IPSec VPN

IPsec VPN is a common method for enabling private communication over the Internet. IPsec supports a similar client server architecture as SSL VPN. However, to support a client server architecture, IPsec clients must install and configure an IPsec VPN client (such as Fortinet’s FortiClient Endpoint Security) on their PCs or mobile devices. IPsec client configurations can be cryptic and complex, usually making SSL VPN more convenient for users with little networking knowledge.

However IPsec VPN supports more configurations than SSL VPN. A common application of IPsec VPN is for a gateway to gateway configuration that allows users to transparently communicate between remote networks over the Internet. When a user on one network starts a communication session with a server on the other network, a security policy configured for IPsec VPN intercepts the communication session and uses an associated IPsec configuration to both encrypt the session for privacy but also transparently route the session over the Internet to the remote network. At the remote network the encrypted communication session is intercepted and decrypted by the IPsec gateway at the remote network and the unencrypted traffic is forwarded to the server. Responses from the server than pass back over the encrypted tunnel to the client.

Many variations of the gateway to gateway configuration are available depending on the requirements. In addition to gateway to gateway IPsec VPNs, FortiGate units also support various mesh IPsec VPN configurations that can allow transparent communication between networks at multiple locations around the world.

FortiGate units also support automated IPsec configuration of FortiClient software running on client PCs.

All communication over IPsec VPNs is controlled by security policies. Security policies allow for full access control and can be used to apply UTM and other features to IPsec VPN traffic.

Fortinet IPsec VPNs employs industry standard features to ensure the best security and interoperability with industry standard VPN solutions provided by other vendors.

This chapter includes the following IPsec VPN examples:

- Protecting communication between offices across the Internet using IPsec VPN
- Using FortiClient VPN for secure remote access to an office network
- Using IPsec VPN to secure iPhone communication with a network protected by a FortiGate unit
- Using IPsec VPN to secure Android mobile device communication with a network protected by a FortiGate unit
- Using the FortiGate FortiClient VPN Wizard to set up a VPN between a remote users and a private network
- My IPsec VPN tunnel isn’t working
Protecting communication between offices across the Internet using IPsec VPN

**Problem**  You need to provide secure transparent communication between company headquarters (HQ) and a branch office.

**Solution**  Create a gateway-to-gateway IPsec VPN between headquarters and the branch office.

This basic gateway-to-gateway IPsec VPN assumes that both office have connections to the Internet with static IP addresses. This configure uses a simple policy-based IPsec VPN configuration.

**Configure the HQ FortiGate**

1. Go to **VPN > IPsec > Auto Key (IKE)**, select **Create Phase 1** and configure the IPsec VPN phase 1 configuration.

<table>
<thead>
<tr>
<th>Name</th>
<th>HQ_to.Branch_p1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Remote Gateway</td>
<td>Static IP Address</td>
</tr>
<tr>
<td>IP Address</td>
<td>172.20.120.122</td>
</tr>
<tr>
<td>Local Interface</td>
<td>wan1</td>
</tr>
<tr>
<td>Mode</td>
<td>Main (ID protection)</td>
</tr>
<tr>
<td>Authentication Method</td>
<td>Preshared Key</td>
</tr>
<tr>
<td>Pre-shared Key</td>
<td>fortinet123</td>
</tr>
</tbody>
</table>

2. Select **OK**.

3. Select **Create Phase 2** and enter the following information.

<table>
<thead>
<tr>
<th>Name</th>
<th>HQ_to.Branch_p2</th>
</tr>
</thead>
<tbody>
<tr>
<td>Phase 1</td>
<td>HQ_to.Branch_p1</td>
</tr>
</tbody>
</table>

4. Select **OK**.

5. Go to **Firewall Objects > Address > Address** and select **Create New** to add a firewall address for the HQ network.

<table>
<thead>
<tr>
<th>Name</th>
<th>HQ.net</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type</td>
<td>Subnet / IP Range</td>
</tr>
<tr>
<td>Subnet / IP Range</td>
<td>10.10.10.0/255.255.255.0</td>
</tr>
<tr>
<td>Interface</td>
<td>internal</td>
</tr>
</tbody>
</table>
6. Select **Create New** to add a firewall address for the branch office network.

<table>
<thead>
<tr>
<th>Name</th>
<th>Branch_net</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type</td>
<td>Subnet / IP Range</td>
</tr>
<tr>
<td>Subnet / IP Range</td>
<td>192.168.1.0/255.255.255.0</td>
</tr>
<tr>
<td>Interface</td>
<td>wan1</td>
</tr>
</tbody>
</table>

7. Select **OK**.

8. Go to **Policy > Policy > Policy** and select **Create New** to add a security policy for the IPsec VPN.

<table>
<thead>
<tr>
<th>Source Interface/Zone</th>
<th>internal</th>
</tr>
</thead>
<tbody>
<tr>
<td>Source Address</td>
<td>HQ_net</td>
</tr>
<tr>
<td>Destination Interface/Zone</td>
<td>wan1</td>
</tr>
<tr>
<td>Destination Address</td>
<td>Branch_net</td>
</tr>
<tr>
<td>Schedule</td>
<td>always</td>
</tr>
<tr>
<td>Service</td>
<td>ANY</td>
</tr>
<tr>
<td>Action</td>
<td>IPSEC</td>
</tr>
<tr>
<td>VPN Tunnel</td>
<td>HQ_to_Branch_p1</td>
</tr>
</tbody>
</table>

9. Select **Allow inbound** and **Allow outbound**.

10. Select **OK**.

**Configure the Branch office**

The branch office settings are almost identical to the HQ settings.

1. Go to **VPN > IPsec > Auto Key (IKE)**, select **Create Phase 1** and configure the IPsec VPN phase 1 configuration.

<table>
<thead>
<tr>
<th>Name</th>
<th>Branch_to_HQ_p1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Remote Gateway</td>
<td>Static IP Address</td>
</tr>
<tr>
<td>IP Address</td>
<td>172.20.120.200</td>
</tr>
<tr>
<td>Local Interface</td>
<td>wan1</td>
</tr>
<tr>
<td>Mode</td>
<td>Main (ID protection)</td>
</tr>
<tr>
<td>Authentication Method</td>
<td>Preshared Key</td>
</tr>
<tr>
<td>Pre-shared Key</td>
<td>fortinet123</td>
</tr>
</tbody>
</table>

2. Select **OK**.

3. Select **Create Phase 2**.
4. Enter the following information, and select OK.

<table>
<thead>
<tr>
<th>Name</th>
<th>Branch_to_HQ_p2</th>
</tr>
</thead>
<tbody>
<tr>
<td>Phase 1</td>
<td>Branch_to_HQ_p1</td>
</tr>
</tbody>
</table>

5. Select **OK**.

6. Go to **Firewall Objects > Address > Address** and select **Create New** to add a firewall address for the HQ network.

<table>
<thead>
<tr>
<th>Name</th>
<th>Branch_net</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type</td>
<td>Subnet / IP Range</td>
</tr>
<tr>
<td>Subnet / IP Range</td>
<td>192.168.1.0/255.255.255.0</td>
</tr>
<tr>
<td>Interface</td>
<td>internal</td>
</tr>
</tbody>
</table>

7. Select **Create New** to add a firewall address for the branch office network.

<table>
<thead>
<tr>
<th>Name</th>
<th>HQ_net</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type</td>
<td>Subnet / IP Range</td>
</tr>
<tr>
<td>Subnet / IP Range</td>
<td>10.10.10.0/255.255.255.0</td>
</tr>
<tr>
<td>Interface</td>
<td>wan1</td>
</tr>
</tbody>
</table>

8. Select **OK**.

9. Go to **Policy > Policy > Policy** and select **Create New** to add a security policy for the IPsec VPN.

<table>
<thead>
<tr>
<th>Source Interface/Zone</th>
<th>internal</th>
</tr>
</thead>
<tbody>
<tr>
<td>Source Address</td>
<td>Branch_net</td>
</tr>
<tr>
<td>Destination Interface/Zone</td>
<td>wan1</td>
</tr>
<tr>
<td>Destination Address</td>
<td>HQ_net</td>
</tr>
<tr>
<td>Schedule</td>
<td>always</td>
</tr>
<tr>
<td>Service</td>
<td>ANY</td>
</tr>
<tr>
<td>Action</td>
<td>IPSEC</td>
</tr>
<tr>
<td>VPN Tunnel</td>
<td>Branch_to_HQ_p1</td>
</tr>
</tbody>
</table>

10. Select **Allow inbound** and **Allow outbound**.

11. Select **OK**.

**Results**

A user on either of the office networks should be able to connect to any address on the other office network transparently. For example, from a PC on the branch office with IP address 192.168.1.100 you should be able to ping a device on the HQ network with PIP address 10.10.10.100.

When the VPN is operating you should be able to go to **VPN > Monitor > IPsec Monitor** and verify that its status is up.
Using FortiClient VPN for secure remote access to an office network

Problem
You need a secure communication channel between FortiClient on a remote user and the office so that the user can access work network resources. You also want to require individual IPsec VPN uses to authenticate to get access.

Solution
Create an IPSec VPN between FortiClient on the remote user's PC and the office FortiGate unit that uses XAuth to authenticate the remote user. The remote user's IP address changes so you need to configure a dialup IPsec VPN on the FortiGate unit. As well the remote user must start the VPN because the office FortiGate unit doesn't know the user's IP address.

Creating a user and user group to support XAuth

1. Go to User > User > User and select Create New to add the user:

<table>
<thead>
<tr>
<th>User Name</th>
<th>fsmith</th>
</tr>
</thead>
<tbody>
<tr>
<td>Password</td>
<td>passw0rd</td>
</tr>
</tbody>
</table>

2. Go to User > User Group > User Group and select Create New to add fsmith to the user group:

<table>
<thead>
<tr>
<th>Name</th>
<th>FortiClient_group</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type</td>
<td>Firewall</td>
</tr>
</tbody>
</table>

3. Move fsmith to the Members list.
4. Select OK.

Creating the IPsec VPN phase 1 and phase 2 and a DHCP server for the IPsec VPN

1. Go to VPN > IPsec > Auto Key (IKE), select Create Phase 1 and configure Phase 1.

<table>
<thead>
<tr>
<th>Name</th>
<th>FortiClient_VPN</th>
</tr>
</thead>
<tbody>
<tr>
<td>Remote Gateway</td>
<td>Dialup User</td>
</tr>
<tr>
<td>Local Interface</td>
<td>wan1</td>
</tr>
<tr>
<td>Mode</td>
<td>Main (ID protection)</td>
</tr>
<tr>
<td>Authentication Method</td>
<td>Preshared Key</td>
</tr>
<tr>
<td>Pre-shared Key</td>
<td>fortinet123</td>
</tr>
<tr>
<td>Peer Options</td>
<td>Accept any peer ID</td>
</tr>
</tbody>
</table>

2. Select Advanced to configure advanced settings.
3. Select **Enable IPsec Interface Mode** and configure the following:

<table>
<thead>
<tr>
<th>Setting</th>
<th>Configuration</th>
</tr>
</thead>
<tbody>
<tr>
<td>IKE Version</td>
<td>1</td>
</tr>
<tr>
<td>IPv6 Version</td>
<td>Clear check box.</td>
</tr>
<tr>
<td>Local Gateway IP</td>
<td>Main Interface IP</td>
</tr>
<tr>
<td>DNS Server</td>
<td>Use System DNS</td>
</tr>
</tbody>
</table>
| P1 Proposal              | 1 - Encryption 3DES Authentication SHA1  
                            | 2 - Encryption AES128 Authentication SHA1 |
| DH Group                 | 5                         |
| Keylife                  | 28800                     |
| Local ID                 | Leave blank.              |
| XAuth                    | Enable as Server          |
| Server Type              | PAP                       |
| User Group               | FortiClient_group         |
| NAT Traversal            | Enable                    |
| Keepalive Frequency      | 10                        |
| Dead Peer Detection      | Enable                    |

4. Select OK.

Go to **System > Network > Interface** and verify that a tunnel interface named **FortiClient_VPN** has been added under the **wan1** interface.

**Edit** the **FortiClient_VPN** tunnel interface and verify that the **IP** and **Remote IP** are both 0.0.0.0. These IPs must be set to 0.0.0.0 for the DHCP server to supply IP addresses to the remote users.

5. Go to **System > Interface > DHCP server** and elect **Create New** to add a DHCP server for the IPsec VPN

<table>
<thead>
<tr>
<th>Setting</th>
<th>Configuration</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface Name</td>
<td>FortiClient_VPN</td>
</tr>
<tr>
<td>Mode</td>
<td>Server</td>
</tr>
<tr>
<td>Enable</td>
<td>Select</td>
</tr>
<tr>
<td>Type</td>
<td>IPsec</td>
</tr>
<tr>
<td>IP</td>
<td>10.254.254.1 - 10.254.254.254</td>
</tr>
<tr>
<td>Network Mask</td>
<td>255.255.255.0</td>
</tr>
<tr>
<td>Default Gateway</td>
<td>172.20.120.146</td>
</tr>
<tr>
<td>DNS Service</td>
<td>Use System DNS Setting</td>
</tr>
</tbody>
</table>

6. Select **OK**.
Using FortiClient VPN for secure remote access to an office network

7 Go to **VPN > IPsec > Auto Key (IKE)** and select **Create Phase 2** to configure the phase 2 for the IPsec VPN.

<table>
<thead>
<tr>
<th>Name</th>
<th>FortiClient_VPN2</th>
</tr>
</thead>
<tbody>
<tr>
<td>Phase 1</td>
<td>FortiClient_VPN</td>
</tr>
</tbody>
</table>

8 Select **Advanced** to configure advanced settings.

| P1 Proposal                      | 1 - Encryption 3DES Authentication SHA1  
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>2 - Encryption AES128 Authentication SHA1</td>
</tr>
<tr>
<td>Enable Replay Detection</td>
<td>Select</td>
</tr>
<tr>
<td>Enable perfect forward secrecy (PFS)</td>
<td>Select</td>
</tr>
<tr>
<td>DH Group</td>
<td>5</td>
</tr>
<tr>
<td>Keylife</td>
<td>1800 Seconds</td>
</tr>
<tr>
<td>Autokey Keep Alive</td>
<td>Do not select</td>
</tr>
<tr>
<td>DHCP-IPsec</td>
<td>Enable</td>
</tr>
</tbody>
</table>

If **DHCP-IPsec** is grey, there is no valid DHCP server attached to the FortiClient _VPN tunnel interface. If there are static IP addresses assigned to the FortiClient_VPN tunnel interface **IP** and **Remote IP** you must delete the Phase1 entry and start again. The DHCP server will not work if static IPs are assigned to the FortiClient_VPN tunnel interface.

Creating a static route and security policies for the IPsec VPN configuration

There is one policy each for inbound and outbound traffic. Network services such as DNS require policies in both directions.

1 Go to **Router > Static > Static Route** and select **Create New** to add a static route for the IPsec VPN.

<table>
<thead>
<tr>
<th>Destination IP/Mask</th>
<th>10.254.254.0/255.255.255.0</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device</td>
<td>FortiClient_VPN</td>
</tr>
</tbody>
</table>

The static route ensures that traffic for the VPN doesn’t leave the FortiGate for the default gateway. When you select the VPN interface as the Device, there is no requirement for a gateway, as shown by it being greyed out.

2 Select **OK**.

3 Go to **Policy > Policy > Policy** and select **Create New** to configure a policy to allow incoming IPsec VPN traffic on the FortiClient_VPN interface.

