캡티브 포털을 사용하여 사용자 제어

캡티브 포털 ID 소스

캡티브 포털(captive portal)은 시스템에서 지원하는 권한 있는 ID 소스 중 하나입니다. 캡티브 포털(captive portal)은 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, 5 페이지

호스트네임 리디렉션 정보

(Snort 3에만 해당) 활성 인증 ID 규칙은 구성된 인터페이스를 사용하여 캡티브 포털 포트로 리디렉션됩니다. 리디렉션은 일반적으로 IP 주소에 대해 수행되므로 사용자에게 신뢰할 수 없는 인증서 오류가 발생하며 이 동작은 중간자 공격과 유사하므로 사용자가 신뢰할 수 없는 인증서를 수락하기를 꺼릴 수 있습니다.

이 문제를 방지하려면 FQDN(정규화된 도메인 이름)을 사용하도록 캡티브 포털을 구성할 수 있습니다. 올바르게 구성된 인증서를 사용하면 신뢰할 수 없는 인증서 오류가 발생하지 않으며, 인증이 더 원활하고 안전해집니다.

관련 항목

호스트네임 네트워크 규칙 조건으로 리디렉션

캡티브 포털 라이선스 요구 사항

Threat Defense 라이선스

모두

기본 라이선스

제어

캡티브 포털 요구 사항 및 사전 요건

지원되는 도메인

모든

사용자 역할

- 관리자
- 액세스 관리자
- 네트워크 관리자

캡티브 포털 가이드라인 및 제한 사항

ID 정책에서 캡티브 포털(captive portal)을 구성 및 구축할 경우, 지정된 영역의 사용자는 threat defense을 사용하여 네트워크에 대한 액세스를 인증합니다.

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. 캡티브 포털에 대한 규칙을 설정할 예정이고 캡티브 포털 디바이스에 인라인 및 라우팅 인터페이스가 포함된 경우, 디바이스에서 라우팅 인터페이스만 대상으로 하도록 액세스 제어 정책에서 인터페이스 규칙 조건을 구성해야 합니다.

액세스 제어 정책에서 참조하는 ID 정책에 하나 이상의 캡티브 포털(captive portal) ID 규칙이 포함되어 있고 라우팅 인터페이스가 구성된 하나 이상의 디바이스를 관리하는 management center에서 정책을 구축하는 경우, 정책 구축이 성공하고 라우팅 인터페이스가 액티브 인증을 수행합니다.

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.

활성 인증 규칙에는 **Active Authentication(**활성 인증**)** 규칙 작업 또는 **Use active authentication if passive or VPN identity cannot be established(**패시브 또는 **VPN ID**를 설정할 수 없는 경우 활성 인증 사용**)**가 선택된 **Passive Authentication(**패시브 인증**)** 규칙 작업이 있습니다. 각각의 경우 시스템은 TLS/SSL 암호화를 투명하게 활성화 또는 비활성화하며, 이에 따라 Snort 프로세스가 재시작됩니다.

주의 TLS/SSL 암호 해독이 비활성화되어 있을 때(액세스 컨트롤 정책에 해독 정책이 포함되지 않을 때) 첫 번째 액티브 인증을 추가하거나 마지막 액티브 인증을 제거함 구성 변경 사항을 배포할 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 참조하십시오.

캡티브 포털이 ID 규칙과 일치하는 사용자를 인증하는 경우, 다운로드되지 않은 Microsoft Active Directory 또는 LDAP 그룹의 사용자는 Unknown(알 수 없음)으로 식별됩니다. 사용자가 Unknown(알 수 없음)으로 식별되는 것을 방지하려면 캡티브 포털(captive portal)로 인증할 것으로 예상하는 모든 그룹의 사용자를 다운로드하도록 영역 를 구성합니다. 알 수 없는 사용자는 연결된 액세스 제어 정책에 따라 처리됩니다. 알 수 없는 사용자를 차단하도록 액세스 제어 정책이 구성된 경우 이러한 사용자는 차단됩니다.

시스템이 영역의 모든 사용자를 다운로드하도록 하려면 해당 그룹이 영역 구성의 Available Groups(사용 가능한 그룹) 목록에 있는지 확인합니다.

사용자 및 그룹 동기화에 대한 자세한 내용은 사용자 및 그룹 동기화의 내용을 참조하십시오.

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, management center에 보고되지 않습니다.
- 캡티브 포털은 TLS v1.0 연결을 협상하지 않습니다.

