HTTP 응답 페이지 및 인터랙티브 차단

다음 주제에서는 시스템에서 웹 요청을 차단할 때 표시할 맞춤형 페이지를 구성하는 방법을 설명합니다.

HTTP 응답 페이지 정보

액세스 제어의 일환으로 액세스 제어 규칙 또는 액세스 제어 정책 기본 작업을 사용하여 시스템이 웹 요청을 차단할 때 표시할 *HTTP* 응답 페이지를 구성할 수 있습니다.

표시되는 응답 페이지는 세션을 차단하는 방법에 따라 달라집니다.

- 응답 페이지 차단: 연결이 거부되었음을 설명하는 기본 브라우저 또는 서버 페이지를 재정의합니다.
- 응답 페이지 인터랙티브 차단: 사용자에게 경고하지만 사용자가 버튼을 클릭하거나 페이지를 새로 고쳐 원래 요청한 사이트를 로드하도록 허용합니다. 사용자는 로드하지 않은 페이지 요소를 로드하기 위해 응답 페이지를 우회한 후 새로 고침해야 할 수 있습니다.

응답 페이지를 선택하지 않으면 상호작용 또는 설명 없이 세션이 차단됩니다.

HTTP 대응 페이지의 제한

응답 페이지는 액세스 제어 규칙/기본 작업에 한정

시스템은 액세스 제어 규칙 또는 액세스 제어 정책 기본 작업을 통해 차단되거나 인터랙티브 차단된 암호화되지 않은 연결 또는 암호 해독된 연결에 대해서만 응답 페이지를 표시합니다. 다른 정책 또는 메커니즘에 의해 차단되거나 차단 목록에 추가된 연결에 대한 응답 페이지는 표시되지 않습니다.

응답 페이지를 표시하면 연결 재설정 비활성화

연결이 재설정되면 시스템이 응답 페이지를 표시할 수 없습니다(RST 패킷 전송). 응답 페이지를 활성화하면 시스템은 해당 구성에 우선 순위를 둡니다. **Block with reset(**차단 후 재설정**)** 또는 **Interactive Block with reset(**인터랙티브 차단 후 재설정**)**을 규칙 작업으로 선택하는 경우, 시스템은 응답 페이지를 표시하고 일치하는 웹 연결을 재설정하지 않습니다. 차단된 해당 웹 연결을 재설정하려면 응답 페이지를 비활성화해야 합니다.

규칙과 일치하는 모든 비 웹 트래픽은 차단 후 재설정됩니다.

암호화된 연결의 응답 페이지 없음

시스템은 세션이 암호화되어 있거나 암호화되었던 경우 응답 페이지를 표시하지 않습니다.

'승격된' 연결의 응답 페이지 없음

승격된 액세스 제어 규칙(단순한 네트워크 조건만 사용하여 초기에 배치된 차단 규칙)으로 인해 웹 트래픽이 차단될 때는 시스템에서 응답 페이지를 표시하지 않습니다.

리디렉트된 특정 연결의 응답 페이지 없음

'http' 또는 'https'를 지정하지 않고 URL을 입력했으며, 브라우저가 포트 80에서 연결을 시작했고, 사용자가 응답 페이지를 클릭하고, 이후 연결이 포트 443으로 리디렉트된다면, 사용자는 두 번째 인터랙티브 페이지를 볼 수 없습니다. 이 URL에 대한 응답이 이미 캐시되었기 때문입니다.

URL 식별 전 응답 페이지 없음

시스템에서 요청된 URL을 식별하기 전에 웹 트래픽이 차단되면 시스템은 응답 페이지를 표시하지 않습니다. URL 필터링 모범 사례를 참조하십시오.

