How do I configure my Firebox to authenticate users against my existing RADIUS authentication server?

Introduction

When you use Fireware's user authentication feature, you can see the user name and IP address of each Firebox connection. You can also configure policies that allow access only to authenticated users. This can be very helpful if you want to track employee Internet usage and limit the users that can access certain resources.

With Fireware, you can set up an authentication server on the Firebox itself, or you can use your existing authentication server. Fireware supports these four types of authentication server:

- Generic LDAP (Lightweight Directory Access Protocol)
- Active Directory
- RADIUS
- SecurID

To use the Firebox with a third-party authentication server, you must configure the Firebox to send authentication requests to your existing server. This document tells you how to configure your Firebox to authenticate users against an existing RADIUS (Remote Authentication Dial-In User Service) server.

There are three types of authentication a user can do:

1. A user tries to authenticate using the Firebox's built-in web server so that the user can access some network resource. The user makes a browser-based HTTPS connection to the Firebox over port 4100.
2. A remote user tries to make a PPTP VPN connection.
3. A remote user tries to make an IPSec VPN connection with WatchGuard’s MUVPN software.

Is there anything I need to know before I start?

Before you configure the Firebox to use your RADIUS authentication server, make sure that the server can successfully accept and process RADIUS authentication requests.

You must know your:

- **RADIUS server IP address and Port**
  - If you have a backup RADIUS server, you must know its IP address and the port it uses for RADIUS.

- **Shared Secret**
  - The shared secret is a password that is case-sensitive. It must be the same on the Firebox and the RADIUS server.

- **Authentication Methods**
  - Your RADIUS server must allow the authentication method the Firebox uses: PAP or MS CHAP v2.
  - To learn which method Fireware uses for each of the three types of RADIUS authentication, see “What authentication methods does the Firebox use for RADIUS?,” on page 5.

How does RADIUS work?

RADIUS is a protocol that was originally designed for authenticating remote users to a dial-in access server. RADIUS is now used in a wide range of authentication scenarios. RADIUS is a client–server protocol, with the Firebox as the client and the RADIUS server as the server. (The RADIUS client is sometimes called the Network Access Server or NAS.)

When a user tries to authenticate, the Firebox sends a message to the RADIUS server. If the RADIUS server is properly configured to have the Firebox as a client, RADIUS sends an “accept” or “reject” message back to the Firebox (the Firebox is the Network Access Server).
When the Firebox uses RADIUS for an authentication attempt, these things happen:

1. The user tries to authenticate with one of the three methods shown in the Introduction. The Firebox reads the user’s name and password.

2. The Firebox creates a message called an Access-Request message and sends it to the RADIUS server. The Firebox uses the RADIUS shared secret in the message. The user’s password is always encrypted in the Access-Request message.

3. The RADIUS server makes sure that the Access-Request message is from a known client (the Firebox). If RADIUS is not configured with the Firebox as a client, RADIUS discards the Access-Request message and does not send a message back.

4. If the Firebox is a client known to the RADIUS server and the shared secret is correct, RADIUS looks at the authentication method requested in the Access-Request message.

5. If the Access-Request message uses an allowed authentication method, RADIUS gets the user’s credentials from the message and looks for a match in a user database. If the user name and password match an entry in the database, the RADIUS server can get additional information about the user from the user database (such as remote access approval, group membership, logon hours, and so on).

6. RADIUS checks to see if it has an access policy or a profile in its configuration that matches all the information it knows about the user. If such a policy exists, RADIUS sends a response.

7. If any of the previous conditions fail, or if the RADIUS server has no matching policy, RADIUS sends an Access-Reject message that shows authentication failure. The RADIUS transaction ends and the user is denied access.

8. If the Access-Request message meets all the previous conditions, RADIUS sends an Access-Accept message to the Firebox.

9. RADIUS uses the shared secret for any response it sends. If the shared secret does not match between the RADIUS server and the Firebox, Fireware rejects any response from RADIUS. To learn more about what log messages you see when the shared secret does not match, see “How do I see diagnostic messages for authentication?,” on page 6.

10. The Firebox reads the value of any Filter-Id attribute in the message. It connects the user name with the Filter-Id attribute to put the user in a RADIUS Group.

