WatchGuard XTM Mobile SSL VPN Integration Guide (RADIUS)

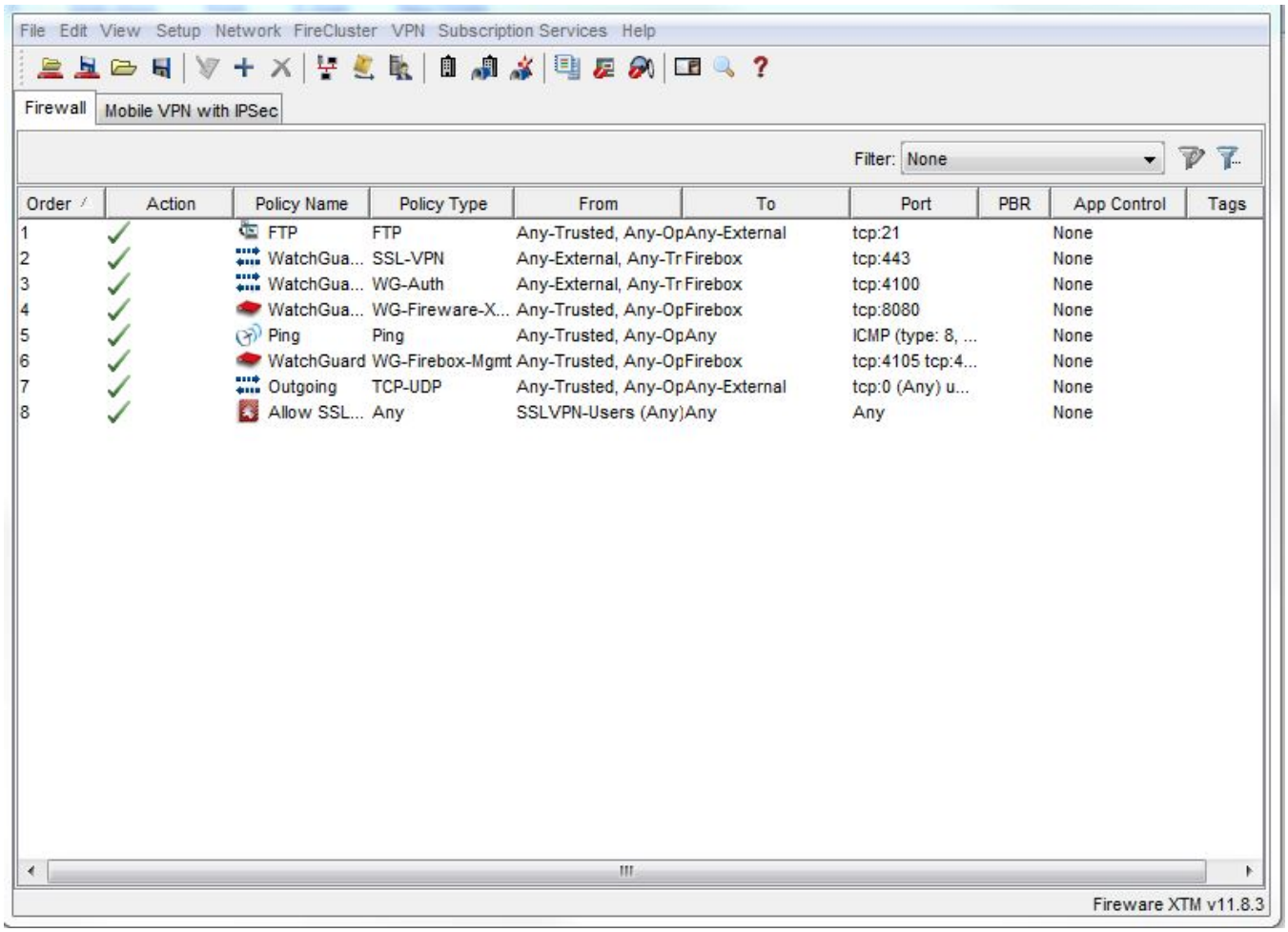
Introduction

Use this guide to enable Multi-Factor Authentication access via RADIUS to WatchGuard XTM Mobile SSL VPN.

