Corporate KnowledgeBase

How to configure and use an ESSVM

Corporate KnowledgeBase ID: KB74844
Last Modified: April 16, 2012

Environment

McAfee Enterprise Security Manager
NitroSecurity ESM 9.x
NitroSecurity ESM 8.x

Summary

This KnowledgeBase article describes how to configure and use an ESSVM.

Solution

1. After the vmplayer installation completes, you are taken to the menu screen of the **ESSVM**. The main block of text shown in the menu describes the different functions available for configuration. The VM has an emulator which recreates the LCD screen that you would normally have access to on a physical NitroSecurity product.
2. The software's IP configuration will be done through this LCD emulator. To enter the LCD emulator menu, press the **ESC** key. Press the **Down Arrow** key and cycle through the menu functions. The IP configuration is done within the **MGT IP Conf** sub menu.
3. Press the ENTER key to open the **MGT IP Conf** menu, then enter the **IP Address** menu.
4. Use the **Left/Right arrow keys** to move left and right under the desired **octet** value. Then use the **Up/Down arrow keys** to increase or decrease the values.
5. When the correct **IP address** has been written, press Enter to return to the **Mgt1** screen. Press the **Down arrow** followed by Enter to configure the **netmask** in the same way used in step 4.
6. After configuring the **netmask** and returning to the **Mgt1** screen press the **Down arrow key** until **Done** is selected. Press Enter to return to the **MGT IP Conf** screen.
7. **Down arrow** to cycle through the **Gateway** and **DNS1** menus. Enter and configure each in the same way used in step 4. Configure **DNS2** if needed. The COMM port will already be set to **22**, no configuration is needed.
8. After configuring the **Gateway** and **DNS1** settings, **Down arrow** in the **MGT IP Conf** menu until you select **Save Changes**. Press the **Enter** key.
9. The VMPlayer now needs to be configured to use a **bridged network** setting, which means that any user on the network who knows the correct credentials will be able to access the NitroView GUI. Press Ctrl+Alt to exit the **ESS VM** menu and select the dropdown next to the ethernet button. Select **Bridged**.
10. The **ESS VM** will now need to be rebooted for the changes to take effect. After returning control to the ESS VM, press **Alt+F2** to arrive at the command prompt, as shown below.
11. Login as **root** with the following password: **w3e4r5t6**
12. After logging, in choose the **Reboot** option to restart the **ESS VM**.
13. When the ESS VM displays the main menu, you should be able to log in to the NitroView GUI via a web browser with the following address, where x.x.x.x is the address you specified in the IP settings: https://x.x.x.x/Application.html
14. After initialization, log in as **NGCP** with the following password: **security.4u**
15. You will be prompted to create a new password after logging in. We will now upgrade the system to the newest version, 8.4.1b.

16. First, **ssh** needs to be enabled to allow the ability to login to the ESM via ssh. Navigate to the **System Properties** button, shown by the red arrow. Click on **Network Settings**. Then enable **ssh**, click **Apply**.
17. Update the VM as necessary.
18. When the update process has completed and you are able to login to NitroView, confirm that the software has been updated. The current software version can be seen in the lower-left pane of the main NitroView screen.

IPS Configuration

1. Before adding the device in the NitroView console, you must first configure the **IP information** in the same way the ESS VM was configure in steps 1-12 of the previous section.
2. After the IP information has been correctly configured, open **NitroView**. In the **System Navigation Tree**, select the **system** or **group** to which you wish to add the device.
3. Click the **Add Device** icon in the **Actions** toolbar.
4. Select **NitroSecurity NitroGuard IPS** and click **Next**.
5. Enter a **name** that is unique in this group for the IPS device in the **Device Name** field and click **Next**. In FIPS mode, this dialog will only show the **Target IP Address** or **URL** and **Port** fields.
6. Enter a **target IP address** or **URL** in the **Target IP Address** or **URL** field.
7. Enter the **target SSH port number**. Ensure that it is valid to be used with the specified IP address. The default port is **22**.
8. Click **Next**.
9. If you have a **key** that you want to import, select **Import Key**. On the **File Upload** dialog, browse to and select the device key file, then click **Upload**.
10. If you don't have a key to import, click **Key Device**.
11. Enter a **password** for this device.
12. Click **OK**. The ESM will test device communication and report on the status of the connection. You will be able to directly launch the **Properties** and **Export Key** screens upon successfully keying the device.

Now that the device is keyed and is communicating securely, you can configure other settings. These settings can be configured by selecting the device in the **System Navigation Tree** and selecting the **Properties** icon in the **Actions Toolbar** or you can launch the **Properties** sections directly from the success screen that is displayed after you complete the add device process. Each option in the dialog's navigation pane is explained in detail. Note that disabled or hidden options indicate either insufficient privileges or the device does not support that function. Also, if the key for the device was imported, there may be insufficient privileges due to specific privileges associated with the imported key.

Related Information

NitroSecurity ID: 15094-217