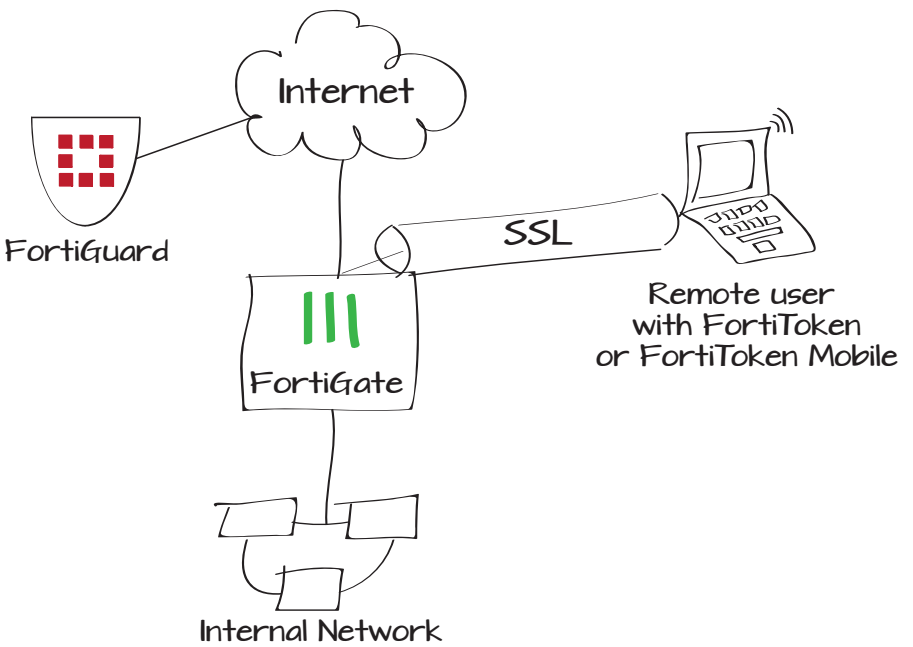
Using two-factor authentication with SSL VPN

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.

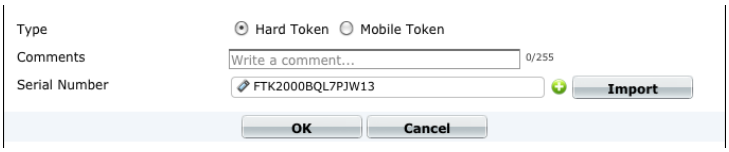
1. Registering FortiToken with a FortiGate unit and FortiGuard
2. Adding two-factor authentication to the user's account
3. Defining an address for the internal network
4. Configuring the SSL VPN on the FortiGate unit.
5. Creating a security policy for SSL VPN users



Registering FortiToken with a FortiGate unit and FortiGuard

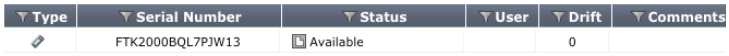
Go to **User & Device > Two-factor Authentication > FortiTokens** and select **Create New**. Select the **Serial Number** field and enter the FortiToken serial number.

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**.

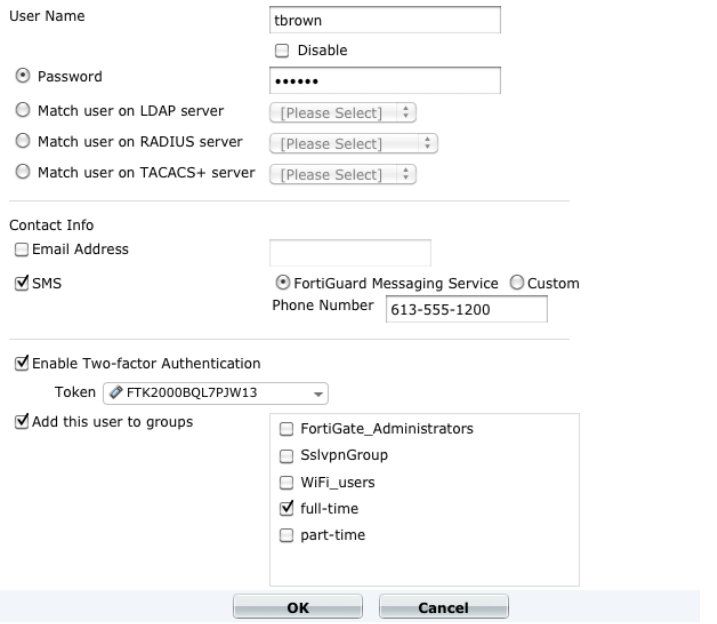


If this FortiToken has already been registered to another FortiGate unit, the Status column shows Error.

Adding two-factor authentication to the user's account

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

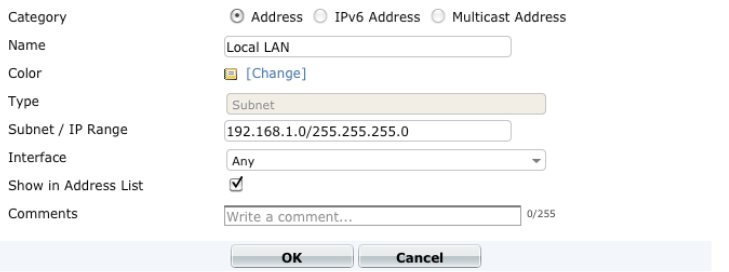
Select **Enable Two-factor Authentication** and then select the FortiToken from the list. Select OK.



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.



