Next-Generation Firewall

Configure an Authentication Profile and Sequence

Previous
Configure Local Database Authentication
Next
Configure Passwordless Authentication

An authentication profile defines the authentication service that validates the login credentials of administrators who access the firewall web interface and end users who access applications through Authentication Portal or GlobalProtect. The service can be Local Authentication that the firewall provides or External Authentication Services. The authentication profile also defines options such as Kerberos single sign-on (SSO).

Some networks have multiple databases (such as TACACS+ and LDAP) for different users and user groups. To authenticate users in such cases, configure an **`authentication sequence`**—a ranked order of authentication profiles that the firewall matches a user against during login. By default, the firewall checks against each profile in sequence until one successfully authenticates the user and a user is denied access only if authentication fails for all the profiles in the sequence. The sequence can specify authentication profiles that are based on any authentication service that the firewall supports except Multi-Factor Authentication (MFA) and SAML.

STEP 1 - (**External service only**) Enable the firewall to connect to an external server for authenticating users:

1. Set up the external server. Refer to your server documentation for instructions.
2. Configure a server profile for the type of authentication service you use.
   - Add a RADIUS server profile.

     If the firewall integrates with an MFA service through RADIUS, you must add a RADIUS server profile. In this case, the MFA service provides all the authentication factors. If the firewall integrates with an MFA service through a vendor API, you can still use a RADIUS server profile for the first factor but MFA server profiles are required for additional factors.
   - Add an MFA server profile.
   - Add a SAML IdP server profile.
   - Add a Kerberos server profile.
   - Add a TACACS+ server profile.
   - Add an LDAP server profile.

STEP 2 - (**Local database authentication only**) Configure a user database that is local to the firewall.

Perform these steps for each user and user group for which you want to configure Local Authentication based on a user identity store that is local to the firewall:

1. Add the user account to the local database.
2. (**Optional**) Add the user group to the local database.

STEP 3 - (**Kerberos SSO only**) Create a Kerberos keytab for the firewall if Kerberos single sign-on (SSO) is the primary authentication service.

Create a Kerberos keytab. A keytab is a file that contains Kerberos account information for the firewall. To support Kerberos SSO, your network must have a Kerberos infrastructure.

STEP 4 - Configure an authentication profile.

Define one or both of the following:

- **Kerberos SSO**—The firewall first tries SSO authentication. If that fails, it falls back to the specified authentication **Type**.
- **External authentication or local database authentication**—The firewall prompts the user to enter login credentials, and uses an external service or local database to authenticate the user.

1. Select **Device > Authentication Profile** and **Add** the authentication profile.
2. Enter a **Name** to identify the authentication profile.
3. Select the **Type** of authentication service.
   - If you use Multi-Factor Authentication, the selected type applies only to the first authentication factor. You select services for additional MFA factors in the **Factors** tab.
   - If you select **RADIUS**, **TACACS+**, **LDAP**, or **Kerberos**, select the **Server Profile**.
   - If you select **LDAP**, select the **Server Profile** and define the **Login Attribute**. For Active Directory, enter **sAMAccountName** as the value.
   - If you select **SAML**, select the **IdP Server Profile**.
   - If you select **Cloud Authentication Service**, configure a Cloud Identity Engine instance to communicate with the firewall. For more information on the Cloud Identity Engine, see the Cloud Identity Engine Getting Started guide.
4. If you want to enable Kerberos SSO, enter the **Kerberos Realm** (usually the DNS domain of the users, except that the realm is UPPERCASE) and **Import** the **Kerberos Keytab** that you created for the firewall or Panorama.
5. (**MFA only**) Select **Factors**, **Enable Additional Authentication Factors**, and **Add** the MFA server profiles you configured.

   The firewall will invoke each MFA service in the listed order, from top to bottom.
6. Select **Advanced** and **Add** the users and groups that can authenticate with this profile.

   You can select users and groups from the local database or, if you configured the firewall to Map Users to Groups, from an LDAP-based directory service such as Active Directory. By default, the list is empty, meaning no users can authenticate.