특정 디바이스에 대한 **URL** 범주가 있는 응답 페이지 없음

5506-X 및 5508-X 디바이스(FMC에서 관리하든 Adaptive Device Security Manager를 사용하든 상관없음)는 URL 범주를 사용하는 액세스 제어 규칙이 TLS 거짓 시작 트래픽과 일치하는 경우 응답 페이지를 표시하지 않습니다. TLS 거짓 시작 트래픽은 RFC 7918에 의해 정의됩니다.

HTTP 응답 페이지 요구 사항 및 사전 요건

모델 지원

Any(모든 상태)

지원되는 도메인

모든

사용자 역할

- 관리자
- 액세스 관리자
- Network Admin(네트워크 관리자)

HTTP 응답 페이지 선택

HTTP 응답 페이지의 안정적 표시 여부는 네트워크 구성, 트래픽 로드, 페이지 크기에 따라 달라집니다. 페이지 크기가 작을수록 성공적으로 표시될 가능성이 높습니다.

프로시저

단계 **1** 액세스 제어 정책 편집기에서 **HTTP Responses(HTTP** 응답**)**를 클릭합니다.

컨트롤이 흐리게 표시되는 경우에는 상위 정책에서 설정이 상속되거나 컨피그레이션을 수정할 권한이 없는 것입니다. 구성이 잠금 해제되어 있으면 **Inherit from base policy(**기본 정책에서 상속**)**의 선택을 취소하여 수정을 활성화합니다.

단계 **2** **Block Response Page(**차단 응답 페이지**)** 및 **Interactive Block Resposne Page(**인터랙티브 차단 응답 페이지**)**를 선택합니다.

- System-provided(시스템 제공) - 일반 응답을 표시합니다. 보기 ( )를 클릭하면 이 페이지의 코드를 확인할 수 있습니다.
- Custom(맞춤형) - 맞춤형 응답 페이지를 생성합니다. 수정( )을 클릭하면 교체 또는 수정할 수 있는 시스템 제공 코드가 미리 채워진 팝업 창이 나타납니다. 사용한 문자 수가 카운터에 표시됩니다.
- None(없음) - 응답 페이지를 비활성화하고 상호작용 또는 설명 없이 세션을 차단합니다. 전체 액세스 제어 정책에서 인터랙티브 차단을 빠르게 비활성화하려면 이 옵션을 선택하십시오.

단계 **3** **Save**를 클릭하여 정책을 저장합니다.

다음에 수행할 작업

- 구성 변경사항을 구축합니다. 컨피그레이션 변경 사항 구축의 내용을 참조하십시오.

HTTP 응답 페이지를 사용한 인터랙티브 차단

인터랙티브 차단을 설정하면 사용자는 경고를 읽은 후 원래 요청된 사이트를 로드할 수 있습니다. 사용자는 로드하지 않은 페이지 요소를 로드하기 위해 응답 페이지를 우회한 후 새로 고침해야 할 수 있습니다.

팁 전체 액세스 제어 정책에서 인터랙티브 차단을 빠르게 비활성화하려면 시스템 제공 페이지나 맞춤형 페이지를 표시하지 마십시오. 그러면 시스템은 상호작용 없이 모든 연결을 차단합니다.

사용자가 인터랙티브 차단을 우회하지 않는 경우, 일치하는 트래픽은 추가 검사 없이 거부됩니다. 사용자가 인터랙티브 차단을 우회하는 경우, 액세스 제어 규칙은 트래픽을 허용하지만 해당 트래픽은 계속 심층 검사 및 차단 대상이 될 수 있습니다.

기본적으로 사용자 우회는 후속 방문 시 경고 페이지 표시 없이 10분(600초) 동안 유효합니다. 이 기간은 최대 1년까지 설정할 수 있으며, 사용자가 매번 차단을 강제로 우회하도록 할 수도 있습니다. 이러한 제한은 정책에서 모든 Interactive Block(인터랙티브 차단) 규칙을 적용합니다. 규칙별 제한은 설정할 수 없습니다.