<table>
<thead>
<tr>
<th>Source Interface/Zone</th>
<th>FortiClient_VPN</th>
</tr>
</thead>
<tbody>
<tr>
<td>Source Address</td>
<td>all</td>
</tr>
<tr>
<td>Destination Interface/Zone</td>
<td>wan1</td>
</tr>
</tbody>
</table>
Select  **Enable Identity Based Policy**.
5 Select  **Add** to add an authentication rule with the following settings:

<table>
<thead>
<tr>
<th>Selected User Groups</th>
<th>FortiClient_group</th>
</tr>
</thead>
<tbody>
<tr>
<td>Selected Services</td>
<td>ANY</td>
</tr>
<tr>
<td>Schedule</td>
<td>always</td>
</tr>
<tr>
<td>Log Allowed Traffic</td>
<td>Enable</td>
</tr>
<tr>
<td>Schedule</td>
<td>always</td>
</tr>
</tbody>
</table>

6 Select  **OK**.
7 Select  **OK** to save the security policy.
8 Select  **Create New** to configure a policy to allow outgoing IPsec VPN traffic on the  FortiClient_VPN interface:

<table>
<thead>
<tr>
<th>Source Interface/Zone</th>
<th>wan1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Source Address</td>
<td>all</td>
</tr>
<tr>
<td>Destination Interface/Zone</td>
<td>FortiClient_VPN</td>
</tr>
<tr>
<td>Destination Address</td>
<td>all</td>
</tr>
<tr>
<td>Schedule</td>
<td>always</td>
</tr>
<tr>
<td>Service</td>
<td>ANY</td>
</tr>
<tr>
<td>Action</td>
<td>ACCEPT</td>
</tr>
</tbody>
</table>

9 Select  **Enable Identity Based Policy**.
10 Select  **Add** to add an authentication rule with the following settings:

<table>
<thead>
<tr>
<th>Selected User Groups</th>
<th>FortiClient_group</th>
</tr>
</thead>
<tbody>
<tr>
<td>Selected Services</td>
<td>ANY</td>
</tr>
<tr>
<td>Schedule</td>
<td>always</td>
</tr>
<tr>
<td>Log Allowed Traffic</td>
<td>Enable</td>
</tr>
<tr>
<td>Schedule</td>
<td>always</td>
</tr>
</tbody>
</table>

11 Select  **OK**.
12 Select  **OK** to save the security policy.
Configure FortiClient

These instructions were tested on FortiClient 4.2.1, and FortiClient 4.3.2.

1. On the remote computer, start the FortiClient console.
2. Go to VPN > Connections.
4. Enter the following information.

<table>
<thead>
<tr>
<th>Connection Name</th>
<th>Work_VPN</th>
</tr>
</thead>
<tbody>
<tr>
<td>VPN Type</td>
<td>Manual IPsec</td>
</tr>
<tr>
<td>Remote Gateway</td>
<td>172.20.120.146</td>
</tr>
<tr>
<td>Remote Network</td>
<td>10.254.254.0 / 255.255.255.0</td>
</tr>
<tr>
<td>Authentication Method</td>
<td>Preshared Key</td>
</tr>
<tr>
<td>Pre-Shared Key</td>
<td>fortinet123</td>
</tr>
</tbody>
</table>

5. Select Advanced to open a new window.
6. Enter the following information.

<table>
<thead>
<tr>
<th>Acquire virtual IP address</th>
<th>Enable and select Config to ensure DHCP is set.</th>
</tr>
</thead>
<tbody>
<tr>
<td>eXtended Authentication</td>
<td>Enable and select Config to ensure Prompt to login is set.</td>
</tr>
<tr>
<td>Remote Network</td>
<td>If you don’t see 172.20.120.0 / 255.255.255.0 here, now is your chance to fix it.</td>
</tr>
</tbody>
</table>

7. Under Policy, select Config to open a new window.
8. For both IKE and IPsec Proposals, remove the MD5 authentication entries.
10. Under Advanced Options, make sure that NAT Traversal is enabled.
11. Select OK three times to close the Connection Detailed Settings, the Advanced Settings, and the New Connection windows.

Results

You know your VPN is successful when you select the VPN on FortiClient, select Connection, and receive a “Connection Successfull!” message. In FortiClient the status next to the VPN connection will read Up with the number of seconds it has been up, in brackets.

To ensure your new VPN works, from FortiClient select the Work_VPN entry, and then select Advanced > Test. This will open a window and show each step of the attempted connection. If there are any problems they will be visible here and easy to troubleshoot. For additional information, check the event log of the FortiGate unit (Log&Report > Log & Archive Access > Event Log) where you especially want to read the Message, Action, and Error Reason parts of the log messages to help you troubleshoot.

Some useful troubleshooting checks include:
- Ensure both pre-shared keys match exactly.
- Ensure both ends use the same P1 Proposal settings.
- Ensure both ends are using main mode, unless there are connection problems and you want to try aggressive mode on both ends which is easier to connect but less secure.
• Ensure XAuth settings are the same for both ends, with the FortiGate unit being the Server if its enabled.

• Ensure P2 Proposal details on the FortiGate unit match those on FortiClient (under Advanced > Policy Config, IKE is Phase1 and IPsec is Phase 2) — DH group, pfs, dpd, replay detection, keylife, and auto keep alive.

• When working with policy routing, ensure you have allowed inbound and outbound, especially if network services such as DNS or DHCP are having problems.

• Check your NAT settings - for best results NAT traversal is enabled in the Phase 1 configuration, and NAT is not enabled in the security policy.

• If the negotiation is OK but there is no traffic, check the route.

• Only the FortiClient end can initiate the VPN tunnel because the FortiGate doesn’t know the FortiClient IP address.

**Best Practices**

There are CLI only options that can help with FortiClient VPNs in certain situations.

<table>
<thead>
<tr>
<th>Phase</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Phase1</td>
<td>set forticlient-enforcement {enable</td>
<td>disable}</td>
</tr>
<tr>
<td>Phase2</td>
<td>set add-route {enable</td>
<td>disable}</td>
</tr>
<tr>
<td></td>
<td>set encapsulation {tunnel-mode</td>
<td>transport-mode}</td>
</tr>
</tbody>
</table>
Using IPsec VPN to secure iPhone communication with a network protected by a FortiGate unit

**Problem** You need to configure an iPhone for a user, F. Smith, to access a web server at work over a secure connection.

**Solution** The easiest way to connect to the office from a remote location is by an IPsec VPN. It is secure and it appears as if you are physically on the network at work. The iPhone IPsec client is a Cisco UNITY client.

In this example, user *fsmith* is part of the iPhone Users usergroup. *fsmith*’s iPhone will be assigned an IP address in the range 172.16.1.1 - 172.16.1.254. The VPN is interface based.

You already have three security policies to allow traffic to flow on your network—Internal to Wan1, Internal to dmz, and dmz to Internal.

For this example an Apple iPhone 4 running iOS 4.3.5 was used. Menu options may vary for different models and iOS versions.

The steps involved include:
- Configure the user *fsmith*, and the user group iPhoneVPN.
- Configure the firewall address ranges called DMZ_WebServers and iPhoneVPNUsers.
- Configure IPsec VPN Phase1.
- Configure IPsec VPN Phase2 in the CLI.
- Configure iPhone VPN Phase 1 access to the DMZ subnet.
- Configure an IPsec security policy between the iPhoneVPNUsers and DMZ_Servers.
- Configure the iPhone VPN settings.

**Create fsmith user account, and iPhoneVPN group**
1. Go to *User > User > User and* select *Create New* and add a user account for and iPhone user.

<table>
<thead>
<tr>
<th>User Name</th>
<th>fsmith</th>
</tr>
</thead>
<tbody>
<tr>
<td>Password</td>
<td>my1pwd</td>
</tr>
</tbody>
</table>

2. Select **OK**.
3. Go to *User > User Group > User Group and* select *Create New* to create a user group for iPhone users.

<table>
<thead>
<tr>
<th>Name</th>
<th>iPhoneVPN</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type</td>
<td>Firewall</td>
</tr>
<tr>
<td>Available USers</td>
<td>Move <em>fsmith</em> to Members list.</td>
</tr>
</tbody>
</table>

4. Select **OK**.
Using IPsec VPN to secure iPhone communication with a network protected by a FortiGate unit

Create a firewall addresses for the web server on DMZ and iPhone Users

1. Go to **Firewall Objects > Address > Address** and select **Create New** to enter the following information.

<table>
<thead>
<tr>
<th>Address Name</th>
<th>DMZ_WebServer</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type</td>
<td>Subnet / IP Range</td>
</tr>
<tr>
<td>Subnet / IP Range</td>
<td>10.0.0.0/255.255.255.0</td>
</tr>
<tr>
<td>Interface</td>
<td>dmz</td>
</tr>
</tbody>
</table>

2. Select **OK**.

3. Select **Create New** and enter the following information.

<table>
<thead>
<tr>
<th>Address Name</th>
<th>iPhoneVPNUsers</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type</td>
<td>Subnet / IP Range</td>
</tr>
<tr>
<td>Subnet / IP Range</td>
<td>172.16.1.0/255.255.255.0</td>
</tr>
<tr>
<td>Interface</td>
<td>Any</td>
</tr>
</tbody>
</table>

4. Select **OK**.

Configure IPsec Phase1 settings

1. Go to **VPN > IPsec Auto Key (IKE)** and select **Create Phase 1** to enter the following information.

<table>
<thead>
<tr>
<th>Name</th>
<th>iPhone</th>
</tr>
</thead>
<tbody>
<tr>
<td>Remote Gateway</td>
<td>Dialup User</td>
</tr>
<tr>
<td>Local Interface</td>
<td>wan1</td>
</tr>
<tr>
<td>Mode</td>
<td>Main</td>
</tr>
<tr>
<td>Authentication Method</td>
<td>Preshared Key</td>
</tr>
<tr>
<td>Preshared Key</td>
<td>mykey123</td>
</tr>
<tr>
<td>Peer Options</td>
<td>Accept any peer ID</td>
</tr>
</tbody>
</table>

2. Select **Advanced** and enter the following information.

<table>
<thead>
<tr>
<th>Enable IPsec Interface Mode</th>
<th>Enable</th>
</tr>
</thead>
<tbody>
<tr>
<td>IKE Version</td>
<td>1</td>
</tr>
<tr>
<td>Local Gateway IP</td>
<td>Main Interface IP</td>
</tr>
<tr>
<td>DNS Server</td>
<td>Use System DNS</td>
</tr>
<tr>
<td>1 - Encryption</td>
<td>AES256</td>
</tr>
<tr>
<td>1 - Authentication</td>
<td>MD5</td>
</tr>
<tr>
<td>2 - Encryption</td>
<td>AES256</td>
</tr>
</tbody>
</table>
Using IPsec VPN to secure iPhone communication with a network protected by a FortiGate unit

2 - Authentication | SHA1
DH Group | 2
Key life (sec) | 28800
XAUTH | Enable as Server
Server Type | AUTO
User Group | iPhoneVPNUsers
NAT Traversal | enable
Keepalive Frequency | 10
Dead Peer Detection | Enable

3 Select **OK**.

Configure IPsec Phase2

1 Go to **VPN > IPSec > Auto Key** and select **Create Phase 2** to enter the following information.

| Name | iPhone_P2 |
| Phase1 | iPhone |

2 Select **Advanced** and enter the following information.

| 1 Encryption | AES256 |
| 1 Authentication | MD5 |
| 2 Encryption | AES256 |
| 2 Authentication | SHA1 |
| Enable replay detection | Enable |
| Enable perfect forward secrecy (PFS) | Enable |
| DH Group | 2 |
| Keylife | Seconds 1800 |
| Auto-key keep alive | Enable |
| Quick Mode Selector | Source Address: 0.0.0.0/0 |
| Source port: 0 |
| Destination Address: 0.0.0.0/0 |
| Destination port: 0 |
| Protocol: 0 |

3 Select **OK**.
Configure iPhone VPN Phase 1 access to the DMZ subnet

1. Enter the following CLI commands.

```
config vpn ipsec phase1-interface
edit iPhone
  set mode-cfg enable
  set unity-support enable
  set assign-ip enable
  set assign-ip-from range
  set mode-cfg-ip-version 4
  set ipv4-start-ip 172.16.1.1
  set ipv4-end-ip 172.16.1.254
  set ipv4-netmask 255.255.255.0
  set ipv4-split-include DMZ_WebServer
end
```

Create a new security policy for the VPN

1. Go to Policy > Policy and select Create new to enter the following information

<table>
<thead>
<tr>
<th>Source Interface/Zone</th>
<th>iPhone</th>
</tr>
</thead>
<tbody>
<tr>
<td>Source Address</td>
<td>iPhoneVPNUsers</td>
</tr>
<tr>
<td>Destination Interface/Zone</td>
<td>DMZ</td>
</tr>
<tr>
<td>Destination Address</td>
<td>DMZ_WebServer</td>
</tr>
<tr>
<td>Schedule</td>
<td>Always</td>
</tr>
<tr>
<td>Service</td>
<td>ANY</td>
</tr>
<tr>
<td>Action</td>
<td>Accept</td>
</tr>
<tr>
<td>Enable NAT</td>
<td>Disable</td>
</tr>
</tbody>
</table>

2. Select OK.
3. Move this policy to the top of the policy list, to ensure it will be matched first.

Configure the iPhone

1. On the iPhone, go to Settings > General > Network > VPN.
2. Select Add VPN Configuration > L2TP
3. Enter the following information, and select Save.

<table>
<thead>
<tr>
<th>Description</th>
<th>Office_VPN</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server</td>
<td>210.0.0.1</td>
</tr>
<tr>
<td>Account</td>
<td>fsmith</td>
</tr>
<tr>
<td>RSA SecurID</td>
<td>OFF</td>
</tr>
<tr>
<td>Password</td>
<td>my1pwd</td>
</tr>
<tr>
<td>Secret</td>
<td>mykey123</td>
</tr>
<tr>
<td>Send All Traffic</td>
<td>ON</td>
</tr>
</tbody>
</table>
The **Send all traffic** option will send everything on the iPhone through the VPN. If this option is turned off, only traffic addressed to the VPN will use the tunnel. If the iPhone is used for work, this option should be turned on to force all iPhone data to be encrypted and forced through the office FortiGate firewall.

**Results**

To test the configuration:

1. Ensure the iPhone has access to a data network.
2. Select the Office_VPN, and turn VPN ON.

The iPhone will attempt to connect for a while.

During this time, on the FortiGate unit you can:

- monitor the VPN connection with the VPN monitor
- refresh the event log entries to see the entry for each step of the VPN connection if you are logging VPN events
- run `diag debug` on the CLI for full details of the connection attempt.

When the VPN connects, you will see event log entries and have access to the internal web server as expected. If there are problems, check the logs for messages to tell you what happened. Also consider running the CLI commands:

```bash
diag debug disable
diag debug application ike -l
diag debug enable
```

When your VPN connection is established on your iPhone there will be a small VPN tag at the top of the screen. However, this is easily missed. If you want a clear message that your VPN connection is up and working on the iPhone, then enter the following CLI command:

```bash
config vpn ipsec phase1-interface
edit iPhone
  set banner "YOU ARE NOW CONNECTED"
next
end
```

This creates a pop-up banner message that is displayed on your iPhone when the VPN connection is successful.

The configuration here allows access to an internal web server. If you want to access additional internal subnets you can create firewall addresses for each one, and then add them to a firewall address group, called `my_addr_grp` for example. Then you will need to enter the following CLI commands:

```bash
config vpn ipsec phase1-interface
edit iPhone
  set ipv4-split-include my_addr_grp
next
end
```
Using IPsec VPN to secure Android mobile device communication with a network protected by a FortiGate unit

Problem  A user on your network, W. Loman, has an Android device and needs access to the office servers over a secure connection.

Solution  The easiest way to connect to the office from a remote location is by VPN. It is secure and it appears as if you are physically on the network at the office. A common type of VPN is L2TP.

