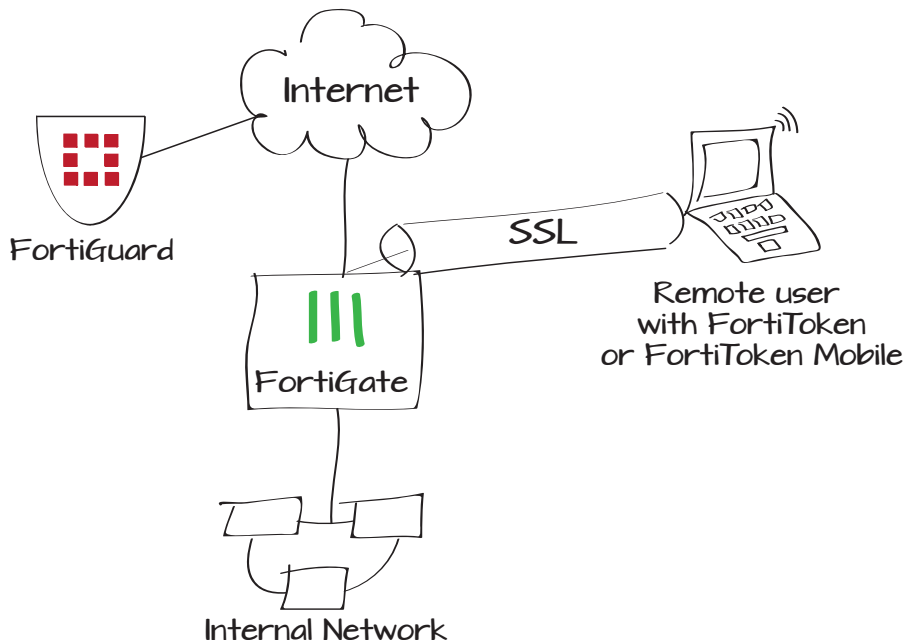


Using two-factor authentication with SSL VPN

An SSL 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 authenticated by User 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 SSL VPN on the FortiGate unit.
5. Creating a security policy for SSL 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.

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

The screenshot shows the 'User Definition' configuration page for a user named 'tbrown'. The 'Password' field is masked with '*****'. There are three radio buttons for matching user information: 'Match user on LDAP server', 'Match user on RADIUS server', and 'Match user on TACACS+ server', all with '[Please Select]' dropdown menus. The 'Contact Info' section has an unchecked 'Email Address' field and a checked 'SMS' option with 'FortiGuard Messaging Service' selected and a phone number of '613-555-1200'. The 'Enable Two-factor Authentication' section is checked, with a token dropdown set to 'FTK2000BQL7P3W13'. A list of groups is shown with 'full-time' checked. At the bottom are 'OK' and 'Cancel' buttons.

Defining an address for the internal network

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

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

The screenshot shows the 'Address' configuration page. The 'Category' is 'Address'. The 'Name' is 'Local LAN'. The 'Color' is '[Change]'. The 'Type' is 'Subnet'. The 'Subnet / IP Range' is '192.168.1.0/255.255.255.0'. The 'Interface' is 'Any'. The 'Show in Address List' checkbox is checked. The 'Comments' field is 'Write a comment...' with a character count of '0/255'. At the bottom are 'OK' and 'Cancel' buttons.

Creating a user group for SSL VPN users

Go to **User & Device > User > User Groups** and create a Firewall type user group, adding the users who will be permitted to use the SSL VPN.

Configuring an SSL VPN web portal

Go to **VPN > SSL > Config**.

The default encryption will work with typical browsers.

Name	<input type="text" value="full-time"/>
Type	<input checked="" type="radio"/> Firewall <input type="radio"/> Fortinet Single Sign-On (FSSO) <input type="radio"/> Guest
Members	<div><div><input type="text" value="tbrown"/> <input type="button" value="x"/> <input type="button" value="+"/></div><div><input type="text" value="jsmith"/> <input type="button" value="x"/></div><div><input type="text" value="blee"/> <input type="button" value="x"/></div></div>
IP Pools	<input type="text" value="SSLVPN_TUNNEL_ADDR1"/> <input type="button" value="x"/> <input type="button" value="+"/>
Server Certificate	<input type="text" value="Self-Signed"/>
Require Client Certificate	<input type="checkbox"/>
Encryption Key Algorithm	<input type="radio"/> High - AES(128/256 bits) and 3DES <input checked="" type="radio"/> Default - RC4(128 bits) and higher <input type="radio"/> Low - RC4(64 bits), DES and higher
Idle Timeout	<input type="text" value="300"/> (seconds)
Login Port	<input type="text" value="10443"/>
	<input type="checkbox"/> Allow Endpoint Registration (Tunnel Mode Only)
Advanced (DNS and WINS Servers)	
<input type="button" value="Apply"/>	

Go to **VPN > SSL > Portal**.

