication server and the XAuth client:

* Select *PAP Server* whenever possible.
* You must select *PAP Server* for all implementations of LDAP and some implementations of Microsoft RADIUS.
* Select *Auto Server* when the authentication server supports *CHAP Server* but the XAuth client does not. The FortiGate will use PAP to communicate with the XAuth client and CHAP to communicate with the authentication server. You can also use *Auto Server* to allow multiple source interfaces to be defined in an IPsec/IKE policy.

Before you begin, create user accounts and user groups to identify the dialup clients that need to access the network behind the FortiGate dialup server. If password protection will be provided through an external RADIUS or LDAP server, you must configure the FortiGate dialup server to forward authentication requests to the authentication server.

**To configure XAuth to authenticate a dialup user group:**

1. On the FortiGate dialup server, go to *VPN > IPsec Tunnels* and create a new tunnel, or edit an existing one.
2. Configure or edit the *Network*, *Authentication*, and *Phase 1 Proposal* sections as needed.
3. In the *XAUTH* section, select the encryption method *Type* to use between the XAuth client, the FortiGate, and the authentication server.
4. For *User Group*:
   1. Click *Inherit from policy* for multiple user groups defined in the IPsec/IKE policy, or
   2. Click *Choose* and in the dropdown, select the user group that needs to access the private network behind the FortiGate.

|  |  |
| --- | --- |
| Note | Only one user group may be defined for *Auto Server*. |

1. Click *OK*.
2. Create as many policies as needed, specifying the source user(s) and destination address.

**XAuth client**

If the FortiGate acts as a dialup client, the remote peer, acting as an XAuth server, might require a username and password. You can configure the FortiGate as an XAuth client with its own username and password, which it provides when challenged.

**To configure the FortiGate dialup client as an XAuth client:**

1. On the FortiGate dialup client, go to *VPN > IPsec Tunnels* and create a new tunnel, or edit an existing one.
2. Configure or edit the *Network*, *Authentication*, and *Phase 1 Proposal* sections as needed.
3. In the *XAUTH* section, for *Type*, select *Client*.
4. For *Username*, enter the FortiGate PAP, CHAP, RADIUS, or LDAP user name that the FortiGate XAuth server will compare to its records when the FortiGate XAuth client attempts to connect.
5. Enter the *Password* for the user name.
6. Click *OK*.

# Dynamic IPsec route control

You can add a route to a peer destination selector by using the add-route option, which is available for all dynamic IPsec phases 1 and 2, for both policy-based and route-based IPsec VPNs.

The add-route option adds a route to the FortiGate routing information base when the dynamic tunnel is negotiated. You can use the distance and priority options to set the distance and priority of this route. If this results in a route with the lowest distance, it is added to the FortiGate forwarding information base.

You can also enable add-route in any policy-based or route-based phase 2 configuration that is associated with a dynamic (dialup) phase 1. In phase 2, add-route can be enabled, disabled, or set to use the same route as phase 1.

The add-route option is enabled by default.

###### To configure add-route in phase 1:

config vpn ipsec

edit <name>

set type dynamic

set add-route {enable | disable}

next

end

###### To configure add-route in phase 2:

config vpn ipsec {phase2 | phase2-interface}

edit <name>

set add-route {phase1 | enable | disable}

next

end

## Blocking IPsec SA negotiation

For interface-based IPsec, IPsec SA negotiation blocking can only be removed if the peer offers a wildcard selector. If a wildcard selector is offered, then the wildcard route will be added to the routing table with the distance/priority value configured in phase 1. If that is the route with the lowest distance, it will be installed into the forwarding information base.

In this scenario, it is important to ensure that the distance value configured for phase 1 is set appropriately.

**Phase 2 configuration**

After phase 1 negotiations end successfully, phase 2 begins. In Phase 2, the VPN peer or client and the FortiGate exchange keys again to establish a secure communication channel. The phase 2 proposal parameters select the encryption and authentication algorithms needed to generate keys for protecting the implementation details of security associations (SAs). The keys are generated automatically using a Diffie-Hellman algorithm.

The basic phase 2 settings associate IPsec phase 2 parameters with the phase 1 configuration that specifies the remote end point of the VPN tunnel. In most cases, you need to configure only basic Phase 2 settings.

