Aim:

IP Security (IPsec) Configuration:
Configure IPsec on network devices to provide secure communication and protect against unauthorized access and attacks.

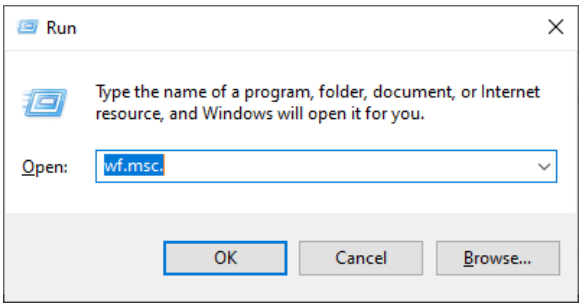
Configure Internet Protocol Security (IPSEC)

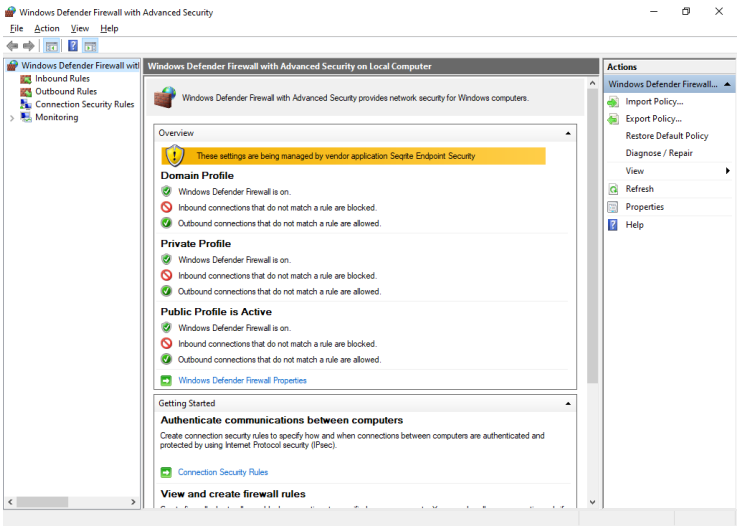
About this task
Historian supports encryption based on Internet Protocol Security to secure traffic between various Historian components and collectors without the need to use VPN or other security protocols.

Procedure

1. Run `wf.msc`.

   The **Windows Defender Firewall with Advanced Security** window appears.

