Configuring WPA-Enterprise/WPA2 with Microsoft RADIUS Authentication

This document describes how to configure WPA-Enterprise and WPA2 security protocols with RADIUS authentication for Check Point Embedded NGX gateways.

Note: Embedded NGX gateways include both Safe@Office and VPN-1 Edge UTM gateways. The Embedded NGX screens that appear in this document relate to VPN-1 Edge UTM gateways.

Note: This document assumes the reader is familiar with the basic concepts of working with Microsoft Management Console, Microsoft Active Directory, and RADIUS Internet Authentication Service (IAS). The document also assumes the reader is familiar with certificate authentication, in case this kind of configuration is desired.

Introduction

The Embedded NGX appliance supports the WPA-Enterprise (Wi-Fi Protected Access) security protocol for authentication of wireless clients. WPA-Enterprise uses MIC (message integrity check) to ensure the integrity of messages, and TKIP (Temporal Key Integrity Protocol) to enhance data encryption. Furthermore, it uses 802.1x and EAP authentication, based on a central Remote Authentication Dial-In User Service (RADIUS) authentication server.

When using the WPA-Enterprise security method, the Embedded NGX appliance enables you to restrict access to the wireless network to wireless stations that support the WPA2 security method. The WPA2 security method uses the more secure Advanced Encryption Standard (AES) cipher, instead of the RC4 cipher used by WPA.

Both WPA-Enterprise and WPA2 require configuring a RADIUS server.

Note: If WPA2 is not configured, the Embedded NGX appliance allows clients to connect using both WPA and WPA2.

System Requirements

The RADIUS server machine must meet the requirements listed below:

- Microsoft Windows 2000 Server / Microsoft Windows 2003 Server
- Microsoft Active Directory
- Certification Authority (installed as Enterprise root CA)
- IIS
- RADIUS Internet Authentication Service (IAS)
Overview of WPA-Enterprise/WPA2 with RADIUS Authentication Configuration

To configure WPA/WPA2 with RADIUS authentication

1. Configure the RADIUS server machine as follows:
   a. Create the certificate authority.
      See “Creating the Certificate Authority,” page 3.
   b. Create a certificate for use with the RADIUS server.
   c. Create a RADIUS client for the Embedded NGX appliance.
      See “Creating a RADIUS Client,” page 8.
   d. Create a Remote Access policy.
   e. Configure the user that should be used for authenticating wireless clients that connect to the Embedded NGX appliance using WPA/WPA2.
      See “Configuring the User in Active Directory,” page 19.

2. Configure the Embedded NGX appliance as follows:
   a. Prepare the appliance for a wireless connection.
      For instructions, refer to the User Guide.
   b. Configure the RADIUS server.
      See “Configuring the RADIUS Server,” page 20.
   c. Configure the wireless network to use the WPA/WPA2 Enterprise security protocol.

3. Configure each wireless client as follows:
   a. Download a certificate from the RADIUS server.
      See “Downloading a Certificate from the RADIUS Server,” page 22.
   b. If the Embedded NGX appliance was configured for WPA2, enable WPA2.
      See “Enabling WPA2 Support on the RADIUS Client,” page 22.
   c. Connect the client to the network.
      See “Connecting to the Network Using Wireless RADIUS Authentication,” page 22.
Configuring the Server

Creating the Certificate Authority

To create the CA

1. Open the Microsoft Management Console.
   The Microsoft Management Console opens.

2. From the Console menu, choose Add/Remove Snap-in.
The Add/Remove Snap-in dialog box opens displaying the Standalone tab.

3. Click **Add**.

The Add Standalone Snap-in dialog box appears.

4. Select **Certificates**.

5. Click **Add**.
A wizard opens displaying the **Certificates snap-in** dialog box.

6. Click **Computer account**.
7. Click **Next**.
   
The **Select Computer** dialog box appears.

8. Click **Local computer**.
9. Click **Finish**.
10. Click **Close**.
11. Click **OK**.
Creating a Certificate

To create a certificate

1. In the Microsoft Management Console tree, click **Certificates > Personal**.
2. Right-click in the right-pane, and click **All Tasks > Request New Certificate** in the popup menu.

![Microsoft Management Console](image)

The **Certificate Request Wizard** opens displaying the **Welcome** screen.

![Certificate Request Wizard Welcome](image)

3. Click **Next**.

The **Certificate Types** dialog box appears.

![Certificate Request Wizard Types](image)
4. Select **Domain Controller**.

5. Click **Next**.

   The **Certificate Friendly Name and Description** dialog box appears.

6. In the **Friendly name** field, type a friendly name for the new certificate.

7. In the **Description** field, type a description for the new certificate.

8. Click **Next**.

   The **Completing the Certificate Request Wizard** screen appears.

