Authentication

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

Introduction

When you use Fireware’s user authentication feature, you can see the user name and IP address of each Firebox connection. This can be very helpful if you want to track employee Internet usage. 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 servers:

- 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 Active Directory server. Active Directory is a directory service used by Microsoft’s operating systems to manage users, groups, and computers and offer secure access to network resources.

Is there anything I need to know before I start?

Before you configure the Firebox to point toward your Active Directory authentication server, make sure that your users can successfully authenticate to your Active Directory server.

You must also know your:

**Active Directory server IP address.**
- If you have a backup Active Directory server, you must know its IP address also.

**Active Directory Search Base**

The Search Base gives a base in the Active Directory structure to start the search for user account entries. To determine your search base, you must refer to your Active Directory documentation. You must know the containers used in your schema. It is within these containers that you assign group policies and access to resources for selected objects. Some common containers are:
- dc = DNS domain
- ou = organization unit
- cn = computer, group, or user

A standard format for the search base setting is: ou=organizational unit,dc=first part of distinguished server name,dc=any part of the distinguished server name appearing after a “dot”.

For example, if your user accounts are in an organizational unit called accounts and your domain name is HQ_main.com, your search base will be: **ou=accounts,dc=HQ_main,dc=com**.

If you have more than one organizational unit that you want users to authenticate against, then the search string would just be **dc=HQ_main,dc=com**. It is a good idea to use the highest level search base string that you feel comfortable with, so you can include as many containers from your AD tree as possible.

**Active Directory Group String**

The attribute string that is used to hold user group information on the Active Directory server. If you have not changed your Active Directory schema, the group string is always **memberOf**.


Configure the Firebox to Use the Active Directory Server

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

2. From the Active Directory tab, select the Enable Active Directory Server check box.

3. In the IP Address text box, type the IP address of the primary Active Directory server for the Firebox to contact with authentication requests. The Active Directory server can be located on any Firebox interface or available through a VPN tunnel.

4. In the Port data entry box, type the TCP port number for the Firebox to use to connect to the Active Directory server. The default port number is 389 and most users do not change this.

5. Type the Search Base.

6. Type the Group String.

7. If necessary, change the timeout value. This is how long the Firebox waits for a response from the authentication server before it tries again.
Frequently Asked Questions about this Procedure

8. Add information for a backup Active Directory server, if you have one.

9. Click OK. From Policy Manager, select File > Save > To Firebox to save your changes to the Firebox.

Frequently Asked Questions about this Procedure

How do I find out what my search base is?
To learn about how to find your Active Directory search base, go to http://www.watchguard.com/support/Fireware_HowTo/HowTo_FindADSearchBase.pdf

Can I use my Active Directory group names in my Firebox policies?
Yes. In Policy Manager, double-click on any policy. Below the From text box, click Add. Select Add User. From the Auth Server drop-down list, select Active Directory. From the User/Group drop-down list, select Group. Type in the group, or organizational unit, or container name, exactly as it appears on the Active Directory server.

Do I need to add a WG-Auth policy to my Firebox configuration?
Fireware® will add 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. This policy controls access to port 4100 on the Firebox itself. This is the port your users will use to send authentication requests to the Firebox from their web browsers.
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 `Active Directory` from the **Domain** drop-down list to have the Firebox send the authentication request to the Active Directory server.
There can be other authentication servers shown in the drop-down list if you configure other server types in the Policy Manager. The next screen shot shows `RADIUS` for the authentication server. Make sure to select the correct Authentication server from the **Domain** drop-down list.

How do I make a policy to allow access for a user making an MUVVPN connection when MUVVPN uses Active Directory for the authentication server?
When you create the MUVVPN group account, the Policy Manager automatically makes a policy that allows the traffic from the MUVVPN clients. This policy is on the **MUVPN** tab of Policy Manager. Traffic is allowed over any port or protocol from the MUVVPN clients to the resources shown in the MUVVPN account settings. No more configuration is necessary to allow access for the MUVVPN client.
To allow access that is restricted to only certain ports, you can remove the automatically-generated 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, not on the **Firewall** tab. When you add a policy to the **MUVPN** tab of Policy Manager, you select the MUVVPN group the policy applies to. You do not add an Active Directory group in the policy because when you select the MUVVPN group, it forces the selection of the Active Directory group. The name of the MUVVPN group is the same as the Active Directory group.