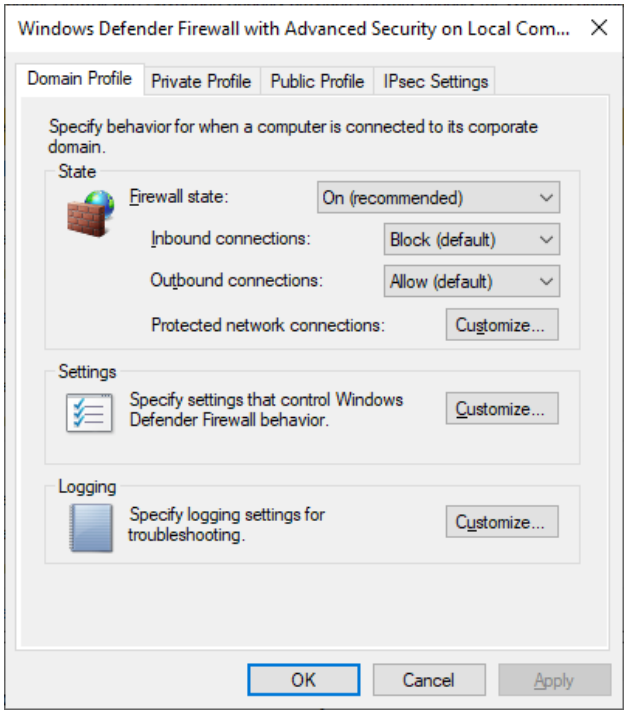




2. Create a security method:

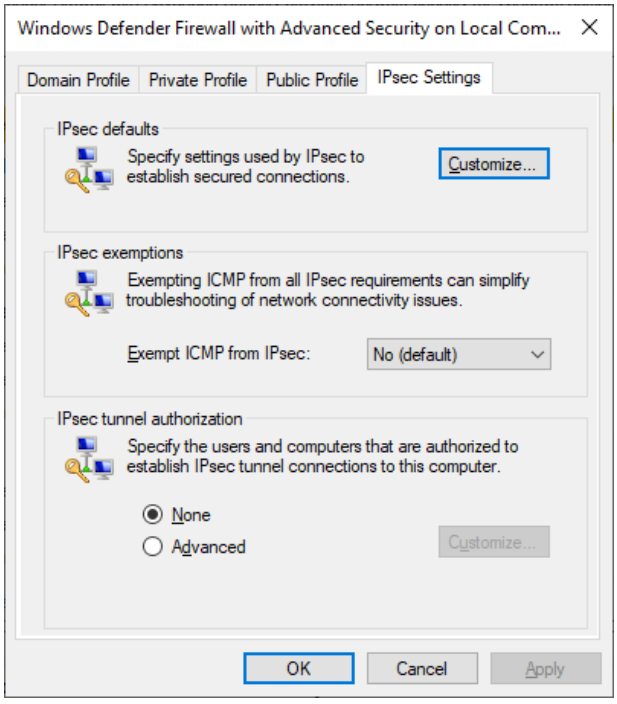
   a. Select **Actions** > **Properties**.

      The **Windows Defender Firewall with Advanced Security on Local Computer** window appears.



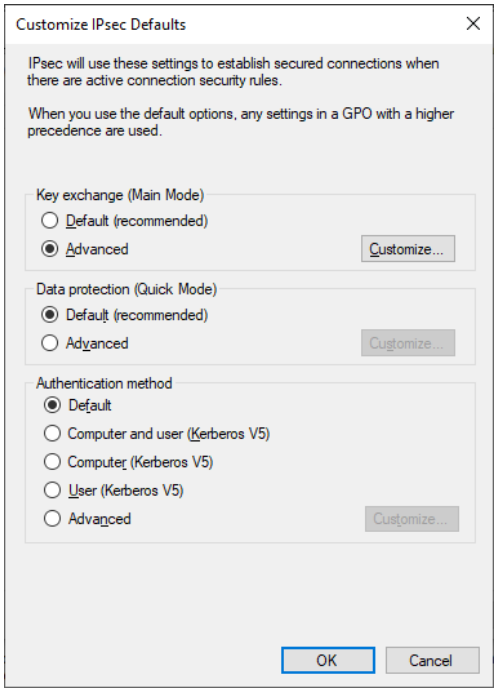
b. Select **IPsec Settings** > **Customize**.

The **IPsec Defaults** window appears.



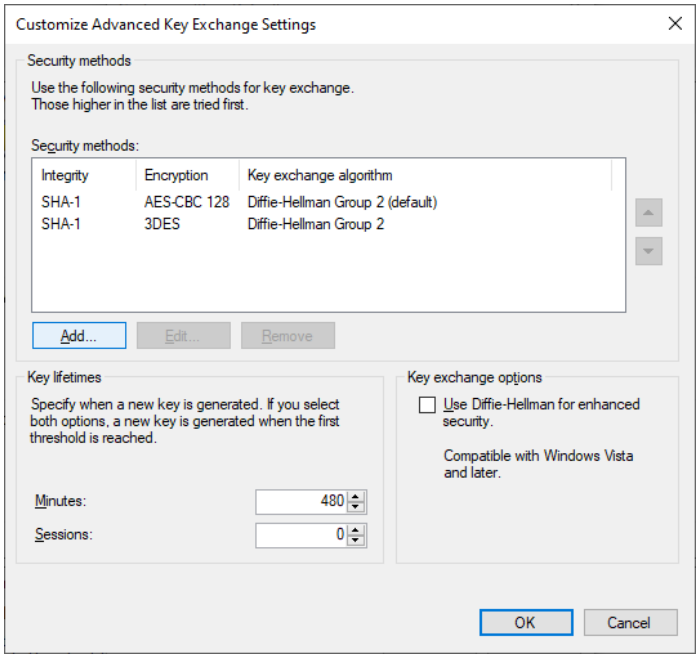
c. Under **Key exchange (Main Mode)**, select **Advanced** > **Customize**.

The **Customize Advanced Key Exchange Settings** window appears.

