Next-Generation Firewall

Configure Authentication Portal

Previous
Authentication Portal Modes
Next
Configure User Mapping for Terminal Server Users

The following procedure shows how to set up Authentication Portal authentication by configuring the PAN-OS integrated User-ID agent to redirect web requests that match an Authentication Policy rule to a firewall interface (redirect host).

> SSL Inbound Inspection does not support Authentication Portal redirect. To use Authentication Portal redirect and decryption, you must use SSL Forward Proxy.

Based on their sensitivity, the applications that users access through Authentication Portal require different authentication methods and settings. To accommodate all authentication requirements, you can use default and custom authentication enforcement objects. Each object associates an Authentication rule with an authentication profile and an Authentication Portal authentication method.

- **Default authentication enforcement objects**—Use the default objects if you want to associate multiple Authentication rules with the same global authentication profile. You must configure this authentication profile before configuring Authentication Portal, and then assign it in the Authentication Portal Settings. For Authentication rules that require Multi-Factor Authentication (MFA), you cannot use default authentication enforcement objects.
- **Custom authentication enforcement objects**—Use a custom object for each Authentication rule that requires an authentication profile that differs from the global profile. Custom objects are mandatory for Authentication rules that require MFA. To use custom objects, create authentication profiles and assign them to the objects after configuring Authentication Portal—when you Configure Authentication Policy.

Keep in mind that authentication profiles are necessary only if users authenticate through a Authentication Portal Web Form or Kerberos SSO. Alternatively, or in addition to these methods, the following procedure also describes how to implement Client Certificate Authentication.

> If you use Authentication Portal without the other User-ID functions (user mapping and group mapping), you don't need to configure a User-ID agent.

STEP 1 - Configure the interfaces that the firewall will use for incoming web requests, authenticating users, and communicating with directory servers to map usernames to IP addresses.

When the firewall connects to authentication servers or User-ID agents, it uses the management interface by default. As a best practice, isolate your management network by configuring service routes to connect to the authentication servers or User-ID agents.

1. (**MGT interface only**) Select **Device > Setup > Interfaces**, edit the **Management** interface, select **User-ID**, and click **OK**.
2. (**Non-MGT interface only**) Assign an Interface Management Profile to the Layer 3 interface that the firewall will use for incoming web requests and communication with directory servers. You must enable **Response Pages** and **User-ID** in the Interface Management profile.
3. (**Non-MGT interface only**) Configure a service route for the interface that the firewall will use to authenticate users. If the firewall has more than one virtual system (vsys), the service route can be global or vsys-specific. The services must include **LDAP** and potentially the following:
   - **Kerberos**, **RADIUS**, **TACACS+**, or **Multi-Factor Authentication**—Configure a service route for any authentication services that you use.
   - **UID Agent**—Configure this service only if you Enable User- and Group-Based Policy.
4. (**Redirect mode for IPv4 only**) Create a DNS address (A) record that maps the IPv4 address on the Layer 3 interface to the redirect host. If you use Kerberos SSO, you must also add a DNS pointer (PTR) record that performs the same mapping.
5. (**Redirect mode for IPv6 only**) If you want to create a DNS address (AAAA) record that maps the IPv6 address on the Layer 3 interface to the redirect host, use the CLI commands to configure the FQDN of the redirect host.

   > IPv6 is supported for deployments using SAML authentication or LDAP with MFA. Support for these commands is available in PAN-OS version 10.2.9 and 11.2.

   - Enter the debug user-id cp-redirect-host-v6 value <redirect-host-FQDN> CLI command on the firewall (where <redirect-host-FQDN> represents the FQDN of the redirect host that uses IPv6).
   - To view the currently configured IPv6 redirect host, use the debug user-id cp-redirect-host-v6 show CLI command on the firewall.
   - To remove the currently configured IPv6 redirect host, use the debug user-id cp-redirect-host-v6 clear CLI command on the firewall.

   > Depending on whether you configure your redirect host for IPv4, IPv6, or both, make sure to include the necessary IP addresses as DNS attributes in the SAN fields for the certificate or certificates that you configure for the Authentication Portal.

If your network doesn't support access to the directory servers from any firewall interface, you must Configure User Mapping Using the Windows User-ID Agent.

STEP 2 - Make sure Domain Name System (DNS) is configured to resolve your domain controller addresses.

To verify proper resolution, ping the server FQDN. For example:

```
admin@PA-220> ping host dc1.acme.com
```

STEP 3 - Configure clients to trust Authentication Portal certificates.

Required for redirect mode—to transparently redirect users without displaying certificate errors. You can generate a self-signed certificate or import a certificate that an external certificate authority (CA) signed.

