캡티브 포털을 사용하여 사용자 제어

캡티브 포털 ID 소스

캡티브 포털(captive portal)은 Firepower System에서 지원하는 권한 있는 ID 소스 중 하나입니다. 이는 관리되는 디바이스를 사용해 네트워크에서 사용자가 인증하는 액티브 인증 방법입니다.

인터넷 또는 제한적 리소스에 액세스하기 위한 인증을 요구하기 위해 캡티브 포털을 사용합니다. 선택적으로 리소스에 게스트 액세스를 설정할 수 있습니다. 시스템이 캡티브 포털 사용자를 인증하면 액세스 제어 규칙에 따라 사용자 트래픽을 처리합니다. 캡티브 포털은 HTTP와 HTTPS 트래픽에 한해 인증을 수행합니다.

참고 캡티브 포털이 인증을 수행할 수 있기 전에 HTTPS 트래픽의 암호를 해독해야 합니다.

캡티브 포털(captive portal)은 실패한 인증 시도도 기록합니다. 실패한 시도는 데이터베이스의 사용자 목록에 새 사용자를 추가하지 않습니다. 캡티브 포털(captive portal)에서 보고하는 실패한 인증 활동의 사용자 활동 유형은 **Failed Auth User(**실패한 인증 사용자**)**입니다.

캡티브 포털(captive portal)에서 수집한 인증 데이터는 사용자 인식 및 사용자 제어에 사용할 수 있습니다.

관련 항목

사용자 제어에 대한 캡티브 포털 설정 방법, 4 페이지

캡티브 포털 라이선스 요구 사항

FTD 라이센스

Any(모든 상태)

기본 라이선스

제어

캡티브 포털 요구 사항 및 사전 요건

모델 지원

NGIPSv를 제외한 모두

지원되는 도메인

모든

사용자 역할

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

캡티브 포털 가이드라인 및 제한 사항

ID 정책에서 캡티브 포털(captive portal)을 구성 및 구축할 경우, 지정된 영역의 사용자는 다음 디바이스를 통해 네트워크에 대한 액세스를 인증합니다.

- 7000 및 8000 Series 디바이스의 가상 라우터
- 버전 9.5(2) 이상을 실행하는 라우팅 모드의 ASA FirePOWER 디바이스
- 라우팅 모드의 Firepower Threat Defense 디바이스

참고 원격 액세스 VPN 사용자가 보안 게이트웨이로 작동하는 매니지드 디바이스를 통해 이미 활성으로 인증된 경우에는 ID 정책에 구성되어 있더라도 캡티브 포털(captive portal) 액티브 인증이 이루어지지 않습니다.

라우팅 인터페이스 필요

캡티브 포털(captive portal) 액티브 인증은 라우팅 인터페이스가 구성된 디바이스에서만 수행할 수 있습니다.

액세스 제어 정책에서 참조한 ID 정책에 하나 이상의 캡티브 포털(captive portal) ID 규칙이 포함되어 있고 다음을 관리하는 Firepower Management Center에서 정책을 구축할 경우:

- 라우팅 인터페이스가 구성된 하나 이상의 디바이스 - 정책 구축에 성공하고 라우팅 인터페이스가 액티브 인증을 수행합니다.

  시스템은 ASA with FirePOWER 디바이스에서 인터페이스의 유형을 검증하지 않습니다. ASA with FirePOWER 디바이스에서 인라인(탭 모드) 인터페이스에 캡티브 포털 정책을 적용하면 정책 구축은 성공하지만 해당 규칙과 일치하는 트래픽의 사용자는 Unknown(알 수 없음)으로 식별됩니다.

- 하나 이상의 NGIPSv 디바이스 - 정책 구축에 실패합니다.

캡티브 포털 및 정책

ID 정책에서 캡티브 포털(captive portal)을 구성하고 ID 규칙에서 액티브 인증을 호출합니다. ID 정책은 액세스 컨트롤 정책과 연결됩니다.

액세스 컨트롤 정책의 **Active Authentication(**액티브 인증**)** 탭 페이지에서 캡티브 포털 ID 정책 일부를 설정하고 액세스 컨트롤 정책과 연결된 ID 규칙에서 나머지를 설정할 수 있습니다.

주의 SSL 암호 해독이 비활성화되어 있을 때(액세스 컨트롤 정책에 SSL 정책이 포함되지 않을 때) 첫 번째 액티브 인증을 추가하거나 마지막 액티브 인증을 제거함 컨피그레이션 변경 사항을 구축할 때 Snort 프로세스가 재시작되므로 트래픽 검사가 일시적으로 중단됩니다. 이 중단 기간 동안 트래픽이 삭제되는지 아니면 추가 검사 없이 통과되는지는 대상 디바이스가 트래픽을 처리하는 방법에 따라 달라집니다. 자세한 내용은 Snort® 재시작 트래픽 동작을 참고하십시오.

캡티브 포털 요건 및 제한 사항

다음 요건 및 제한 사항을 참고하십시오.

- 시스템은 초당 최대 20개의 캡티브 포털(captive portal) 로그인을 지원합니다.
- 실패한 로그인 시도가 최대 로그인 시도 횟수에 적용될 때, 실패한 로그인 시도 사이에는 최대 5분의 제한이 적용됩니다. 5분 제한은 사용자가 설정할 수 없습니다.