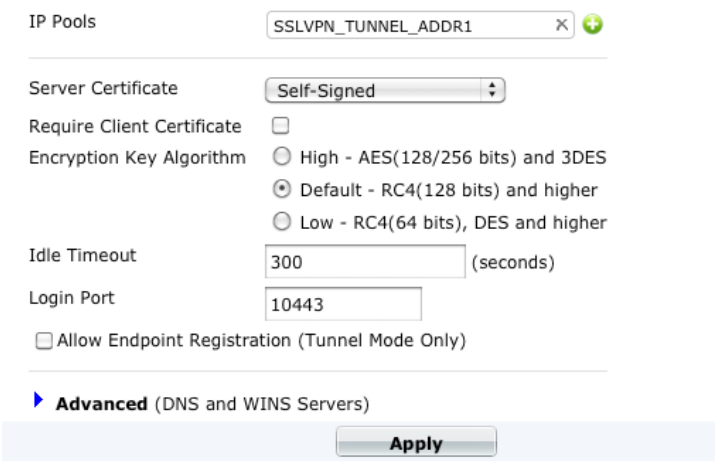
Creating a user group for SSL VPN users

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.

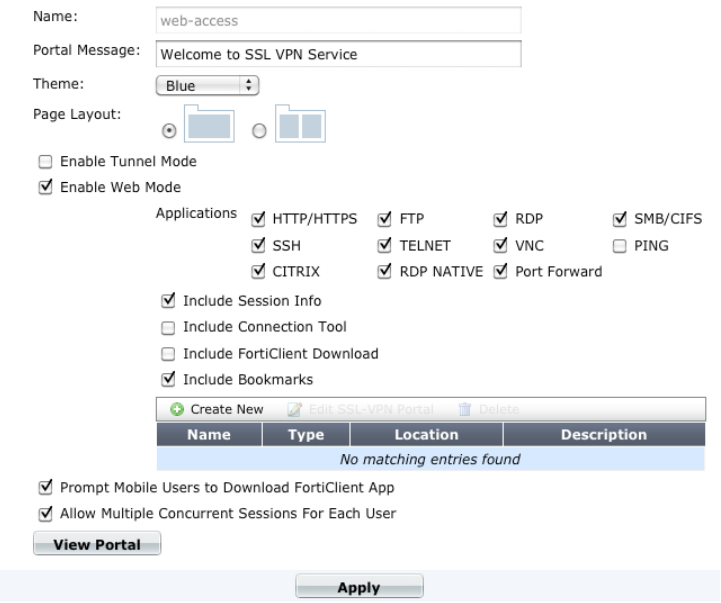
Configuring an SSL VPN web portal

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

The default encryption will work with typical browsers.

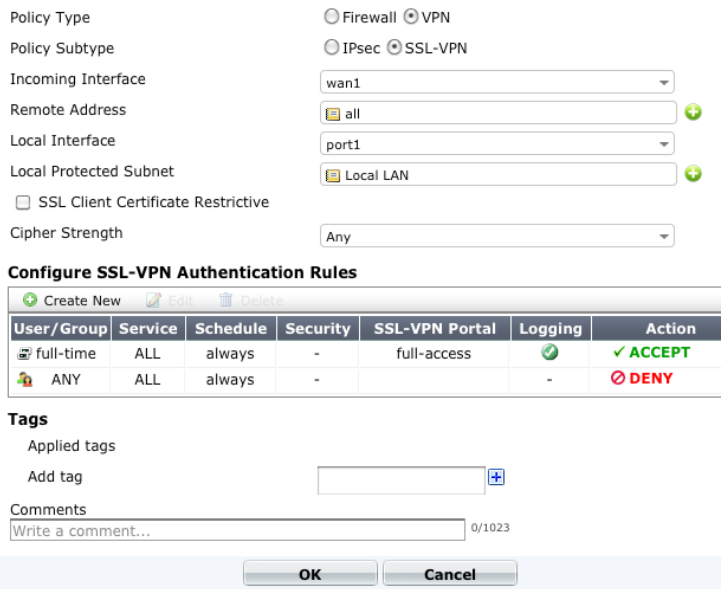


Go to **VPN > SSL > Portal**.



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.

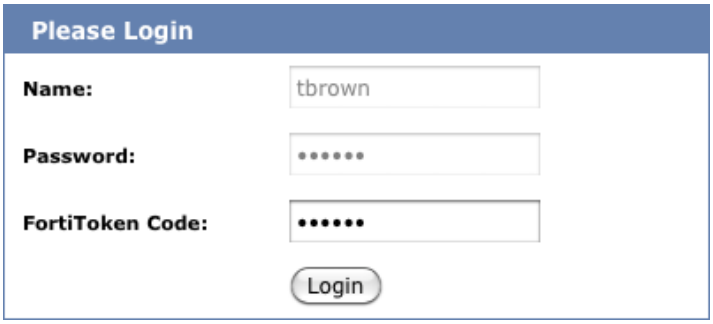


Results

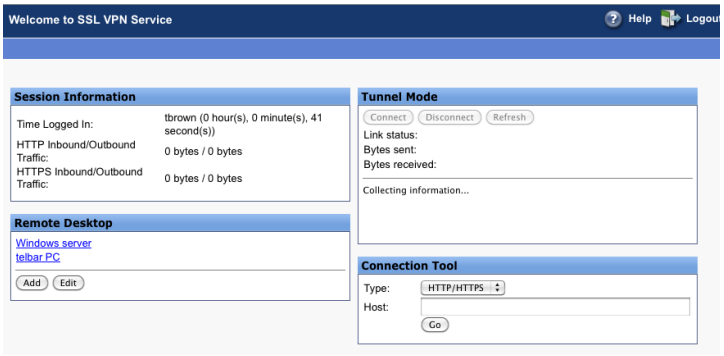
In a browser, enter the FortiGate IP address and port 10443. For example https://172.20.120.123:10443.

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.