Configuring SSL VPN with strong authentication using certificates

The FortiGate unit can require SSL VPN users to authenticate using a certificate. Similarly, the client can require the FortiGate unit to authenticate using a certificate. The client browser must have a local certificate installed, and the FortiGate unit must have the corresponding CA certificate installed.

This example includes requiring client authentication as well as enabling FortiGate unit authentication.

This example assumes that the correct CA certificate is installed on the FortiGate, and that the client browser has a corresponding local certificate.

1. Creating an SSL VPN tunnel for remote users
2. Creating a user and a user group
3. Adding an address for the local network
4. Adding security policies for access to the Internet and internal network
5. Configuring the SSL VPN server certificate
6. Results
Creating an SSL VPN tunnel for remote users

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

Edit the full-access portal.

The full-access portal allows the use of tunnel mode and/or web mode. In this example you will use both modes.

**Enable Split Tunneling** is *not* enabled so that all Internet traffic will go through the FortiGate unit and be subject to the corporate security profiles.

Creating a user and a user group

Go to **User & Device > User > User Definition**.

Add a remote user with the User Creation Wizard (in the example, ‘twhite’).
Go to **User & Device > User > User Groups.**

Add the user to a user group for SSL VPN connections.

### Adding an address for the local network

Go to **Firewall Objects > Address > Addresses.**

Add the address for the local network. Set **Type** to *Subnet, Subnet/ IP Range* to the local subnet, and **Interface** to an internal port.

### Adding security policies for access to the Internet and internal network

Go to **Policy > Policy > Policy.**

Add a security policy allowing access to the internal network. Set **Type** to *VPN* and **Subtype** to *SSL-VPN.***

Set **Incoming Interface** to your Internet-facing interface, **Local Interface** to an internal port and **Local Protected Subnet** to the address for the local network.

Create a new **Authentication Rule** to allow the remote user group access.

Enable **SSL Client Certificate Restrictive.**
You must enable the SSL Client Certificate Restrictive checkbox or certificates will not be required for the tunnel.

Add a second security policy allowing access to the Internet.

For this policy, Incoming Interface is sslvpn tunnel interface and Outgoing Interface is your Internet-facing interface.

Configuring the SSL VPN server certificate

Go to VPN > SSL > Config.

Select the desired server certificate and enable Require Client Certificate.

You must enable the Require Client Certificate checkbox or certificates will not be required for the tunnel.

Optionally, set the Encryption Key Algorithm, Idle Timeout, and Login Port as desired.

Results

On the remote client, attempt to connect to the SSL VPN tunnel using a web browser or FortiClient.
Using a web browser

Enter the tunnel IP into your web browser’s address bar.

If the client certificate has not yet been installed in the browser, you will be prompted by a warning message.

If you are absolutely certain that this is the IP you wish to connect to, click Proceed anyway to accept the certificate. Otherwise, click Back to safety (these options may vary from browser to browser).

Once the browser acknowledges the FortiGate certificate, you will be presented with a web portal login screen.

Enter the username and password associated with the VPN and click Login.

The web portal opens and displays the session information and any bookmarks that may have been assigned.

Use this portal to connect to the SSL VPN tunnel. Under Tunnel Mode, click Connect.

The connection is successful when the Link status is ‘Up’ and traffic flows.
Using FortiClient

Open the FortiClient application and create a new SSL VPN connection.

When connecting to this tunnel the first time, you are presented with a security alert asking whether or not to trust the certificate.

To install the certificate permanently, click View Certificate > Install Certificate.

Follow the Certificate Import Wizard. Click Next.
When the wizard asks you which store to place the certificate in, browse to and select the **Trusted Root Certification Authorities** store.

Click **Next**, confirm the import options, and click **Finish**. The wizard will inform you that the certificate imported successfully.

Click **OK** until you are back at the security alert and click **Yes**.

The tunnel should now activate.

The next time you connect to this tunnel you won’t need to reimport the certificate, unless of course you imported it incorrectly the first time.