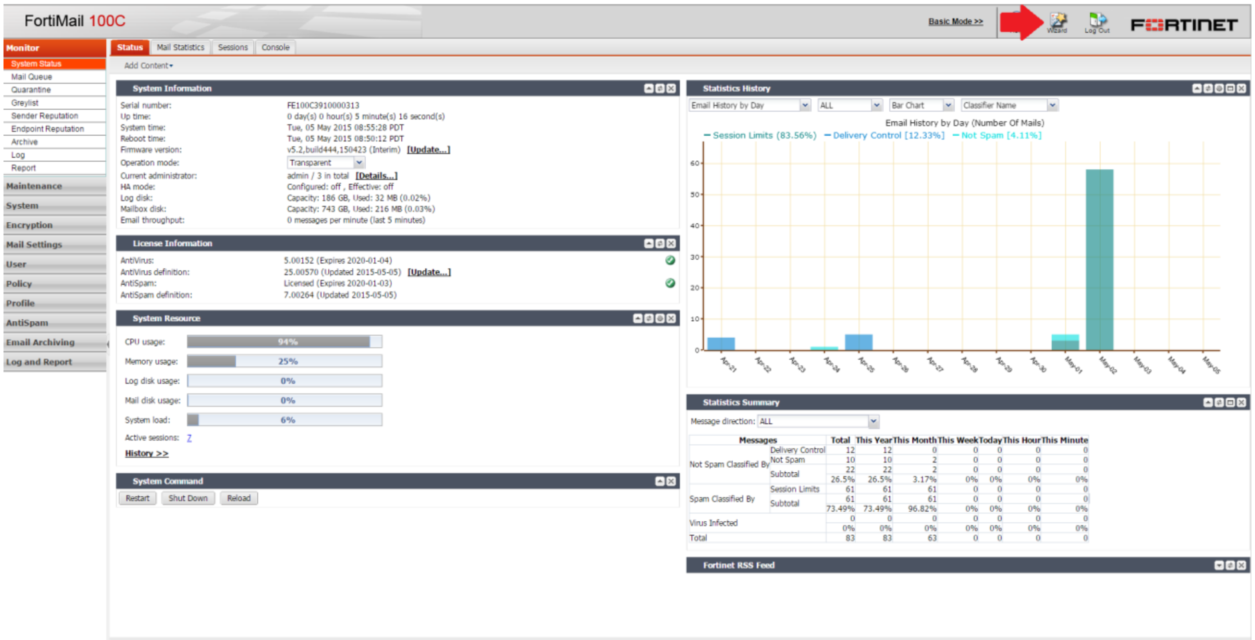
FortiMail: How does an ISP avoid being blacklisted?

As a service provider you want to ensure that your IP address will not be blacklisted. Unfortunately, sometimes subscribers will send out spam, either on purpose, or accidentally, which will result in your IP being blacklisted. Thankfully, your FortiMail unit can help you avoid being blacklisted.

This recipe covers how to minimize the risk of innocent blacklisting.

Initiating Transparent Mode

1. Navigate to **Monitor > System Status > Status.**
2. Select **Transparent** from the Operation mode dropdown menu.
3. Run the Quick Start Wizard by selecting the **Wizard** button.



Serial number: FE100C3910000313
Up time: 0 day(s) 0 hour(s) 5 minute(s) 16 second(s)
System time: Tue, 05 May 2015 08:55:28 PDT
Reboot time: Tue, 05 May 2015 08:50:12 PDT
Firmware version: v5.2,build444,150423 (Interim) [Update...]
Operation mode: Transparent
Current administrator: admin / 3 in total [Details...]
HA mode: Configured: off , Effective: off
Log disk: Capacity: 186 GB, Used: 32 MB (0.02%)
Mailbox disk: Capacity: 743 GB, Used: 216 MB (0.03%)
Email throughput: 0 messages per minute (last 5 minutes)

AntiVirus: 5.00152 (Expires 2020-01-04) ✓
AntiVirus definition: 25.00570 (Updated 2015-05-05) [Update...]
AntiSpam: Licensed (Expires 2020-01-03) ✓
AntiSpam definition: 7.00264 (Updated 2015-05-05)

CPU usage: 94%
Memory usage: 25%
Log disk usage: 0%
Mail disk usage: 0%
System load: 6%
Active sessions: 7
History >>

Message direction: ALL

Messages		Total	This Year	This Month	This Week	Today	This Hour	This Minute
Not Spam Classified By	Delivery Control	12	12	0	0	0	0	0
	Not Spam	10	10	2	0	0	0	0
	Subtotal	22	22	2	0	0	0	0
		26.5%	26.5%	3.17%	0%	0%	0%	0%
Spam Classified By	Session Limits	61	61	61	0	0	0	0
	Subtotal	61	61	61	0	0	0	0
		73.49%	73.49%	96.82%	0%	0%	0%	0%
Virus Infected		0	0	0	0	0	0	0
		0%	0%	0%	0%	0%	0%	0%
Total		83	83	63	0	0	0	0

Configuring the Connection with the Radius Server

Your FortiMail unit uses RADIUS accounting records to combat spam and viruses originating from your network and reduces the likelihood that your public IP addresses will be blacklisted.

To configure your RADIUS server

1. Configure the FortiMail unit as an auxiliary RADIUS server on your RADIUS server.
2. Ensure it sends the *Calling-Station-ID* and *Framed-IP-Address* attributes to the FortiMail unit.
3. Determine whether your RADIUS server sends the *Framed-IP-Address* attribute's value in network order (192.168.1.10) or host order (10.1.168.192).
4. Verify that routing and firewall policies permit RADIUS accounting records to reach the FortiMail unit.

