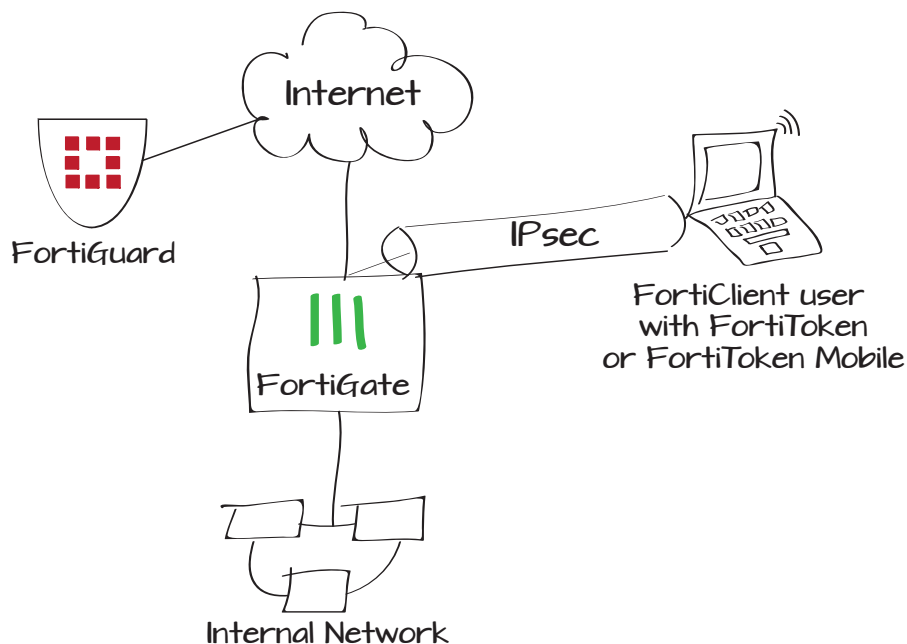


Using two-factor authentication with IPsec VPN

An IPsec VPN can use two-factor user authentication for enhanced security. In this example, a remote user uses FortiClient to connect to a private network behind a FortiGate unit. The FortiGate unit and FortiClient authenticate each other using a pre-shared key. The user is then authenticated by XAUTH (ID/password), plus a FortiToken token code.

1. Registering FortiToken with a FortiGate unit and FortiGuard
2. Adding two-factor authentication to the user's account
3. Defining an address for the internal network
4. Configuring the VPN on the FortiGate unit.
5. Configuring the VPN in FortiClient
6. Creating a security policy for VPN users



Registering FortiToken with a FortiGate unit and FortiGuard

Go to **User & Device > Two-factor Authentication > FortiTokens** and select **Create New**. Select the **Serial Number** field and enter the FortiToken serial number.

If you have several FortiTokens to add, you can list their serial numbers one per line in a text file and use the Import function.



FortiOS reports the serial number as invalid if you mistype it or if it is a duplicate.

Wait for the FortiGuard to validate your FortiToken's serial number. When you first enter the serial number, its status is listed as **Pending**. When FortiGuard validates the serial number, the status changes to **Available**.



If this FortiToken has already been registered to another FortiGate unit, the Status column shows Error.

Type Hard Token Mobile Token
Comments 0/255
Serial Number

Type	Serial Number	Status	User	Drift	Comments
	FTK2000BQL7PJW13	Available		0	

Adding two-factor authentication to the user's account

Go to **User & Device > User > User Definition** and open the user's account for editing.

Enable Two-factor Authentication and select the FortiToken from the list. Select OK.

User Name

Disable

Password

Match user on LDAP server

Match user on RADIUS server

Match user on TACACS+ server

Contact Info

Email Address

SMS FortiGuard Messaging Service Custom

Phone Number

Enable Two-factor Authentication

Token

Add this user to groups

- FortiGate_Administrators
- SslvpnGroup
- WiFi_users
- full-time
- part-time

Defining an address for the internal network

The VPN configuration and the firewall policy require a defined address for the Internal network.

Go to **Firewall Objects > Address > Addresses** and select **Create New**.

Category Address IPv6 Address Multicast Address

Name

Color

Type

Subnet / IP Range

Interface

Show in Address List

Comments 0/255

Configuring the VPN on the FortiGate unit

Go to **VPN > IPsec > Auto Key (IKE)** and select **Create VPN Wizard**.

Follow the wizard, entering the information that it requests.

The user group that you select determines who is allowed to connect to this VPN.

Clients will connect to the FortiGate unit through the WAN1 interface, which is connected to the Internet.

Address Range defines the IP address range to assign to clients.

Select the **Accessible Networks** for your clients, by selected the defined firewall address(es), or select All.

The options on the final wizard page can make the VPN more convenient to use. They are disabled by default.

1 VPN Setup 2 Authentication 3 Network 4 Client Options

Name

VPN Type

Dial Up - FortiClient Windows, Mac and Android

Dial Up - iPhone / iPad Native IPsec Client

1 VPN Setup 2 Authentication 3 Network 4 Client Options

Authentication Method Pre-shared Key RSA Signature

Pre-shared Key

User Group

1 VPN Setup 2 Authentication 3 Network 4 Client Options

Local Outgoing Interface

Address Range

Subnet Mask

DNS Server

Use System DNS

Specify

Enable IPv4 Split Tunnel

Accessible Networks

Allow Endpoint Registration

1 VPN Setup 2 Authentication 3 Network 4 Client Options

Save Password

Auto Connect

Always Up (Keep Alive)

Creating a security policy for VPN users

Go to **Policy > Policy > Policy** and select **Create New**. Enter a policy to enable VPN users to authenticate and communicate with the local network.

Policy Type Firewall VPN

Policy Subtype Address User Identity Device Identity

Incoming Interface

Source Address

Outgoing Interface

Enable NAT

- Use Destination Interface Address Fixed Port
- Use Dynamic IP Pool
- Use Central NAT Table

Enable Web cache

Enable WAN Optimization

Configure Authentication Rules

User/Group	Destination Address	Service	Schedule	Security	Traffic Shaping	Logging	Action
full-time	Local LAN	ALL	always	-			ACCEPT
ANY	all	ALL	always	-			DENY

Skip this policy for unauthenticated user

Disclaimer

Customize Authentication Messages

Tags

Applied tags

Add tag

Comments 0/1023

Configuring the VPN in FortiClient

In the FortiClient Console, select **Remote Access**, then select **Configure VPN**.



If FortiClient has other VPNs configured, select **Add a new connection** from the menu.

Enter the VPN configuration and select OK.

VPN1

- Add a new connection
- Edit the selected connection
- Delete the selected connection

Username

Password

Connection Name

Type SSL-VPN IPsec VPN

Description

Remote Gateway

Authentication Method

Pre-Shared Key

Authentication (XAuth) Prompt on login Save login

Results

In FortiClient console, select Remote Access. Select the VPN and enter the user name and password.

After connecting and authenticating by user name and password, FortiClient requests the FortiToken code.

Get the code from the FortiToken (hard token), or FortiToken Mobile app (soft token) and enter it.

If the token code is correct, the VPN connects and FortiClient minimizes its window.

On the FortiGate unit, the **VPN > Monitor > IPsec Monitor** page shows the connected client.

Auto Connect

Connect

FortiToken Code

Auto Connect

OK

Cancel

Name	Type	Username	Remote Gateway	Proxy ID	Destination
fc_vpn_0	Dialup	tbrown	172.20.120.52	10.11.10.1-10.11.10.1	