Chapter 20

Authenticating Users on a C-series Platform

This chapter describes how to configure RADIUS and TACACS+ authentication for users who access a C-series platform. Topics include:

Configuring RADIUS and TACACS+ Authentication

The SRC software always performs password authentication on a C-series platform. You can configure RADIUS and/ or TACACS+ authentication to complement password authentication. In this case, the software performs RADIUS and or TACACS+ authentication before password authentication.

To configure RADIUS and TACACS+ authentication for users who access a C-series platform:

1. Configure the connection to the RADIUS or TACACS+ server.

   See *Configuring RADIUS Authentication* on page 180.

   See *Configuring TACACS+ Authentication* on page 181.

2. Configure the authentication order.

   See *Configuring More Than One Authentication Method* on page 182.

3. Configure template accounts.

   See *Configuring Template Accounts for RADIUS and TACACS+ Authentication* on page 185.

4. (Optional) Configure individual user profiles.

   See *Chapter 19, Configuring User Access*.

Configuring RADIUS Authentication

Use the following configuration statements to configure information about one or more RADIUS servers on the network at the [edit] hierarchy level:

```
system radius-server address {
    port port;
    secret secret;
    timeout timeout;
    retry retry;
}
```

To configure information about RADIUS servers for authentication:

1. From configuration mode, access the configuration statement that adds a RADIUS server.

   ```
   [edit]
   user@host# edit system radius-server address
   ```

2. Specify a port number on which to contact the RADIUS server.

   ```
   [edit system radius-server address]
   user@host# set port port
   ```

   By default, port number 1812 is used as specified in RFC 2865—Remote Authentication Dial In User Service (RADIUS) (June 2000).

3. Specify a password. Passwords can contain spaces. The secret used by the C-series platform must match that used by the server.

   ```
   [edit system radius-server address]
   user@host# set secret secret
   ```

4. (Optional) Specify the amount of time that the C-series platform waits to receive a response from a RADIUS server.

   [edit system radius-server *address*]
   user@host# **set timeout** *timeout*

   By default, the C-series platform waits 3 seconds. You can change the timeout to a value from 1 through 90 seconds.

5. Specify the number of times that the C-series platform attempts to contact a RADIUS authentication server.

   [edit system radius-server *address*]
   user@host# **set retry** *retry*

   By default, the C-series platform retry property is set to 3 times. You can change the retry value to a number from 1 through 10 times.

To configure a set of users that share a single account for authorization purposes, you create a template user. See *Configuring Template Accounts for RADIUS and TACACS+ Authentication* on page 185.

Configuring TACACS+ Authentication

Use the following configuration statements to configure information about one or more TACACS+ servers on the network at the [edit] hierarchy level:

```
system tacplus-server {
    address address;
    secret secret;
}
```

To configure information about TACACS+ servers for authentication:

1. From configuration mode, access the configuration statement that adds a RADIUS server.

   [edit]
   user@host# **edit system** tacplus-server

2. Specify the address of the TACACS+ server.

   [edit system tacplus-server]
   user@host# **set address** *address*

   To configure multiple TACACS+ servers, include multiple values for the address option.

3. Specify a secret (password) that the C-series platform passes to the TACACS+ client by including the **secret** statement. Secrets can contain spaces. The secret used by the C-series platform must match the secret used by the TACACS+ server.

   [edit system tacplus-server]
   user@host# **set secret** *secret*

To configure a set of users that share a single account for authorization purposes, you create a template user. See *Configuring Template Accounts for RADIUS and TACACS+ Authentication* on page 185.

Configuring More Than One Authentication Method

On a C-series platform, you can use more than one authentication method. You can configure the C-series platform to be a RADIUS and TACACS+ client by:

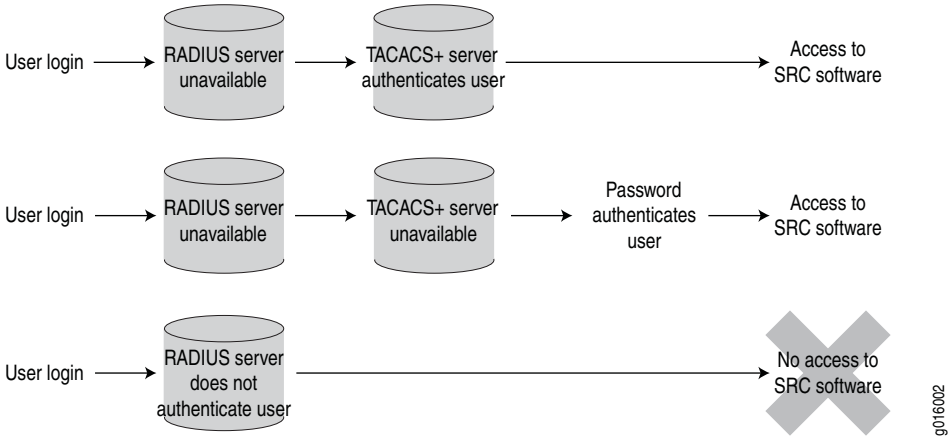
- Configuring RADIUS and TACACS+ authentication.
- Configuring the authentication order to prioritize the order in which the C-series platform uses configured authentication methods.

For each login attempt, the SRC software tries the authentication methods in the order configured, until the password matches. If one of the authentication methods in the authentication order fails to authenticate a user, the user is denied access to the C-series platform.

If password authentication does not appear in the prioritized list of authentication methods, the SRC software uses password authentication last. The SRC software always uses password authentication, whether or not it appears in the list of authentication methods to be used. As a result, users can log in to the C-series platform through password authentication if configured authentication servers are unavailable.