  (최대 로그인 시도는 연결 이벤트: **Analysis(**분석**)** > **Connections(**연결**)** > **Events(**이벤트**)**에 표시됩니다.)

  실패한 로그인 사이의 경과 시간을 5분을 초과하는 경우 사용자는 인증을 위해 캡티브 포털로 재전송되며, 실패한 로그인 사용자나 게스트 사용자로 지정하지 않고, Firepower Management Center에 보고되지 않습니다.

- 캡티브 포털은 TLS v1.0 연결을 협상하지 않습니다.

TLS v1.1 및 v1.2 연결만 지원됩니다.

- 사용자 로그아웃을 확인하는 유일한 방법은 브라우저를 닫고 다시 여는 것입니다. 그러지 않으면, 경우에 따라 사용자가 캡티브 포털에서 로그아웃한 다음 같은 브라우저를 이용해 다시 인증하지 않고도 네트워크에 액세스할 수 있습니다.
- 영역이 상위 도메인에 대해 생성되었고 매니지드 디바이스가 해당 상위 도메인의 하위 도메인에 대한 로그인을 탐지했다면, 사용자의 이후 로그아웃은 매니지드 디바이스가 탐지하지 않습니다.
- 캡티브 포털(captive portal)에 ASA FirePOWER 디바이스를 사용하려는 경우(ASA 버전 9.5(2) 이상을 실행하는 라우팅 모드에서), **captive-portal** ASA CLI 명령을 사용하여 액티브 인증을 위한 캡티브 포털(captive portal)을 활성화하고 *ASA Firewall* 설정 가이드(버전 9.5(2) 이상): https://www.cisco.com/c/en/us/support/security/adaptive-security-appliance-asa-software/products-installation-and-configuration-guides-list.html에 설명된 대로 포트를 정의합니다.
- 캡티브 포털에 사용할 디바이스의 IP 주소 및 포트를 대상으로 하는 트래픽을 허용해야 합니다.
- HTTPS 트래픽에 대한 캡티브 포털(captive portal) 액티브 인증을 수행하려면, SSL 정책을 사용하여 인증하려는 사용자의 트래픽을 암호 해독해야 합니다. 매니지드 디바이스에서 캡티브 포털(captive portal) 사용자의 웹 브라우저와 캡티브 포털(captive portal) 데몬 간의 연결에서 트래픽을 암호 해독할 수 없습니다. 이 연결은 캡티브 포털(captive portal) 사용자를 인증하는 데 사용됩니다.
- 매니지드 디바이스를 통해 허용되는 비 HTTP 또는 HTTPS 트래픽의 양을 제한하려면 ID 정책의 **Ports(포트)** 탭 페이지에 일반적인 HTTP 및 HTTPS 포트를 입력해야 합니다.

  매니지드 디바이스는 수신하는 요청이 HTTP 또는 HTTPS 프로토콜을 사용하지 않는다고 판단하면 이전에 확인하지 않은 사용자를 **Pending(보류 중)**에서 **Unknown(알 수 없음)**으로 변경합니다. 매니지드 디바이스가 사용자를 **Pending(보류 중)**에서 다른 상태로 변경하면, 액세스 컨트롤과 서비스 품질 및 SSL 정책이 해당 트래픽에 적용될 수 있습니다. 다른 정책이 비 HTTP 또는 HTTPS 트래픽을 허용하지 않는다면, 캡티브 포털 ID 정책에 대한 포트 설정으로 원치 않는 트래픽이 매니지드 디바이스를 통해 허용되는 일을 방지할 수 있습니다.

사용자 제어에 대한 캡티브 포털 설정 방법

캡티브 포털로 사용자 활동을 제어하는 방법 개요:

시작하기 전에

캡티브 포털을 액티브 인증에 활용하려면, 액세스 컨트롤 정책과 ID 정책, SSL 정책을 설정하고 ID와 SSL 정책을 액세스 컨트롤 정책에 연결해야 합니다. 마지막으로, 사용자는 정책을 매니지드 디바이스에 구축해야 합니다. 이 주제는 이러한 작업에 대한 개략적인 정보를 제공합니다.

전체 절차 예시는 캡티브 포털 설정 1부: ID 정책 생성, 6 페이지에서부터 시작합니다.

먼저 다음 작업을 수행하십시오.

- 라우팅 인터페이스가 구성된 하나 이상의 디바이스를 Firepower Management Center에서 관리하는지 확인합니다.

  특히 Firepower Management Center가 FirePOWER 디바이스를 이용해 ASA를 관리한다면, 캡티브 포털 가이드라인 및 제한 사항, 2 페이지을(를) 반드시 참조하십시오.

- 암호화된 인증을 캡티브 포털과 함께 사용하려면 PKI 개체를 만들거나, 액세스하는 Firepower Management Center의 장치에서 인증서 데이터와 키를 사용할 수 있게 해야 합니다. PKI 개체를 생성하는 방법은 PKI 개체 섹션을 참조하십시오.

