



Mercurion Systems, Inc.

Information Technology Consulting and Support Services

Phone: 919.266.5957 Fax: 919.217.5769
<http://www.mercurionsystems.com>

INTEGRATING WATCHGUARD VPN AUTHENTICATION WITH ACTIVE DIRECTORY

Products: WatchGuard Firebox System v6.2 or later; Windows 2000 Server or Advanced Server or later; PPTP-based VPN client

Overview

The WatchGuard Firebox is a multi-function security appliance offering a range of security functions. These include packet filters, application proxies for services such as HTTP and SMTP, and VPN functionality with both IPSec- and PPTP-based VPNs. With version 6.2 of the WatchGuard Firebox System (WFS) software, the Firebox gains the ability to use RADIUS to authenticate incoming PPTP-based VPN tunnels, allowing WFS to integrate with a number of RADIUS-compatible directory services.

This technical note describes how to use Internet Authentication Service (IAS), a service included with Windows 2000 Server and Windows Server 2003 that provides RADIUS-based access to authentication information stored in Active Directory, to integrate with WFS for authenticating inbound PPTP-based VPN tunnels.

More Information

To integrate WFS and Active Directory, several configuration steps must be taken on both the Windows side as well as on the firewall side. These steps are described below.

Configuring Windows and Active Directory

Configuring Windows and Active Directory really involves installing and configuring Internet Authentication Service (IAS). This technical note will not delve into the details of actually installing IAS, but rather focuses on the correct configuration of IAS in order to interoperate with WFS for VPN authentication.

Use the following steps as a general guideline for configuring IAS, substituting the appropriate group names and IP addresses where applicable.

1. Once IAS has been installed, add the Firebox as a RADIUS client. Specify the IP address of the Firebox's trusted interface and a shared secret that will also be needed when configuring the Firebox (see the section titled "Configuring the Firebox").
2. Create a new remote access policy to control authentication from the Firebox. Figure 1, on the following page, shows an example of a remote access policy. In this particular case, the policy is controlled by two criteria: membership in a Windows group ("VPN Users"; note that the domain name has been removed from this diagram but would normally be included here)

and the source IP address of the RADIUS client (not the VPN client, but the RADIUS client—the Firebox itself). Authentication requests that meet these criteria will be handled by this policy. In the IAS MMC console, move this remote access policy to the top of the list.