RADIUS can put a large amount of additional information in the Access-Accept message, but the Firebox ignores most of it. Additional information can include the protocols the user is allowed to use (PPP, SLIP, etc.), the ports the user can access, idle time-outs, and other attributes that the Firebox ignores. The only attribute the Firebox looks for in the Access-Accept message is the Filter-Id attribute (RADIUS attribute number 11). The Filter-Id is a string of text that you configure RADIUS to include in the Access-Accept message. The Filter-Id attribute is necessary for the Firebox to assign the user to a RADIUS Group. See the next section about RADIUS Groups.

About Groups when you use RADIUS

When you configure RADIUS authentication in Fireware Policy Manager you can set the Group Attribute number. Fireware reads the Group Attribute number from Policy Manager to tell which RADIUS attribute carries RADIUS Group information. Fireware recognizes only RADIUS attribute number 11, Filter-Id, as the Group Attribute. In the steps to configure the RADIUS server, do not change the Group Attribute number from its default value of 11.

When the Firebox gets the Access-Accept message from RADIUS, it reads the value of the Filter-Id attribute and uses this value to associate the user to a RADIUS Group. (You must manually configure the Filter-Id in your RADIUS configuration.) Thus, the value of the Filter-Id attribute is the name of the RADIUS Group the Firebox puts the user in. The RADIUS Groups you use in the Policy Manager are not the same as the Windows groups defined in your domain controller, or any other groups that exist in your domain’s user database. A RADIUS Group is only a logical grouping of users the Firebox uses. Give consideration to the string of text you use for the Filter-Id. If you like, you can make the value of the Filter-Id match the name of a local group or domain group in your organization but it is not necessary. We suggest using a descriptive name that helps you remember the reason for grouping users this way.

Practical use of RADIUS Groups

If your organization has many users to authenticate, you can make your Firebox policies easier to administer by configuring RADIUS to send the same Filter-Id value for many users. The Firebox puts those users into one logical group so you can more easily administer user access. When you make a policy in Policy Manager that allows only authenticated users to access a network resource, you use the RADIUS Group name instead of adding a list of many individual users. For example, if the Filter-Id string RADIUS sends when Mary authenticates is “Sales”, that is the name of the RADIUS Group the Firebox puts Mary in for as long as Mary is authenticated. If users John and Alice subsequently authenticate,
Configure the Firebox to use the RADIUS server

1. From your Fireware Policy Manager, select **Setup > Authentication Servers**.

2. From the **RADIUS** tab, select the **Enable RADIUS Server** check box.

3. In the **IP Address** text box, type the IP address of the primary RADIUS server for the Firebox to contact with authentication requests.

4. From the **Port** drop-down list, select the UDP port number for the Firebox to use to send RADIUS requests. The default port number is UDP port 1812. Older RADIUS servers may use UDP port 1645.

5. Type and confirm the RADIUS **Secret**.
To set the time-out value, use the **Timeout** value control to set the value you want. This sets how long the Firebox waits for a response from the authentication server before it tries again.

To set how many connection attempts the Firebox makes, use the **Retry** value control to set the number you want. This is the number of times the Firebox tries to connect to the authentication server (using the time-out specified above) before it reports a failed connection for one authentication attempt.

Do not change the **Group Attribute** default value.

Add information for a backup RADIUS server, if you have one.

Click **OK**. Save your changes to the Firebox with Policy Manager > File > Save > To Firebox.

**Frequently asked questions about this procedure**

**How do the Timeout and Retry values work? (When does Fireware switch to the Backup RADIUS Server?)**

Fireware starts to use the backup server after three authentication attempts fail because of “no response”. (Note that this number is not the same as the **Retry** number. You cannot change this fail-over threshold.)

The Firebox sends an Access-Request message to the first RADIUS server shown. If there is no response, Fireware waits the number of seconds shown in the **Timeout** box, and then it sends another Access-Request. This continues for the number of times indicated in the **Retry** box (or until there is a valid response). If there is no valid response from the RADIUS server after this, Fireware counts this as one failed authentication attempt due to no response. (Note that if the RADIUS shared secret does not match, Fireware treats the bad response as no response.)

After three authentication attempts fail due to no response, Fireware uses the backup RADIUS server for its next authentication attempt.