In this example, user w\textit{loman} is part of the Android\textunderscore Users usergroup. The Android mobile device will be assigned an IP address in the range 192.168.1.[90-99]. This is a VPN policy — it is not interface based.

For this example an LG P999 mobile phone running Android 2.2.2 was used. Menu options may vary for different models or versions of the Android OS.

The steps involved include:

- Configure the user w\textit{loman}, and the user group Android\textunderscore Users.
- Configure the firewall address ranges called Android\textunderscore Range, and DMZ\textunderscore Servers.
- Configure the FortiGate as an L2TP server in the CLI.
- Configure IPsec VPN Phase 1.
- Configure IPsec VPN Phase 2 in the CLI, also known as the Security Association (SA).
- Configure an IPsec security policy between the Android\textunderscore Users and DMZ\textunderscore Servers.
- Configure the Android device VPN settings.

Create the user account for w\textit{loman}

1. Go to \textit{User > User > User}, select \textit{Create New} and create the following user account:

   \begin{tabular}{|l|l|}
   \hline
   Name & w\textit{loman} \\
   \hline
   Password & my1pass \\
   \hline
   \end{tabular}

2. Select \textit{OK}.

3. Go to \textit{User > User Group > User Group} select \textit{Create New} to create a user group for Android users.

   \begin{tabular}{|l|l|}
   \hline
   Name & Android\textunderscore users \\
   \hline
   Type & Firewall \\
   \hline
   Available Users & Select \textit{w\textit{loman}} and move to Members list \\
   \hline
   \end{tabular}

4. Select \textit{OK}.
Using IPsec VPN to secure Android mobile device communication with a network protected by a FortiGate unit

Configure the firewall address for Android_Range and DMZ_Servers

1. Go to **Firewall Objects > Address > Address** and select **Create New** to add a firewall address for Android users.

<table>
<thead>
<tr>
<th>Address Name</th>
<th>Android_Users</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type</td>
<td>Subnet / IP Range</td>
</tr>
<tr>
<td>Subnet / IP Range</td>
<td>192.168.1.[90-99]</td>
</tr>
<tr>
<td>Interface</td>
<td>wan1</td>
</tr>
</tbody>
</table>

2. Select **OK**.

3. Select **Create New** to add a firewall address for the DMZ network.

<table>
<thead>
<tr>
<th>Address Name</th>
<th>DMZ_Servers</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type</td>
<td>Subnet / IP Range</td>
</tr>
<tr>
<td>Subnet / IP Range</td>
<td>10.10.10.0/255.255.255.0</td>
</tr>
<tr>
<td>Interface</td>
<td>dmz</td>
</tr>
</tbody>
</table>

4. Select **OK**.

Configure the FortiGate as an LT2P server.

1. Enter the following CLI commands:
   ```
   config vpn l2tp
   set sip 192.168.1.90
   set eip 192.168.1.99
   set status enable
   set usrgrp Android_Users
   end
   ```

Configure IPsec tunnel Phase1

1. Go to **VPN > IPsec > Auto Key (IKE)**, and select **Create Phase 1** and configure following Phase 1 settings.

<table>
<thead>
<tr>
<th>Name</th>
<th>AndroidVPN</th>
</tr>
</thead>
<tbody>
<tr>
<td>Remote Gateway</td>
<td>Dialup User</td>
</tr>
<tr>
<td>Local Interface</td>
<td>wan1</td>
</tr>
<tr>
<td>Mode</td>
<td>Main</td>
</tr>
<tr>
<td>Authentication Method</td>
<td>Preshared Key</td>
</tr>
<tr>
<td>Preshared Key</td>
<td>fortinet123</td>
</tr>
<tr>
<td>Peer Options</td>
<td>Accept any peer ID</td>
</tr>
</tbody>
</table>

If you are entering the Phase1 settings in the CLI, remember that the CLI type **dynamic** is equivalent to the **dialup** type in the web-based manager.
2  Select **Advanced** to configure the following advanced settings.

<table>
<thead>
<tr>
<th>Enable IPsec Interface Mode</th>
<th>Disable</th>
</tr>
</thead>
<tbody>
<tr>
<td>IKE Version</td>
<td>Grayed out</td>
</tr>
<tr>
<td>Local Gateway IP</td>
<td></td>
</tr>
<tr>
<td>DNS Server</td>
<td></td>
</tr>
<tr>
<td>1 - Encryption</td>
<td>AES256</td>
</tr>
<tr>
<td>1 - Authentication</td>
<td>MD5</td>
</tr>
<tr>
<td>2 - Encryption</td>
<td>3DES</td>
</tr>
<tr>
<td>2 - Authentication</td>
<td>SHA1</td>
</tr>
<tr>
<td>DH Group</td>
<td>2</td>
</tr>
<tr>
<td>Key life (sec)</td>
<td>28800</td>
</tr>
<tr>
<td>XAUTH</td>
<td>Enable as Server</td>
</tr>
<tr>
<td>Server Type</td>
<td>AUTO</td>
</tr>
<tr>
<td>User Group</td>
<td>Android_Users</td>
</tr>
<tr>
<td>NAT Traversal</td>
<td>enable</td>
</tr>
<tr>
<td>Keepalive Frequency</td>
<td>10</td>
</tr>
<tr>
<td>Dead Peer Detection</td>
<td>Enable</td>
</tr>
</tbody>
</table>

3  Select **OK**.

4  Configure IPsec tunnel Phase2 in the CLI.

```plaintext
config vpn ipsec phase2
edit AndroidVPN2
    set phase1name AndroidVPN
    set proposal aes256-md5 3des-sha1
    set replay enable
    set pfs disable
    set keylifeseconds 3600
    set encapsulation transport-mode
end
```

Create a new security policy to establish the VPN connection

1  Go to *Policy > Policy > Policy* select **Create New** and enter the following information.

<table>
<thead>
<tr>
<th>Source Interface/Zone</th>
<th>dmz</th>
</tr>
</thead>
<tbody>
<tr>
<td>Source Address</td>
<td>DMZ_Servers</td>
</tr>
<tr>
<td>Destination Interface/Zone</td>
<td>wan1</td>
</tr>
<tr>
<td>Destination Address</td>
<td>Android_Users</td>
</tr>
</tbody>
</table>
Using IPsec VPN to secure Android mobile device communication with a network protected by a FortiGate unit

<table>
<thead>
<tr>
<th>Action</th>
<th>IPSEC</th>
</tr>
</thead>
<tbody>
<tr>
<td>Log Allowed Traffic</td>
<td>enable</td>
</tr>
<tr>
<td>VPN Tunnel</td>
<td>AndroidVPN</td>
</tr>
<tr>
<td>Inbound</td>
<td>enable</td>
</tr>
<tr>
<td>Outbound</td>
<td>enable</td>
</tr>
</tbody>
</table>

2. Select **OK**.
3. Move the policy to the top of your policy list to ensure it is matched first.

**Configure the Android device.**
1. On the Android device, go to **Settings > Wireless & Networks > VPN Settings**.
2. Select **Add VPN**.
3. Select **Add L2TP/IPsec PSK VPN**.
4. Enter the following information, and select the **Menu Key > Save**.

<table>
<thead>
<tr>
<th>VPN Name</th>
<th>Office_DMZ_servers</th>
</tr>
</thead>
<tbody>
<tr>
<td>VPN Server</td>
<td>210.0.0.1</td>
</tr>
<tr>
<td>Set IPsec Pre-Shared Key</td>
<td>fortinet123</td>
</tr>
</tbody>
</table>

**Results**

To test the configuration:
1. Ensure the Android device has access to a data network.
2. Select the **Office_DMZ_servers** VPN.

It will attempt to connect for a while. During this time you can:
- monitor the VPN connection with the VPN monitor
- refresh the log entries to see the entry for each step of the connection
- run `diag debug on the CLI for full details of the connection attempt`

When the VPN connects, you will have access to the office servers as expected. If there are problems check the logs for messages to tell you what happened. Also consider running the CLI commands:

```
  diag debug disable
  diag debug application ike -l
  diag debug enable
```

To ensure your new VPN works, bring up the VPN tunnel. For information about this attempt to bring up the tunnel, check the event log of the FortiGate unit ([Log & Report > Log & Archive Access > Event Log](http://docs.fortinet.com/)) where you especially want to read the **Message**, **Action**, and **Error Reason** parts of the log messages to help you troubleshoot.
Using the FortiGate FortiClient VPN Wizard to set up a VPN between a remote users and a private network

**Problem** You want to setup a VPN between FortiClient Endpoint Security users and a FortiGate unit quickly and easily.

**Solution** There is a new feature in FortiOS 4.3.1 called the FortiClient VPN Wizard. It is an easier way to setup a VPN with your FortiClient Connect with less options to configure. The wizard and FortiClient connect take care of encryption, authentication and related options for you.

In this example, user sgreen is part of the Wizard_Users usergroup. Once the VPN tunnel is up, sgreen's FortiClient Connect will be assigned an IP address in the range 192.168.1.90-99. If there are multiple devices sharing the VPN tunnel they will use that same range of IP addresses to share the tunnel. The VPN is a VPN route — it is interface based.

The FortiClient VPN Wizard configuration here was tested with FortiClient 4.2.1, FortiClient Connect (4.3), and FortiClient 4.3.2.

On the FortiGate unit, the VPN is on the wan1 interface, the public facing interface with a domain of example.com. The office network is on the FortiGate internal interface.

The FortiGate unit's public facing interface, wan1 here, must have a public IP address, a public domain name, or a domain name resolved by dynamic DNS. This example uses the domain name example.com for the FortiGate unit gateway information.

1. If the user account sgreen does not exist, go to User > User > User and create the account including a password.
2. If the user group Wizard_users does not exist, go to User > User Group > User Group and create it as a Firewall group and add sgreen to the group.
3. Configure the firewall address for Wizard_Range as 192.168.1.80-89
4. Go to VPN > IPsec > Auto Key, select Create FortiClient VPN and enter the following:

<table>
<thead>
<tr>
<th>Name</th>
<th>Wiz</th>
</tr>
</thead>
<tbody>
<tr>
<td>Local Outgoing Interface</td>
<td>wan1</td>
</tr>
<tr>
<td>Authentication Method</td>
<td>Pre-shared key</td>
</tr>
<tr>
<td>Pre-shared Key</td>
<td>fortinet123</td>
</tr>
<tr>
<td>User Group</td>
<td>Wizard_users</td>
</tr>
<tr>
<td>Address Range Start IP</td>
<td>192.168.1.80</td>
</tr>
<tr>
<td>Address Range End IP</td>
<td>192.168.1.89</td>
</tr>
<tr>
<td>Subnet Mask</td>
<td>255.255.255.0</td>
</tr>
<tr>
<td>DNS Server</td>
<td>Use system DNS</td>
</tr>
</tbody>
</table>

5. Create a Phase2 called Wiz2 that uses the wiz Phase1. Use default settings for Phase2 otherwise. The wizard part only configures Phase1.
6 Create a new security policy to establish the VPN connection using the following information, and select OK.

<table>
<thead>
<tr>
<th>Source Interface/Zone</th>
<th>Wiz</th>
</tr>
</thead>
<tbody>
<tr>
<td>Source Address</td>
<td>all</td>
</tr>
<tr>
<td>Destination Interface/Zone</td>
<td>Wan1</td>
</tr>
<tr>
<td>Destination Address</td>
<td>all</td>
</tr>
<tr>
<td>Action</td>
<td>ACCEPT</td>
</tr>
<tr>
<td>Log Allowed Traffic</td>
<td>enable</td>
</tr>
<tr>
<td>Enable NAT</td>
<td>disable</td>
</tr>
</tbody>
</table>

7 Move the policy to the proper location in the policy list.

8 Create another policy to allow the FortiClient IP addresses access to the rest of the office network:

<table>
<thead>
<tr>
<th>Source Interface/Zone</th>
<th>Wan1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Source Address</td>
<td>Wizard_Range</td>
</tr>
<tr>
<td>Destination Interface/Zone</td>
<td>Wiz</td>
</tr>
<tr>
<td>Destination Address</td>
<td>all</td>
</tr>
<tr>
<td>Action</td>
<td>ACCEPT</td>
</tr>
<tr>
<td>Log Allowed Traffic</td>
<td>enable</td>
</tr>
<tr>
<td>Enable NAT</td>
<td>disable</td>
</tr>
</tbody>
</table>

9 Move the policy to the proper location in the policy list.

**Configure FortiClient Connect**

1 Go to **IPsec VPN**.

2 Select + at the bottom of the **IPsec VPN connections** list.

3 Enter the following information.

<table>
<thead>
<tr>
<th>Connection name</th>
<th>Wizard</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description</td>
<td>VPN connection with office. Used Wizard to set it up.</td>
</tr>
<tr>
<td>Remote gateway</td>
<td>example.com</td>
</tr>
<tr>
<td>Authentication Method</td>
<td>Pre-shared Key</td>
</tr>
<tr>
<td>Pre-shared Key</td>
<td>fortinet123</td>
</tr>
<tr>
<td>Authentication (XAuth)</td>
<td>Prompt on Login</td>
</tr>
</tbody>
</table>

4 Select **OK**.
Results  To test the configuration, select the Wizard VPN configuration in FortiClient Connect and select Connect. If you connect, status will say UP, Duration will increase, and bytes sent and received will increase as well.

If you need information about the connection process, such as for troubleshooting, use the following methods:

- monitor the VPN connection with the VPN monitor
- refresh the log entries to see the entry for each step of the connection
- run diag debug on the CLI for full details of the connection attempt.

If the VPN connects, you will have access to the office network as expected. If there are problems check the logs for messages to tell you what happened. Also consider running the CLI commands:

```bash
diag debug disable
diag debug application ike -1
diag debug enable
```

Remember that only the Android can open the tunnel because this is a dialup VPN — the FortiGate unit doesn’t know the Android’s IP or location until the Android tries to open the tunnel.
My IPsec VPN tunnel isn’t working

Problem
You have an IPsec VPN tunnel configuration that won’t come up or pass traffic.

Solution
IPsec VPN tunnels have multiple layers of protocols that need to all connect properly for the tunnel to come up and pass traffic.

To make things a bit simpler, this information assumes a site-to-site VPN connection, not a hub-and-spoke VPN connection. Local will refer to a FortiGate unit at the main office. Remote or client will refer to the FortiClient PC or FortiGate unit at a home or branch office.

1. Turn on logging everywhere possible.
   When you are troubleshooting VPN, information is your friend. Whenever possible turn on logging on both ends. If you enable logging in the security policy on the FortiGate, you should be able to tell at what point the connection is failing — phase1, phase2, or IP address and routing.

2. For FortiClient, test the connection.
   FortiClient allows you to select a VPN configuration, and test it before actually using it. This test goes through all the set up steps to ensure they work. It outputs messages during the test so you know what passed and what failed.

3. Ensure both ends have the same Phase 1 and Phase 2 settings.
   For a VPN to work, both ends must have the same settings. For both Phase 1 and 2 this includes matching encryption and authentication pairs, and DH group. Additionally for Phase one check the IKE version, and if XAUTH is used or not. If you have multiple VPNs, ensure you are using the correct Phase 1 configuration.

4. If the Phase 1 VPN type is dialup, the remote end must initiate the connection.
   If you have a dialup VPN, that means the local FortiGate does not know the IP address of the remote end to start the connection. This is common with home networks connecting to the office as they do not have public IP addresses. In this situation, the remote end must initiate the VPN tunnel. Once the tunnel is up, it is two-way communication as normal.

5. Check routing.
   If you are getting successful connection messages during the setting up of the VPN tunnel but no traffic is flowing, there is a good chance you have a routing problem.

6. Count the interfaces used.
   If you are using policy VPNs, this is not an issue. However, if you are configuring many VPN interfaces, you may run into the interface limit of 256 interfaces. This applies to physical and virtual interfaces. There are some situations, such as Transparent mode in a VDOM, where extra interfaces are created by default so you may not be able to create all 256 interfaces. In the TP mode example, only 254 interfaces are available.

