RADIUS

RADIUS, the acronym of *Remote Authentication Dial In User Service* is a widespread protocol for allowing network devices such as routers to authenticate users against a central database. In addition to user information, RADIUS can store technical information used by network devices, such as supported protocols, IP addresses, routing information, and so on. This information constitutes a user profile, which is stored in a file or database on the RADIUS server.

The RADIUS protocol is very flexible, and servers are available for most operating systems. The RADIUS implementation on Sophos UTM allows you to configure access rights on the basis of proxies and users. Before you can use RADIUS authentication, you must have a running RADIUS server on the network. Whereas passwords are encrypted using the RADIUS secret, the username is transmitted in plain text.

To configure RADIUS authentication, proceed as follows:

1. **On the *Servers* tab, click *New Authentication Server*.**
   The dialog box *Add Authentication Server* opens.

2. **Make the following settings:**
   Backend: Select *RADIUS* as backend directory service.

   Position: Select a position for the backend server. Backend servers with lower numbers will be queried first. For better performance, make sure that the backend server that is likely to get the most requests is on top of the list.

   Server: Select or add a RADIUS server. How to add a definition is explained on the *Definitions & Users > Network Definitions > Network Definitions* page.

   Port: Enter the port of the RADIUS server. By default, this is port `1812`.

   Shared Secret: The shared secret is a text string that serves as a password between a RADIUS client and a RADIUS server. Enter the shared secret.

   Test server settings: Pressing the *Test* button performs a bind test with the configured server. This verifies that the settings on this tab are correct, and the server is up and accepts connections.

   Username: Enter the username of a test user to perform a regular authentication.

   Password: Enter the password of the test user.

   NAS identifier: Select the appropriate NAS identifier from the list. For more information see the Note and the table below.

   Authenticate example user: Click the *Test* button to start the authentication test for the test user. This verifies that all server settings are correct, the server is up and accepting connections, and users can be successfully authenticated.

3. **Optionally, make the following advanced settings:**
   Authentication timeout (sec): Enter the timeout for the communication with the server to support higher latency scenarios if you use third party authentication solutions.

4. **Click *Save*.**
   The server will be displayed in the *Servers* list.

Note – Each user authentication service of Sophos UTM such as PPTP or L2TP querying the RADIUS server sends a different identifier (NAS identifier) to the RADIUS server. For example, the PPTP service sends the NAS identifier `pptp` to the RADIUS server when trying to authenticate this user.That way, the various services can be differentiated on the RADIUS server, which is useful for authorization purposes, that is, the granting of specific types of service to users. Below you can find the list of user authentication services and their corresponding NAS identifier.

User Authentication Service	NAS Identifier
SSL VPN	`ssl`
PPTP	`pptp`
IPsec	`ipsec`
L2TP over IPsec	`l2tp`
SMTP proxy	`smtp`
User Portal	`portal`
WebAdmin	`webadmin`
SOCKS proxy	`socks`
Web Filter	`http`
Authentication Client	`agent`
Web Application Filter (WAF)	`reverseproxy`
Wireless Access Points	NAS ID is the wireless network name.

RADIUS NAS Identifiers

Related Topics

Network Definitions