HTTP 応答ページとインタラクティブ ブロッキング

ここでは、システムが Web 要求をブロックしたときに表示されるカスタム ページの設定方法について説明します。

HTTP 応答ページについて

アクセス制御の一部として、アクセス コントロール ルールあるいはアクセス コントロール ポリシーのデフォルト アクションを使って、システムが Web リクエストをブロックしたときに表示する *HTTP* 応答ページを設定できます。

システム提供の汎用応答ページを選択するか、カスタム HTML を入力できます。表示される応答ページは、セッションのブロック方法によって異なります。

- ブロックまたはリセット付きブロックの場合、ブロックされたセッションはタイムアウトするかリセットされます。**ブロック応答ページ**により、接続が拒否されたことを示すデフォルトのブラウザ ページまたはサーバ ページは上書きされます。
- インタラクティブ ブロックまたはリセット付きインタラクティブ ブロックの場合、システムは**インタラクティブ ブロック応答ページ**を表示してユーザに警告しますが、ユーザはボタンをクリック（あるいはページを更新）して要求したサイトをロードできます。応答ページをバイパスした後、ロードされなかったページの要素をロードするために、ページを更新しなければならない場合があります。

システムが Web トラフィックをブロックしたときに必ず HTTP 応答ページが表示されるわけではありません。HTTP 応答ページの制限 （2 ページ）を参照してください。

HTTP 応答ページの制限

システムがWebトラフィックをブロックする場合に、常に、HTTP応答ページが表示されるわけではありません。

アクセス制御ルール以外の設定

システムは、アクセス制御ルールまたはアクセス制御ルールのデフォルトアクションのいずれかによってブロックされた（またはインタラクティブにブロックされた）暗号化されていない接続または復号された接続の場合にのみ、応答ページを表示します。次の場合には応答ページが表示されません。

- プレフィルタ ポリシーによってブロックされたトンネルおよびその他の接続
- セキュリティ インテリジェンスによってブラックリストに載せられた接続
- SSL ポリシーによってブロックされた暗号化接続

プロモートされたアクセス制御ルール

Webトラフィックがプロモートされたアクセス制御ルール（単純なネットワーク条件のみの早期に適用されたブロッキングルール）の結果としてブロックされている場合、システムは応答ページを表示しません。

URL 識別の前

システムは、システムが要求されたURLを識別する前にトラフィックがブロックされた場合は、応答ページを表示しません。URLフィルタリングのガイドラインと制限事項を参照してください。

暗号化されたトラフィック

システムは、SSLポリシーによって復号された後に、アクセス制御ルールまたはアクセス制御ルールのデフォルトアクションのいずれかによってブロックされた（またはインタラクティブにブロックされた）接続の場合に、応答ページを表示します。このような場合、システムは応答ページを暗号化して、再暗号化されたSSLストリームの最後にそれを送信します。

ただし、アクセス制御ルール（または、その他の設定）によってブロックされている暗号化された接続の場合、システムは応答ページを表示しません。アクセス制御ルールはSSLポリシーを設定しなかった場合に暗号化された接続を評価し、それ以外の場合は、SSLポリシーが暗号化されたトラフィックを受け渡します。

たとえば、システムはHTTP/2またはSPDYセッションを復号できません。これらのプロトコルのいずれかを使用して暗号化されたWebトラフィックがアクセス制御ルールの評価に達したが、セッションがブロックされている場合、システムは応答ページを表示しません。

HTTP 応答ページの選択

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス
任意（Any）	任意（Any）	任意（Any）	任意（Any）	Admin/Access Admin/Network Admin

HTTP応答ページを確実に表示できるかは、ネットワーク設定、トラフィック負荷、およびページのサイズによって異なります。ページが小さいほど、正常に表示される傾向にあります。

手順

ステップ 1 アクセス コントロール ポリシーのエディタで、[HTTP 応答（HTTP Responses）] タブをクリックします。

コントロールが淡色表示されている場合、設定は先祖ポリシーから継承され、設定を変更する権限がありません。設定がロック解除されている場合は、[ベース ポリシーから継承する（Inherit from base policy）] をオフにして、編集を有効にします。

ステップ 2 [応答ページをブロック（Block Response Page）] および [応答ページのインタラクティブ ブロック（Interactive Block Response Page）] を選択します。

- [System-provided]：一般的な応答が表示されます。表示アイコン（  ）をクリックすると、このページのコードが表示されます。
- [Custom]：カスタム応答ページが作成されます。ポップアップ ウィンドウが表示されます。このウィンドウに事前入力されているシステムによって提供されるコードを編集アイコン（  ）をクリックして置換または変更できます。カウンタで使用した文字数が表示されます。
- [None]：応答ページを無効にして、インタラクションや説明なしでセッションをブロックします。アクセス コントロール ポリシー全体でインタラクティブ ブロッキングを無効にするには、このオプションを選択します。