To use a self-signed certificate, create a root CA certificate and use it to sign the certificate you will use for Authentication Portal:

1. Select **Device > Certificate Management > Certificates**, then **Device Certificates** (**PAN-OS 11.2 and earlier**) or **Custom Certificates** (**PAN-OS 12.1.0 and later**).
2. Create a Self-Signed Root CA Certificate or import a CA certificate (see Import a Certificate and Private Key).
3. Generate a Certificate to use for Authentication Portal. Be sure to configure the following fields:
   - **Common Name**—Enter the DNS name of the intranet host for the Layer 3 interface.
   - **Signed By**—Select the CA certificate you just created or imported.
   - Certificate Attributes—Click **Add**, for the **Type** select **IP** and, for the **Value**, enter the IP address of the Layer 3 interface to which the firewall will redirect requests.
4. Configure an SSL/TLS Service Profile. Assign the Authentication Portal certificate you just created to the profile.

   > If you don't assign an SSL/TLS Service Profile, the firewall uses TLS 1.2 by default. To use a different TLS version, configure an SSL/TLS Service Profile for the TLS version you want to use.

5. Configure clients to trust the certificate:
   1. Export the CA certificate you created or imported.
   2. Import the certificate as a trusted root CA into all client browsers, either by manually configuring the browser or by adding the certificate to the trusted roots in an Active Directory (AD) Group Policy Object (GPO).

STEP 4 - (**Optional**) Configure Client Certificate Authentication.

> You don't need an authentication profile or sequence for client certificate authentication. If you configure both an authentication profile/sequence and certificate authentication, users must authenticate using both.

1. Use a root CA certificate to generate a client certificate for each user who will authenticate through Authentication Portal. The CA in this case is usually your enterprise CA, not the firewall.
2. Export the CA certificate in PEM format to a system that the firewall can access.
3. Import the CA certificate onto the firewall: see Import a Certificate and Private Key. After the import, click the imported certificate, select **Trusted Root CA**, and click **OK**.
4. Configure a Certificate Profile.
   - In the **Username Field** drop-down, select the certificate field that contains the user identity information.
   - In the **CA Certificates** list, click **Add** and select the CA certificate you just imported.

STEP 5 - (**Optional**) Configure Authentication Portal for the Apple Captive Network Assistant.

This step is only required if you are using Authentication Portal with the Apple Captive Network Assistant (CNA). To use Authentication Portal with CNA, perform the following steps.

1. Verify you have specified an FQDN for the redirect host (not just an IP address).
2. Select an SSL/TLS service profile that uses a publicly-signed certificate for the specified FQDN.
3. Enter the following command to adjust the number of requests supported for Authentication Portal: **`set deviceconfig setting ctd cap-portal-ask-requests <threshold-value>`**

   By default, the firewall has a rate limit threshold for Authentication Portal that limits the number of requests to one request every two seconds. The CNA sends multiple requests that can exceed this limit, which can result in a TCP reset and an error from the CNA. The recommended threshold value is 5 (default is one). This value will allow up to 5 requests every two seconds. Based on your environment, you may need to configure a different value. If the current value is not sufficient to handle the number of requests, increase the value.

STEP 6 - Configure the Authentication Portal settings.

1. Select **Device > User Identification > Authentication Portal Settings** and edit the settings.
2. **Enable Authentication Portal** (default is enabled).
3. Specify the **Timer**, which is the maximum time in minutes that the firewall retains an IP address-to-username mapping for a user after that user authenticates through Authentication Portal (default is 60; range is 1 to 1,440). After the **Timer** expires, the firewall removes the mapping and any associated Authentication Timestamps used to evaluate the **Timeout** in Authentication policy rules.

   > When evaluating the Authentication Portal **Timer** and the **Timeout** value in each Authentication policy rule, the firewall prompts the user to re-authenticate for whichever setting expires first. Upon re-authenticating, the firewall resets the time count for the Authentication Portal **Timer** and records new authentication timestamps for the user. Therefore, to enable different **Timeout** periods for different Authentication rules, set the Authentication Portal **Timer** to a value the same as or higher than any rule **Timeout**.

4. Select the **SSL/TLS Service Profile** you created for redirect requests over TLS. See Configure an SSL/TLS Service Profile.
5. Select the **Mode** (in this example, **Redirect**).
6. (**Redirect mode only**) Specify the **Redirect Host**, which is the intranet hostname (a hostname with no period in its name) that resolves to the IP address of the Layer 3 interface on the firewall to which web requests are redirected.

   If users authenticate through Kerberos single sign-on (SSO), the **Redirect Host** must be the same as the hostname specified in the Kerberos keytab.
7. Select the fall back authentication method to use:
   - To use client certificate authentication, select the **Certificate Profile** you created.
   - To use global settings for interactive or SSO authentication, select the **Authentication Profile** you configured.
   - To use Authentication policy rule-specific settings for interactive or SSO authentication, assign authentication profiles to authentication enforcement objects when you Configure Authentication Policy.
8. Click **OK** and **Commit** the Authentication Portal configuration.

STEP 7 - Next steps...

The firewall does not display the Authentication Portal web form to users until you Configure Authentication Policy rules that trigger authentication when users request services or applications.

Previous
Authentication Portal Modes
Next
Configure User Mapping for Terminal Server Users