Figure 16 shows three authentication scenarios. In the first two, a user is authenticated while authentication servers are unavailable. In the third scenario, a users is not authenticated by an active server.

Figure 16: Authentication Order: RADIUS, TACACS+, Password



Configuring Authentication Order

To configure the order in which to use authentication servers:

1. From configuration mode, access the [system] hierarchy level.

2. Specify the authentication order.

   [edit system]
   user@host# **set authentication-order** [(radius | tacplus | password)]

   Specify one or more of the following in the preferred order, from first authentication method tried to last tried:

   - radius—Verify the user using RADIUS authentication services.
   - tacplus—Verify the user using TACACS+ authentication services.
   - password—Verify the user using the password configured for the user with the authentication statement at the [edit system login user] hierarchy level.

If you do not include the authentication-order statement, users are verified based on their configured passwords.

Configuring TACACS+ or RADIUS Authentication

To configure the SRC software to try to authenticate users through TACACS + and, if the TACACS + server is unavailable, to use password authentication:

- Specify the following authentication order:

  ```
  [edit]
  user@host# set system authentication-order [tacplus password]
  ```

  or

  ```
  [edit]
  user@host# set system authentication-order tacplus
  ```

To configure the SRC software to try to authenticate users through RADIUS and, if the RADIUS server is unavailable, to use password authentication:

- Specify the following authentication order:

  ```
  [edit]
  user@host# set system authentication-order [radius password]
  ```

  or

  ```
  [edit]
  user@host# set system authentication-order radius
  ```

Configuring TACACS+ and RADIUS Authentication

To configure the SRC software to try to authenticate users through TACACS + and, if the TACACS + server is unavailable, to use RADIUS authentication; and then, if the RADIUS server is unavailable, to use password authentication:

- Specify the following authentication order:

  ```
  [edit]
  user@host# set system authentication-order [tacplus radius password]
  ```

  or

  ```
  [edit]
  user@host# set system authentication-order [tacplus radius]
  ```

To configure the SRC software to try to authenticate users through RADIUS and, if the RADIUS server is unavailable, to use TACACS+ authentication; and then, if the TACACS+ server is unavailable, to use password authentication:

- Specify the following authentication order:

  ```
  [edit]
  user@host# set system authentication-order [radius tacplus password]
  ```

  or

  ```
  [edit]
  user@host# set system authentication-order [radius tacplus]
  ```

Removing an Authentication Method from the Authentication Order

To delete the radius statement from the authentication order:

- Enter the following command:

  ```
  [edit system]
  user@host# delete authentication-order [(radius | tacplus)]
  ```

  For example:

  ```
  [edit system]
  user@host# delete authentication-order radius
  ```

Configuring Template Accounts for RADIUS and TACACS+ Authentication

When a user logs in to the CLI, the following authentication is performed:

- RADIUS and /or TACSACS+ server authentication
- Authentication through a user account configured under [system login user]

For authorization purposes, you can use a template account to create a single account that can be shared by a set of users at the same time.

Typically when you use RADIUS and/or TACACS+ authentication, the user account is shared among a group of users who have the same privileges. You create template accounts for sets of users. Template accounts can be named:

- remote—(Default) A single account that defines user permissions for all users that authenticate through RADIUS or TACACS+
- *name-of-your-choice*—Account for a group of users

Use a named template account when you need different types of templates. Each template can define a different set of permissions appropriate to a group of users who use that template. For example, you can configure a set of remote users to concurrently share a single UID.

When a user is part of a group that uses a template account, the command-line interface (CLI) username is the login name; however, the privileges, file ownership, and effective username are inherited from the template account.

Using Remote Template Accounts

To configure the remote template account and specify the privileges that you want to grant to remote users:

- Include the system login user remote statement at the [edit] hierarchy level, and specify the "All remote users" for the full-name option:

```
[edit]
system login user remote {
    full-name "All remote users";
    uid uid-value;
    class class-name;
}
```

All users who share the remote template account have the same access privileges.

Using Named Template Accounts

Template accounts for which you define a name are defined on a C-series platform and are referenced by the TACACS+ and RADIUS authentication servers through usernames. All users who share a local user template account have the same access privileges.

When a user who accesses the C-series platform through a name template account logs in:

1. The SRC software issues a request to the authentication server to authenticate the user's login name.
2. If a user is authenticated, the server returns the username to the SRC software.
3. The SRC software determines whether a username is specified for that login name.
4. If there is a username, the SRC software selects the appropriate template.
5. If a user template does not exist for the authenticated user, the C-series platform uses the remote template.

Configuring a Local User Template

To configure a local user template and specify the privileges that you want to grant to the local users to whom the template applies:

- Include the system login user *local-username* statement at the [edit] hierarchy level, and specify the name of the group for the full-name option.

```
[edit]
system login user username {
    full-name "name of group";
    uid uid-value;
    class class-name;
}
```

Example: Configuring System Authentication

The following example allows login only by:

- Individual user Philip
- Users who have been authenticated by a remote RADIUS server

If a user logs in and is not authenticated by the RADIUS server, the user is denied access to the C-series platform. However, if the RADIUS server is not available, the user can be authenticated through an SRC password.

In this example, user configuration includes:

- An individual user account for Philip that provides privileges for the super-user class after RADIUS authentication.
- A remote user template account for all other users to share the same class and user ID (UID) after RADIUS authentication.

Individual SRC accounts are not configured for other users. When they log in to the system and the RADIUS server authenticates them, they are given access using the same UID 9999 and the same privileges for the operator class.

```
[edit]
system {
    authentication-order radius;
    login {
      user philip {
        full-name "Philip";
        uid 1001;
        class super-user;
        }
      user remote {
        full-name "All remote users";
        uid 9999;
        class operator;
      }
    }
}
```