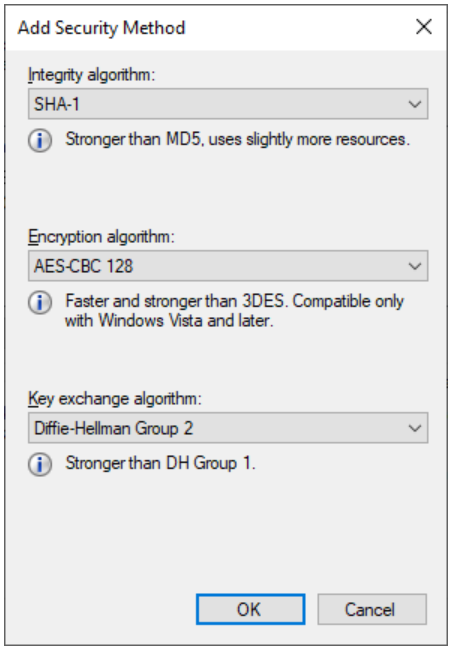


d. Select **Add**.

The **Add Security Method** window appears.



e. Select the algorithms that you want to use for each purpose. The following image shows an example.



Important: You must provide the same values for all the machines for which you want to configure IP security.

The security method that you have added appears in the list.

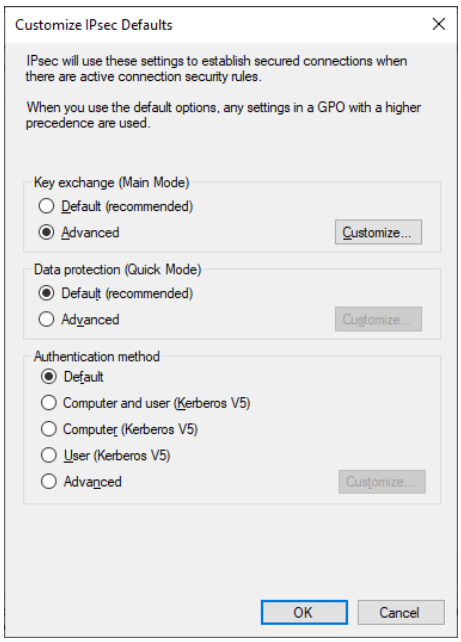
f. Move the security method that you have added to the top of the list. We recommend that you remove the other methods.

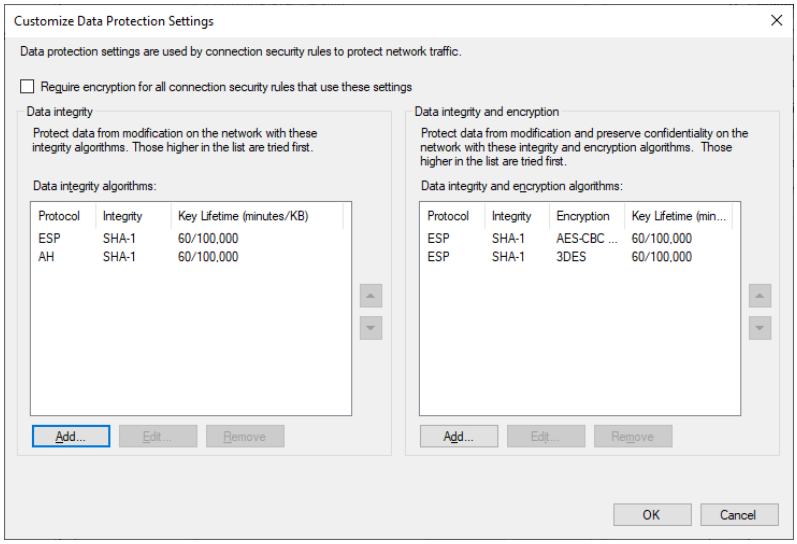
g. Select **OK**.

3. Add integrity and encryption algorithms:

a. In the **Customize IPsec Defaults** window, under **Data protection (Quick Mode)**, select **Advanced** > **Customize**.

The **Customize Data Protection Settings** window appears.