9. Click **Finish**.

   A certificate is created. This certificate will be used with the RADIUS server.
Creating a RADIUS Client

To create a RADIUS client

1. Open the RADIUS Internet Authentication Service (IAS).
2. In the tree, right-click **Radius Clients**, and click **New RADIUS Client** in the popup menu.

The **New RADIUS Client** wizard opens displaying the **Name and Address** dialog box.

3. In the **Friendly name** field, type a friendly name for the RADIUS client.
4. In the **Client address (IP or DNS)** field, type the IP address of the RADIUS client.
5. Click **Next**.
The **Additional Information** dialog box appears.

6. In the **Shared secret** and **Confirm shared secret** fields, type the shared secret to use for secure communication with the RADIUS server.

7. Click **Finish**.

The RADIUS client is added.

**Creating a Remote Access Policy**

**To create a Remote Access policy**

The Add Remote Access Policy Wizard opens displaying the Welcome screen.

2. Click Next.

The Policy Configuration Method Dialog box appears.

3. Click Set up a custom policy.

4. In the Policy name field, type a name for the policy.

5. Click Next.
The Policy Conditions dialog box appears.

6. Click **Add**.

The Select Attribute dialog box appears.

7. Select **NAS-Port-Type**.

8. Click **Add**.

The NAS-Port-Type dialog box appears.

9. In the **Available types** list, select **Wireless - IEEE 802.11**.
10. Click Add.
   The selected NAS port type moves to the Selected types list.

11. Click OK.
   The Policy Conditions Dialog box re-appears listing the specified policy conditions.

12. Click Add.
   The Select Attributes dialog box appears.

14. For each Windows group you want to add, do the following:

a. Click **Add**.
   
   The **Groups** dialog box appears.

b. Click **Add**.
   
   The **Select Groups** dialog box appears.

c. In the text box, type the desired object names for RADIUS authentication.

d. Click **OK**.
   
   The **Groups** dialog box reappears displaying the selected group.
15. Click **OK**.

The Policy Conditions dialog box reappears displaying the conditions you created.

16. Click **Next**.

The **Permissions** dialog box appears.

17. Click **Grant remote access permission**.
18. Click Next.

The Profile dialog box appears.

![Profile dialog box]

19. Click Edit Profile.

The Edit Dial-in Profile dialog box appears.

Note: You can leave the fields in the Multilink, IP, and Advanced tabs at their default settings, unless specific values are needed.

20. Click the Dial-in Constraints tab.

The Dial-in Constraints tab appears.

![Dial-in Constraints tab]

21. Make sure that the check boxes are all cleared.
22. Click the **Encryption** tab.

The **Encryption** tab appears.

![Encryption Tab](image)

23. Select the desired check boxes.

The recommended encryption level is **Strong encryption (MPPE 128 bit)**.

![Encryption Options](image)

Note: If desired, you can select the **No Encryption** check box, verify that your wireless network works, and then go back and clear this check box.

24. Click the **Authentication** tab.

The **Authentication** tab appears.

![Authentication Tab](image)

25. Clear all the check boxes.
26. Click EAP Methods.

The Select EAP Providers dialog box appears.

27. Click Add.

The Add EAP dialog box appears.

28. Do one of the following:
   - To use a secure password for authentication, select Protected EAP (PEAP).
   - To use certificate authentication, select Smart Card or other certificate.

29. Click OK.

The Select EAP Providers dialog box reappears displaying the EAP method you selected.
30. Click **Edit**.

The **Protected EAP Properties** dialog box appear.

31. In the **Certificate issued** drop-down list, select the certificate you created in step “Creating a Certificate,” page 6.
32. Click **OK**.

The **Select EAP Providers** dialog box reappears.
33. Click **OK**.

The **Edit Dial in Profile** dialog box reappears.
34. Click **OK**.

The **Profile** dialog box reappears.
35. Click **Next**.

The **Completing the New Remote Access Policy Wizard** screen appears.

36. Click **Finish**.
Configuring the User in Active Directory

To configure the user in Active Directory

1. Open Active Directory.

2. Double-click on the user that should be used for authenticating wireless clients that connect to the Embedded NGX appliance using WPA/WPA2.

The Properties dialog box appears.

3. Click the Dial-in tab.

The Dial-in tab appears.

4. In the Remote Access Permission area, click Allow access.

5. Click OK.
Configuring the Embedded NGX Appliance

Configuring the RADIUS Server

To configure the RADIUS server

1. Click **Users** in the main menu, and click the **RADIUS** tab.

   The RADIUS page appears.