7. Remote end cannot resolve domain names, or is not assigned an IP address.
   If the local FortiGate assigns the remote end an IP address via DHCP and it is not working, the two most likely reasons are either that the DHCP server is not configured properly or...
you have problems with your outbound VPN security policy. The same security policy solution is true for DNS resolution problems as well.

Security policies vary for VPN depending if you are using an interface VPN (route mode) or a tunnel VPN (policy mode).

With route mode, the VPN is treated just like another interface. This means you have to specify everything as you would with another interface — ensure the policy action is ACCEPT, connects the correct two interfaces, the correct policy addresses are selected (if any), and logging is enabled. Ensure there are policies for each direction; otherwise, protocols that the local side initiates will not be able to reach the remote end of the tunnel.

With policy mode, the policy is IPsec VPN specific — ensure the policy action is IPSEC, correct VPN tunnel is selected, allow inbound and outbound are enabled, and logging is enabled.

8 Ensure the Phase 1 Peer Options to Accept peer ID in dialup group is properly set.

If you are serving IP addresses via a DHCP server, and you are using RADIUS user group attributes to assign those addresses, the Phase 1 field **Peer Options to Accept peer ID** must be set to the correct group. For example if your RADIUS is configured to authenticate users in the sales group (the group name “sales” is sent in the RADIUS start record), the Phase 1 field must also be set to sales. If it is not, no user will be assigned an IP address.

9 If using interface mode, recreate VPN Phase1 using policy mode.

There may be configuration details that you are missing in your current setup and not realize it. Many people find policy VPNs easier to configure. If you are using interface mode (set in Advanced section of Phase1 settings), try creating a new Phase1 with the same settings but using policy VPN instead of interface. You will need to create a new IPSEC security policy for the VPN to match the new Phase1.

10 Restart the IKE daemon.

If you have problems with changes not being visible or unpredictable results, you may want to re-start the IKE daemon and start fresh. The down side is that any VPN tunnels will be disconnected, so you need to give anyone using VPN warning before restarting the daemon. The CLI command to restart the daemon is: *diag vpn ike restart*. You may want to turn on IKE debugging before restarting the daemon so you will see all the shutdown and start up messages will it is rebuilding its tables. The restart reloads all the IPsec configuration so this will remove any lingering issues that may have been “cached”.

11 Debug the VPN handshake for detailed information.

When the VPN is being established, there is a lot of information being passed back and forth between the local and remote ends of the tunnel. To see all this information, start a telnet session on the local end and log the output to a file. Enter the CLI commands:

```bash
diagnose debug application ike -1

diagnose debug enable
```

These commands tell debug to print all the IKE related information, and the enable command starts it. From this point you should see all IPsec related information that is being passed between the two ends of the tunnel as it is being set up. Here is a sample output. After each major section of output there will be comments to explain what is going on.

```bash
diagnose debug enable
ike 0: comes 10.10.80.110:500->10.10.80.3:500,ifindex=17....
ike 0: IKEv1 exchange=Identity Protection
    id=df1ade8dd5613b41/0000000000000000 len=296
```
My IPsec VPN tunnel isn't working

ike 0: in

DF1ADE8DD5613B41000000000000000011020000000000000128000009C
000000100000000000000000000000000000000100004030000020010100008B000180C7080
801000580030001800200018004000503000020020100008B000180C7080
80100058003000180020002800400050300002040000050000000002404010000000000001
800C708080010007008008003000180020001800400050000000002404010000000000001
800C708080010007008008003000180020002800400050D0000144A131C81
070358455C5728F20E95452F0D000014C60464335DF21F87CFDB2FC68B6A448
0D00001490CB80913EBB66E0863B1B5EC427B1F0D00001435DB6C9CDDE4F023
1D6F692E1D7C77D1E80000C09002689DFD6B712000000014AFCAD71368A1FC9
6B866EFC77570100
ike 0: cache rebuild start
ike 0: AndroidVPN: cached as dynamic
ike 0: FCL: cached as dynamic
ike 0: iPhone: cached as dynamic
ike 0: cache rebuild done

The cache contains all VPN configurations on the FortiGate server. In this case there were three — AndroidVPN, FCL (the one we want), and iPhone.

ike 0:FCL:0: responder: main mode get 1st message...
ike 0:FCL:0: VID RFC 3947 4A131C81070358455C5728F20E95452F
ike 0:FCL:0: VID draft-ietf-ipsec-nat-t-ike-02
CD6046435DF21F87CFDB2FC68B6A448
ike 0:FCL:0: VID draft-ietf-ipsec-nat-t-ike-02\n90CB80913EBB696E086381B5EC427B1F
ike 0:FCL:0: VID unknown (16): 35DB6C9CDDE4F0231DF692E1D7C77D1E8
ike 0:FCL:0: VID draft-ietf-ipsra-isakmp-xauth-06.txt
09002689DFD6B712
ike 0:FCL:0: VID DPD AFCAD71368A1FC96B8696FC77570100
ike 0:FCL:0: DPD negotiated

Note that FCL has been selected at this point, and some basic things have been negotiated — IKE version and DPD. If you are going to debug VPN output like this its better to use shorter VPN tunnel names to help with readability of the output.

ike 0:FCL:0: negotiation result
ike 0:FCL:0: proposal id = 1:
ike 0:FCL:0: protocol id = ISAKMP:
ike 0:FCL:0: trans_id = KEY_IKE.
ike 0:FCL:0: encapsulation = IKE/none
ike 0:FCL:0: type=OAKLEY_ENCRYPT_ALG, val=3DES_CBC.
ike 0:FCL:0: type=OAKLEY_HASH_ALG, val=SHA.
ike 0:FCL:0: type=AUTH_METHOD, val=PRESHARED_KEY.
ike 0:FCL:0: type=OAKLEY_GROUP, val=1536.
ike 0:FCL:0: ISKAMP SA lifetime=28800
ike 0:FCL:0: selected NAT-T version: RFC 3947

This section lists the proposals tried. If there is only one, then the first one tried was a match. You can see the settings here if you know what to look for — encryption is 3des-sha1, authentication is pre-shared key, the key lifetime is 28,800 seconds, and nat traversal is enabled.

ike 0:FCL:0: cookie df1ade8dd5613b41/4bb2750030bc8a06
ike 0:FCL:0: out

DF1ADE8DD5613B414BB2750030BC8A06011020000000000000000000000000011020000000000000128000009C
000000100000000000000000000000000000000100004030000020010100008B000180C7080
801000580030001800200018004000503000020020100008B000180C7080
80100058003000180020002800400050300002040000050000000002404010000000000001
800C708080010007008008003000180020001800400050000000002404010000000000001
800C708080010007008008003000180020002800400050D0000144A131C81
070358455C5728F20E95452F0D000014C60464335DF21F87CFDB2FC68B6A448
0D00001490CB80913EBB66E0863B1B5EC427B1F0D00001435DB6C9CDDE4F023
1D6F692E1D7C77D1E80000C09002689DFD6B712000000014AFCAD71368A1FC9
6B866EFC77570100
My IPsec VPN tunnel isn't working

ike 0:FCL:0: sent IKE msg (ident_r1send): 10.10.80.3:500->10.10.80.110:500, len=140, id=df1ade88dd5613b41/4bb2750030bc8a06
ike 0: comes 10.10.80.110:500->10.10.80.3:500, ifindex=17....
ike 0: IKEv1 exchange=Identity Protection
   id=df1ade88dd5613b41/4bb2750030bc8a06 len=292
ike 0: in
   DF1ADE8DD5613B414BBB2750030BC8A0604100200000000000001240A0000C4
   B1BB998514C7F6F595C9F1A0CA1DEE10625676E264878024079E1E41198583
   97D1C951A7DD40F93F5B57AF8ADACD63A9408ED540F9B304F1A0626C
   20289119B362CA45ACA153120B1E242A64629FCA09A042276E256F4128E986
   150C17CE9F7AF6C6B402B8574DD685E66E51FCE7218E2887B444989AAEA
   A8B4962A2FD11BFA79C2A84613ED3DA5FA57C1E49507971BD3185CF5616
   26CCB764919E278A7E155A195E58D658C7AB124F9C311052C2887D64B9B36
   14000014AC80EB704C90E1D4CEFC75B7CA1CCA0B1400001866DCE39FA4DB9B93
   D3AC45665952B5E45F32859A000000018255171E5A6979B9974D657D422BEAB
   B8756493
ike 0:FCL:0: responder:main mode get 2nd message...
ike 0:FCL:0: NAT not detected

Here is the main mode and NAT is not used. Responder means the FortiGate unit is responding to a remote attempt to initiate the VPN tunnel. The remote end is the initiator and the FortiGate is the responder. Knowing this can help you locate errors in the negotiation.

ike 0:FCL:0: out
   DF1ADE8DD5613B414BBB2750030BC8A0604100200000000000001240A0000C4
   B92ECAFB75B1687F6F2C2B40BAEA5FDBB2DB871F1F5760E48B97E7E37B1BDE4
   CA41CA19D77981DA37976902543B9A1401C9964CE7AA94765CE6059AE566B3
   081BA9619691C5683A875961E0F9B3013A449FDFC1826C69FE1DFB3E43621D
   8CA51969F6F6E80891F423FD4DF3DFB58251C4C7C4D4125711F228D0143CD
   B40FD9AFA1827CF6C9696A199BB9B686CA381918751F457F9774FD0423D8FAF
   3F50B0496911FA01EADE981C2A6D22E1EFE8CE106980BD42D0F675398B6526
   1400001480187A2D9803178C54C7295CE2E574A14000018255171E5A6979B9
   974D6A5D7422BEABB87564930000001866DCE39FA4DB9B93D3AC45665952B5E4
   5F32859A
ike 0:FCL:0: sent IKE msg (ident_r2send): 10.10.80.3:500->10.10.80.110:500, len=292, id=df1ade88dd5613b41/4bb2750030bc8a06
ike 0:FCL:0: ISAKMP SA df1ade88dd5613b41/4bb2750030bc8a06 key 24:549399B9FF81AE7DE8E57886538F3767B8180D1A55C89B1
ike 0: comes 10.10.80.110:500->10.10.80.3:500, ifindex=17....
ike 0: IKEv1 exchange=Identity Protection
   id=df1ade88dd5613b41/4bb2750030bc8a06 len=100
ike 0: in
   DF1ADE8DD5613B414BBB2750030BC8A0605100201000000000000064EE47E9F
   E00EBC19A7B01185C1A004A6236B1897E48C8D7B88DB9669519D3A03F6C7
   57E58548B54F9817315D236A70FA01B0E28CB35A1FE2762DBC425508A5F5C9C
   1BB99D49
ike 0:FCL:0: responder:main mode get 3rd message...
ike 0:FCL:0: dec
   DF1ADE8DD5613B414BBB2750030BC8A0605100201000000000000064080000C
   010000000A0A5060B000018E916BDE7F9F5A4733726EA91BC9649A9962494
   0000001C0000000101106002DF1ADE8DD5613B414BBB2750030BC8A06B2FB197
   A0DE9A07
ike 0:FCL:0: received notify type 24578
ike 0:FCL:0: PSK authentication succeeded
ike 0:FCL:0: authentication OK
By this point nearly all the configuration information from Phase1 has shown up in the negotiations. Phase2 hasn’t come yet or we would see FCL2 in the lines. Things are going well because we have seen the 2nd and 3rd messages come up. At this point things are going well. Notice the last two lines are the pre-shared secret is OK, and the authentication is good.

ike 0:FCL:0: enc
DF1ADE8DBD5613B414BB2750030BC8A060510020100000000000000000000000000
0100000000010000000000000000000000004008000000C
ike 0:FCL:0: out
DF1ADE8DBD5613B414BB2750030BC8A0605100201000000000000000000000000000
ike 0:FCL:0: sent IKE msg (ident_r3send): 10.10.80.3:500->10.10.80.110:500, len=68, id=df1ade8dd5613b41/4bb2750030bc8a06
ike 0:FCL:0: established IKE SA df1ade8dd5613b41/4bb2750030bc8a06
ike 0:FCL: adding new dynamic tunnel for 10.10.80.110:500
ike 0:FCL: added new dynamic tunnel for 10.10.80.110:500
ike 0:FCL:0: processing INITIAL-CONTACT
ike 0:FCL:0: flushing
ike 0:FCL:0: processed INITIAL-CONTACT
ike 0:FCL:0: no pending Quick-Mode negotiations
ike 0: comes 10.10.80.110:500->10.10.80.3:500, ifindex=17....
ike 0: IKEv1 exchange=Informational
id=df1ade8dd5613b41/4bb2750030bc8a06:82044f57 len=84
ike 0: in
DF1ADE8DBD5613B414BB2750030BC8A060810050182044F570000000541FC0E53
9233B368C7434635E718C6D873A4CD897D2AC5972D69EFA6CC37B3D83F1424
35C6CF4A5E103BC72B1F543C31AEBAFD3732AC40
ike 0:FCL:0: dec
DF1ADE8DBD5613B414BB2750030BC8A060810050182044F570000000541FC0E53
9233B368C7434635E718C6D873A4CD897D2AC5972D69EFA6CC37B3D83F1424
35C6CF4A5E103BC72B1F543C31AEBAFD3732AC40
ike 0:FCL:0: notify msg received: INITIAL-CONTACT
ike 0:FCL:0: processing INITIAL-CONTACT
ike 0:FCL:0: flushing
ike 0:FCL:0: flushed
ike 0:FCL:0: processed INITIAL-CONTACT
ike 0: comes 10.10.80.110:500->10.10.80.3:500, ifindex=17....
ike 0: IKEv1 exchange=Quick
id=df1ade8dd5613b41/4bb2750030bc8a06:c378b320 len=548
My IPsec VPN tunnel isn't working

ike 0: in
DF1ADE8DD5613B414BB2750030BC8A0680102001C378B3200000022443EB6862
1324B61C15F3BB0AED0D3B1CC042EC769978AEC6EC422F03E7FB578B433FCB5A
07E7C4BB69CB0F9090E6A826B68C6B9EE3D49B6A68C1AC7C161DF22FC35
8FD9A9DB7098C3356900020317359C18353CD855BCE57103D1878F3A90DF36
37E2126CEC9137CD68DC47C0C1CB054739E83A0C94D053475067C216452B30DFF
6538B980959E176329692E278386601FBFC4815F6A1AD532A2CC14618A4815
9E3C8EFC1DF035E74D98F3762C72A467E9292720CC2894619266D0807FA6DC0
9CB5A9DB19284F3373381CFDFDE493341C2EF6402594B01C82016F4D8D8589B6
B9A922784355F203A08127DBCA63B711BA6775013A7873C30E4AF4841E
0288CD431D35A953D31D6A3ACC67335D804C2368016912245F87F16959B1FA
CE093FE488F38AF18BE2260117544D276A69FB42298A8655EA9DF4AFAD038
A572244E74B9A86B78B1BD685A1520831C9497560091E22D64989F31E858A
B59C4149B9CAE8EEBECDE08776A944E70B104633F1464BE3E5ECBD382512C17E
E51C6541FC47721C2F6C8D52E989964B269645BF038251467A1FD51A407FF45
6C37178F25486867918PE307100C31C83253C59EAD52101383F2C251305C0
C1CA2D55C38F96A2ED036DA046170F4ED381358101377A7A2CB1B4417801D93
D6A3D391A3B313CAEE54EA855FB6852396BF2D7D43F4800166461DA62A4BB23
40F946FF
ike 0:FCL_0:0:0: responder received first quick-mode message
ike 0:FCL_0:0: dec
ike 0:FCL_0:0:0: peer proposal is: peer:0:10.10.80.110-
ike 0:FCL_0:0:0: matched phase2
ike 0:FCL_0:0:0: dynamic client
ike 0:FCL_0:0:0: my proposal:
ike 0:FCL_0:0:0: proposal id = 1:
ike 0:FCL_0:0:0: protocol id = IPSEC_ESP:
ike 0:FCL_0:0:0: trans_id = ESP_3DES
ike 0:FCL_0:0:0: encapsulation = ENCAPSULATION_MODE_TUNNEL
ike 0:FCL_0:0:0: type = AUTH_ALG, val=SHA1
ike 0:FCL_0:0:0: trans_id = ESP_AES (key_len = 128)
ike 0:FCL_0:0:0: encapsulation = ENCAPSULATION_MODE_TUNNEL
ike 0:FCL_0:0:0: type = AUTH_ALG, val=SHA1
ike 0:FCL_0:0:0: incoming proposal:

This section has both FCL and FLC2 which indicates we are into Phase2 negotiations.
When you see my proposal and incoming proposal, it means there was a proposal mismatch. If everything goes well, you will just see the successful proposal match.