If the same thing happens with the backup server (three authentication attempts fail due to no valid response), Fireware waits ten minutes for an administrator to correct the problem. After ten minutes Fireware tries to use the primary RADIUS server again.

**How do I use RADIUS Group names in my Firebox policies?**

In the Firewall tab of Policy Manager, double-click on a policy to edit it. Below the From text box, click Add. Then select Add User. From the Choose Type drop-down list, select Firewall. From the Auth Server drop-down list, select RADIUS. From the User/Group drop-down list, select Group. Type in the Filter-ID value RADIUS sends, exactly as you configure it on the RADIUS server. (Select User instead of Group if you want to type individual user names instead of a Group name in the policy.) Do the procedure again to add more than one RADIUS Group name or more than one user name. You can add user names and group names in the same policy.
How does a user do web-based authentication?

The user makes an HTTPS connection with the Firebox over port 4100 using a browser. To do this, type https:// in the address bar of a web browser, the IP address of the nearest Firebox interface, and then :4100. Do not use http in the address bar; you must use https.

For example, assume that the trusted interface IP address of the Firebox is 192.168.2.1. To authenticate from the trusted network, a user types https://192.168.2.1:4100 into the browser address bar.

Select RADIUS from the Domain drop-down list to have the Firebox send the authentication request to the RADIUS server. (There can be other authentication servers shown in the drop-down list if you configure other server types in the Policy Manager.)

Is it necessary for a remote user connecting with MUVPN or PPTP to do this web-based authentication?

No. When a remote user makes an MUVPN or a PPTP connection, the Firebox puts the user in the RADIUS Group shown by the Filter-ID attribute RADIUS sends. If the remote user does web-based authentication after this, there is no problem, but the Firebox already has RADIUS Group information for the user.

How do I make a policy to allow access for a user making a PPTP connection?

If you use RADIUS to authenticate PPTP sessions, add a policy to the Firewall tab of Policy Manager and use the Filter-ID value in the From box. From the policy’s Policy tab, click Add below the From text box. Select Add User. From the Choose Type drop-down list select Firewall. (Use the “PPTP” option in this drop-down list only if the Firebox uses its internal database for PPTP authentication.) From the Auth Server drop-down list, select RADIUS. Type in the Filter-ID value RADIUS sends.

How do I make a policy to allow access for a user making an MUVPN connection?

When you create the MUVPN group account, the Policy Manager automatically makes a policy that allows the traffic from the MUVPN clients. This policy is on the MUVPN tab of Policy Manager. Traffic is allowed over any port or protocol from the MUVPN clients to the resources shown in the MUVPN account settings. No more configuration is necessary to allow access for the MUVPN client.

To allow access that is restricted to only certain ports, you can remove this policy from the MUVPN tab of Policy Manager and replace it with one or more policies that allow only certain ports. Make sure to do this on the MUVPN tab of Policy Manager. When you add a policy to the MUVPN tab of Policy Manager, you select the MUVPN group the policy applies to. You do not add a RADIUS Group in the policy because when you select the MUVPN group, it forces the selection of the RADIUS Group. The name of the MUVPN group is the same as the RADIUS Group. Your RADIUS server must return a Filter-ID value that matches the name of the MUVPN group.

What authentication methods does the Firebox use for RADIUS?

- For web-based authentication using RADIUS, Fireware uses PAP (Password Authentication Protocol).
- For MUVPN authentication using RADIUS, Fireware uses PAP.
- For PPTP authentication using RADIUS, Fireware uses MS CHAP v2 (Microsoft Challenge-Handshake Authentication Protocol version 2).

Isn't PAP insecure?

When Fireware uses RADIUS, user passwords are not sent in the clear, even when Fireware uses PAP for the RADIUS request.

There are some RADIUS applications in which PAP can send clear-text passwords. This only happens in the communication from the user’s computer to the Network Access Server (not from the Access Server to the RADIUS server) but certain legacy applications can transmit clear-text passwords.

For example: When a dial-up user requests PPP authentication to an Internet Service Provider or a Remote Access Server that uses PAP, the PAP exchange sends the user’s password in clear-text between the user’s computer and the
Network Access Server. The Network Access Server encrypts the user’s password when it sends an Access-Request to the RADIUS server. Although the RADIUS protocol encrypts the password, it is sent as plaintext across the dial-up connection.