Creating a security policy for SSL 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.

Name:

Portal Message:

Theme:

Page Layout:

Enable Tunnel Mode

Enable Web Mode

Applications

<input checked="" type="checkbox"/> HTTP/HTTPS	<input checked="" type="checkbox"/> FTP	<input checked="" type="checkbox"/> RDP	<input checked="" type="checkbox"/> SMB/CIFS
<input checked="" type="checkbox"/> SSH	<input checked="" type="checkbox"/> TELNET	<input checked="" type="checkbox"/> VNC	<input type="checkbox"/> PING
<input checked="" type="checkbox"/> CITRIX	<input checked="" type="checkbox"/> RDP NATIVE	<input checked="" type="checkbox"/> Port Forward	

Include Session Info

Include Connection Tool

Include FortiClient Download

Include Bookmarks

Name	Type	Location	Description
No matching entries found			

Prompt Mobile Users to Download FortiClient App

Allow Multiple Concurrent Sessions For Each User

Policy Type: Firewall VPN

Policy Subtype: IPsec SSL-VPN

Incoming Interface:

Remote Address:

Local Interface:

Local Protected Subnet:

SSL Client Certificate Restrictive

Cipher Strength:

Configure SSL-VPN Authentication Rules

User/Group	Service	Schedule	Security	SSL-VPN Portal	Logging	Action
full-time	ALL	always	-	full-access		ACCEPT
ANY	ALL	always	-		-	DENY

Tags

Applied tags

Add tag

Comments

Write a comment... 0/1023

Results

In a browser, enter the FortiGate IP address and port 10443. For example <https://172.20.120.123:10443>.

If you receive a warning about the certificate being unrecognized, allow the browser to continue access.

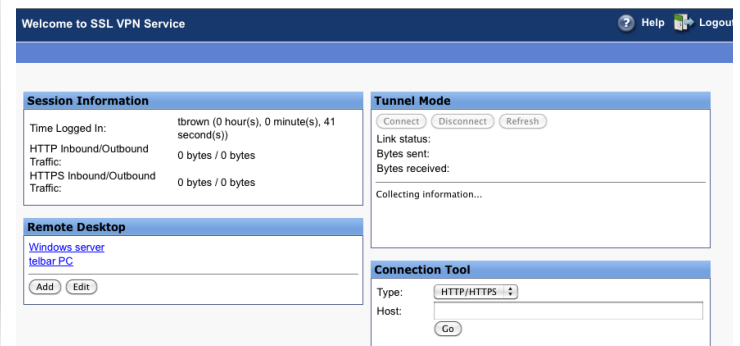
Enter the user name and password and then select **Login**. If the user account has two-factor authentication enabled, the **FortiToken Code** field is added. Obtain the code from the FortiToken device or FortiToken Mobile app and enter it. Select **Login** again.

You are connected to the SSL VPN portal.

The **VPN > Monitor > SSL-VPN Monitor** page shows the connected SSL VPN client.



The 'Please Login' form contains three input fields: 'Name' with the value 'tbrown', 'Password' with masked characters '*****', and 'FortiToken Code' with masked characters '*****'. A 'Login' button is located at the bottom right of the form.



The dashboard displays session information, tunnel mode, remote desktop, and connection tool. The session information shows the user 'tbrown' logged in for 41 seconds with zero traffic. The tunnel mode shows 'Collecting information...'. The remote desktop section lists 'Windows server' and 'telbar PC'. The connection tool shows the type as 'HTTP/HTTPS' and the host as '172.20.120.123'.

No.	User	Source IP	Begin Time	Description
1	tbrown	172.20.120.52	Thu Sep 12 10:04:32 2013	
		Subsession		Tunnel IP:10.212.134.200