Next-Generation Firewall

Configure Authentication Policy

Previous
Authentication Timestamps
Next
Troubleshoot Authentication Issues

Perform the following steps to configure Authentication policy for end users who access services through Authentication Portal. Before starting, ensure that your Security Policy allows users to access the services and URL categories that require authentication.

Before you configure an Authentication policy rule, make sure you understand that the set of IPv4 addresses is treated as a subset of the set of IPv6 addresses, as described in detail in Policy.

STEP 1 - Configure Authentication Portal. If you use Multi-Factor Authentication (MFA) services to authenticate users, you must set the **Mode** to **Redirect**.

STEP 2 - Configure the firewall to use one of the following services to authenticate users.

- External Authentication Services—Configure a server profile to define how the firewall connects to the service.
- Local database authentication—Add each user account to the local user database on the firewall.
- Kerberos single sign-on (SSO)—Create a Kerberos keytab for the firewall. Optionally, you can configure the firewall to use Kerberos SSO as the primary authentication service and, if SSO failures occur, fall back to an external service or local database authentication.

STEP 3 - Configure an Authentication Profile and Sequence for each set of users and Authentication policy rules that require the same authentication services and settings.

Select the **Type** of authentication service and related settings:

- **External service**—Select the **Type** of external server and select the **Server Profile** you created for it.
- **Local database authentication**—Set the **Type** to **Local Database**. In the **Advanced** settings, **Add** the Authentication Portal users and user groups you created.
- **Kerberos SSO**—Specify the **Kerberos Realm** and **Import** the **Kerberos Keytab**.

STEP 4 - Configure an authentication enforcement object.

The object associates each authentication profile with an Authentication Portal method. The method determines whether the first authentication challenge (factor) is transparent or requires a user response.

1. Select **Objects > Authentication** and **Add** an object.
2. Enter a **Name** to identify the object.
3. Select an **Authentication Method** for the authentication service **Type** you specified in the authentication profile:
   - **browser-challenge**—Select this method if you want the client browser to respond to the first authentication factor instead of having the user enter login credentials. For this method, you must configure Kerberos SSO in the authentication profile. If the browser challenge fails, the firewall falls back to the **web-form** method.
   - **web-form**—Select this method if you want the firewall to display a Authentication Portal web form for users to enter login credentials.
4. Select the **Authentication Profile** you configured.
5. Enter the **Message** that the Authentication Portal web form will display to tell users how to authenticate for the first authentication factor.
6. Click **OK** to save the object.

STEP 5 - Configure an Authentication policy rule.

Create a rule for each set of users, services, and URL categories that require the same authentication services and settings.

> The firewall does not apply the Authentication Portal timeout if your authentication policy uses default authentication enforcement objects (for example, **default-browser-challenge**).To require users to re-authenticate after the Authentication Portal timeout, clone the rule for the default authentication object and move it before the existing rule for the default authentication object.

1. Select **Policies > Authentication** and **Add** a rule.
2. Enter a **Name** to identify the rule.
3. Select **Source** and **Add** specific zones and IP addresses or select **Any** zones or IP addresses.

   The rule applies only to traffic coming from the specified IP addresses or from interfaces in the specified zones.
4. Select **User** and select or **Add** the source users and user groups to which the rule applies (default is **any**).
5. Select or **Add** the Host Information Profiles to which the rule applies (default is **any**).
6. Select **Destination** and **Add** specific zones and IP addresses or select **any** zones or IP addresses.

   The IP addresses can be resources (such as servers) for which you want to control access.
7. Select **Service/URL Category** and select or **Add** the services and service groups for which the rule controls access (default is **service-http**).
8. Select or **Add** the URL categories for which the rule controls access (default is **any**). For example, you can create a custom URL category that specifies your most sensitive internal sites.
9. Select **Actions** and select the **Authentication Enforcement** object you created.
10. Specify the **Timeout** period in minutes (default 60) during which the firewall prompts the user to authenticate only once for repeated access to services and applications.

    > **Timeout** is a tradeoff between tighter security (less time between authentication prompts) and the user experience (more time between authentication prompts). More frequent authentication is often the right choice for access to critical systems and sensitive areas such as a data center. Less frequent authentication is often the right choice at the network perimeter and for businesses for which the user experience is key.
11. Click **OK** to save the rule.

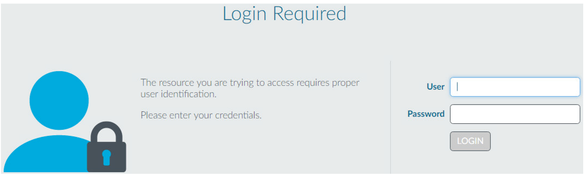
STEP 6 - (**MFA only**) Customize the MFA login page.

The firewall displays this page so that users can authenticate for any additional MFA factors.

STEP 7 - Verify that the firewall enforces Authentication policy.

1. Log in to your network as one of the source users specified in an Authentication policy rule.
2. Request a service or URL category that matches one specified in the rule.

   The firewall displays the Authentication Portal web form for the first authentication factor. For example:



   > If you configured the firewall to use one or more MFA services, authenticate for the additional authentication factors.
3. End the session for the service or URL you just accessed.
4. Start a new session for the same service or application. Be sure to perform this step within the **Timeout** period you configured in the Authentication rule.

   The firewall allows access without re-authenticating.
5. Wait until the **Timeout** period expires and request the same service or application.

   The firewall prompts you to re-authenticate.

STEP 8 - (**Optional**) Redistribute Data and Authentication Timestamps to other firewalls that enforce Authentication policy to ensure they all apply the timeouts consistently for all users.

Previous
Authentication Timestamps
Next
Troubleshoot Authentication Issues