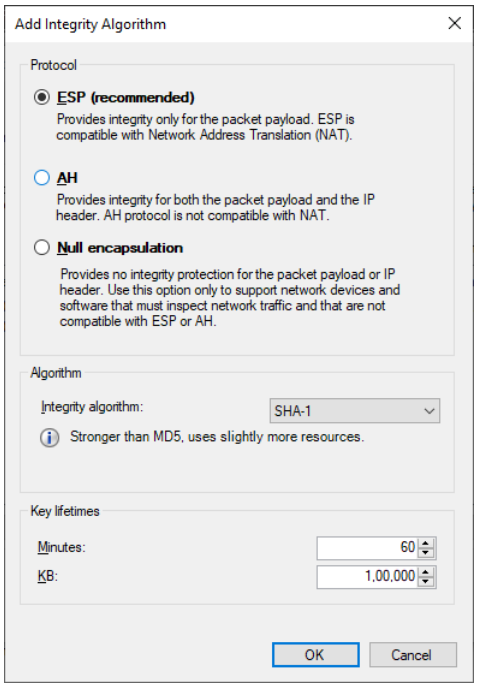




b. Select the **Require encryption for all connection and security rules that use these settings** check box.

c. Under **Data integrity and encryption**, select **Add**.

The **Add Integrity and Encryption Algorithms** window appears.



d. Under **Protocol**, ensure that **ESP** is selected.

e. Select the algorithms that you want to use for each purpose, and then select **OK**.

The algorithms that you have selected appear in the list.

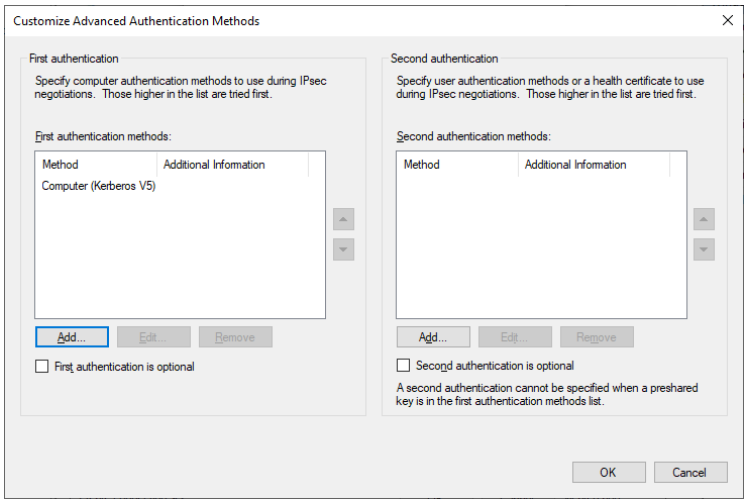
f. Move the algorithms to the top of the list. We recommend that you remove the remaining items in the list.

g. Select **OK**.

4. Create a first authentication method:

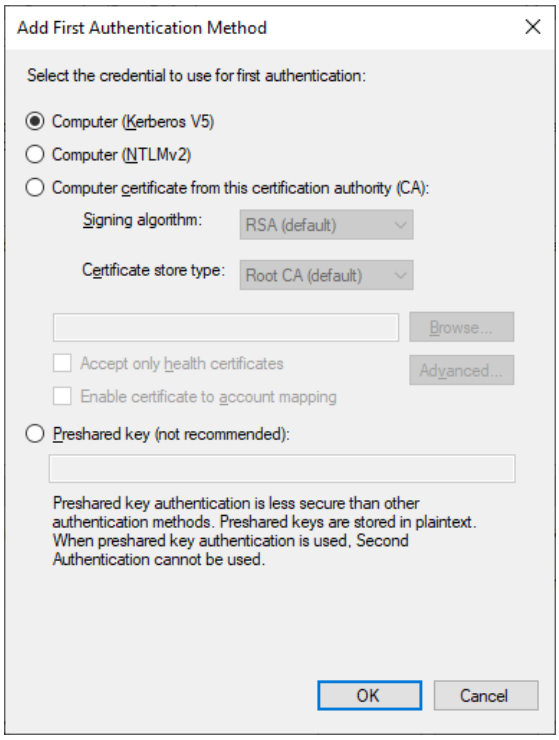
   a. In the **Customize IPsec Defaults** window, under **Authentication Method**, select **Advanced** > **Customize**.

   The **Customize Advanced Authentication Methods** window appears.



   b. Under **First authentication methods**, select **Add**.

   The **Add First Authentication Method** window appears.



   c. Provide the CA certificate that you want to use, and then select **OK**.

   d. The certificate that you have provided appears in the list.

e. Move the certificate to the top of the list. We recommend that you remove the remaining items in the list.

f. Select **OK**.