Prerequisites

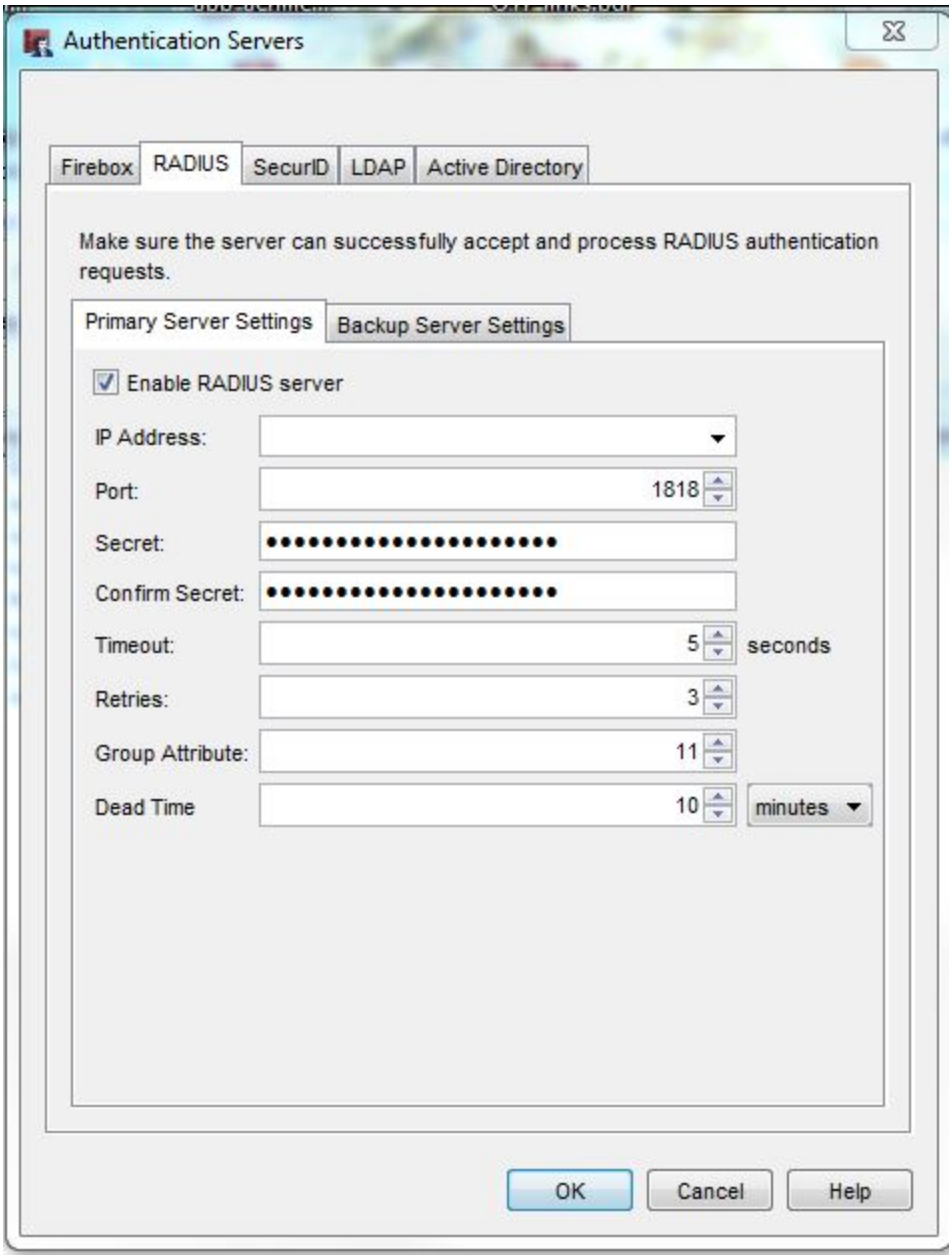
1. Have the **Multi-Factor App Enrollment Realm** configured on the SecureAuth IdP appliance
2. Have RADIUS Server running on the SecureAuth IdP Appliance
3. Have Mobile SSL VPN configured on WatchGuard XTM

WatchGuard Configuration Steps



1. Launch the WatchGuard System Manager
2. From the menu, select **Setup**, **Authentication**, then **Authentication Servers**

