Blocking the Email of a Known Threat in FortiMail

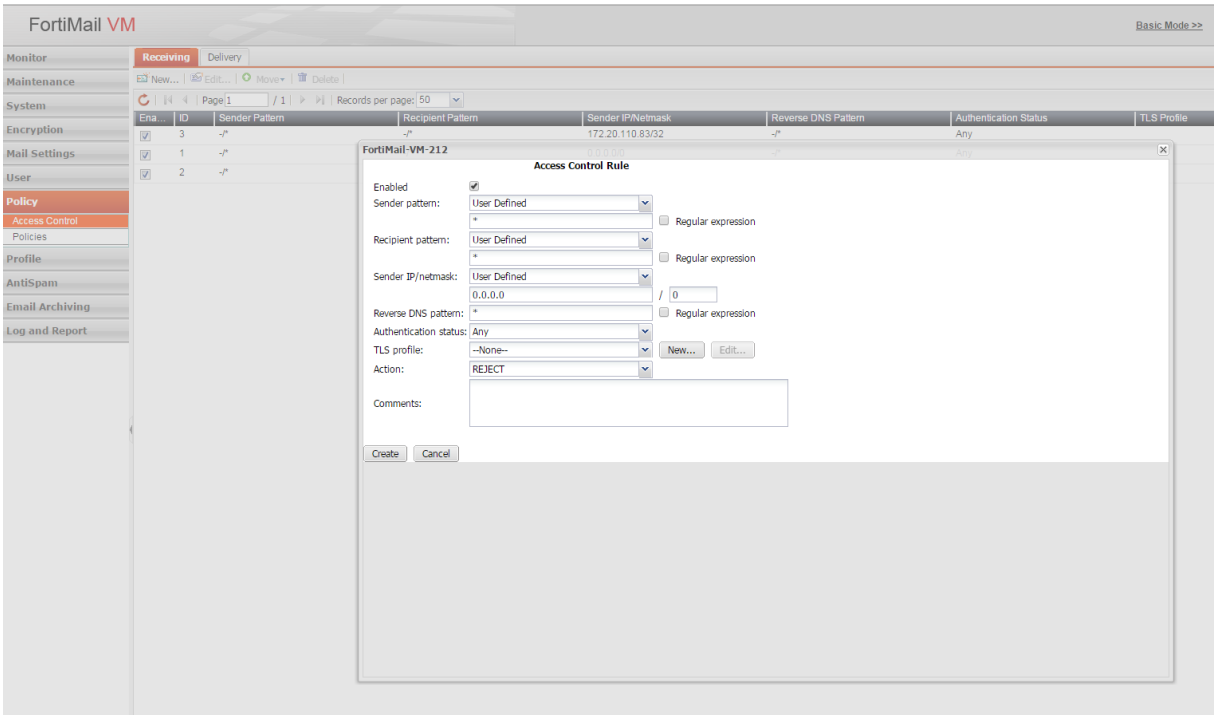
What if a user on your network has recently downloaded a virus onto their computer and they are now sending out emails that contain harmful malware to other people in the office? Until you solve the infection, you need a way to temporarily prevent the infected computer from sending out emails within the network.

Thankfully, FortiMail supports customizable access controls that can automatically reject emails from sources that you know to be infected.

Access control rules, or the access control list (ACL), controls how the FortiMail unit processes email messages. When an SMTP client attempts to deliver email through the FortiMail unit, the FortiMail unit compares each access control rule to the commands used by the SMTP client during the SMTP session. So, if you wanted to prevent a known infected source from sending you email you would set your FortiMail unit to reject emails from that source.

Configuring Access Controls

1. Navigate to **Policy > Access Control > Receiving.**
2. Select **New** to add an access control rule or double-click an existing access control rule to modify the rule.
3. Select the **Enabled** checkbox.



4. Select **User Defined** from the Sender pattern dropdown menu.
5. Enter the email address of the infected computer.

   Note: It might be better to block the machine's IP address instead of the user's email address.
6. Select **User Defined** from the Sender IP dropdown menu and then enter the user's IP address.