프로시저

단계 **1** 다음 주제에서 설명하는 방법에 따라 영역을 생성하고 활성화합니다.

- 영역 디렉터리 설정
- 사용자 및 그룹 다운로드

단계 **2** 캡티브 포털에 대한 액티브 인증 ID 정책을 생성합니다.

ID 정책을 이용하면 영역에 있는 선택된 사용자는 캡티브 포털로 인증 후 리소스에 액세스할 수 있습니다.

자세한 내용은 캡티브 포털 설정 1부: ID 정책 생성, 6 페이지를 참고하십시오.

단계 **3** 캡티브 포털 포트(기본적으로 TCP 885)의 트래픽을 허용하는, 캡티브 포털에 대한 액세스 컨트롤 규칙을 설정합니다.

캡티브 포털이 사용할 수 있는 모든 TCP 포트를 선택할 수 있습니다. 어떤 포트를 선택하든, 해당 포트에서의 트래픽을 허용하는 규칙을 생성해야 합니다.

자세한 내용은 캡티브 포털 2부 설정: TCP 포트 액세스 컨트롤 규칙 생성, 8 페이지를 참고하십시오.

단계 **4** 다른 액세스 컨트롤 규칙을 추가해 선택한 영역의 사용자가 캡티브 포털을 이용해 리소스에 액세스하게 합니다.

이렇게 하면 사용자는 캡티브 포털을 이용해 인증할 수 있습니다.

자세한 내용은 캡티브 포털 설정 3부: 사용자 액세스 컨트롤 규칙 생성, 9 페이지를 참고하십시오.

단계 **5** SSL 암호 해독 설정 - 캡티브 포털 사용자가 HTTPS 프로토콜을 이용해 웹 페이지에 액세스할 수 있도록 **Unknown(**알 수 없는**)** 사용자에 대한 정책을 재서명합니다.

캡티브 포털은 먼저 HTTPS 트래픽이 해독된 후 캡티브 포털로 전송된 경우에만 사용자를 인증할 수 있습니다. 캡티브 포털은 시스템이 **Unknown(**알 수 없는**)** 사용자로 인식합니다.

자세한 내용은 캡티브 포털 설정 4부: SSL 암호 해독 생성-정책 재서명, 10 페이지를 참고하십시오.

단계 **6** ID 및 SSL p정책을 2단계의 액세스 컨트롤 정책에 연결합니다.

이 마지막 단계는 시스템이 캡티브 포털을 이용해 인증하게 합니다.

자세한 내용은 캡티브 포털 설정 5부: ID 및 SSL 정책과 액세스 컨트롤 정책 연결, 11 페이지를 참고하십시오.

다음에 수행할 작업

캡티브 포털 설정 1부: ID 정책 생성, 6 페이지의 내용을 참조하십시오.

관련 항목

- 캡티브 포털에서 애플리케이션 제외, 13 페이지
- PKI 개체
- 캡티브 포털(captive portal) ID 소스 문제 해결, 14 페이지
- Snort® 재시작 시나리오

캡티브 포털 설정 1부: ID 정책 생성

시작하기 전에

이 5단계 절차는 캡티브 포털과 SSL 암호화 모두에 대해 기본 TCP 포트 885와 Firepower Management Center 서버 인증서를 사용해 캡티브 포털을 설정하는 방법을 보여줍니다. 이 예시의 각 단계는 액티브 인증 수행을 위해 캡티브 포털을 활성화하는 데 필요한 작업을 하나씩 설명합니다.

이 절차의 모든 단계를 수행하면, 도메인에 있는 사용자를 위해 작동하도록 캡티브 포털을 설정할 수 있습니다. 원한다면 절차의 각 단계에서 설명하는 추가 작업을 수행할 수도 있습니다.

전체 절차의 개요는 사용자 제어에 대한 캡티브 포털 설정 방법, 4 페이지에서 확인할 수 있습니다.

프로시저

단계 **1** 아직 하지 않았다면 Firepower Management Center에 로그인합니다.

단계 **2** **Policies(**정책**)** > **Access Control(**액세스 컨트롤**)** > **Identity(ID)**를 클릭하고 ID 정책을 만들거나 편집합니다.

단계 **3** (선택 사항). **Add Category(**카테고리 추가**)**를 클릭해 캡티브 포털 ID 규칙의 카테고리를 추가하고 카테고리의 **Name(**이름**)**을 입력합니다.