Testing the FortiMail unit

Once you are connected with the RADIUS server, you'll need to make sure the FortiMail unit is receiving the RADIUS records.

1. Connect to the CLI.
   Note: You cannot connect to the CLI through the web interface. For more information on how to connect to the CLI, see "Connecting to the Web UI or CLI" (LINK).
2. Enter the following command to enable the FortiMail unit to receive RADIUS records by starting the endpoint reputation daemon:
   ```
   config antispam settings
      set carrier-endpoint-status enable
   end
   ```
3. *E*nter the following command to configure the RADIUS secret:
   ```
   config antispam settings
      set carrier-endpoint-acc-secret
   end
   ```
4. Enter the following command to configure whether to enable or disable the FortiMail unit to validate RADIUS requests using the RADIUS secret:
   ```
   config antispam settings
       set carrier-endpoint-acc-validate
   end
   ```
5. Enter the following command to configure whether or not the FortiMail unit will acknowledge accounting records:
   ```
   config antispam settings
      set carrier-endpoint-acc-response {enable | disable}
   end
   ```
6. Enter the following command to indicate that the RADIUS server will send the value of the *Framed-IP-Address* attribute in network order:
   ```
   config antispam settings
      set carrier-endpoint-framed-ip-order {host-order | network-order}
   end
   ```

Removing the Network Interfaces from the Bridge

To remove port2 and port3 from the bridge repeat the following steps for each individual port.

1. Go to **System > Network > Interface** in the advanced mode of the web interface.
2. Double-click on port2 to edit it.
3. Select *Do not associate with management IP.*
   The network interface will be removed from the bridge and may be configured with its own IP address.
4. In *IP/Netmask*, type the IP address and netmask of the network interface.
5. Disable all administrative access protocols, including *HTTPS, SSH, and PING.*
6. Select **UP** and then select **OK.**

Configuring the Session Profiles

To configure the session profile for connections from external SMTP clients

Note: For a more detailed look at configuration settings, see your FortiMail Administrator guide.

1. Navigate to **Profile > Session** in the advanced mode of the web interface.
2. Select **New.**
3. Type a name in the **Profile name** textbox (external_session_profile).
4. Enable **Hide this box from the mail server** in the **Connection Settings** section to preserve the IP address or domain name of the SMTP client.
5. Select the **Enable sender reputation** checkbox in the **Sender Reputation**
   Note: The rest of the settings under **Sender Reputation** can be left to their default value. For an explanation of each settings see the FortiMail Administrator guide (LINK).
6. Enable the block *STARTTLS*/MD5 commands in the **Session Settings** section so that email connections cannot be TLS-encrypted.
7. Enable **Prevent open relaying** in the **Unauthenticated Session Settings.**
8. Select **Create.**

You will need to repeat the same steps to configure the session profile for connections from internal SMT clients.

Configuring IP-Based Policies

To configure the IP-based policy for connections from internal SMTP clients.

1. Navigate to **Policy > Policies > IP Policies** in the advanced mode of the web interface.
2. Select **New.**
3. Type the IP address and netmask of your subscriber network in the **Source.**
4. **Se**lect internal_session_profile from the **Session** dropdown menu in the **Profiles.**
5. **S**elect the antispam profile from the **AntiSpam** dropdown menu.
6. **S**elect an antivirus profile from the **AntiVirus** dropdown menu.
7. Select **Create.**

To configure the IP-based policy for connection from external SMTP clients

1. Navigate to **Policy > Policies > IP Policies** in the advanced mode of the web interface.
2. Select **Edit** for the default policy whose *Match* column contains 0.0.0.0/0 –> 0.0.0.0/0
3. Select *external_session_profile* from Session.
4. Select **OK**.

Configuring the Outgoing Proxy

When operating in transparent mode, the FortiMail unit can use either transparent proxies or an implicit relay to inspect SMTP connections. If connection pick-up is enabled for connections on that network interface, the FortiMail unit can scan and process the connection. If not enabled, the FortiMail unit can either block or permit the connection to pass through unmodified. To configure outgoing proxy pick-up

To configure outgoing proxy pick-up

1. Navigate to **Mail Settings > Proxies** in the advanced mode of the web interface.
2. Enable *Use client-specified SMTP server to send email*.
3. Navigate to **System > Network.**
4. Edit SMTP proxy settings on both port 2 and port 3:
   Port 2 and 3
   Incoming connections: Drop
   Outgoing connections: Proxy
   Local connections: Disallow

To configure the IP-based policy for connections from internal SMTP clients.

1. Navigate to **Policy > Policies > IP Policies** in the advanced mode of the web interface.
2. Select **New.**
3. Type the IP address and netmask of your subscriber network in the **Source.**
4. **Se**lect internal_session_profile from the **Session** dropdown menu in the **Profiles.**
5. Select the antispam profile from the **AntiSpam** dropdown menu.
6. Select an antivirus profile from the **AntiVirus** dropdown menu.
7. Select **Create**.

To configure the IP-based policy for connection from external SMTP clients

1. Navigate to **Policy > Policies > IP Policies** in the advanced mode of the web interface.
2. Select **Edit** for the default policy whose *Match* column contains 0.0.0.0/0 –> 0.0.0.0/0
3. Select *external_session_profile* from Session.
4. Select **OK**.

Configuring Policy-based Routes on the Router

After you have configured the FortiMail settings, you must create policy routes on the router to redirect the SMTP traffic (from and to the subscribers) to the FortiMail unit for scanning.

For example, you use a FortiGate unit as the router/firewall, you can go to Router > Policy Route to create two routes: one for the external-to-subscribers SMTP traffic and one for the subscribers-to-external SMTP traffic.

For details, see the FortiGate Handbook on docs.fortinet.com.