This output shows the proposals from both sides — my proposal (the FortiGate unit), and incoming proposal (the remote end). Note there are 2 entries for my proposal (3des-sha1 and aes-sha1). If there were more than two entries configured in Phase2 they would be listed here.

There are many more incoming proposals — 20 or more. This means the remote end is trying to cover all possible encryption and authentication possible. The problem with this approach is the output here gets very long, and you will be connecting with the same information in most cases which lets you remove the unused proposals here.

At the end of all the proposals it lists the proposal result, which is the one that is being used.

ike 0:FCL_0:0:FCL2:0: proposal id = 1:
ike 0:FCL_0:0:FCL2:0: protocol id = IPSEC_ESP:
ike 0:FCL_0:0:FCL2:0: encapsulation = ENCAPSULATION_MODE_TUNNEL
ike 0:FCL_0:0:FCL2:0: type = AUTH_ALG, val=MD5
ike 0:FCL_0:0:FCL2:0: encapsulation = ENCAPSULATION_MODE_TUNNEL
ike 0:FCL_0:0:FCL2:0: type = AUTH_ALG, val=SHA1
ike 0:FCL_0:0:FCL2:0: encapsulation = ENCAPSULATION_MODE_TUNNEL
ike 0:FCL_0:0:FCL2:0: type = AUTH_ALG, val=SHA1
ike 0:FCL_0:0:FCL2:0: encapsulation = ENCAPSULATION_MODE_TUNNEL
ike 0:FCL_0:0:FCL2:0: type = AUTH_ALG, val=MD5
ike 0:FCL_0:0:FCL2:0: trans_id = ESP_AES (key_len = 128)
ike 0:FCL_0:0:FCL2:0: encapsulation = ENCAPSULATION_MODE_TUNNEL
ike 0:FCL_0:0:FCL2:0: type = AUTH_ALG, val=MD5
ike 0:FCL_0:0:FCL2:0: trans_id = ESP_AES (key_len = 128)
ike 0:FCL_0:0:FCL2:0: encapsulation = ENCAPSULATION_MODE_TUNNEL
ike 0:FCL_0:0:FCL2:0: type = AUTH_ALG, val=SHA1
ike 0:FCL_0:0:FCL2:0: trans_id = ESP_AES (key_len = 128)
ike 0:FCL_0:0:FCL2:0: encapsulation = ENCAPSULATION_MODE_TUNNEL
ike 0:FCL_0:0:FCL2:0: type = AUTH_ALG, val=MD5
ike 0:FCL_0:0:FCL2:0: encapsulation = ENCAPSULATION_MODE_TUNNEL
ike 0:FCL_0:0:FCL2:0: type = AUTH_ALG, val=SHA1
ike 0:FCL_0:0:FCL2:0: trans_id = ESP_AES (key_len = 128)
ike 0:FCL_0:0:FCL2:0: encapsulation = ENCAPSULATION_MODE_TUNNEL
ike 0:FCL_0:0:FCL2:0: type = AUTH_ALG, val=MD5
ike 0:FCL_0:0:FCL2:0: trans_id = ESP_AES (key_len = 128)
ike 0:FCL_0:0:FCL2:0: encapsulation = ENCAPSULATION_MODE_TUNNEL
ike 0:FCL_0:0:FCL2:0: type = AUTH_ALG, val=SHA1
ike 0:FCL_0:0:FCL2:0: trans_id = ESP_AES (key_len = 128)
My IPsec VPN tunnel isn't working

ike 0:FCL_0:FCL2:0: encapsulation = ENCAPSULATION_MODE_TUNNEL
ike 0:FCL_0:FCL2:0: type = AUTH_ALG, val=MD5
ike 0:FCL_0:FCL2:0: trans_id = ESP_AES (key_len = 128)
ike 0:FCL_0:FCL2:0: encapsulation = ENCAPSULATION_MODE_TUNNEL
ike 0:FCL_0:FCL2:0: type = AUTH_ALG, val=SHA1
ike 0:FCL_0:FCL2:0: negotiation result
ike 0:FCL_0:FCL2:0: proposal id = 1:
ike 0:FCL_0:FCL2:0: protocol id = IPSEC_ESP:
ike 0:FCL_0:FCL2:0: trans_id = ESP_3DES
ike 0:FCL_0:FCL2:0: using tunnel mode.
ike 0:FCL_0: enc
    DF1ADE8DD5613B414BB2750030BC8A0608102001C378B3200000009401000018
    0A105570023A0518E9C3517A26C22386549727D10A0000300000000010000001
    0000002401030401DB36040000000180203000080100018207088004001
    8005000205000143FA0B878D6189B6585C6A4E4E854F16405000000C01000000
    0A0A506E0000000100400000000A0A5000FFFF0F00
ike 0:FCL_0: out
    DF1ADE8DD5613B414BB2750030BC8A0608102001C378B3200000009C180D9E06
    9E53579921C35ACC514AB63548D044BE6319E49B1B461A9D7DB5E166469A
    6DAB9C921F2EAD6F6F5A71686D12324D1E6B996A3DE264D58803407379C88
    C58C201AE9155281FFEAE72E8C542F9EF10F9EAEE68594014E344B37DA5D6E9A
    C1470694B3E5987E7654420C19E1EB8AA2AC642A6A7C86B3437B222
ike 0:FCL_0: sent IKE msg (quick_rlsend): 10.10.80.3:500->10.10.80.110:500, len=156,
    id=df1ade8dd5613b41/4bb2750030bc8a06:c378b320
ike 0: comes 10.10.80.110:500->10.10.80.3:500, ifindex=17....
ike 0: IKEv1 exchange=Quick
    id=df1ade8dd5613b41/4bb2750030bc8a06:c378b320 len=60
ike 0: in
    DF1ADE8DD5613B414BB2750030BC8A0608102001C378B3200000000C0180D9E06
    DC1EE2B5C33869C64C7C806CE915049DD6554FC3122CEA1AA9DDEA6
ike 0:FCL_0: dec
    DF1ADE8DD5613B414BB2750030BC8A0608102001C378B3200000003C8B15588C
    E68D68750B8785E346C6C5B3E1A1FC6EB9000229A7B1C81C1DB0807
ike 0:FCL_0: FCL2:0: replay protection enabled
ike 0:FCL_0: FCL2:0: SA life soft seconds=1786.
ike 0:FCL_0: FCL2:0: SA life hard seconds=1800.
ike 0:FCL_0: FCL2:0: IPSec SA selectors #src=1 #dst=1
ike 0:FCL_0: FCL2:0: src 0 7 0:10.10.80.0-10.10.80.255:0
ike 0:FCL_0: FCL2:0: dst 0 7 0:10.10.80.110-10.10.80.110:0
ike 0:FCL_0: FCL2:0: add dynamic IPSec SA selectors
ike 0:FCL_0: FCL2:0: tunnel 1 of VDOM limit 0/0
ike 0:FCL_0: FCL2:0: add IPSec SA: SPIs=d1b36040/5ef744c5
ike 0:FCL_0: FCL2:0: IPSec SA dec spi d1b36040 key
    24:7F0F504EA42ED86512A2C4808A56B1F353C3CCD805FF3A9 auth
    20:294209ED6B82FBD01430801BE482ECFA166D06C
ike 0:FCL_0: FCL2:0: IPSec SA enc spi 5ef744c5 key
    24:593E6734ED63A4C85246932F9CD41A62B5A5E1A18E1 auth
    20:6D8E9CDA2D560A7D80F05A4A846590488155CC
ike 0:FCL_0: FCL2:0: added IPSec SA: SPIs=d1b36040/5ef744c5
ike 0:FCL_0: FCL2:0: sending SNMP tunnel UP trap

These last few lines are finishing up the Security Association (SA) negotiation. The important part here is the last line “sending SNMP tunnel UP trap”. This is saying the tunnel is up and ready to go. If you see this in the diag output the VPN came up successfully.
Another line you can look for is the R-U-THERE and R-U-THERE ack messages. Its the keep alive message sent between the ends of the VPN to make sure both ends are still functional. Its easy to see in the output, and it only happens after the tunnel is up.

ike shrank heap by 65536 bytes
ike 0:FCL_0: link is idle 17 10.10.80.3->10.10.80.110:500 dpd=1
  seqno=1
ike 0:FCL_0: link is idle 17 10.10.80.3->10.10.80.110:500 dpd=1
  seqno=2
ike 0:FCL_0:0: send IKEv1 DPD probe, seqno 2
ike 0:FCL_0: enc
  DF1ADE8DD5613B414BB2750030BC8A0608100501147397C2000000540B000018
  ADC2E9DF61F03E2980D6CE15C4128DE8A7E6AB7A0000002000000000101108D28
  DF1ADE8DD5613B414BB2750030BC8A0600000002
ike 0:FCL_0: out
  DF1ADE8DD5613B414BB2750030BC8A0608100501147397C20000005C5BB65CCC
  42DC2B33B4850FBF2657521B521BD00DA651D1E10E4B331CC03C9212010034C33
  ADD290457E8C2B02891D7AE0E0149D1D5DB78EF649B7548B659B0D45
ike 0:FCL_0:0: send IKE msg (R-U-THERE): 10.10.80.3:500-
  >10.10.80.110:500
ike 0:FCL_0:0: sent IKE msg (R-U-THERE): 10.10.80.3:500-
  >10.10.80.110:500
  id=df1ade8dd5613b41/4bb2750030bc8a06:147397c2
ike 0: comes 10.10.80.110:500->10.10.80.3:500,ifindex=17....
ike 0: IKEv1 exchange=Informational
  id=df1ade8dd5613b41/4bb2750030bc8a06:b620421b len=92
ike 0: in
  DF1ADE8DD5613B414BB2750030BC8A0608100501B620421B0000005CFBAA22BA2
  AE4EA89C46B8AE1C9D5B639669EA5E50C3225D98CB3BDC2A3786D59B834FE7D
  96A656049908D0AF6D28BDEE03968C31BA58F7158B156C59D1B9EFE7
ike 0:FCL_0:0: dec
  DF1ADE8DD5613B414BB2750030BC8A0608100501B620421B0000005C0B000018
  FBE51A0B7132BA625A1F6F25D674196BE337EBA0000002000000000101108D29
  DF1ADE8DD5613B414BB2750030BC8A06000000002F5D890FBC01CB607
ike 0:FCL_0:0: notify msg received: R-U-THERE-ACK
ike shrank heap by 4096 bytes

Results: These steps configure ends of an IPsec VPN tunnel on the office FortiGate unit, and the home computer FortiClient.

To ensure your new VPN works, select the Work_VPN entry, and then select Advanced > Test. This will open a window and show each step of the attempted connection. If there are any problems they will be visible here and easy to troubleshoot. For additional information, check the event log of the FortiGate unit (Log&Report > Log & Archive Access > Event Log) where you especially want to read the Message, Action, and Error Reason parts of the log messages to help you troubleshoot.
My IPsec VPN tunnel isn't working
Authentication

Identifying users and other computers (authentication) is a key part of network security. This chapter describes some basic elements and concepts of authentication.

Businesses need to authenticate people who have access to company resources. In the physical world this may be a swipe card to enter the building, or a code to enter a locked door. If a person has this swipe card or code, they have been authenticated as someone allowed in that building or room.

Authentication is the act of confirming the identity of a person or other entity. In the context of a private computer network, the identities of users or host computers must be established to ensure that only authorized parties can access the network. The FortiGate unit enables controlled network access and applies authentication to users of security policies and VPN clients.

This chapter includes the following authentication examples:

- Creating a security policy to identify users
- Creating a security policy to identify users and restrict access to websites by category
- Creating a security policy to identify users, restrict access to certain websites, and control use of applications
- Adding FortiToken two-factor authentication to a user account
- Adding SMS token code delivery two-factor authentication to a FortiGate administrator's account
- Stopping the “Connection is untrusted” message
Creating a security policy to identify users

**Problem**
How do you identify the users who are accessing Internet services through your FortiGate unit. This is the first step towards controlling user’s access to resources through the FortiGate unit.

**Solution**
Enable FortiGate user authentication by creating a user group named Sales and adding a user named wloman to this group. Then add an identity based policy to a security policy that accepts connections from the internal network to the Internet. Add the Sales user group to the identity based policy. Test the configuration by authenticating with the FortiGate unit and viewing the information displayed in the user monitor.

1. Go to User > User Group > User Group and select Create New to add a user group with the following settings:

<table>
<thead>
<tr>
<th>Name</th>
<th>Sales</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type</td>
<td>Firewall</td>
</tr>
</tbody>
</table>

2. Select OK.

3. Go to User > User > User and select Create New to a user with the following settings:

<table>
<thead>
<tr>
<th>Name</th>
<th>wloman</th>
</tr>
</thead>
<tbody>
<tr>
<td>Password</td>
<td>password</td>
</tr>
</tbody>
</table>

   Add this user to Groups | Sales

4. Select OK.

5. Go to Policy > Policy > Policy and Edit a policy that allows users to access the Internet.

6. Select Enable Identity Based Policy and Add an identity-based policy with the following settings:

<table>
<thead>
<tr>
<th>Selected User Groups</th>
<th>Sales</th>
</tr>
</thead>
<tbody>
<tr>
<td>Selected Services</td>
<td>ANY</td>
</tr>
<tr>
<td>Schedule</td>
<td>always</td>
</tr>
</tbody>
</table>

7. Select OK to save the security policy.

**Results**
From a web browser on the internal network, attempt to access the Internet. If the session is accepted by the policy that you added the identity based policy to you should be prompted for a user name and password. Enter wloman and password. If authentication is successful you should be able to browse anywhere on the Internet.

This solution describes adding a user to the FortiGate local user database. FortiOS user authentication can also integrate with LDAP, RADIUS, or TACAS+ servers, Windows NTLM, Fortinet single sign on (FSSO), and PKI solutions.
Form the FortiGate web-based manager go to User > Monitor > Firewall to view the list of authenticated firewall users. An entry similar to the following should appear,

<table>
<thead>
<tr>
<th>User Name</th>
<th>User Group</th>
<th>Policy ID</th>
<th>Duration</th>
<th>IP Address</th>
<th>Traffic Volume</th>
<th>Method</th>
</tr>
</thead>
<tbody>
<tr>
<td>women</td>
<td>Sales</td>
<td>1</td>
<td>0 day(s) 0 hour(s) 1 minute(s)</td>
<td>10.31.10.20</td>
<td>335.7 KB</td>
<td>FW-auth</td>
</tr>
</tbody>
</table>

If you select De-authenticate All Users or if you select the De-authenticate user icon for Example_user you will have to authenticate with the firewall again to continue browsing the Internet.

You can also go to Log&Report > Log & Archive Access > Event Log to view log messages recorded when the users authenticated. (more info to be provided about reports and so on that include authenticated users user names in them.)