*There are important differences when the Firebox is the Network Access Server:*

- For web-based authentication, the connection between the user and the Firebox is encrypted with HTTPS, the same type of encryption used for secure web sites such as your online banking site. *All* data is encrypted between the user’s browser and the Firebox during web-based authentication.
- For MUVPN authentication, the user’s computer sends the user name and password *after* Phase 1 of IPSec is complete. During Phase 1, IPSec negotiates parameters to encrypt the rest of the transaction. When the user’s computer sends the user name and password, the information is protected with Phase 1 encryption. The remaining IPSec negotiations (Phase 2) are also encrypted with Phase 1 encryption.
- For PPTP, the authentication method is MS CHAP v2. This is a challenge-response protocol that does not send passwords at all. Instead, a series of encrypted challenges and responses are built from hashed forms of the password.

**Do I need to add a WG-Auth policy to my Firebox configuration?**
The **WG-Auth** policy controls access to port 4100 on the Firebox itself. For web-based firewall authentication this is the port the browser uses to send authentication requests to the Firebox. If there is no policy for port 4100, the Firebox discards port 4100 packets. Fireware adds the WG-Auth policy to your Firebox configuration for you automatically when you first configure a policy with a user or group name in the From field of a policy.

**How do I see diagnostic messages for authentication?**
To see debugging information about authentication in the Firebox log file, enable Advanced Diagnostics for the ADM module. From Policy Manager select **Setup > Logging.** Click the **Advanced Diagnostics** button. In the left “Category” box, expand **Authentication.** Click ADM and use the slider bar in the “Settings” box to enable more verbose debug information.

Do the same thing for the PPTP and IKE daemons to see messages that can help diagnose problems with PPTP and MUVPN connections that use RADIUS. In the left “Category” box, expand **VPN** to see the PPTP and IKE daemons.

To see the most useful authentication debug messages, turn diagnostic logging to **High.** To see these messages in the Traffic Monitor, select the box **Display diagnostic messages in Traffic Monitor.**

**What are some diagnostic messages to look for?**
When the RADIUS Shared Secret does not match, you see these messages in the Firebox log file:

```plaintext
rc_check_reply: Invalid digest from RADIUS server
admRadPktRcvPrs check RADIUS authenticator failed
```

For web-based authentication, when there is a Filter-Id attribute in the Access-Accept message you see this:

```plaintext
Got 1 type(11) attribute [filter-id_string] len 16
```
The `[filter-id_string]` part of the message shows the actual value of the Filter-Id attribute. "len" shows the length of the string.

**Windows IAS tells me the PPTP client was authenticated. Why does the user get error 734?**
This is a common error if you use the RADIUS server in the Windows Internet Authentication Service (IAS) to authenticate PPTP sessions. The user can get this error if the profile for the remote access policy that authenticates the user allows the option “No Encryption”. If you have diagnostic logging enabled for the PPTP module, you can see the error **MPPE required, but keys are not available** in the Firebox logs. To correct the error, edit the remote access policy in IAS that authenticates PPTP users. Click the **Edit Profile** button, then select the **Encryption** tab. Clear the check box labeled “No encryption”. This check box is selected by default with any new remote access policy you add to IAS.

The user can also get this error 734 if the user changes the default security settings for the PPTP connection. If you have diagnostic logging enabled for PPTP you can see the message “MPPE required but peer negotiation failed” in the Firebox log file. This is not a problem with the RADIUS server, but use these steps to correct the problem for Windows XP:

1. Edit the PPTP connection settings on the user’s computer. Click on the Security tab. If the radio button “Advanced (custom settings)” is selected, click the “Settings” button. From the “Data encryption” drop-down list select “Maximum Strength encryption” or “Require encryption”. Do not select “Optional encryption” or “No encryption”.
2. Or, on the Security tab for the PPTP connection properties, select the radio button “Typical (recommended settings)”.
3. From the “Validate my identity as follows” drop-down list, select “Require a secure password”. Select the check box “Require data encryption”.

**Do the same thing for the**

**Getting started**