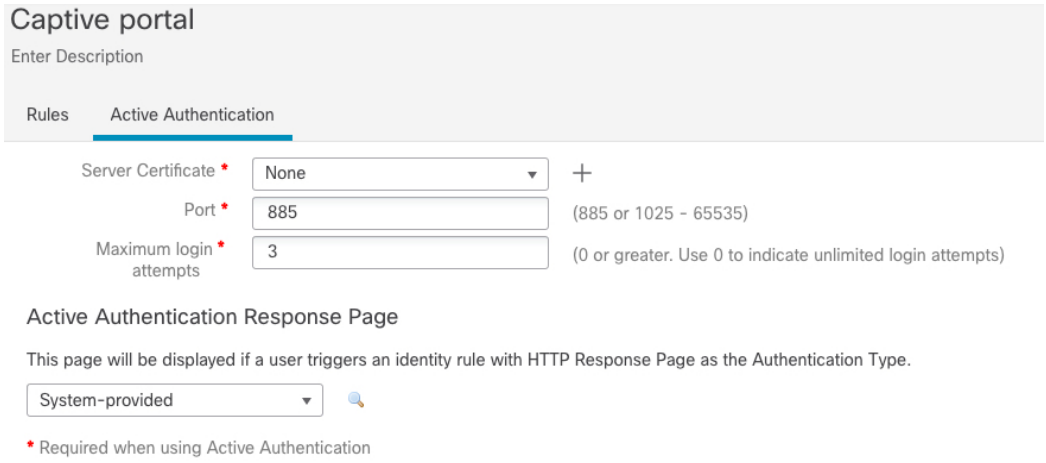
단계 **4** **Active Authentication(**활성 인증**)**을 클릭합니다.

단계 **5** 목록에서 적절한 **Server Certificate(**서버 인증서**)**를 선택하거나 추가(+)를 클릭하여 인증서를 추가합니다.

참고 캡티브 포털은 DSA(Digital Signature Algorithm) 또는 ECDSA(Elliptic Curve Digital Signature Algorithm) 인증서 사용을 지원하지 않습니다.

단계 **6** **885**을(를) **Port(**포트**)** 필드에 입력하고 **Maximum login attempts(**최도 로그인 시도 횟수**)**를 지정합니다.

단계 7 (선택 사항). 캡티브 포털(captive portal) 필드, 12 페이지에 설명된 대로 **Active Authentication Response Page(**액티브 인증 응답 페이지**)**를 선택합니다.
다음 그림은 예를 보여줍니다.



단계 8 **Save(**저장**)**를 클릭합니다.

단계 9 **Rules(**규칙**)**를 클릭합니다.

단계 10 **Add Rule(**규칙 추가**)**를 클릭하여 새 캡티브 포털 ID 정책 규칙을 추가하거나 수정( )을 클릭하여 기존 규칙을 편집합니다.

단계 11 규칙의 **Name(**이름**)**을 입력합니다.

단계 12 **Action(**작업**)** 목록에서 **Active Authentication(**액티브 인증**)**을 선택합니다.

시스템은 HTTP 및 HTTPS 트래픽에서만 캡티브 포털 액티브 인증을 시행할 수 있습니다. ID 규칙 **Action(**작업**)**이 **Active Authentication(**액티브 인증**)**(사용자가 캡티브 포털을 이용 중임)이거나, 사용자가 패시브 인증을 이용하며 **Realms & Settings(**영역 및 설정**)** 페이지에서 **Use active authentication if passive or VPN identity cannot be established(**패시브 또는 **VPN ID**를 설정할 수 없다면 액티브 인증 사용**)**에 대한 옵션을 선택했다면 TCP 포트 제약 조건만 사용합니다.

단계 13 **Realm & Settings(**영역 및 설정**)**를 클릭합니다.

단계 14 **Realms(**영역**)** 목록에서 사용자 인증에 사용할 영역을 선택합니다.

단계 15 (선택 사항). **Identify as Guest if authentication cannot identify user(**인증이 사용자를 식별할 수 없는 경우 게스트로 식별**)**를 선택합니다. 자세한 내용은 캡티브 포털(captive portal) 필드, 12 페이지를 참고하십시오.

단계 16 목록에서 **Authentication Protocol(**인증 프로토콜**)**을 선택합니다.

단계 17 (선택 사항). 특정 애플리케이션 트래픽을 캡티브 포털에서 제외하는 방법은 캡티브 포털에서 애플리케이션 제외, 13 페이지 섹션을 참조하십시오.

단계 18 규칙 조건 유형에 설명된 대로 조건을 규칙(포트, 네트워크 등)에 추가합니다.

단계 19 **Add(**추가**)**를 클릭합니다.

단계 20 페이지 상단에서 **Save(**저장**)**를 클릭합니다.

다음에 수행할 작업

캡티브 포털 2부 설정: TCP 포트 액세스 컨트롤 규칙 생성, 8 페이지를 계속 진행합니다.

캡티브 포털 2부 설정: TCP 포트 액세스 컨트롤 규칙 생성

절차의 이 부분은 캡티브 포털이 캡티브 포털의 기본 포트인 TCP 포트 885를 이용해 클라이언트로 통신하게 하는, 액세스 컨트롤 규칙 생성 방법을 보여줍니다. 원한다면 다른 포트를 선택할 수도 있지만, 반드시 캡티브 포털 설정 1부: ID 정책 생성, 6 페이지에서 선택한 포트여야 합니다.

시작하기 전에

전체 캡티브 포털 설정에 대한 개요는 사용자 제어에 대한 캡티브 포털 설정 방법, 4 페이지에서 확인할 수 있습니다.

프로시저

단계 1 아직 하지 않았다면 Firepower Management Center에 로그인합니다.

단계 2 아직 하지 않았다면, PKI 개체에 설명된 대로 종속 포털에 대한 인증서를 만듭니다.

단계 3 **Policies(**정책**)** > **Access Control(**액세스 제어**)** > **Access Control(**액세스 제어**)**을 클릭하고 액세스 컨트롤 정책을 편집합니다.