2. Configure the primary RADIUS server as follows:
   a. In the **Address** field, type the RADIUS server's IP address.
   b. In the **Port** field, type the port number on the RADIUS server’s host computer.
   c. In the **Shared Secret** field, type the shared secret to use for secure communication with the RADIUS server.
     This is the shared secret you configured in “Creating a RADIUS Client,” page 8.
   d. In the **Realm** field, type the realm to append to RADIUS requests.
     The realm will be appended to the username as follows: `<username>@<realm>`.
     This field is only relevant if the organization uses RADIUS realms.
   e. In the **Timeout** field, type the interval of time in seconds between attempts to communicate with the RADIUS server.

3. Click **Apply**.
Configuring WPA/WPA2 Security Protocol

To configure WPA/WPA2 security

1. Click **Network** in the main menu, and click the **My Network** tab.

   The **My Network** page appears.

2. In the desired wireless network's row, click **Edit**.

   The **Edit Network Settings** page appears.
3. In the **Mode** drop-down list, select **Enabled**.
   The fields are enabled.

4. In the **Security** drop-down list, select **WPA-Enterprise**.
   This enables the WPA security protocol.

5. To enable WPA2, in the **Require WPA2 (802.11i)** drop-down list, select **Enabled**.
   If WPA2 is enabled, then only wireless stations using WPA2 can access the WLAN network. If WPA2 is not enabled, then wireless stations using either WPA or WPA2 can access the WLAN network.

6. Complete the rest of the fields as desired.
   For information, refer to the User Guide.

7. Click **Apply**.

**Configuring Wireless Clients**

**Downloading a Certificate from the RADIUS Server**

You can configure a certificate on the wireless client in various ways. For information on the possible certificate configuration methods and the recommended implementation, see:

http://www.microsoft.com/technet/prodtechnol/winxppro/deploy/ed80211.mspx

**Enabling WPA2 Support on the RADIUS Client**

To enable WPA2 support on the default Windows wireless client, you can use the patch found on I:\Drivers\Windows WPA2 Patch. Alternatively, you can also use the Atheros client version 4.0 at I:\Drivers\Atheros WLAN 4.0.

**Connecting to the Network Using Wireless RADIUS Authentication**

To connect to the network using wireless RADIUS authentication

1. In the START menu, click **Control Panel**.

2. Click **Network Connections**.

3. Double-click on the wireless network connection.

4. Do one of the following:
   - If the **Choose a Wireless Network** screen appears, click **Change Advanced Settings**.
   - If you are already connected to a wireless network, click **Properties**.

The **Wireless Network Connection Properties** dialog box appears displaying the **General** tab.
5. Click the **Wireless Networks** tab.

The **Wireless Networks** tab appears.

![Wireless Networks tab](image)

6. Click **Add** and add your network.

The **Wireless network properties** dialog box appears.

![Wireless network properties](image)

7. In the **Network name (SSID)** field, type the network name.

8. In the **Network Authentication** drop-down list, select **WPA** or **WPA2**.

9. In the **Data encryption** drop-down list, select **AES**.
10. Click the **Authentication** tab.

The **Authentication** tab appears.

![Wireless network properties dialog box]

11. In the **EAP type** drop-down list, do one of the following:
   - To use a protected password for authentication, select **Protected EAP (PEAP)**.
   - To use certificate authentication, select **Smart Card or other certificate**.

12. If you chose to use a protected password, do the following:
   a. Click **Properties**.
      
      The **Protected EAP Properties** dialog box appears.

      ![Protected EAP Properties dialog box]

      b. In the **Select Authentication Method** drop-down list, select **Secured password (EAP-MSCHAP v2)**.
c. Click **Configure**.

The **EAP MSCHAP Properties** dialog box appears.

![EAP MSCHAPv2 Properties dialog box]

d. Do one of the following:

- To use your Windows logon name and password when connecting, select the check box.
- To use a different logon name and password when connecting, clear the check box.

e. Click **OK**.

The **Protected EAP Properties** dialog box reappears.

f. Click **OK**.

The **Wireless network properties** dialog box reappears.

13. Click **OK**.

The **Wireless Network Connection Properties** dialog box reappears.

14. Click **OK**.

The list of wireless networks reappears.

15. Select the wireless network to which you want to connect.

16. Click **Connect**.

A popup message appears asking you to supply credentials.

![Wireless Network Connection pop up message]

17. Click on the popup message.

One of the following things happens:

- If secure password authentication is configured, the **Enter Credentials** dialog box appears.
Type your RADIUS user name and password in the fields provided.

- If certificate authentication is configured, the **Connect** window appears.

![Connect Wireless Network Connection](image)

In the drop-down list, select the desired certificate.

18. Click **OK**.

The wireless client attempts to connect to the network.

![Choose a wireless network](image)
Upon successful connection, the client indicates that it is connected to the network.