Some settings can be configured in the CLI. The following options are available in the *VPN Creation Wizard* after the tunnel is created:

|  |  |  |  |
| --- | --- | --- | --- |
| **New Phase 2** | |  |  |
|  | **Name** | Phase 2 definition name. |  |
|  | **Local Address** | A value of 0.0.0.0/0 means all IP addresses behind the local VPN peer. Add a specific address or range to allow traffic from and to only this local address.  See [Quick mode selectors](https://docs.fortinet.com/document/fortigate/7.4.0/administration-guide/604285/phase-2-configuration#quick). |  |
|  | **Remote Address** | Enter the destination IP address that corresponds to the recipients or network behind the remote VPN peer. A value of 0.0.0.0/0 means all IP addresses behind the remote VPN peer.  See [Quick mode selectors](https://docs.fortinet.com/document/fortigate/7.4.0/administration-guide/604285/phase-2-configuration#quick). |  |
| **Advanced** | | Select the encryption and authentication algorithms that will be proposed to the remote VPN peer. To establish a VPN connection, at least one of the proposals specified must match the configuration on the remote peer. |  |
|  | **Encryption** | The following symmetric-key encryption algorithms are available:   * *NULL*: do not use an encryption algorithm. * *DES*: Digital Encryption Standard, a 64-bit block algorithm that uses a 56-bit key. * *3DES*: triple-DES; plain text is encrypted three times by three keys. * *AES128*: Advanced Encryption Standard, a 128-bit block algorithm that uses a 128-bit key. * *AES128GCM*: AES in Galois/Counter Mode, a 128-bit block algorithm that uses a 128-bit key. Only available for IKEv2. * *AES192*: a 128-bit block algorithm that uses a 192-bit key. * *AES256*: a 128-bit block algorithm that uses a 256-bit key. * *AES256GCM*: AES in Galois/Counter Mode, a 128-bit block algorithm that uses a 256-bit key. Only available for IKEv2. * *CHACHA20POLY1305*: a 128-bit block algorithm that uses a 128-bit key and a symmetric cipher. Only available for IKEv2.   See [ChaCha20 and Poly1305 AEAD cipher](https://docs.fortinet.com/document/fortigate/7.4.0/administration-guide/604285/phase-2-configuration#chacha), [AES-GCM for IKEv2 phase 1](https://docs.fortinet.com/document/fortigate/7.4.0/administration-guide/604285/phase-2-configuration#aesgcm), and [HMAC settings](https://docs.fortinet.com/document/fortigate/7.4.0/administration-guide/790613/phase-1-configuration#HMAC). |  |
|  | **Authentication** | The following message digests that check the message authenticity during an encrypted session are available:   * NULL: do not use a message digest. * *MD5*: message digest 5. * *SHA1*: secure hash algorithm 1; a 160-bit message digest. * *SHA256*: a 256-bit message digest. * *SHA384*: a 384-bit message digest. * *SHA512*: a 512-bit message digest.   See also [HMAC settings](https://docs.fortinet.com/document/fortigate/7.4.0/administration-guide/790613/phase-1-configuration#HMAC). |  |
|  | **Enable Replay Detection** | Replay attacks occur when an unauthorized party intercepts a series of IPsec packets and replays them back into the tunnel.  Replay detection allows the FortiGate to check all IPsec packets to see if they have been received before. If any encrypted packets arrive out of order, the FortiGate discards them.  Note that 64-bit extended sequence numbers (as described in RFC 4303, RFC 4304 as an addition to IKEv1, and RFC 5996 for IKEv2) are supported for IPsec when replay detection is enabled. |  |
|  | **Enable Perfect Forward Secrecy (PFS)** | Perfect forward secrecy (PFS) improves security by forcing a new Diffie‑Hellman exchange whenever keylife expires. |  |
|  | **Diffie-Hellman Group** | Asymmetric key algorithms used for public key cryptography.  Select one or more from groups 1, 2, 5, and 14 through 32. At least one of the *Diffie-Hellman Groups* (DH) settings on the remote peer or client must match one the selections on the FortiGate. Failure to match one or more DH groups will result in failed negotiations. |  |
|  | **Local Port** | Enter the port number that the local VPN peer uses to transport traffic related to the specified service (protocol number). The range is from 0 to 65535. To specify all ports, select *All*, or enter 0. |  |
|  | **Remote Port** | Enter the port number that the remote VPN peer uses to transport traffic related to the specified service (protocol number). To specify all ports, select *All*, or enter 0. |  |
|  | **Protocol** | Enter the IP protocol number of the service. To specify all services, select *All*, or enter 0. |  |
|  | **Auto-negotiate** | Select this option for the tunnel to be automatically renegotiated when the it expires. See [Auto-negotiate](https://docs.fortinet.com/document/fortigate/7.4.0/administration-guide/604285/phase-2-configuration#auto). |  |
|  | **Autokey Keep Alive** | Select this option for the tunnel to remain active when no data is being processed. |  |
|  | **Key Lifetime** | Select the method for determining when the phase 2 key expires:   * *Seconds* * *Kilobytes* * *Both*   Enter a corresponding value for *Seconds* and/or *Kilobytes* in the text boxes.  If *Both* is selected, the key expires when either the time has passed or the number of kilobytes have been processed. |  |

**Quick mode selectors**

Quick mode selectors determine which IP addresses can perform IKE negotiations to establish a tunnel. By only allowing authorized IP addresses access to the VPN tunnel, the network is more secure.