Authentication Servers



3. In the **Authentication Servers** window, select the **RADIUS** tab

4. Set the **IP Address** to the SecureAuth IdP appliance running the RADIUS Server

5. Set the **Port** to the Port on which the SecureAuth IdP appliance (with RADIUS Server) runs (default **1812**)

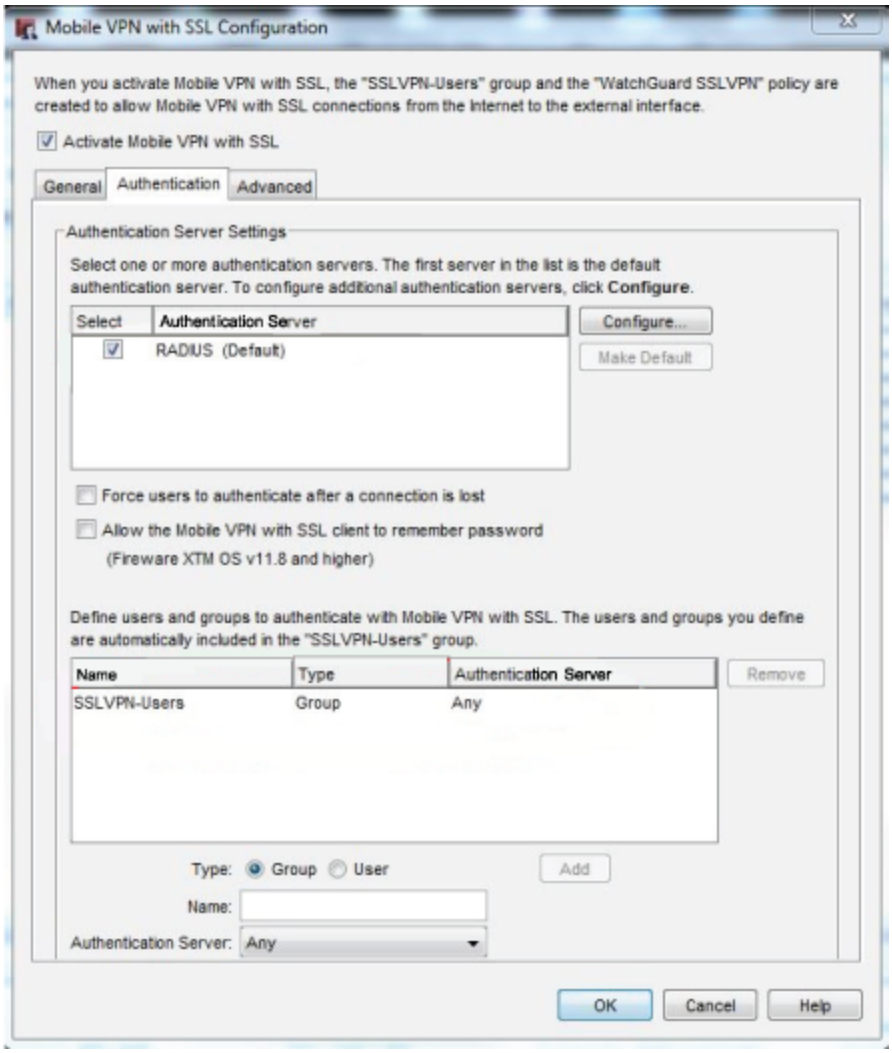
6. Set the **Secret** to the secret configured on the SecureAuth IdP RADIUS service

7. Set the **Timeout** to a time up to 30 seconds

8. Click **OK** to save the settings

> The remaining settings can be left as default

Mobile VPN with SSL Configuration



9. From the WatchGuard System Manager menu, select **VPN**, **Mobile VPN**, then **SSL**

10. In the **Mobile VPN with SSL Configuration** window, select the **Authentication** tab

11. Check the **RADIUS** option in the **Authentication Server** field, and make it **Default**

12. Set the **Name** to **SSLVPN-Users** as a **Group**, and select **RADIUS** or **Any** from the **Authentication Server** dropdown

13. Click **Add**, and it will appear in the box above

14. Click **OK** to save the settings