ステップ 3 [保存（Save）] をクリックしてポリシーを保存します。

次のタスク

- 設定変更を展開します。設定変更の展開を参照してください。

HTTP 応答ページでのインタラクティブ ブロッキング

インタラクティブブロッキングを設定すると、ユーザは警告を読んだ後に当初要求したサイトを読み込むことができます。応答ページをバイパスした後、ロードされなかったページの要素をロードするために、ページを最新表示しなければならない場合があります。

ヒント アクセス コントロール ポリシー全体に対してインタラクティブ ブロッキングを素早く無効にするには、システム提供のページもカスタムページも表示しないでください。そうすると、システムにより操作なしですべての接続がブロックされます。

ユーザがインタラクティブ ブロックをバイパスしない場合、一致するトラフィックは拒否され、追加のインスペクションは行われません。ユーザがインタラクティブブロックをバイパスするとアクセス コントロール ルールはトラフィックを許可しますが、引き続きトラフィックはディープ インスペクションやブロッキングの対象となる場合があります。

デフォルトでは、ユーザのバイパスは後続のアクセスで警告ページを表示することなく、10分（600 秒）間有効です。期間を 1 年に設定したり、ユーザに毎回ブロックをバイパスするように強制できます。この制限は、ポリシー内のすべてのインタラクティブ ブロック ルールに適用されます。ルールごとに制限を設定することはできません。

インタラクティブ ブロックされるトラフィックに関するロギング オプションは、許可されたトラフィックに関するオプションと同じですが、ユーザがインタラクティブブロックをバイパスしない場合、システムがログに記録できるのは接続開始イベントだけです。システムが最初にユーザに警告すると、ロギングされた接続開始イベントはシステムにより [インタラクティブ ブロック（Interactive Block）] または [リセットしてインタラクティブ ブロック（Interactive Block with reset）] アクションでマークされます。ユーザがブロックをバイパスすると、セッションが記録される追加の接続イベントに [許可（Allow）] アクションが付きます。

インタラクティブ ブロッキングの設定

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス
任意（Any）	任意（Any）	任意（Any）	任意（Any）	Admin Access Admin Network Admin

手順

ステップ 1 アクセス コントロールの一部として、Web トラフィックと一致するアクセス コントロール ルールを設定します。アクセス コントロール ルールの作成および編集を参照してください。

- アクション：ルール アクションを [インタラクティブ ブロック（Interactive Block）]、または [リセットしてインタラクティブ ブロック（Interactive Block with reset）] に設定します。アクセス コントロール ルール インタラクティブ ブロック アクションを参照してください。
- 条件：URL 条件を使用して、インタラクティブにブロックする Web トラフィックを指定します。URL 条件（URL フィルタリング）を参照してください。
- ロギング：ユーザがブロックをバイパスすると想定し、それに応じてロギング オプションを選択します。許可された接続のロギングを参照してください。
- インスペクション：ユーザがブロックをバイパスすると想定し、それに応じてディープ インスペクション オプションを選択します。侵入ポリシーとファイル ポリシーを使用したアクセス制御を参照してください。

ステップ 2 （オプション）アクセス コントロール ポリシーの [HTTP 応答（HTTP Responses）] タブで、カスタム インタラクティブ ブロックの HTTP 応答ページを選択します。HTTP 応答ページの選択 （3 ページ）を参照してください。

ステップ 3 （オプション）アクセス コントロール ポリシーの [詳細（Advanced）] タブで、ユーザのバイパス タイムアウトを変更します。ブロックされた Web サイトのユーザ バイパス タイムアウトの設定 （5 ページ）を参照してください。

ユーザはブロックをバイパスした後、そのページを参照でき、タイムアウト期間が経過するまで警告は表示されません。

ステップ 4 アクセス コントロール ポリシーを保存します。

ステップ 5 設定変更を展開します。設定変更の展開を参照してください。

ブロックされた Web サイトのユーザ バイパス タイムアウトの設定

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス
任意（Any）	任意（Any）	任意（Any）	任意（Any）	Admin/Access Admin/Network Admin

手順

ステップ 1 アクセス コントロール ポリシー エディタで、[詳細（Advanced）] タブをクリックします。

ステップ 2 [全般設定（General Settings）] の横にある編集アイコン（  ）をクリックします。

代わりに表示アイコン（  ）が表示される場合、設定は先祖ポリシーから継承され、設定を変更する権限がありません。設定がロック解除されている場合は、[ベース ポリシーから継承する（Inherit from base policy）] をオフにして、編集を有効にします。

ステップ 3 [ブロックをバイパスするためのインタラクティブ ブロックを許可する期間（秒）（Allow an Interactive Block to bypass blocking for (seconds)）] フィールドに、ユーザ バイパスの期限が切れるまでの経過時間を秒数で入力します。ゼロを指定すると、ユーザはブロックを毎回強制的にバイパスします。

ステップ 4 [OK] をクリックします。

ステップ 5 [保存（Save）] をクリックしてポリシーを保存します。

次のタスク

- 設定変更を展開します。設定変更の展開を参照してください。