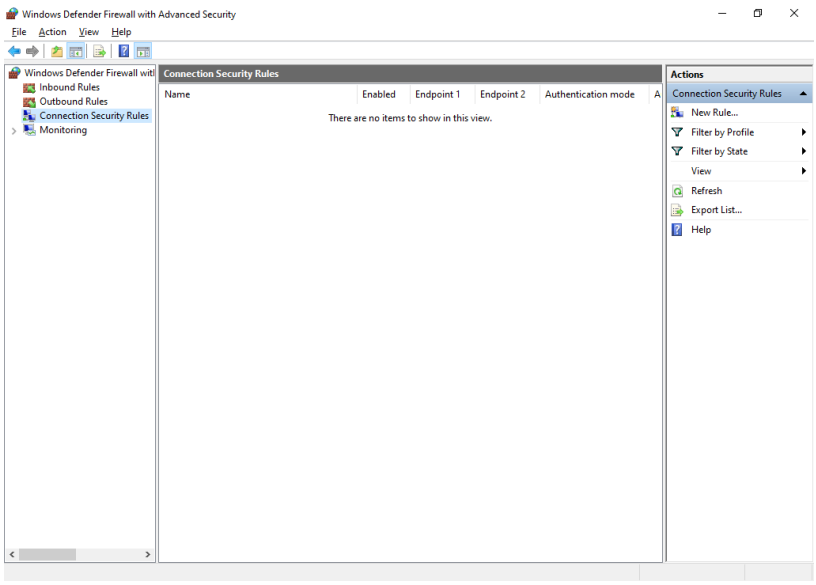
5. Create a connection security rule:

For Windows x86, run the following set of commands to create a rule:

```
netsh  advfirewall consec add rule name=""<rule name>""
endpoint1=any endpoint2=any protocol=tcp port1=any port2=2010
action=requestinrequestout
```

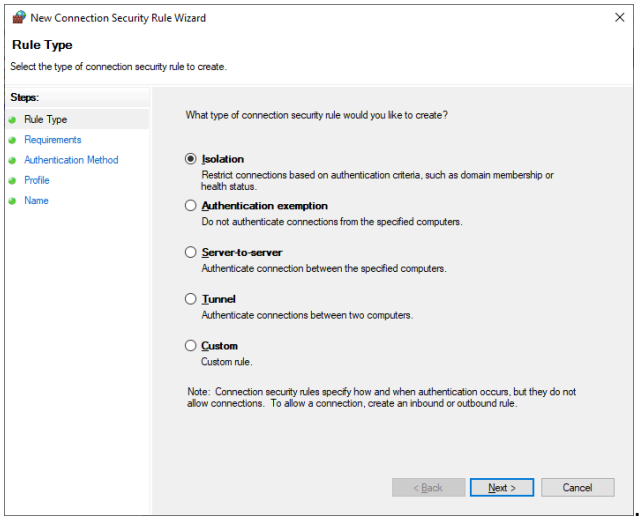
For other versions, perform the following steps:

a. In the **Windows Defender Firewall with Advanced Security** window, select **Connection Security Rules**.



b. Select **Actions** > **New Rule**.

The **New Connection Security Rule Wizard** window appears



c. Select **Custom**, and then select **Next**.

d. Both for Endpoint 1 and Endpoint 2, select **Any IP Address**, and then select **Next**.

e. Select **Require authentication for inbound and outbound connections**, and then select **Next**.

f. Select **Default**, and then select **Next**.

g. Enter values as described in the following table, and then select **Next**.

Field	Description
Protocol type	Select **TCP**.
Endpoint 1 port	Select **All Ports**.
Endpoint 2 port	Select **Specific Ports**, and then enter 2010.

h. Select when to apply the rule, and then select **Next**.