The default settings are as broad as possible: any IP address or configured address object using any protocol on any port.

|  |  |
| --- | --- |
| Caution | While the dropdown menus for specifying an address also show address groups, the use of address groups may not be supported on a remote endpoint device that is not a FortiGate. |

When configuring a quick mode selector for *Local Address* and *Remote Address*, valid options include IPv4 and IPv6 single addresses, subnets, or ranges.

There are some configurations that require specific selectors:

* The VPN peer is a third-party device that uses specific phase2 selectors.
* The FortiGate connects as a dialup client to another FortiGate, in which case (usually) you must specify a local IP address, IP address range, or subnet. However, this is not required if you are using dynamic routing and mode-cfg.

With FortiOS VPNs, your network has multiple layers of security, with quick mode selectors being an important line of defense:

* Routes guide traffic from one IP address to another.
* Phase 1 and phase 2 connection settings ensure there is a valid remote end point for the VPN tunnel that agrees on the encryption and parameters.
* Quick mode selectors allow IKE negotiations only for allowed peers.
* Security policies control which IP addresses can connect to the VPN.
* Security policies also control what protocols are allowed over the VPN along with any bandwidth limiting.

If you are editing an existing phase 2 configuration, the local address and remote address fields are unavailable if the tunnel has been configured to use firewall addresses as selectors. This option exists only in the CLI.

**Using the add-route option**

Consider using the add-route option to add a route to a peer destination selector in phase 2 to automatically match the settings in phase 1.

**To configure add-route:**

config vpn ipsec {phase2 | phase2-interface}

edit <name>

set add-route {phase1 | enable | disable}

next

end

**Auto-negotiate**

By default, the phase 2 security association (SA) is not negotiated until a peer attempts to send data. The triggering packet and some subsequent packets are dropped until the SA is established. Applications normally resend this data, so there is no loss, but there might be a noticeable delay in response to the user.

If the tunnel goes down, the auto-negotiate feature (when enabled) attempts to re-establish the tunnel. Auto-negotiate initiates the phase 2 SA negotiation automatically, repeating every five seconds until the SA is established.

Automatically establishing the SA can be important for a dialup peer. It ensures that the VPN tunnel is available for peers at the server end to initiate traffic to the dialup peer. Otherwise, the VPN tunnel does not exist until the dialup peer initiates traffic.

**To configure auto-negotiate:**

config vpn ipsec phase2

edit <phase2\_name>

set auto-negotiate enable

next

end

**Installing dynamic selectors via auto-negotiate**

The IPsec SA connect message generated is used to install dynamic selectors. These selectors can be installed via the auto-negotiate mechanism. When phase 2 has auto-negotiate enabled, and phase 1 has mesh-selector-type set to subnet, a new dynamic selector will be installed for each combination of source and destination subnets. Each dynamic selector will inherit the auto-negotiate option from the template selector and begin SA negotiation. Phase 2 selector sources from dialup clients will all establish SAs without traffic being initiated from the client subnets to the hub.

**DHCP**

The dhcp-ipsec option lets the FortiGate assign VIP addresses to FortiClient dialup clients through a DHCP server or relay. This option is only available if the remote gateway in the phase 1 configuration is set to dialup user, and it only works in policy-based VPNs.

With dhcp-ipsec, the FortiGate dialup server acts as a proxy for FortiClient dialup clients that have VIP addresses on the subnet of the private network behind the FortiGate. In this case, the FortiGate dialup server acts as a proxy on the local private network for the FortiClient dialup client. A host on the network behind the dialup server issues an ARP request, corresponding to the device MAC address of the FortiClient host (when a remote server sends an ARP to the local FortiClient dialup client). The FortiGate then answers the ARP request on behalf of the FortiClient host, and then forwards the associated traffic to the FortiClient host through the tunnel.

Acting as a proxy prevents the VIP address assigned to the FortiClient dialup client from causing possible ARP broadcast problems—the normal and VIP addresses can confuse some network switches when two addresses have the same MAC address.

**ChaCha20 and Poly1305 AEAD cipher**

In IKEv2 to support [RFC 7634](https://tools.ietf.org/html/rfc7634), the ChaCha20 and Poly1305 crypto algorithms can be used together as a combined mode AEAD cipher (like AES-GCM) in the crypto\_ftnt cipher in cipher\_chacha20poly1305.c:

config vpn ipsec phase2-interface

edit <name>

set phase1name <name>

set proposal chacha20poly1305

next

end

**AES-GCM for IKEv2 phase 1**

In IKEv2 to support [RFC 5282](https://tools.ietf.org/html/rfc7634), the AEAD algorithm AES-GCM supports 128- and 256-bit variants:

config vpn ipsec phase2-interface

edit <name>

set phase1name <name>

set proposal [aes128gcm | aes256gcm]

next

end