HTTP Response Pages and Interactive Blocking

The following topics describe how to configure custom pages to display when the system blocks web requests:

About HTTP Response Pages

As part of access control, you can configure an *HTTP response page* to display when the system blocks web requests, using either access control rules or the access control policy default action.

The response page displayed depends on how you block the session:

- **Block Response Page**: Overrides the default browser or server page that explains that the connection was denied.
- **Interactive Block Response Page**: Warns users, but also allows them to click a button (or refresh the page) to load the originally requested site. Users may have to refresh after bypassing the response page to load page elements that did not load.

If you do not choose a response page, the system blocks sessions without interaction or explanation.

Limitations to HTTP Response Pages

Response Pages are for Access Control Rules/Default Action Only

The system displays a response page only for unencrypted or decrypted HTTP/HTTPS connections blocked (or interactively blocked) either by access control rules or by the access control policy default action. The system does not display a response page for connections blocked by any other policy or mechanism.

Displaying the Response Page Disables Connection Reset

The system cannot display a response page if the connection is reset (RST packet sent). If you enable response pages, the system prioritizes that configuration. Even if you choose **Block with reset** or **Interactive Block with reset** as the rule action, the system displays the response page and does not reset matching web connections. To ensure that blocked web connections reset, you must disable response pages.

Note that all non-web traffic that matches the rule *is* blocked with reset.

No Response Page for Encrypted Connections (Must Decrypt)

The system does not display a response page for encrypted connections blocked by access control rules (or any other configuration). Access control rules evaluate encrypted connections if you did not configure an SSL policy, or your SSL policy passes encrypted traffic.

For example, the system cannot decrypt HTTP/2 or SPDY sessions. If web traffic encrypted using one of these protocols reaches access control rule evaluation, the system does not display a response page if the session is blocked.

However, the system does display a response page for connections decrypted by the SSL policy, then blocked (or interactively blocked) either by access control rules or by the access control policy default action. In these cases, the system encrypts the response page and sends it at the end of the reencrypted SSL stream.

No Response Page for "Promoted" Connections

The system does not display a response page when web traffic is blocked as a result of a promoted access control rule (an early-placed blocking rule with only simple network conditions).

No Response Page for Certain Redirected Connections

If a URL is entered without specifying "http" or "https", and the browser initiates the connection on port 80, and the user clicks through a response page, and the connection is subsequently redirected to port 443, the user will not see a second interactive response page because the response to this URL is already cached.

No Response Page Before URL Identification

The system does not display a response page when web traffic is blocked before the system identifies the requested URL; see Best Practices for URL Filtering.

No Response Page with URL Category for Certain Devices

5506-X and 5508-X devices—whether managed by an FMC or using Adaptive Device Security Manager—do not display a response page if an access control rule using URL categories is matched TLS false start traffic. TLS false start traffic is defined by RFC 7918.

Requirements and Prerequisites for HTTP Response Pages

Model Support

Any

Supported Domains

Any

User Roles

- Admin
- Access Admin

- Network Admin

Choosing HTTP Response Pages

Reliable display of HTTP response pages depends on your network configuration, traffic loads, and size of the page. Smaller pages are more likely to display successfully.

Procedure

Step 1 In the access control policy editor, click **HTTP Responses**.

If the controls are dimmed, settings are inherited from an ancestor policy, or you do not have permission to modify the configuration. If the configuration is unlocked, uncheck **Inherit from base policy** to enable editing.

Step 2 Choose the **Block Response Page** and **Interactive Block Response Page**:

- System-provided—Displays a generic response. Click **View** ( ) to view the code for this page.
- Custom—Create a custom response page. A pop-up window appears, prepopulated with system-provided code that you can replace or modify by clicking **Edit** ( ). A counter shows how many characters you have used.
- None—Disables the response page and blocks sessions without interaction or explanation. To quickly disable interactive blocking for the whole access control policy, choose this option.

Step 3 Click **Save** to save the policy.

What to do next

- Deploy configuration changes; see Deploy Configuration Changes.

Interactive Blocking with HTTP Response Pages

When you configure interactive blocking, users can load an originally requested site after reading a warning. Users may have to refresh after bypassing the response page to load page elements that did not load.

Tip To quickly disable interactive blocking for the whole access control policy, display neither the system-provided page nor a custom page. The system then blocks all connections without interaction.

If a user does not bypass an interactive block, matching traffic is denied without further inspection. If a user bypasses an interactive block, the access control rule allows the traffic, although the traffic may still be subject to deep inspection and blocking.

By default, a user bypass is in effect for 10 minutes (600 seconds) without displaying the warning page on subsequent visits. You can set the duration to as long as a year, or you can force the user to bypass the block every time. This limit applies to every Interactive Block rule in the policy. You cannot set the limit per rule.

Logging options for interactively blocked traffic are identical to those in allowed traffic, but if a user does not bypass the interactive block, the system can log only beginning-of-connection events. When the system initially warns the user, it marks any logged beginning-of-connection event with the `Interactive Block` or `Interactive Block with reset` action. If the user bypasses the block, additional connection events logged for the session have an action of `Allow`.

Configuring Interactive Blocking

Procedure

Step 1 As part of access control, configure an access control rule that matches web traffic; see Create and Edit Access Control Rules:

- Action—Set the rule action to **Interactive Block** or **Interactive Block with reset**; see Access Control Rule Interactive Blocking Actions.
- Conditions—Use URL conditions to specify the web traffic to interactively block; see URL Conditions (URL Filtering).
- Logging—Assume users will bypass the block and choose logging options accordingly; see Logging for Allowed Connections.
- Inspection—Assume users will bypass the block and choose deep inspection options accordingly; see Understanding Access Control.

Step 2 (Optional) On access control policy **HTTP Responses**, choose a custom interactive-block HTTP response page; see Choosing HTTP Response Pages, on page 3.

Step 3 (Optional) On access control policy **Advanced**, change the user bypass timeout; see Setting the User Bypass Timeout for a Blocked Website, on page 4.

After a user bypasses a block, the system allows the user to browse to that page without warning until the timeout period elapses.

Step 4 Save the access control policy.

Step 5 Deploy configuration changes; see Deploy Configuration Changes.

Setting the User Bypass Timeout for a Blocked Website

Procedure

Step 1 Log in to the FMC if you haven't already done so.

Step 2 Click **Policies** > **Access Control** .

Step 3 Click **Edit** ( ).

Step 4 Click **Edit** ( ) next to General Settings.

If **View** ( ) appears instead, settings are inherited from an ancestor policy, or you do not have permission to modify the settings.If the configuration is unlocked, uncheck **Inherit from base policy** to enable editing.

Step 5 In the **Allow an Interactive Block to bypass blocking for (seconds)** field, type the number of seconds that must elapse before the user bypass expires. Setting this value to `0` means the interactive block response is displayed once and the user bypass never expires.

Step 6 Click **OK**.

Step 7 Click **Save** to save the policy.

What to do next

- Deploy configuration changes; see Deploy Configuration Changes.