단계 4 **Add Rule(**규칙 추가**)**을 클릭합니다.

단계 5 규칙의 **Name(**이름**)**을 입력합니다.

단계 6 **Action(**작업**)** 목록에서 **Allow(**허용**)**를 선택합니다.

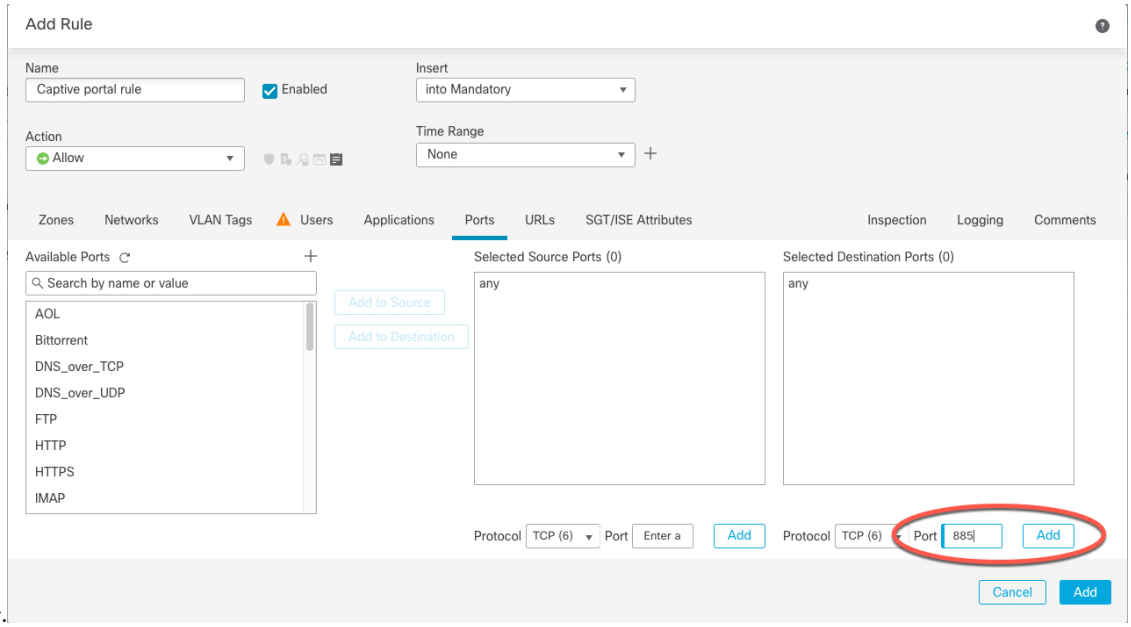
단계 7 **Ports(**포트**)**를 클릭합니다.

단계 8 **Selected Destination Ports(**선택한 대상 포트**)**의 **Protocol(**프로토콜**)** 목록에서 **TCP**를 선택합니다.

단계 9 **Port(**포트**)** 필드에 **885**을(를) 입력합니다.

단계 10 **Port(**포트**)** 필드에 **Add(**추가**)**를 클릭합니다.

다음 그림은 관련 예시를 보여줍니



다.

단계 **11** 페이지 하단의 **Add(**추가**)**를 클릭합니다.

다음에 수행할 작업

캡티브 포털 설정 3부: 사용자 액세스 컨트롤 규칙 생성, 9 페이지를 계속 진행합니다.

캡티브 포털 설정 **3**부: 사용자 액세스 컨트롤 규칙 생성

절차의 이 부분은 영역 내 사용자가 캡티브 포털을 이용해 인증할 수 있게 하는 액세스 컨트롤 규칙을 추가하는 방법을 설명합니다.

시작하기 전에

전체 캡티브 포털 설정에 대한 개요는 사용자 제어에 대한 캡티브 포털 설정 방법, 4 페이지에서 확인할 수 있습니다.

프로시저

단계 **1** 규칙 편집기에서 **Add Rule(**규칙 추가**)**을 클릭합니다.

단계 **2** 규칙의 **Name(**이름**)**을 입력합니다.

단계 **3** **Action(**작업**)** 목록에서 **Allow(**허용**)**를 선택합니다.

단계 **4** **Users(**사용자**)**를 클릭합니다.

단계 **5** **Available Realms(**사용 가능한 영역**)** 목록에서 허용할 영역을 클릭합니다.

단계 **6** 영역이 표시되지 않는다면 새로 로침( )을 클릭합니다.

단계 7 **Available Users(**사용 가능한 사용자**)** 목록에서 규칙에 추가할 사용자를 선택하고 **Add to Rule(**규칙에 추가**)**을 클릭합니다.

단계 8 (선택 사항). 규칙 조건 유형에 설명된 대로 액세스 컨트롤 정책에 조건을 추가합니다.

단계 9 **Add(**추가**)**를 클릭합니다.

단계 10 액세스 컨트롤 규칙 페이지에서 **Save(**저장**)**를 클릭합니다.