   You can also select custom groups defined in a group mapping configuration.
7. (**Optional**) To modify the user information before the firewall sends the authentication request to the server, configure a **Username Modifier**.
   - **%USERDOMAIN%\%USERINPUT%**—If the source does not include the domain (for example, it uses the sAMAccountName), the firewall adds the **User Domain** you specify before the username. If the source includes the domain, the firewall replaces that domain with the **User Domain**. If the **User Domain** is empty, the firewall removes the domain from the user information that the firewall receives from source before the firewall sends the request to the authentication server.

     Because LDAP servers don't support backslashes in the sAMAccountName, don't use this option to authenticate with an LDAP server.
   - **%USERINPUT%**—(Default) The firewall sends the user information to the authentication server in the format it receives from the source.
   - **%USERINPUT%@%USERDOMAIN%**—If the source does not include the domain, the firewall adds the **User Domain** value after the username. If the source includes domain, the firewall replaces that domain with the **User Domain** value. If the **User Domain** is empty, the firewall removes the domain from the user information that the firewall receives from the source before the firewall sends the request to the authentication server.
   - **None**—If you manually enter **`None`**:
     - For LDAP and Kerberos server profiles, the firewall uses the domain it receives from the source to select the appropriate authentication profile, then removes the domain when it sends the authentication request to the server. This allows you to include the **User Domain** during the authentication sequence but remove the domain before the firewall sends the authentication request to the server. For example, if you are using an LDAP server profile and the samAccountName as the attribute, use this option so that the firewall does not send the domain to the authentication server that expects only a username and not a domain.
     - For RADIUS server profiles:
       - If the source sends the user information in **`domain\username`** format, the firewall sends the user information to the server in the same format.
       - If the source sends the user information in **`username@domain`** format, the firewall normalizes the user information to the **`domain\username`** format before sending it to the server.
       - If the source sends only the username, the firewall adds the **User Domain** you specify before sending the information to the server in **`domain\username`** format.
     - For local databases, TACACS+, and SAML, the firewall sends the user information to the authentication server in the format it receives from the source.
8. Click **OK** to save the authentication profile.

STEP 5 - Configure an authentication sequence.

Required if you want the firewall to try one or more authentication profiles to authenticate users.

1. Select **Device > Authentication Sequence** and **Add** the authentication sequence.
2. Enter a **Name** to identify the authentication sequence.
3. (Optional but recommended) To expedite the authentication process and avoid the computational load of running the entire authentication sequence if it is not necessary, you can have the firewall **Exit the sequence on failed authentication**.

   This option supports the following authentication methods:
   - Kerberos
   - RADIUS
   - TACACS+
   - LDAP
   - Local database

   If you select this option, the authentication sequence ends when the firewall successfully authenticates the authentication profile or if the authentication fails (for example, due to an incorrect password). If the attempt times out or if the firewall does not find a matching user on the allow list, the authentication sequence proceeds to the next authentication profile in the sequence.

   If you do not select this option, the firewall attempts authentication with all authentication profiles in the sequence and ends the sequence only when an authentication profile authenticates successfully or if all authentication attempts with the authentication profiles in the sequence fail.
4. (Optional but recommended) To expedite the authentication process, select **Use domain to determine authentication profile**. When you select this option, the firewall matches the domain name that a user enters during login with an authentication profile in the sequence then uses that profile to authenticate the user. If the firewall does not find a match or if you disable the option, the firewall tries the profiles in the top-to-bottom sequence.
5. (Optional but recommended) To normalize the domain name that the user enters during login before applying the authentication sequence, select **Use User-ID domain to determine authentication profile**. If you do not select this option, the firewall does not normalize the domain name that the user enters during login before applying the authentication profile sequence.
6. **Add** each authentication profile. To change the evaluation order of the profiles, select a profile and **Move Up** or **Move Down**.
7. Click **OK** to save the authentication sequence.

STEP 6 - Assign the authentication profile or sequence to an administrative account for firewall administrators or to Authentication policy for end users.

- **Administrators**—Assign the authentication profile based on how you manage administrator authorization:
  Authorization managed locally on the firewall—Configure a Firewall Administrator Account.

  Authorization managed on a SAML, TACACS+, or RADIUS server—Select **Device > Setup > Management**, edit the Authentication Settings, and select the **Authentication Profile**.
- **End users**—For the full procedure to configure authentication for end users, see Configure Authentication Policy.

STEP 7 - Verify that the firewall can Test Authentication Server Connectivity to authenticate users.

Previous
Configure Local Database Authentication
Next
Configure Passwordless Authentication