If you do not see an authentication page, verify that the identity based policy has been added to the correct security policy by viewing the Count column in the policy list. If the count is increasing the policy is processing traffic. You can also view policy usage from Policy > Monitor > Policy Monitor.

You can customize the authentication page that users see by going to System > Config > Replacement Message > Authentication > Login page.
Creating a security policy to identify users and restrict access to websites by category

**Problem**  How to allow only authorized users to access the Internet and block these users from accessing online shopping and auction websites.

**Solution**  Block access to shopping and auction websites by adding a web filter profile named Sales_web_filter that blocks shopping and auction websites. Enable web filtering for the identity based policy created in “Creating a security policy to identify users” on page 260 and add the Sales_web_filter profile to it. Test the configuration by authenticating and then attempting to browse to an online shopping web site. This example requires the FortiGate unit to have a valid FortiGuard Web Filtering license.

1. Go to **UTM Profiles > Web Filter > Profile** and select **Create New** to add a new web filter profile group named Sales_web_filter.
2. Select the **FortiGuard Categories > General Interest - Personal > Shopping and Auction** category, then select **Block** as the action for selected categories.
3. Select **OK** to save the web filter profile.
4. Go to **Policy > Policy > Policy** and **Edit** the policy that allows users to access the Internet and contains the identity based policy.
5. **Edit** the identity based policy that includes the Sales user group.
6. Select **UTM**.
7. Select **Enable Web Filter** and select the Sales_web_filter profile.
8. Save the changes to the identity based policy and the security policy.

**Results**  Go to **User > Monitor > Firewall** and deauthenticate the wloman user. From a web browser on the internal network, attempt to access the Internet. If the session is accepted by the identity based policy you should be prompted for a user name and password. Enter wloman and password. If authentication is successful you should be able to browse the Internet.

Attempt to access an online shopping or auction website. FortiGuard Web Filtering web page blocked message appears, blocking access to the website.

If you attempt to access an online shopping page before authenticating, the FortiGate unit would ask you to authenticate. After authenticating the FortiGuard web page blocked message appears.

You can customize the FortiGuard web filtering page that appears by going to **System > Config > Replacement Message > FortiGuard Web Filtering > URL block message**.

Form the FortiGate web-based manager go to **UTM Profiles > Monitor > Web Monitor** to view graphs of FortiGuard Web Filtering activity. The graphs should show the Shopping and Auction category has been blocked,
Creating a security policy to identify users and restrict access to websites by category

If you can access the online shopping site it may not be in the FortiGuard web filtering database. Try another online shopping site to see if it is blocked. You can browse to http://www.fortiguard.com/webfiltering/webfiltering.html and look up the URL to see what category it has been added to. You can also request to have the category changed.

All sites will be blocked if the FortiGate unit cannot access the FortiGuard network to get web site ratings. This happens because the Allow Websites When a Rating Error Occurs option under Advanced Filter in the web filter profile is disabled by default.
Creating a security policy to identify users, restrict access to certain websites, and control use of applications

Problem: How to allow only authorized users to access the Internet and block these users from accessing online shopping and auction websites, and block them from using any excessive bandwidth consuming applications, including Skype.

Solution: Blocking nuisance applications is common on corporate networks to control bandwidth usage, illegal file sharing, and employee time wasting.

Enable web filtering and block access to shopping and auction websites for the identity based policy as described in “Creating a security policy to identify users and restrict access to websites by category” on page 262. Then add the Sales_app_sensor profile to it to block excessive bandwidth applications. Test the configuration by authenticating and then attempting to use a blocked application such as bitTorrent, KaZaa, or eDonkey.

This example requires the FortiGate unit to have a valid FortiGuard Web Filtering license.

1. Go to UTM Profiles > Application Control > Application Sensor and select Create New to add a new detection list named Sales_app_sensor.
2. Select Create New above the list to create a new application detection entry that blocks all running applications in the instant messaging category.
3. Select OK to save the IM blocking application detection entry.
4. Select Create New to create a new application detection entry that allows Skype. Select Instant Messaging category, and specify the application. Select Filter by Vendor and find Skype Technologies in the list, and select Allow for the action.
5. Select OK to save the application detection entry.
6. Move the Skype entry above the block all instant messaging. Otherwise, Skype will be blocked with all the other IM applications.
7. Select OK to save the web filter profile.
8. Go to Policy > Policy > Policy and Edit the policy that allows users to access the Internet and contains the identity based policy.
9. Edit the identity based policy that includes the Sales user group.
10. Select UTM.
11. Select Enable Web Filter and select the Sales_web_filter profile.
12. Save the changes to the identity based policy and the security policy.

Results: Go to User > Monitor > Firewall and deauthenticate wlloman. From a web browser on the internal network, attempt to access the Internet. If the session is accepted by the policy that you added the identity based policy to, you should be prompted for a user name and password. Enter wlloman and password. If authentication is successful you should be able to browse the Internet.

Attempt to access an online shopping or auction website. FortiGuard Web Filtering web page blocked message appears, blocking access to the website.

Attempt to use one of the blocked high bandwidth applications. It should be blocked through the Application Sensor.
Creating a security policy to identify users, restrict access to certain websites, and control use of applications

If you attempt to access an online shopping page before authenticating, the FortiGate unit would ask you to authenticate. After authenticating the FortiGuard web page blocked message appears.

You can customize the FortiGuard web filtering page that appears by going to System > Config > Replacement Message > FortiGuard Web Filtering > URL block message.

Form the FortiGate web-based manager go to UTM Profiles > Monitor > Web Monitor to view graphs of FortiGuard Web Filtering activity. The graphs should show the Shopping and Auction category has been blocked.

If you can access the online shopping site it may not be in the FortiGuard web filtering database. Try another online shopping site to see if it is blocked. You can browse to http://www.fortiguard.com/webfiltering/webfiltering.html and look up the URL to see what category it has been added to. You can also request to have the category changed.

All sites will be blocked if the FortiGate unit cannot access the FortiGuard network to get web site ratings. This happens because the Allow Websites When a Rating Error Occurs option under Advanced Filter in the web filter profile is disabled by default.

If the behavior is not what you expect, check the logs. Turning on logging leaves a trail whenever you authenticate or access is blocked. For Authentication entries look in the Event Log, for blocked websites look in Web Filter Log, and for blocked applications look in Application Control log. You can use these log messages or lack of them to find details that will help fix the problem.

If you use the Application Sensor to block games if you are not logged in, the games will not be able to connect and because of that some just will not start up. For example World of Warcraft launcher never appears after you start it when it is blocked like this. Where other games, such as World of Tanks, load their loading application before attempting to connect so you will get an error message with those games.
Adding FortiToken two-factor authentication to a user account

**Problem**
How do you add a FortiToken to a user account.

**Solution**
Two-factor authentication is fast becoming an industry requirement. FortiToken is a cost effective solution. With its combination of information you know (your username and password) and something you have (the FortiToken device), it improves your network security with little extra work for administrators.

FortiToken is a one-time password generator that users must carry with them. It generates a six-digit token that the user enters in addition to username and password at logon as an extra factor of security. It serves a similar purpose to RSA's SecureID tokens.

To add a new FortiToken to a user, the FortiToken must first be added to the FortiGate unit, verified by the FortiGuard system, and FortiGate and FortiToken time must be synchronized. Then the FortiToken can be applied to the user account. Test the configuration by the user logging in and being prompted for the FortiToken generated code.

This solution assumes you have a FortiToken, the user account *wloman* is already created, and is part of a user group that is used in an identity-based security policy.

FortiTokens and other two-factor authentication can be added to local or remote users or administrators. This applies to FortiToken-200, with other models having minor variations.

1. Get your FortiToken and make sure it is working. Press the button. It should display a six-digit number and to the left a stack of up to six bars. These represent the time until the code changes, one bar for each 10 seconds. After a few seconds the display should turn off to save power. Turn the FortiToken over and verify there is a serial number. It is 16-digits long and starts with FTK. For this example the token serial number is FTK2000BHV1KRZCC.

2. Go to **User > FortiToken > FortiToken** and select **Create New**.

3. Enter the serial number and select **OK**.

<table>
<thead>
<tr>
<th>Serial Number #1</th>
<th>FTK2000BHV1KRZCC</th>
</tr>
</thead>
<tbody>
<tr>
<td>Automatically Send Activate Request to FortiGuard</td>
<td>Select</td>
</tr>
</tbody>
</table>

You may have problems entering the serial number. If any of the characters are wrong it will be invalid. If you already entered this serial number, it will be invalid. If it is the wrong length, it will be invalid. For security reasons there is no hint of what is wrong — you must determine that by yourself.

3. Wait for the FortiGuard system to validate your FortiToken’s serial number. When you first enter the serial number its status is listed as **New**. Once FortiGuard validates the serial number, the status will change to **Active**.
Adding FortiToken two-factor authentication to a user account

4 Go to **User > FortiToken > FortiToken**, select the FortiToken serial number you just added, and select **Synchronization**.
   The FortiToken Synchronization window appears.

![Synchronize FortiToken window](image)

5 Press the button on your FortiToken, and enter the resulting six-digit number in the **First Code** field. The bars displayed on the left size of the FortiToken display are a count down to when the code changes. When the displayed code changes, press the FortiToken button again, and enter that code in the **Second Code** field.

6 Go to **User > User > User** and edit the user account. Select **Enable Two-factor Authentication**, under **Deliver Token Code by** ensure FortiToken is selected, and choose your serial number from the drop-down list.

If there are no FortiTokens listed in the drop-down list on the user edit page, go to **User > FortiToken > FortiToken** and verify the status of the entry. If it does not say Active, it is not available to be associated with a user's account. Generally the FortiGuard system will verify the FortiToken serial number after a short period of time. If this does not happen, ensure you have a valid connection to the FortiGuard network. See ([FortiGuard Troubleshooting section](#)).

7 Select **OK** to save the user.

**Results**
To verify the user has two-factor authentication configured, go to **User > User > User**. On the list of users that is displayed *wloman* will have a green check under two-factor authentication. This verifies that some form of two-factor authentication is associated with this account.

![User list](image)

To verify the user has FortiToken two-factor authentication properly configured, go to **User > FortiToken > FortiToken**. On the list of FortiToken serial numbers, the one associated with the *wloman* account will have *wloman* displayed in the User column.

![FortiToken list](image)

You can also go to **Log&Report > Log & Archive Access > Event Log** to view log messages recorded while registering the FortiToken, and changing the user account:

![Event Log](image)

**Best Practices**
If you are assigning an administrator a FortiToken, ensure there is another administrator account configured as a backdoor in if there are problems authenticating. Otherwise you will be unable to logon.

On a regular basis, check all FortiTokens for drift. To do this take the token in your hand, go to **User > FortiToken > FortiToken**, and select **Synchronize**. When you enter the 2 codes, you are updating the FortiGate unit clock with any drift in the FortiToken clock that might have happened. This prevents logon issues due to drift.
Adding SMS token code delivery two-factor authentication to a FortiGate administrator’s account

**Problem**  
I need an alternative to FortiToken devices — users don’t want to carry them around.

**Solution**  
An alternative to FortiToken for 2-factor authentication is using SMS text messaging to send users their token code. Using this method, users only need to carry their mobile phone with them which they likely do already.

SMS token code delivery generates a six-digit token on the FortiGate unit. The token code is then delivered to a mobile phone via SMS text messaging, so you can enter it when you logon.

This solution assumes the FortiGate administrator account admin2 is already created, and is part of a user group that is used in an identity-based security policy.

To deliver the token code by SMS text message, you must first configure the SMTP email address for your FortiGate unit, configure the Mobile Provider, and then add the two-factor SMS information to the user account.

For this example, the user is in Canada and uses the mobile provider mproexample. The company is example.com. The administrator’s email address is admin2@example.com and their password is 123456, a very bad password. Their mobile phone number is 613-555-5555.

1. Go to the email server at Log&Report > Log Config > Alert E-mail.
2. Enter the following information and select Apply when done.

<table>
<thead>
<tr>
<th>SMTP Server</th>
<th>mail.example.com</th>
</tr>
</thead>
<tbody>
<tr>
<td>Email from</td>
<td><a href="mailto:my_fortigate@example.com">my_fortigate@example.com</a></td>
</tr>
<tr>
<td>Authentication</td>
<td>enable</td>
</tr>
<tr>
<td>SMTP user</td>
<td><a href="mailto:admin2@example.com">admin2@example.com</a></td>
</tr>
<tr>
<td>Password</td>
<td>123456</td>
</tr>
</tbody>
</table>

You should test your settings at this point to ensure the email can be delivered as expected. This is done by selecting the Test Connectivity button shown in the image above. If the settings are correct, email will be sent to admin1 and admin2. If they do not receive email, something is wrong. Check the spelling of each entry, ensure the SMTP server uses authentication, ensure there is a default route to the mail server, and that SMTP traffic is allowed by security policies on the FortiGate unit.

3. In the CLI, enter the following information to add mproexample as an SMS provider:

```plaintext
config user sms-provider
edit mproexample
    set mail-server mproexample.ca
next
end
```
You will need to contact your mobile provider for their mail server address. This is the mail server that you can email and it will forward your message as an SMS text message to the customer’s mobile phone. At that time you should verify that your mobile phone service includes SMS text messaging.

4 Go to System > Admin > Administrators, select admin2, and select Edit.

5 Select Enable Two-factor Authentication, under Deliver Token Code by ensure SMS is selected, and choose mproexample as the mobile provider.

6 Enter your mobile phone’s telephone number including area code and/or country code as required by your mobile provider.

7 Select OK.

Results When the token code is sent via SMS text messaging the message will appear similar to:

fortigate@example.com(AuthCode: 039130) Your authentication token code is 039130.

To verify the administrator has two-factor authentication configured, go to System > Admin > Administrators. On the list of administrators that is displayed admin2 will have a green check in the two-factor authentication column. This verifies that some form of two-factor authentication is associated with this account.

You can also go to Log&Report > Log & Archive Access > Event Log to view log messages recorded while registering the FortiToken, and changing the user account:

<table>
<thead>
<tr>
<th>#</th>
<th>Date</th>
<th>Time</th>
<th>Level</th>
<th>User Interface</th>
<th>Action</th>
<th>Message</th>
</tr>
</thead>
<tbody>
<tr>
<td>77</td>
<td>2011-08-10 19:04:38</td>
<td>GUI(172.20.120.17)</td>
<td>fortoken-synchronize</td>
<td>User admin resynchronized FortiToken FTK2008BH-V1KRZCC with result: success</td>
<td></td>
<td></td>
</tr>
<tr>
<td>87</td>
<td>2011-08-10 14:40:14</td>
<td>GUI(172.20.120.17)</td>
<td>fortoken-activate</td>
<td>Activation of FortiToken FTK2008BH-V1KRZCC succeeded.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>88</td>
<td>2011-08-10 14:39:46</td>
<td>GUI(172.20.120.17)</td>
<td>fortoken-activate</td>
<td>User admin has requested to activate FortiToken FTK2008BH-V1KRZCC.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

When admin2 attempts to logon to the FortiGate unit GUI or access network resources through an identity-based security policy, they will be presented with a two-factor authentication logon prompt. This prompt includes the normal username and password, but after wloman has entered and verified their username and password, a third field appears where the token code is entered by admin2 once it has been received on their mobile phone. On validation, wloman is allowed access. If any of the username, password, or token code are not valid admin2 is not authenticated and is not granted access.
Stopping the “Connection is untrusted” message

Problem  When you first connect to a FortiGate unit with your web browser, a message may appear questioning the connection's security. How do you prevent this?

Solution  When you see a “Connection is untrusted” type message, it means there is a problem with the certificate for the website you are connecting to.