단계 11 정책 편집기에서 규칙 위치를 설정합니다. 이렇게 하려면 규칙을 클릭하여 끌거나 오른쪽 클릭 메뉴를 사용하여 잘라내고 붙여넣습니다. 규칙은 번호가 지정되며 1부터 시작합니다. 시스템은 오름차순 규칙 번호에 따라 하향식 순서로 트래픽이 규칙과 일치하는지를 확인합니다. 트래픽에 일치하는 첫 번째 규칙이 트래픽을 처리하는 규칙입니다. 규칙 순서가 올바르면 네트워크 트래픽 처리에 필요한 리소스가 줄어들면서 규칙 선점이 방지됩니다.

다음에 수행할 작업

캡티브 포털 설정 4부: SSL 암호 해독 생성-정책 재서명, 10 페이지를 계속 진행합니다.

캡티브 포털 설정 4부: SSL 암호 해독 생성-정책 재서명

절차의 이 부분은 트래픽이 캡티브 포털에 도달하기 전에 트래픽을 해독하고 재서명하는 SSL 액세스 정책을 생성하는 방법을 설명합니다. 캡티브 포털은 해독한 트래픽만 인증할 수 있습니다.

시작하기 전에

전체 캡티브 포털 설정에 대한 개요는 사용자 제어에 대한 캡티브 포털 설정 방법, 4 페이지에서 확인할 수 있습니다.

프로시저

단계 1 아직 하지 않았다면, PKI 개체에 설명된 대로 SSL 트래픽을 해독하는 인증서 개체를 만듭니다.

단계 2 **Policies(**정책**)** > **Access Control(**액세스 컨트롤**)** > **SSL**을 클릭합니다.

단계 3 **New Policy(**새로운 정책**)**를 클릭합니다.

단계 4 **Name(**이름**)**을 입력하고 정책에 대한 **Default Action(**기본 작업**)**을 선택합니다. 기본 작업은 SSL 정책 기본 작업에서 설명합니다.

단계 5 **Save(**저장**)**를 클릭합니다.

단계 6 **Add Rule(**규칙 추가**)**을 클릭합니다.

단계 7 규칙의 **Name(**이름**)**을 입력합니다.

단계 8 **Action(**작업**)** 목록에서 **Decrypt - Resign(**암호 해독 - 재서명**)**을 선택합니다.

단계 9 **with** 목록에서 PKI 개체를 선택합니다.

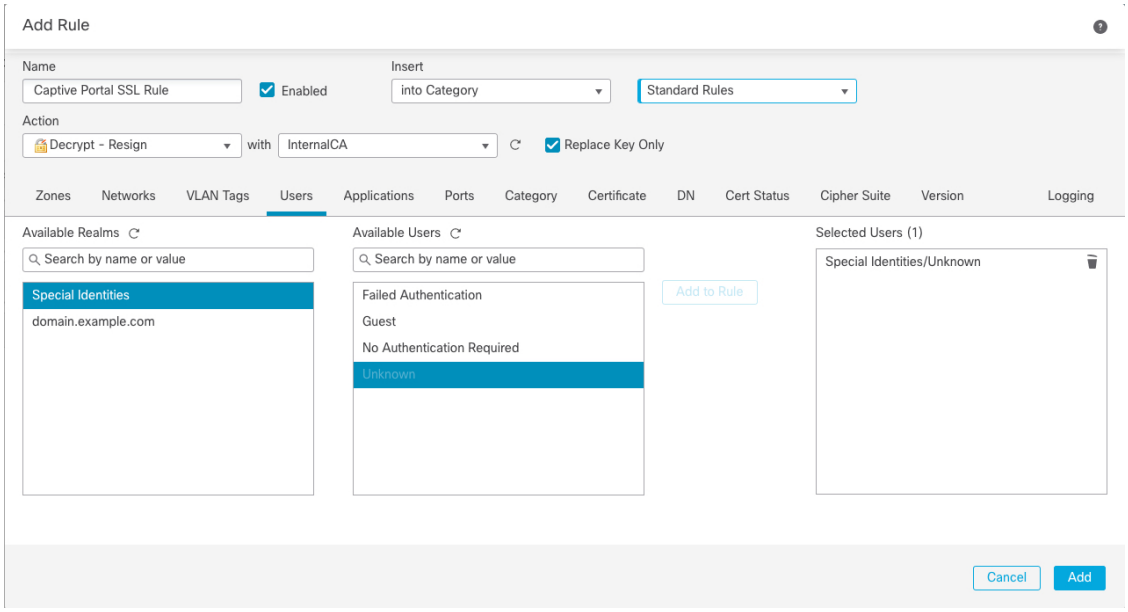
단계 10 **Users(**사용자**)**를 클릭합니다.

단계 11 **Available Realms(**사용 가능한 영역**)** 목록 위에 있는 새로 로침( )을(를) 클릭합니다.

단계 12 **Available Realms(**사용 가능한 영역**)** 목록에서 **Special Identities(** 특수 **ID)**를 클릭합니다.

단계 **13** **Available Users**(사용 가능한 사용자) 목록에서 **Unknown**(알 수 없음)을 클릭합니다.

단계 **14** **Add to Rule**(규칙에 추가)을 클릭합니다.
다음 그림은 예를 보여줍니다.