  TLS v1.1, v1.2 및 TLS 1.3 연결만 지원됩니다.
- 캡티브 포털에서는 영역 시퀀스를 사용할 수 없습니다.
- 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 포털에 사용할 디바이스의 IP 주소 및 포트를 대상으로 하는 트래픽을 허용해야 합니다.
- HTTPS 트래픽에 대한 캡티브 포털(captive portal) 액티브 인증을 수행하려면, 해독 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 제헌하려면 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 해독 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.
- 캡티브 포털이 ID 규칙과 일치하는 사용자를 인증하는 경우, 다운로드되지 않은 Microsoft Active Directory 또는 LDAP 그룹의 사용자는 Unknown(알 수 없음)으로 식별됩니다. 사용자가 Unknown(알 수 없음)으로 식별되는 것을 방지하려면 캡티브 포털(captive portal)로 인증할 것으로 예상하는 모든 그룹의 사용자를 다운로드하도록 영역 를 구성합니다. 알 수 없는 사용자는 연결된 액세스

제어 정책에 따라 처리됩니다. 알 수 없는 사용자를 차단하도록 액세스 제어 정책이 구성된 경우 이러한 사용자는 차단됩니다.

시스템이 영역의 모든 사용자를 다운로드하도록 하려면 해당 그룹이 영역 구성의 Available Groups(사용 가능한 그룹) 목록에 있는지 확인합니다.

자세한 내용은 사용자 및 그룹 동기화를 참고하십시오.

Kerberos 사전 요건

Kerberos 인증을 사용하는 경우 매니지드 디바이스의 호스트 이름은 15자 미만이어야 합니다(Windows에서 설정한 NetBIOS 제한). 그렇지 않으면 캡티브 포털 인증이 실패합니다. 디바이스를 설정할 때 매니지드 디바이스 호스트 이름을 설정합니다. 자세한 내용은 Microsoft 설명서 사이트에서 컴퓨터, 도메인, 사이트 및 OU에 대한 Active Directory의 명명 규칙과 유사한 문서를 참조하십시오.

DNS는 호스트 이름에 대해 64KB 이하의 응답을 반환해야 합니다. 그렇지 않으면 연결 테스트에서 AD 연결이 실패합니다. 이 제한은 양방향으로 적용되며 RFC 6891 섹션-6.2.5에 설명되어 있습니다.

사용자 제어에 대한 캡티브 포털 설정 방법

시작하기 전에

캡티브 포털을 액티브 인증에 활용하려면, Microsoft AD 또는 LDAP 영역(영역 시퀀스가 아님), 액세스 컨트롤 정책과 ID 정책, 해독 정책을 설정하고 ID와 해독 정책을 액세스 제어 정책에 연결해야 합니다. 마지막으로, 사용자는 정책을 매니지드 디바이스에 구축해야 합니다. 이 주제는 이러한 작업에 대한 개략적인 정보를 제공합니다.

전체 절차 예시는 캡티브 포털 구성 1부: 네트워크 개체 생성, 7 페이지에서부터 시작합니다.

먼저 다음 작업을 수행하십시오.

- 라우팅 인터페이스가 구성된 하나 이상의 디바이스를 management center에서 관리하는지 확인합니다.
- 암호화된 인증을 캡티브 포털과 함께 사용하려면 PKI 개체를 만들거나, 액세스하는 management center의 장치에서 인증서 데이터와 키를 사용할 수 있게 해야 합니다. PKI 개체를 생성하는 방법은 PKI 섹션을 참조하십시오.

프로시저

단계 **1** 다음 항목에서 설명한 대로 Microsoft AD 영역 를 만들고 사용하도록 설정합니다.

- Active Directory 영역 및 영역 디렉터리 생성
- 사용자 및 그룹 동기화

영역 시퀀스는 캡티브 포털에서 지원되지 않습니다.

캡티브 포털이 ID 규칙과 일치하는 사용자를 인증하는 경우, 다운로드되지 않은 Microsoft Active Directory 또는 LDAP 그룹의 사용자는 Unknown(알 수 없음)으로 식별됩니다. 사용자가 Unknown(알 수 없음)으로 식별되는 것을 방지하려면 캡티브 포털(captive portal)로 인증할 것으로 예상하는 모든 그룹의 사용자를 다운로드하도록 영역 를 구성합니다. 알 수 없는 사용자는 연결된 액세스 제어 정책에 따라 처리됩니다. 알 수 없는 사용자를 차단하도록 액세스 제어 정책이 구성된 경우 이러한 사용자는 차단됩니다.