Anytime you browse a website, you are using either HTTP or HTTPS. The difference between them is that HTTPS has security. This security is in the form of certificates that identify the source as being legitimate. Without a valid certificate, the customer does not know if it is really the true website, or if a hacker hijacked their connection with malicious intent.

With FortiGate units, this message occurs for two reasons — because the default certificate used by the FortiGate unit is a self-signed certificate, and because the certificate is valid only for the FortiGate unit. To be trusted, a certificate must be signed by a known certificate authority (CA) that the web browser can verify. For example if Fred’s certificate is signed by Bob, and Bob’s certificate is signed by Peter, then anytime someone check’s Fred’s certificate they must be able to trace it back to Peter and verify that Peter is trustworthy. Any break in that chain, and Fred’s certificate is seen as untrustworthy.

Contact your ISP or other online services provider to get a trusted intermediate CA certificate for your FortiGate unit. When you are giving them the information, make sure it is clear where you will be using this certificate: on an internal network, a public facing website, or across your enterprise. Ensure it is a CA certificate as this allows you to sign certificates for local users for applications such as VPN.

Generally online services providers include a form for you to fill out to create your certificate when you are paying for it on their website. However another common method is to generate a certificate signing request (CSR) with an application like openssl. This is a request that is sent to the certificate authority providing you with your certificate. They process the request, usually automatically, and return a certificate to the email address provided based on the information in the CSR.

The certificate from the CA is a text file that contains the information you included in the CSR as well as details about the CA who issued the certificate, when it was issued and when it expires, and the “fingerprints” or encryption associated with it.

To install a CA certificate from your computer to the FortiGate unit you go to System > Certificates > CA Certificates and select Import. After you browse to the certificate file, which is usually a .cer or .p12 format text file, and select it will be installed on your FortiGate unit. You can verify this by refreshing the display to see the new certificate. It will be displayed by name and subject, and you can select it for more in-depth details if you need to verify it.

Now when you are using HTTPS or other SSL connection, your FortiGate unit will not generate “untrusted” certificate-based error messages.
Logging and Reporting

You can use FortiGate logging to record all traffic passing through the FortiGate unit and record all events such as when application activity, virus events, attacks and so on. In security policies you can also enable traffic logging to record log messages for all of the traffic accepted by security policies.

On FortiGate units with hard disks, all of the information captured by logging is compiled into the weekly activity report. You can view this report at any time to see details of the activity captured by FortiGate logging. Included in the report is bandwidth and application data, web usage data, email usage data, threats intercepted, and VPN usage. In addition to real time viewing you can view historical versions of the report which is recorded each week.

You can also view the actual log messages recorded by the FortiGate unit. Viewing log messages supplies more details about specific events recorded by the FortiGate unit and can be used to trace activity and diagnose problems.

FortiGate units without hard disks support a port of these logging and reporting features. On any FortiGate unit you can send log messages to a FortiAnalyzer unit or remote syslog server and use these devices to report on FortiGate activity recorded by log messages.

Throughout the web-based manager you can find monitor pages that display real time information about that part of the product. For example, in the policy section of the web-based manager you can view the list of active sessions being processed by the FortiGate unit and view a graph of the most active security policies. In the UTM profiles section of the web-based manager monitoring pages are available for most UTM functions, including application usage, intrusion monitoring, and endpoint monitoring.

Many of the reporting and monitoring functions include drill down options to view more details or different views of the information on the monitor or report page.

This chapter includes the following logging and reporting examples:

- Understanding log messages
- Creating a backup log solution
- Logging to remote Syslog servers
- Alert email notification of SSL VPN login failures
- Modifying a default report
- Testing the log configuration
Understanding log messages

**Problem**  There are several application control log messages with the message “web: HTTP.BROWSER”. What does this mean?

**Solution**  Find out what these log messages mean by understanding each part of the log message.

The parts of the log message, called log fields, contain specific information. For example, the date log field contains information about the day, month and year of when the log message was recorded.

You can look at log messages as puzzles — each piece of the log message is a piece of a puzzle, and when those pieces are put together, they show the whole picture. Log messages provide valuable insight into how to better protect the network traffic against attacks, misuse and abuse.

1  Go to **Log&Report > Log & Archive Access > UTM Log**.

The application control log messages appear on the page. Even though you can view the individual fields from the log viewer table, not all log fields are visible. You should always download a log file so that you can clearly see all log fields. A text editor, such as jEdit, can help to better display the log messages when viewing them from your computer.

2  Download the UTM log file by selecting **Download Raw Log**.

The log messages saved to your computer are in a format called Raw. This format is how the log messages appear in the log file on the FortiGate unit. When viewing the log messages in the web-based manager, you are viewing them in the format called Format. This view allows you to customize what information you see on the page, where in Raw format you cannot.
3 On your computer, open the file up and scroll down to locate the application control log messages with the message “web: HTTP.BROWSER”.

4 Since these log messages are the same, pick one and break it into the two groups that make up a log message: the log header and log body. The first group is what will be looked at first, the log header.

```
2011-08-17 13:40:20 log_id=28704 type=app-ctrl subtype=app-ctrl-all
pri=information vd=root
date=2011-08-17
```

- **Date:** The year, month and day of when the event occurred in yyyy-mm-dd format.
- **Time:** The hour, minute and second of when the event occurred in the format hh:mm:ss.
- **Log ID:** A five-digit unique identification number. The number represents that log message and is unique to that log message. This five-digit number helps to identify the log message.
- **Type:** The section of system where the event occurred.
- **Subtype:** The subtype category of the log message.
- **Priority:** The severity level of the event. In this log message, this means that there is general system information.
- **Virtual Domain:** The name of the virtual domain where the action/event occurred in. If no virtual domains exist, this field is always root.

Now we know the first part of the what the log message is saying — an application control event occurred on August 17, 2011 at 1:40 pm and this is just general system information.

Next, understanding the rest of the log message from the log body.

5 The log body contains the following information:

```
attack_id=15893 src="10.10.20.3" src_port=52315 src_int="internal"
dst="67.69.176.57" dst_port=80 dst_int="wan1" src_name=10.10.20.3
dst_name=67.69.176.57 proto=6 service="http" policymid=1
serial=20596 app_list="default" app_type="web" app="HTTP.BROWSER"
action="pass" count=1 msg="web: HTTP.BROWSER"
```

- **Attack ID:** The identification number of the IM (IPS) log message.
- **Source IP:** The source IP address. In this case, it is the internal interface that is used with the IP address of 10.10.20.3
- **Source Port:** The source port number. Usually a random number that keeps track of sessions.
- **Source Interface:** The source interface is the internal interface.
- **Destination IP:** The destination IP address.
- **Destination Port:** The destination port number. Port 80 is typically HTTP.
- **Destination Interface:** The destination interface is wan1.
- **Source Name:** The source name. The source name is usually the source IP address.
From the log body, we now know the traffic that was flowing through wan1 (the external interface on the FortiGate unit) was scanned by the FortiGate unit using the security policy 1, which had the default application control profile applied to it. From those rules, the FortiGate unit matched the traffic. The user (internal=10.10.20.3) was accessing the Internet and was using the application HTTP.BROWSER.

Knowing the application was HTTP.BROWSER, we can lookup exactly what this application is by going to the FortiGuard Center.

6 In the web-based manager, go to UTM Profiles > Application Control > Application List.
7 In the search field, enter HTTP.BROWSER; when it appears in the list on the page, select its name.

You are automatically redirected to the FortiGuard Center page that contains all the information you need to know about the application, HTTP.BROWSER.

8 The description for this log message on the FortiGuard Center page says this application only has a medium risk, and indicates that an HTTP client request attempted to contact with a HTTP server, which usually listens on port 80. This is not an attack or an exploit.

You can use the FortiGate Log Message Reference to understand log messages. It contains an explanation of each log field for each log message.
Creating a backup log solution

**Problem** You have recently setup a FortiAnalyzer unit and need a backup solution. Before integrating the FortiGate unit into your network, you were using a Syslog server, which you would like to use again.

**Solution** Configure the FortiAnalyzer and Syslog server first, and then configure the FortiGate unit to send logs to both log devices.

The FortiAnalyzer unit, a Fortinet log device, can help you provide another storage location for storing logs. The FortiAnalyzer unit can log all FortiGate activity that is available for logging, including archival of log files. The FortiAnalyzer unit has many features, for example managing multiple FortiGate units’ logging requirements, as well as creating FortiAnalyzer customized reports that organize and monitor FortiAnalyzer unit information.

The following steps begin immediately after you have set up the FortiAnalyzer unit on your network.

1. Update your third party Syslog server software, and verify that it is up and running properly.
2. On the FortiGate unit, use the CLI command `execute ping` to ping the FortiAnalyzer unit and then do the same for your Syslog server.
   
   If there is 100 percent packet loss, troubleshoot the networking problem before proceeding.
3. On the FortiGate unit, go to `Log&Report > Log Config > Log Setting` and verify that you are currently logging to the FortiGate unit’s local disk.
4. Enter the following CLI commands:
   ```
   config log fortianalyzer setting
   set status enable
   set address-mode static
   set server 172.20.120.138
   set upload-option realtime
   end
   config log syslogd setting
   set status enable
   set server 10.10.20.4
   set facility local1
   end
   ```
5. Test the connection between the FortiGate unit and FortiAnalyzer unit. On your FortiGate unit go to `Log&Report > Log Config > Log Setting`, select `Upload logs remotely`, and then select `Test Connectivity`.
   
   By selecting Test Connectivity, you can see if there are any issues with the settings. For example, **Connection Status** in the FortiAnalyzer Connection Summary window has **Logs not received**. This means that there is an issue about sending the logs to the FortiAnalyzer.
unit. You must troubleshoot the problem. If the **Connection Status** has a green checkmark, you are able to successfully log to the first FortiAnalyzer.

### Results

On the FortiAnalyzer unit, you should now see logs appearing on each unit, in **Log & Archive > Log Access**. You should also be seeing logs appear on the Syslog server.

If you are not seeing any logs on the FortiAnalyzer unit, verify that the device has been included in the Devices menu list. Check with the FortiAnalyzer documentation to help troubleshoot any FortiAnalyzer problems that appear.

There is no command to verify the FortiGate unit’s connection with the Syslog server. If you are having issues between the Syslog server and FortiGate unit, you should verify that you can ping to the Syslog server through your FortiGate unit.

You should test that logs can be sent to the FortiAnalyzer units to ensure log messages are being sent. By testing the connection, you can easily and quickly resolve any issues that may occur, such as logs not being sent or an issue that is on the FortiAnalyzer side, such as the device is not appearing on the FortiAnalyzer unit’s Devices list.
To test that the FortiGate unit can send logs to the FortiAnalyzer unit, use the `diag log test` command to generate logs and view them from the FortiAnalyzer unit to verify that they were sent.

```
diag log test
```

generating a system event message with level - warning
generating an infected virus message with level - warning
generating a blocked virus message with level - warning
generating a URL block message with level - warning
generating a DLP message with level - warning
generating an attack detection message with level - warning
generating an application control IM message with level - information
generating an antispam message with level - notification
generating an allowed traffic message with level - notice
generating a wanopt traffic log message with level - notification
generating a HA event message with level - warning
generating netscan log messages with level - notice
generating a VOIP event message with level - information
generating authentication event messages
Logging to remote Syslog servers

**Problem** You want to configure the FortiGate unit to send logs to three Syslog servers and ensure the reliability that the logs were sent to the servers.

**Solution** Use the reliable Syslog feature, available when configuring the Syslog servers.

When configuring logging to three Syslog servers, it is best to configure all three using the CLI instead of going to the web-based manager and configuring one there, and then the other two in the CLI.

This type of logging configuration is called a log redundancy configuration. A redundancy logging configuration sends the same logs to each of the log devices, so that there is always a copy of the same log file on each device. In FortiOS, this configuration is supported only with FortiAnalyzer units and Syslog servers.

1. Log in to the CLI.
2. Enter the following command syntax to configure the three Syslog servers, as well as enabling reliable logging to Syslog servers:

   ```bash
   config log syslogd setting
   set status enable
   set server 10.10.20.4
   set reliable enable
   set csv enable
   set facility local1
   end
   config log syslogd setting
   set status enable
   set server 10.10.20.5
   set reliable enable
   set csv enable
   set facility local2
   end
   config log syslogd3 setting
   set status enable
   set server 10.10.20.6
   set reliable enable
   set csv enable
   set facility local3
   end
   ```
3 Test the configuration by using the `diag log test` command syntax.

The FortiGate unit generates log messages and then sends them to the Syslog servers.

4 View the Syslog server log entries to verify that the logs were successfully sent.

Results The log messages should be going directly to all three Syslog servers. You can verify this by going directly to each Syslog server and viewing the logs that are displayed in the server's window.
Alert email notification of SSL VPN login failures

**Problem**
You need to be immediately notified when an SSL VPN login failure occurs so that you can quickly fix the problem, regardless of where you are.

**Solution**
Create an alert email to notify you that an SSL VPN login failure occurred.

The following assumes that you have already set up logging and that event logging has been enabled. For this example, turn off all event logging before you start to prevent other possible non-SSL VPN log messages from confusing things.

Event logging must be enabled (in Log & Report > Log Config > Log Setting) so that this alert email can be sent. SSL VPN events are one of the event types logged to the event log and therefore must be enabled in Event Logging.

When entering the email addresses for the alert email configuration, you need to enter two email addresses. The first email address is for the sender of the alert email and the second is for receiver of the alert email. The sender can be any email address that helps to identify that the email has been sent from the FortiGate unit. In this solution, we use fortigate@example.com to help identify that the alert email is sent by the FortiGate unit. The email that you receive is your email address, and in this solution it is referred to as myemail@example.com

2. Under Event Logging, select SSL VPN user authentication so that all SSL VPN authentication events are logged.
3. Go to Log & Report > Log Config > Alert E-mail and configure the following:

<table>
<thead>
<tr>
<th>SMTP server</th>
<th>mail.example.com</th>
</tr>
</thead>
<tbody>
<tr>
<td>Email from</td>
<td><a href="mailto:fortigate@example.com">fortigate@example.com</a></td>
</tr>
<tr>
<td>Email to</td>
<td><a href="mailto:myemail@example.com">myemail@example.com</a></td>
</tr>
</tbody>
</table>

4. Select Authentication and provide the following authentication log in credentials for the SMTP server.

<table>
<thead>
<tr>
<th>SMTP user</th>
<th>myemail</th>
</tr>
</thead>
<tbody>
<tr>
<td>Password</td>
<td>!eMa1L9</td>
</tr>
</tbody>
</table>

5. Verify that all information is correct and then select Test Connectivity.
When you select Test Connectivity, the FortiGate unit generates a test alert email message and sends it to your email address. If you do not receive an email, you need to troubleshoot the problem. An email log message is only recorded if the SMTP server name is misspelled.
Alert email notification of SSL VPN login failures

If you accidently have a typo in the SMTP server field it appears as follows:

```
2010-04-05 13:34:31 log_id=01000200003 type=event subtype=system
vd=root pri=notice user=system ui=system action=alert-email
status=failure count=5 msg="Failed to send alert email from
mail.exmpl.com to myemailaddress@example.com"
```

In the above log message, highlighted in bold, you can see that mail.example.com has been misspelled. To fix the problem, make the spelling correction and select **Test Connectivity** again.

6. Select **SSL VPN login failure** in **Send alert email for the following**.
7. Select **Apply** to save the alert email configuration.

**Results**

When an SSL VPN user attempts to authenticate using the SSL VPN tunnel, and they are unsuccessful, this event is logged by the FortiGate unit and you receive an alert email in your inbox. The body of the email contains the event log message.