단계 **15** (선택 사항). TLS/SSL 규칙 조건에 설명된 대로 다른 옵션을 설정합니다.

단계 **16** **Add**(추가)를 클릭합니다.

단계 **17** 페이지 상단에서 **Save**(저장)를 클릭합니다.

다음에 수행할 작업

캡티브 포털 설정 5부: ID 및 SSL 정책과 액세스 컨트롤 정책 연결, 11 페이지를 계속 진행합니다.

캡티브 포털 설정 5부: ID 및 SSL 정책과 액세스 컨트롤 정책 연결

절차의 이 부분은 ID 정책과 SSL **Decrypt - Resign**(암호 해독 - 재서명) 규칙을 앞에서 생성한 액세스 컨트롤 정책과 연결하는 방법을 설명합니다. 이렇게 하면 사용자는 캡티브 포털을 이용해 인증할 수 있습니다.

시작하기 전에

전체 캡티브 포털 설정에 대한 개요는 사용자 제어에 대한 캡티브 포털 설정 방법, 4 페이지에서 확인할 수 있습니다.

프로시저

단계 **1** **Policies**(정책) > **Access Control**(액세스 컨트롤) > **Access Control**(액세스 컨트롤)을 클릭하고 캡티브 포털 2부 설정: TCP 포트 액세스 컨트롤 규칙 생성, 8 페이지에서 설명한 방법에 따라 생성한 액세

스 컨트롤 정책을 편집합니다. 보기 ( )이 대신 표시되는 경우에는 설정이 상위 도메인에 속하거나 설정을 수정할 권한이 없는 것입니다.

단계 **2** 새로운 액세스 컨트롤 정책을 만들거나 기존 정책을 편집합니다.

단계 **3** 페이지 상단에서 **Identity Policy(ID** 정책**)** 옆에 있는 링크를 클릭합니다.

단계 **4** 목록에서 ID 정책의 이름을 선택하고, 페이지 상단의 **Save(**저장**)**를 클릭합니다.

단계 **5** 앞의 단계를 반복해 캡티브 포털 SSL 정책을 액세스 컨트롤 정책과 연결합니다.

단계 **6** 아직 하지 않았다면, 액세스 제어 정책에 대한 대상 디바이스 설정에 설명된 대로 매니지드 디바이스에 정책을 대상으로 지정합니다.

다음에 수행할 작업

- 컨피그레이션 변경 사항 구축에 설명된 대로 관리되는 디바이스에 ID 및 액세스 제어 정책을 구축합니다.
- 워크플로 사용에 설명된 대로 사용자 활동을 모니터링합니다.

캡티브 포털(captive portal) 필드

다음 필드를 사용하여 ID 정책의 **Active Authentication(**액티브 인증**)** 탭에서 캡티브 포털(captive portal)을 설정합니다. Identity Rule Fields(ID 규칙 필드)도 참조하십시오.

서버 인증서

캡티브 포털(captive portal) 데몬에서 표시되는 서버 인증서.

참고 캡티브 포털은 DSA(Digital Signature Algorithm) 또는 ECDSA(Elliptic Curve Digital Signature Algorithm) 인증서 사용을 지원하지 않습니다.

Port(포트**)**

캡티브 포털(captive portal) 연결에 사용할 포트 번호입니다. ASA FirePOWER 디바이스를 캡티브 포털(captive portal)에 사용하려는 경우, 이 필드의 포트 번호는 **captive-portal** CLI 명령을 사용하여 ASA FirePOWER 디바이스에서 설정한 포트 번호와 일치해야 합니다.

Maximum login attempts(최대 로그인 시도 횟수**)**

시스템이 사용자의 로그인 요청을 거부하기 전까지 허용되는 최대 실패 로그인 시도 횟수.

Active Authentication Response Page(액티브 인증 응답 페이지**)**

다음 옵션을 선택합니다.

- 일반적인 응답을 사용하려면, **System-provided(**시스템 제공**)**를 클릭합니다. 이 페이지에 대한 HTML 코드를 보려면 보기 ( )를 클릭합니다.

- 맞춤형 응답을 생성하려면, **Custom(**맞춤형**)**을 선택합니다. 대체하거나 수정할 수 있는 시스템 제공 코드가 표시되는 창이 나타납니다. 완료했으면 변경사항을 저장합니다. 수정( )을 클릭하여 사용자 지정 페이지를 편집할 수 있습니다.

관련 항목

내부 인증서 개체

캡티브 포털에서 애플리케이션 제외

애플리케이션(HTTP 사용자-에이전트 설정에서 식별됨)을 선택하고 캡티브 포털(captive portal) 액티브 인증에서 이를 제외할 수 있습니다. 이렇게 하면 선택한 애플리케이션의 트래픽이 인증 없이 ID 정책을 통과할 수 있습니다.

참고 **User-Agent Exclusion(**사용자-에이전트 제외**) Tag(**태그**)**가 있는 애플리케이션만 이 목록에 표시됩니다.

프로시저

단계 **1** ID 규칙 편집기 페이지의 **Realm & Settings(**영역 및 설정**)**에서 **Application Filters(**애플리케이션 필터**)** 목록에 있는 Cisco 제공 필터를 사용하여 필터에 추가할 애플리케이션 목록의 범위를 좁힙니다.