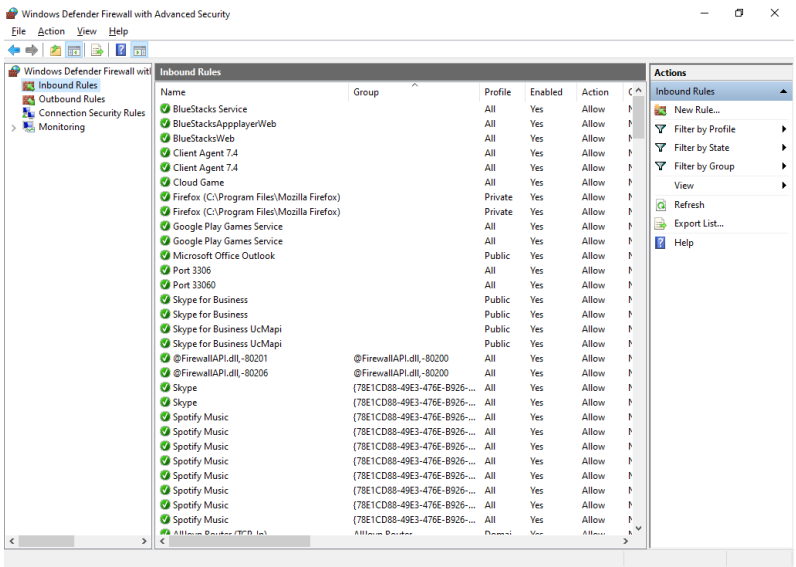
i. Enter a name and description for the rule, and then select **Finish**.

The rule appears in the **Connection Security Rules** window.

j. Ensure that the rule is enabled.

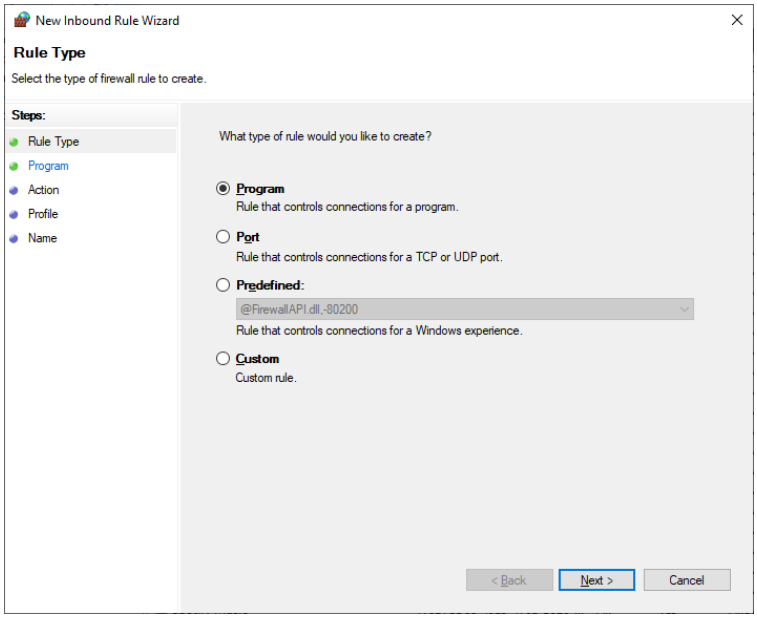
6. If using Microsoft Windows Server 2019, 2016, 2012 R2 and/or Windows 8, 8.1, open up port number 5000:

a. In the **Windows Defender Firewall with Advanced Security** window, select **Inbound Rules**.



b. Select **Actions** > **New Rule**.

The **New Inbound Rule Wizard** window appears.



c. Select **Custom**, and then select **Next**.

d. Select **All programs**, and then select **Next**.

e. Enter values as described in the following table, and then select **Next**.

Field	Description
Protocol type	Select **UDP**.
Protocol number	Leave the default value as is.
Local port	Select **Specific Ports**, and then enter 5000.
Remote port	Leave the default value as is.

f. Both for the local and remote IP addresses, set the scope to **Any IP address**, and then select **Next**.

g. Select **Allow the connection**, and then select **Next**.

h. Select when to apply the rule, and then select **Next**.

i. Enter a name and description for the rule, and then select **Finish**.

The rule appears in the **Inbound Rules** window.

j. Ensure that the rule is enabled.

IPSEC is now configured on the machine.

7. Repeat all the steps above on all the machines that host the Historian server and/or its components/clients.
8. To verify that the IPSEC cryptography is used:

a. Ensure that the Historian server is running.

b. Ensure that the collectors are connected to the Historian server, and that the collectors are running.

c. Specify the tags for data collection. You can do so using Configuration Hub or Historian Administrator.

d. Verify that the collector is collected data.

e. On each machine on which you configured IPSEC, run `wf.msc`.

The **Windows Defender Firewall with Advanced Security** window appears.

f. Select **Monitoring** > **Security Associations** > **Main Mode**.

The **Main Mode** section displays the connection that you have created.