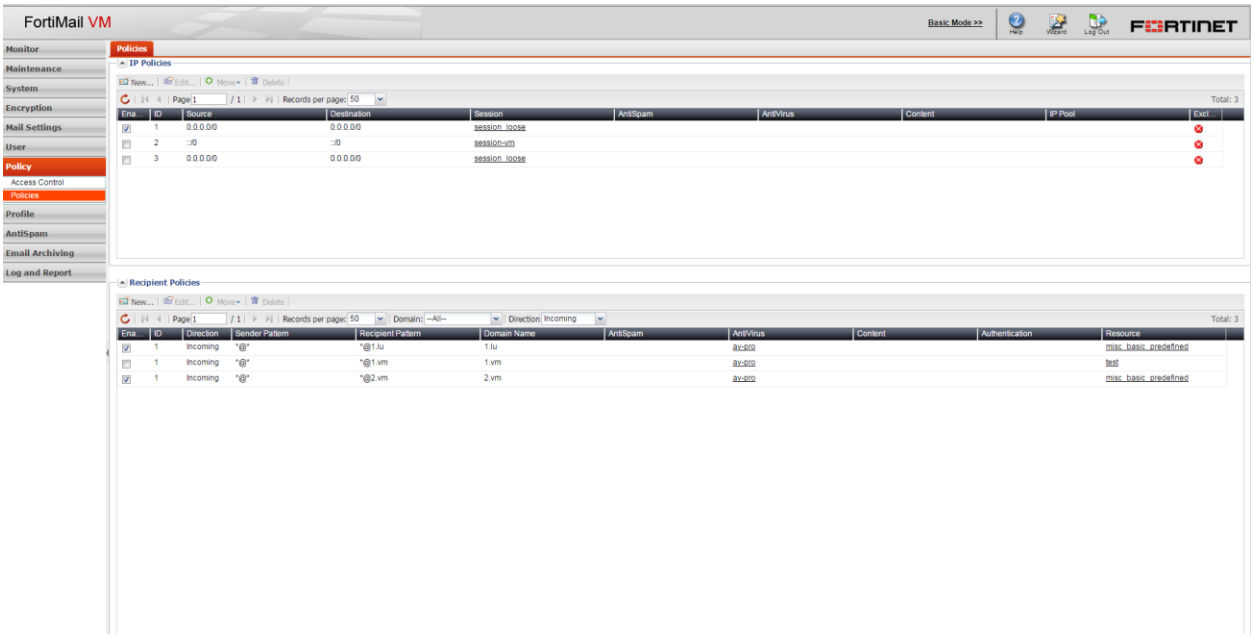
   Note: Blocking a person's IP address instead of their email address will allow them to send emails from their email address on a different machine that is not infected.
7. **S**elect **REJECT** from the **Action** dropdown menu.
8. Select the **Create** button.

Configuring Policies

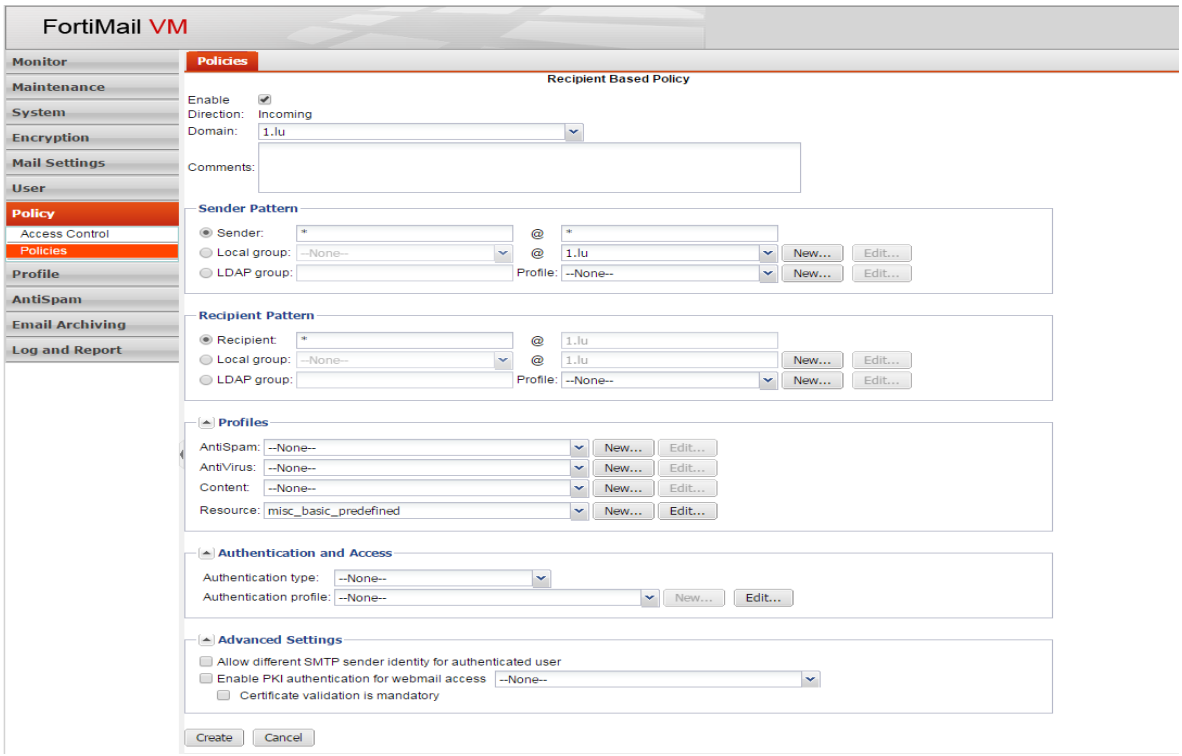
Since it is possible for an individual to intentionally send an infected email by changing the sender's email address, you must disable **Allow different SMTP sender identify for authenticated user** in the relevant recipient based policies.

These steps are not necessary if you have blocked the machine's IP address.

1. Navigate to **Policy > Policies > Recipient Policies.**



2. **S**elect the recently created policy.
3. Select the **Edit** button.
4. Uncheck the **allow different SMTP sender identify for authenticated user** checkbox under **Advanced Settings**.



5. Select **OK.**