How to Exclude or Include Blocked IP on Symantec?

Last Modified on 02/10/2022 11:44 am EST

How to Exclude or Include Blocked IP on Symantec?

Scenario: Customer states that the LNVR is offline, all exemption for folders were created, and the local IT wants proof from Lenel that something is being blocked.

The most likely reason, if all troubleshooting steps were tried, is that Symantec firewall or packets are being blocked, even when Symantec is disabled.

If deleting Symantec is not an option, then try this procedure to prove that Symantec is blocking traffic.

Procedure Steps

1. Open the Symantec client user interface.
2. Click on **Network and Host Exploit Mitigation**.
3. Select **Configure Firewall Rules**.
4. Click [Add].
5. On the General tab, select **Allow this rule**.
6. On the Hosts tab, enter the IP address.

You can try this procedure as well, if the user has admin rights or permission to do so:

- Check the security logs under **Client Management** for **Denial of Service Detections** for the communication server IP address to confirm the issue.

To resolve the issue, you must disable Denial of Service detection within your Intrusion Prevention policy, or you will need to add the communication server IP address in "Excluded Hosts."

To add the Communication Server to "Excluded Hosts":

1. Open your Intrusion Prevention Policy.
2. Choose the Settings on the left side.
3. Check the box for **Enable excluded hosts**, and then click [Excluded Hosts].
4. Add the IP address of your communication server, then click [OK].

For more information:

http://www.symantec.com/business/support

You can also try creating an exception for Intrusion Prevention Policy to allow a specific ID:

1. Open Symantec Endpoint Protection Manager console.
2. Select the **Policies** tab.
3. Under **View Policies**, select **Intrusion Prevention**.
4. Select **Intrusion Prevention policy**, then under **Tasks** select **Edit the Policy**.
5. Select the **Exceptions** tab.
6. Click [Add].
7. Search and select the blocked ID.
8. Click [Next].
9. Change **Action** from **Block** to **Allow**.
10. Click [OK].
11. Check if the edited exception has been added to the **Intrusion Prevention Exceptions** list.
12. Click [OK] to save changes in the Intrusion Prevention policy.

You can also Disable DoS detection:

1. Log into the Symantec Endpoint Protection Manager (SEPM).
2. Click **Policies**, then click **Intrusion Prevention**.
3. Edit the intrusion prevention policy that applies to the client.
4. Click **Settings**.
5. Uncheck **Enable denial of service detection**.

Once the policy is applied to the client, the DoS detections (and associated Active Response, if configured) should not occur.
Note: This will completely disable DoS detection on the client. There is not currently a way to add an exclusion for DoS detection.

You can also enable Smart Traffic filtering. For more information:
http://www.symantec.com/business/support

You can also uninstall the Network Threat Protection and Application and Device Control:

1. Go to Control Panel.
2. From **Add/Remove Programs**, select Symantec Endpoint Protection and click [Modify].
3. Disable the Network Threat Protection and Application and Device Control.

Applies To

Additional Information