- 목록을 확장 및 축소하려면 각 필터 유형 옆에 있는 화살표를 클릭합니다.
- 필터 유형을 마우스 오른쪽 버튼으로 클릭하고 **Check All(**모두 선택**)** 또는 **Uncheck All(**모두 선택해제**)**을 클릭합니다. 목록은 각 유형의 필터를 얼마나 많이 선택했는지를 나타낸다는 점에 유의하십시오.
- 나타나는 필터를 축소하려면, **Search by name(**이름으로 검색**)** 필드에 검색 문자열을 입력합니다. 이는 카테고리 및 태그에 특히 유용합니다. 검색을 지우려면 지우기( ) 아이콘을 클릭합니다.
- 필터 목록을 새로 고침하고 선택한 모든 필터를 지우려면 다시 로드( )을 클릭합니다.
- 모든 필터 및 검색 필드를 지우려면, **Clear All Filters(**모든 필터 지우기**)**를 클릭합니다.

참고 목록은 한 번에 100개의 애플리케이션을 표시합니다.

단계 **2** **Available Applications(**사용 가능한 애플리케이션**)** 목록에서 필터에 추가하려는 애플리케이션을 선택합니다.

- 나타나는 개별 애플리케이션의 범위를 좁히려면 **Search by name(**이름으로 검색**)** 필드에 검색 문자열을 입력합니다. 검색을 지우려면 지우기( ) 아이콘을 클릭합니다.
- 개별 가용 애플리케이션 목록을 조회하려면 목록 하단의 페이징을 사용합니다.

- 애플리케이션을 새로 고침하고 선택한 모든 애플리케이션을 지우려면 다시 로드( )을 클릭합니다.

단계 **3** 선택한 애플리케이션을 추가하여 외부 인증에서 제외합니다. 클릭하여 드래그하거나 **Add to Rule(**규칙에 추가**)**을 클릭할 수 있습니다. 결과는 선택한 애플리케이션 필터의 조합이 됩니다.

다음에 수행할 작업

- ID 규칙 생성에 설명된 대로 ID 규칙을 계속 구성합니다.

캡티브 포털(captive portal) ID 소스 문제 해결

기타 관련 문제 해결 정보를 보려면 영역 및 사용자 다운로드 문제 해결 및 사용자 제어 문제 해결을 참조하십시오.

캡티브 포털(captive portal)에 문제가 발생한 경우 다음을 확인하십시오.

- 캡티브 포털(captive portal) 서버의 시간은 Firepower Management Center의 시간과 동기화되어야 합니다.
-
- Firepower Management Center와 매니지드 디바이스 간의 연결에 실패했을 때, 사용자가 이전에 확인된 적이 있고 Firepower Management Center에 다운로드된 경우가 아니라면 다운타임 동안에는 디바이스에서 보고된 어떤 캡티브 포털(captive portal) 로그인도 식별할 수 없습니다. 식별되지 않은 사용자는 Firepower Management Center에서 알 수 없는 사용자로 로깅됩니다. 다운타임이 끝나면 ID 정책의 규칙에 따라 알 수 없는 사용자가 다시 식별되고 처리됩니다.
- 캡티브 포털(captive portal)에 사용할 디바이스에 인라인 및 라우팅 인터페이스가 모두 포함된 경우, 캡티브 포털(captive portal) ID 규칙에 영역 조건을 구성하여 캡티브 포털(captive portal) 디바이스에서 라우팅 인터페이스만 대상이 되도록 해야 합니다.
- 시스템은 ASA with FirePOWER 디바이스에서 인터페이스의 유형을 검증하지 않습니다. ASA with FirePOWER 디바이스에서 인라인(탭 모드) 인터페이스에 캡티브 포털 정책을 적용하면 정책 구축은 성공하지만 해당 규칙과 일치하는 트래픽의 사용자는 Unknown(알 수 없음)으로 식별됩니다.
- Kerberos 인증에 성공하려면 매니지드 디바이스의 호스트 이름이 15자 미만이어야 합니다.
- 사용자 로그아웃을 확인하는 유일한 방법은 브라우저를 닫고 다시 여는 것입니다. 그러지 않으면, 경우에 따라 사용자가 캡티브 포털에서 로그아웃한 다음 같은 브라우저를 이용해 다시 인증하지 않고도 네트워크에 액세스할 수 있습니다.
- 활성 FTP 세션이 이벤트에서 **Unknown**사용자로 표시됩니다. 활성 FTP에서는 서버(클라이언트 아님)가 연결을 시작하고 FTP 서버에는 관련 사용자 이름이 없으므로 이는 정상입니다. 활성 FTP에 대한 자세한 내용은 RFC 959를 참조하십시오.

캡티브 포털 기록

기능	버전	세부 사항
캡티브 포털입니다.	6.0	기능이 도입되었습니다. 캡티브 포털을 이용하면 브라우저 창의 메시지를 통해 사용자가 자격 증명을 입력하게 할 수 있습니다. 이러한 매핑을 통해 사용자 또는 사용자 그룹을 기반으로 정책을 설정할 수 있습니다.