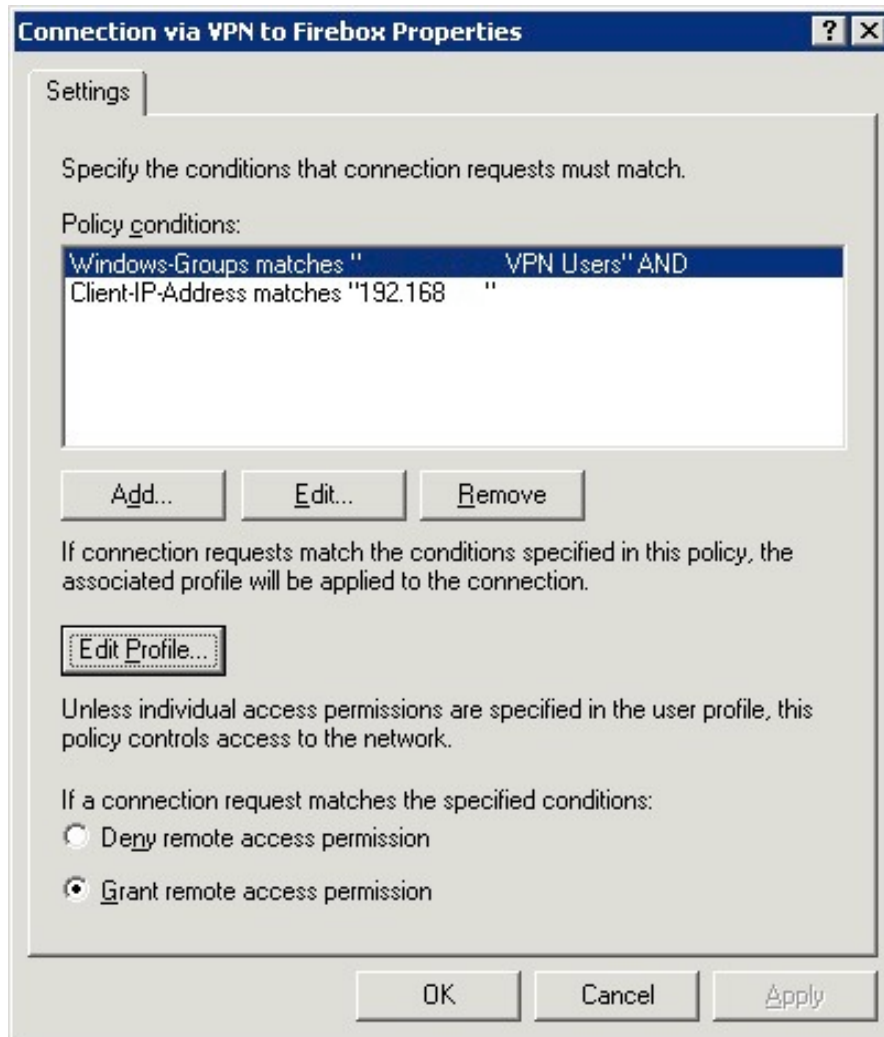


Figure 1. Creating a new remote access policy

3. Click the “Edit Profile” button to edit the remote access profile that will be enforced for authentication requests handled by this policy. For interoperability with the Firebox, remove all attributes from the Advanced tab and add only a single attribute back to the list: Filter-Id. Set the value of Filter-Id to be “pptp_users.”
4. While editing the profile, be sure that MS-CHAP and MS-CHAP v2 are enabled on the Authentication tab.

IAS is now configured. In order to complete the configuration, the Firebox must now be configured to query IAS for VPN authentication information.

Configuring the Firebox

Configuring the Firebox is a fairly straightforward process. The steps below provide additional information (note that these instructions assume version 6.2 SP1 of the WatchGuard Firebox System software). All these steps are performed within Policy Manager.

1. Go to Setup > Firewall Authentication and select “RADIUS.”
2. Go to Setup > Authentication Servers and on the RADIUS Servers tab, enter the IP address, port number, and shared secret. This information will correspond directly to the information used in configuring IAS earlier. The default port, 1645, should work fine with IAS’ default settings.
3. From the Network > Remote User VPN dialog box, click on the PPTP tab and select the box marked “Use Radius authentication to authenticate remote users”.
4. Proceed with configuring the PPTP-based VPN as usual. Be sure to add a rule to the services arena allowing traffic to/from the “pptp_users” group to/from the trusted interface; otherwise, the VPN users will be subject to the same rules as all other inbound traffic. (The “Any” service is typically useful for this.)

Because the Filter-Id on the IAS server was set to “pptp_users”, the same group name must be used in any service definitions for VPN users. This is the link that informs the Firebox that a user authenticated by IAS should be treated as a member of the pptp_users group and therefore be subject to rules applied to that group. (Note that this pseudo-membership in the pptp_users group is not the same as group membership in configuring the remote access policy. In that case, users must be members of an Active Directory group in order for the remote access policy to apply to them; if they aren’t members, then remote access will be denied.)

Additional technical notes are available to assist with configuring a Firebox for PPTP-based VPNs.

Other Notes

This technical note was tested using a Firebox II running version 6.2 (with Service Pack 1) of the WatchGuard Firebox System (WFS) software. A server running Windows Server 2003, Standard Edition, was running Internet Authentication Service (IAS) in a native mode Active Directory domain. A VPN client running Mac OS X 10.2.8 was used to test VPN client connectivity.

Related Articles/Resources

None

Legal Information

This document was created by Mercurion Systems, Inc., and may be freely distributed as long as it is distributed without modification and in its entirety. Mercurion Systems assumes no liability as a result of using the information contained in this document.