인터랙티브 차단된 트래픽에 대한 로깅 옵션은 허용된 트래픽의 옵션과 동일하지만 사용자가 인터랙티브 차단을 우회하지 않는 경우, 시스템은 연결 시작 이벤트만 로깅할 수 있습니다. 시스템은 사용자에게 처음 경고할 때 인터랙티브 차단 또는 인터랙티브 차단 후 재설정 작업과 함께 로깅된 모든 연결 시작 이벤트를 표시합니다. 사용자가 차단을 우회하는 경우, 세션에 대해 로깅된 추가 연결 이벤트에는 `Allow(허용)` 작업이 있습니다.

인터랙티브 차단 설정

프로시저

단계 **1** 액세스 제어의 일부로 웹 트래픽과 일치하는 액세스 제어 규칙을 구성하십시오. 액세스 제어 규칙 생성 및 수정의 내용을 참조하십시오.

- 작업 - 규칙 작업을 **Interactive Block(**인터랙티브 차단**)** 또는 **Interactive Block with reset(**인터랙티브 차단 후 재설정**)**으로 설정하십시오. 액세스 제어 규칙 인터랙티브 차단 작업의 내용을 참조하십시오.
- 조건 - URL 조건을 사용하여 인터랙티브 차단할 웹 트래픽을 지정합니다. URL 조건(URL 필터링)의 내용을 참조하십시오.
- 로깅 - 사용자가 차단을 우회할 것이라고 가정하고 그에 따라 로깅 옵션을 선택합니다. 허용된 연결에 대한 로깅의 내용을 참조하십시오.
- 검사 - 사용자가 차단을 우회할 것이라고 가정하고 그에 따라 심층 검사 옵션을 선택합니다. 액세스 제어의 이해의 내용을 참조하십시오.

단계 **2** (선택 사항) 액세스 제어 정책 **HTTP Responses(HTTP** 응답**)**에서 맞춤형 인터랙티브 차단 HTTP 응답 페이지를 선택합니다. HTTP 응답 페이지 선택, 3 페이지의 내용을 참조하십시오.

단계 **3** (선택 사항) 액세스 제어 정책 **Advanced(**고급**)**에서 사용자 우회 시간 제한을 변경합니다. 차단된 웹사이트의 사용자 우회 시간 제한 설정, 5 페이지의 내용을 참조하십시오.

사용자가 차단을 우회한 후 시스템은 시간 제한 기간이 경과할 때까지 사용자가 해당 페이지를 탐색하는 것을 경고 없이 허용합니다.

단계 **4** 액세스 제어 정책을 저장합니다.

단계 **5** 구성 변경사항을 구축합니다. 컨피그레이션 변경 사항 구축의 내용을 참조하십시오.

차단된 웹사이트의 사용자 우회 시간 제한 설정

프로시저

단계 **1** 액세스 제어 정책 편집기에서 **Advanced(**고급**)**를 클릭합니다.

단계 **2** General Settings(일반 설정) 옆의 수정( )을 클릭합니다.

보기 아이콘(보기 ( ))이 대신 표시되는 경우에는 설정이 상위 정책에서 상속되거나 설정을 수정할 권한이 없는 것입니다.구성이 잠금 해제되어 있으면 **Inherit from base policy(**기본 정책에서 상속**)**의 선택을 취소하여 수정을 활성화합니다.

단계 **3** **Allow an Interactive Block to bypass blocking for (seconds)((**초**)** 동안 차단 우회를 위한 인터랙티브 차단 허용**)** 필드에 사용자 우회가 만료되기 전에 경과해야 하는 시간(초)을 입력합니다. 0을 지정하면 사용자가 매번 차단을 강제로 우회하도록 합니다.

단계 **4** **OK(**확인**)**를 클릭합니다.

단계 **5** **Save**를 클릭하여 정책을 저장합니다.

다음에 수행할 작업

- 구성 변경사항을 구축합니다. 컨피그레이션 변경 사항 구축의 내용을 참조하십시오.