To test that you can receive an alert email notification, on the Alert E-Mail page, select **Administrator login/logout** and then select **Apply**. Log out of the web-based manager and then log back in again. Check your inbox; an alert email message should be there, with the subject line “Message meets Alert condition” and appears as follows:

```
from: fortigate@example.com
subject: Message meets Alert condition
to: You

Message meets Alert condition
date=2011-08-17 time=13:50:45 devname=FG50BH3G09601792 device_id=FG50BH3G09601792 log_id=0104032001 type=event
subtype=admin pri=information vd=root user="admin" ui=ui0 action=logout status=success reason=none
msg="Administrator admin logged in successfully from http(10.10.20.3)"
```

Alert email can be sent for any configured event logging events such as DHCP event, IPsec event, or quarantine event. The complete list of available events can be found at **Log&Report > Log Config > Log Setting**.

Select only specific alert email notification options that you require. Otherwise your inbox could be flooded with unwanted email messages.
Modifying a default report

Problem You want to create a report from the information you found after viewing a list of the web sites your users have visited.

Solution Modify the default FortiOS UTM report so that it has exactly what you need.

Modifying this report is easy and less time consuming than creating a custom report. However, you can create a custom report for this but it is entirely done in the CLI.

After creating your modified version of the default FortiOS UTM report, you can restore the report back to its default settings which includes all pages and charts.

2. Change the following information:

<table>
<thead>
<tr>
<th>FortiGate UTM</th>
<th>Top Web Sites Employees Visit</th>
</tr>
</thead>
</table>

3. Remove the FortiGate Host Name and FortiGate Serial Number text boxes.
4. Remove the The FortiGate Advantage text box.
5. Select Save to save the changes to the cover page.

The page automatically goes back to its unedited view when you save the page, regardless of which page you are modifying.

6. Select Edit and then select Options.
7. Under Sections, select VPN Usage, Threats, Emails, and Bandwidth and Application Usage and then select Delete.
8. Under Report Schedule, select Demand from the Schedule Type list.

When you select Demand, you are creating an on-demand report which is available for generating whenever you want.

9. Select OK.
10. Select Save to save the changes.
12. Scroll down until you locate the chart Top Search Phrases; remove the chart and its text boxes.
13. Select Save to save the changes.

If you have been logging web usage for a while, you may see information in some of the charts.

14. Select Run to immediately generate the report.

The report may take a while, depending on how much information has been gathered from the logs.
**Results**  A generated report should appear in the list on the Historical Reports page. The following shows a page of the report in a PDF.

You can view the generated report either as a HTML report, by selecting the report’s name in the Report File column, or as a PDF, by selecting PDF in the Other Formats column.

The PDF can be easily downloaded to your computer and then distributed in an email to others.
Testing the log configuration

**Problem**
How do I test my log configuration?

**Solution**
Test the configuration by using **Test Connectivity**, as well as the `diag log test` command.

Testing connections between a FortiGate unit and a WebTrends server or Syslog server are not available. Testing between the FortiGuard Analysis server and the FortiGate unit is also supported.

The test involves using both the CLI and web-based manager.

1. In the web-based manager, go to **Log & Report > Log Config > Log Setting**.

2. Under **Logging and Archiving**, select **Test Connectivity**.
   The FortiAnalyzer Connection Summary window appears. You should have all green check marks for the **Privileges** and **Connection Status**. If there is a caution icon with the words **Logs not received in Connection Status**, you will need to troubleshoot the issue. You may have to troubleshoot both the FortiGate unit and the FortiAnalyzer unit.

3. To test the connection other than using the web-based manager, in the CLI use `diag log test` command.
   This command sends logs to the FortiAnalyzer unit.

4. To verify the number of logs sent, failed, dropped or buffered to the FortiAnalyzer unit, use the `diag fortianalyzer-log mgstats show` command.

5. Go to the FortiAnalyzer unit, and under **Log & Archive**, view the logs that you just sent from your FortiGate device.

6. To check the connectivity between your FortiGate and the FortiGuard Analysis server, in **Log & Report > Log Config > Log Setting**, under **Logging and Archiving**, select **Test Connectivity** for the **FortiGuard Analysis & Management Service**.
   The FortiGuard Connection Summary window appears, showing the expiry date, disk quota and daily volume, and whether or not you are sending DLP archives to the server.

**Results**
You should be seeing successful results, where logging is being sent to the log device, either a FortiGuard Analysis server or a FortiAnalyzer unit.
Index

A
access point, 107
Active Directory, 126
address
   FQDN firewall address, 135
admin profile
   custom, 83
   super_admin, 34
administrator
   creating, 34, 83
admin profile
   custom, 83
alert email, 280
alert notification email for SSL VPN login failures, 280
antivirus
   changing the maximum file size, 185
   flow-based, 187
   software, 225
application control, 202, 264
   adding a sensor to a policy, 202
   blocking access to social media, 204
   blocking instant messaging, 203
   blocking peer to peer file sharing, 205
   troubleshooting, 202
application monitor, 202
   drill down, 202
applications
   bandwidth use, 189, 202, 204, 205, 228, 231, 237, 242, 246, 249, 270, 272, 275, 278
   blocking, 264
   debugging, 104
   visualizing, 202
ARP
   packet sniffer, 95
assigning IP addresses, 86
authenticate
   web filtering, 190
authentication
   debugging, 102
   two-factor, 266, 268
authoritative dns, 85

B
backup
   configuration, 28, 74
   backup Internet connection, 38, 44
backup log solution, 275
bandwidth
   application use, 189, 202, 204, 205, 228, 231, 237, 242, 246, 249, 270, 272, 275, 278
   bandwidth consuming
   web filtering, 189
Bing
   safe search, 191
bridge table, 26

C
CA Authority, 126
captive portal
   WiFi, 117
capture
   packet, 89
central NAT table, 166
certification, 10
Cisco UNITY client, 237
cluster, 69
   connecting an HA cluster, 70
configuration
   backup, 28, 74
   connecting a FortiGate HA cluster, 70
count, 144
   policy, 144
   security policy, 202
customer service, 10

D
Data Leak Prevention, 209
dhcp server, 123
debug
   application, 104
   authentication, 102
   diagnose command, 101
   flow, 104, 139, 140, 146
   info, 104
   ipsec VPN, 103
   packet flow, 103
   SSL VPN, 101
   URL filtering, 103
debug flow, 139, 140
debugging FortiGate configurations, 101
default route failover, 41, 47
demilitarized zone
   network, 50
denial of service
   protection, 207
deny policy
   count column, 149
   verifying, 147
destination NAT, 169, 171, 173, 176, 179
dhcp, 15
   IP reservation, 86
Dhcp relay
   WiFi, 123
diag debug flow, 139, 140, 146

FortiOS 4.0 MR3
http://docs.fortinet.com/
Index

diag log test, 277
diagnose
  quick reference, 104
diagnose debug, 101
diagnose debug flow, 139, 140
DLP, 209
  flow-based, 188
DMZ network, 50
DNAT, 169, 171, 173, 176, 179
  web server, 51
DNS
  creating a local DNS server, 85
  verifying the configuration, 20, 25
dns
  authoritative, 85
  database, 85
documentation, 10
  Fortinet, 10
domain name service, 85
DoS
  policy, 207
  protection, 207
  sensor, 207
drift
  FortiToken, 104
dual internet connections, 48
dynamic SNAT, 162
dynamic source address translation, 162
  central NAT table, 166
E
ECMP
  route priority, 42
  routing, 42, 48
  spillover, 48
  usage-based, 48
e-mail filtering, 208
  FortiGuard, 32
terprise security
  wireless, 114
equal cost multipath
  routing, 42, 48
ESP
  packet sniffer, 95
event log, 280
extended
  virus database, 184
extreme
  virus database, 184
F
failover
  default route, 41, 47
FAQ, 10
file size
  antivirus maximum, 185
filter
  packet capture, 98
  packet sniffer, 94
firewall
  ordering policies, 148
  restricting all DNS queries to a selected DNS server, 151
  restricting employees’ Internet access, 135
  restricting Internet access per IP address, 141
  schedule, 135
  using geographic addresses, 158
  verifying that traffic is hitting a security policy, 144
firewall address
  FQDN, 135
firewall statistics
  diag, 104
firmware
  download from Fortinet support, 27
  TFTP upgrade, 28
  upgrading, 27, 73
  version, 27, 73
flow
  debug, 104
  diag debug, 139, 140, 146
  diagnose debug flow, 139, 140
flow-based
  antivirus, 187
  DLP, 187
  UTM, 187
  web filtering, 187
FortiAnalyzer, 275
  FortiAnalyzer unit, 275
  testing sending logs, 277
FortiAP, 107, 110, 123
  FortiAP, troubleshooting, 112
FortiASIC, 213
FortiClient
  SSL VPN, 221
FortiClient SSL VPN, 218
FortiGuard
  Antivirus, 9
  email filtering lookups, 32
  overriding web filtering, 190
  ports used, 32
  server list, 32
  services, 9
  setup, 30
  transparent mode, 26
  troubleshooting, 30
  web filtering category, 192
  web filtering lookups, 32
FortiGuard Centre, 192
FortiGuard web filtering, 189
  check IP addresses, 199
  images, 200
Fortinet
  customer service, 10
  Knowledge Base, 10
  Knowledge Center, 10
  MIB, 87
  SSL VPN clients, 213
  Technical Documentation, 10
  Technical Support, 10
  Technical Support, registering with, 9
  Technical Support, web site, 9
  Training Services, 10
Fortinet documentation, 10
Fortitoken
  drift, 104
O
one-to-one NAT, 164
override
web filtering, 190
override internal DNS DHCP, 17
oversized email, 186
oversized file, 186

P
packet
sniffer, 89
packet capture, 94, 98
filters, 98
packet flow
debugging, 103
packet sniffer
filters, 94
protocols, 95
packet sniffing, 89, 98
PAT, 160
pcap
packet capture file, 98
PEAP, 128
PEAP authentication, 126
peer-to-peer file sharing
blocking, 205
ping server, 41
policy
adding an application control sensor, 202
count, 144
DoS, 207
local-in, 88
policy monitor, 144
port address translation, 160
port forwarding, 169, 171, 173, 176, 179
web server, 51
port mapping, 169, 171, 173, 176, 179
port pairing
transparent mode, 63
portal
WiFi, 117
preshared key, 121, 124
Primary Internet connection, 44
primary Internet connection, 38
priority
route, 42
product registration, 9
protocol options, 186
proxy avoidance
web filtering, 189

R
RADIUS (NPS), 126
rating error, 21, 26
web filtering, 21, 26
recursive
DNS server mode, 85
recursive dns, 85
redundant Internet connections, 38
registering
with Fortinet Technical Support, 9
release notes, 27
remote Internet access, 218
replacement message
virus message, 62
reporting
FortiOS UTM report, 282
modifying default report, 282
RFC
1918, 7
route
priority, 42
route failover, 41, 47
route mode, 66
security policy, 52
routing
ECMP, 42, 48
equal cost multipath, 42, 48

S
safe search
web filtering, 191
schedule
firewall, 135
security policies
ordering, 148
restricting all DNS queries to a selected DNS server, 151
restricting employee’s Internet access, 135
using geographic addresses, 158
security policy, 144
adding an application control sensor, 202
count column, 202
limit Internet access, 135
restricting Internet access per IP address, 141
verifying traffic, 144
security risk
web filtering, 189
sensitive information
blocking, 209
sensor
DoS, 207
service
multiple, 52
shared shapers, 154
SMS used in two-factor authentication, 268
SNAT, 160, 162, 166
sniffer packet
diagnose, 105
sniffing
packet, 89
social media
blocking, 204
software switch
WiFi, 120
source address translation, 160
spam
filtering, 208
spillover
ECMP, 48
split tunnel, 220
split tunneling
SSL VPN, 221
split-brain
HA, 70
SSID, 120, 123
Index

SSL VPN, 214
  access email server, 214
debugging, 101
dataflow security, 213
FortiClient, 221
FortiGuard, 221
remote user, 225
split tunneling, 221
Subsession, 220
tunnel mode, 213
virtual desktop, 213
ssl.root, 219, 222
ssl.root interface, 220
static SNAT, 160
storage location, 275
storage location, 275
streaming media
  blocking, 195
suggest a URL category
  web filtering, 192
super admin
  administrator profile, 34
sys session full-stat
diagnose, 105
Syslog server, 275
Syslog servers, log device, 278
T
  technical
documentation, 10
  notes, 10
  support, 10
technical support, 10
test log
diagnose, 105
test update info
diagnose, 105
TFTP, 28
thin AP, 107
threshold
  oversized file/email, 186
traceroute, 31
traffic shaping
  shared shapers, 154
VoIP, 154
Training Services, 10
Transparent mode, 26
transparent mode
  port pairing, 63
  protecting a server, 57
troubleshooting, 25
transport-mode, 236
troubleshooting
  DHCP, 16
  FortiGuard, 30
  ISP connection, 16
  NAT configuration, 16
  packet sniffing, 89, 94
  transparent mode, 25
  verifying that traffic is hitting a security policy, 144
VPNs, 249
Tunnel Mode, 218

U
  unity-support, 240
upgrade
  firmware, 27
  HA cluster firmware, 73
uploading logs, 276
URL
  FortiGuard web filtering category, 192
URL filtering
debugging, 103
usage-based
  ECMP, 48
USB modem, 46
users
  identifying, 260
  monitoring, 260
V
  VDOM, 78
VIP
  web server
    firewall VIP, 51
virtual domain, 78
virtual FortiOS instances, 78
virtual interface, 120
virtual LANs, 75
virus
  legacy, 184
virus database
  extended, 184
extreme, 184
visual
  applications, 202
VLANs, 75
  configuring, 75
VoIP
  traffic shaping, 154
VPN
  Cisco UNITY client, 237
  Dialup, 231
  L2TP, 236
  SSL, 214
vpn tunnel list
diagnose, 105
VPN, IPsec
  from Android device, 242
  from FortiClient PC, 231
  from iPhone, 237, 242
overview, 227
vulnerability scanner, 210
W
web browsing
  blocking web sites by category, 262
web filter
  blocking streaming media, 195
  record websites, 193
safe search, 191
whitelist, 197
Web filtering
  correct a URL category, 192
web filtering, 21, 26, 189
authenticate, 190
errors, 21
flow-based, 187
FortiGuard, 32, 189, 262
suggest a URL category, 192
web monitoring, 262
web portal, 214
web server
port forwarding, 51
web sites users have visited, 193
websites
blocking, 262
whitelist
web filter, 197
WiFi
captive portal, 117
DHCP relay, 123
software switch, 120
WiFi access, 108, 110, 114, 123
WiFi access point, 107
WiFi Controller, 109
WiFi controller feature, 107
Windows AD, 126
Windows Security Health Validator, 128
Windows Server 2008, 126
wireless
WPA/WPA2 enterprise security, 114
WPA2 security, 108
WPA/WPA2 enterprise security
wireless security, 114
WPA2
wireless security, 108
WPA2-Personal, 110, 123
WPA-Enterprise, 126
Y
Yahoo
safe search, 191
The FortiGate Cookbook is designed to help new FortiGate users solve problems on their networks by implementing FortiGate features such as UTM, WiFi, and VPN. The cookbook contains sections (recipes) that describe step-by-step solutions for solving problems and verifying the results of the solution. Many recipes also contain troubleshooting information, best practices and additional details.

Scattered throughout this document you will also find dedicated troubleshooting sections and details about using the FortiGate packet sniffer and diagnose debug commands.

The FortiGate Cookbook was written for FortiOS 4.0 MR3 patch 2 (FortiOS 4.3.2) and is compatible with most FortiOS 4.0 MR3 firmware versions.

**Fortinet Knowledge Base** - http://kb.fortinet.com  
**Technical Documentation** - http://docs.fortinet.com  
**Training Services** - http://campus.training.fortinet.com  
**Technical Support** - http://support.fortinet.com

You can report errors or omissions in this or any Fortinet technical document to techdoc@fortinet.com.