시스템이 영역의 모든 사용자를 다운로드하도록 하려면 해당 그룹이 영역 구성의 Available Groups(사용 가능한 그룹) 목록에 있는지 확인합니다.

자세한 내용은 사용자 및 그룹 동기화를 참고하십시오.

단계 **2** (선택 사항) 캡티브 포털을 IP 주소 대신 호스트로 리디렉션하려면 연결된 신뢰할 수 있는 인증 기관이 있는 네트워크 개체를 생성합니다.

캡티브 포털 구성 1부: 네트워크 개체 생성, 7 페이지의 내용을 참조하십시오.

단계 **3** 캡티브 포털에 대한 액티브 인증이 있는 ID 정책을 생성합니다.

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

자세한 내용은 캡티브 포털 설정 2부: ID 정책 생성, 9 페이지를 참고하십시오.

단계 **4** 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 3부 설정: TCP 포트 액세스 컨트롤 규칙 생성, 10 페이지를 참고하십시오.

단계 **5** 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 4부: 사용자 액세스 컨트롤 규칙 생성, 12 페이지를 참고하십시오.

단계 **6** 암호 해독 설정 - 캡티브 포털 사용자가 HTTPS 프로토콜을 이용해 웹 페이지에 액세스할 수 있도록 **Unknown**(알 수 없는) 사용자에 대한 **Decrypt - Resign(**암호 해독 - 재서명**)**정책으로 해독 정책 정책을 구성합니다.

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 5부: TLS/SSL 암호 해독 생성-정책 재서명, 12 페이지를 참고하십시오.

단계 **7** ID 및 해독 정책을 3단계의 액세스 제어 정책에 연결합니다.

이 마지막 단계는 시스템이 캡티브 포털을 이용해 인증하게 합니다.

자세한 내용은 캡티브 포털 설정 6부: ID 및 해독 정책과 액세스 컨트롤 정책 연결, 14 페이지를 참고하십시오.

다음에 수행할 작업

캡티브 포털 구성 1부: 네트워크 개체 생성, 7 페이지를 참고해 주십시오.

관련 항목

캡티브 포털에서 애플리케이션 제외, 16 페이지
PKI
캡티브 포털(captive portal) ID 소스 문제 해결, 17 페이지
Snort 재시작 시나리오

캡티브 포털 구성 1부: 네트워크 개체 생성

이 작업은 캡티브 포털을 ID 소스로 활용하는 방법을 설명합니다.

Threat Defense 기능 기록:

- 7.1 - 캡티브 포털 인증 요청을 선택적으로 정규화된 도메인 이름으로 리디렉션할 수 있습니다.

시작하기 전에

(Snort 3만 해당.) 이 작업은 선택 사항입니다. DNS 서버를 사용하여 FQDN(Fully Qualified Host Name)을 생성합니다. 이전에 수행한 적이 없는 경우 이와 같은 리소스를 참조할 수 있습니다. 사용자의 management center에 의해 관리되는 디바이스 중 하나에서 라우팅 인터페이스의 IP 주소를 지정합니다.

네트워크 개체에 대한 자세한 내용은 호스트네임 네트워크 규칙 조건으로 리디렉션의 내용을 참조하십시오.

프로시저

단계 **1** 아직 로그인하지 않았다면 management center에 로그인합니다.

단계 **2** **Objects(**개체**)** > **Object Management(**개체 관리**)** 버튼을 클릭합니다.

단계 **3** **PKI**를 확장합니다.

단계 **4** **Internal Certs(**내부 인증서**)**를 클릭합니다.

단계 **5** **Add Internal Cert**를 클릭합니다.

단계 **6** **Name(**이름**)** 필드에 신뢰할 수 있는 CA를 식별하는 이름을 입력합니다(예: **`MyCaptivePortal`**).

단계 **7** **Certificate Data(**인증서 데이터**)** 필드에 인증서를 붙여넣거나 **Browse(**찾아보기**)** 버튼을 사용하여 찾습니다.

인증서 Common Name(일반 이름)은 캡티브 포털(captive portal) 사용자가 인증할 FDQN과 정확히 일치해야 합니다.

단계 8 **Key(**키**)** 필드에 인증서의 개인 키를 붙여넣거나 **Browse(**찾아보기**)** 버튼을 사용하여 찾습니다.

단계 9 인증서가 암호화된 경우 **Encrypted(**암호화됨**)** 확인란을 선택하고 옆에 있는 필드에 비밀번호를 입력합니다.

단계 10 **Save(**저장**)**를 클릭합니다.

단계 11 **Network(**네트워크**)**를 클릭합니다.

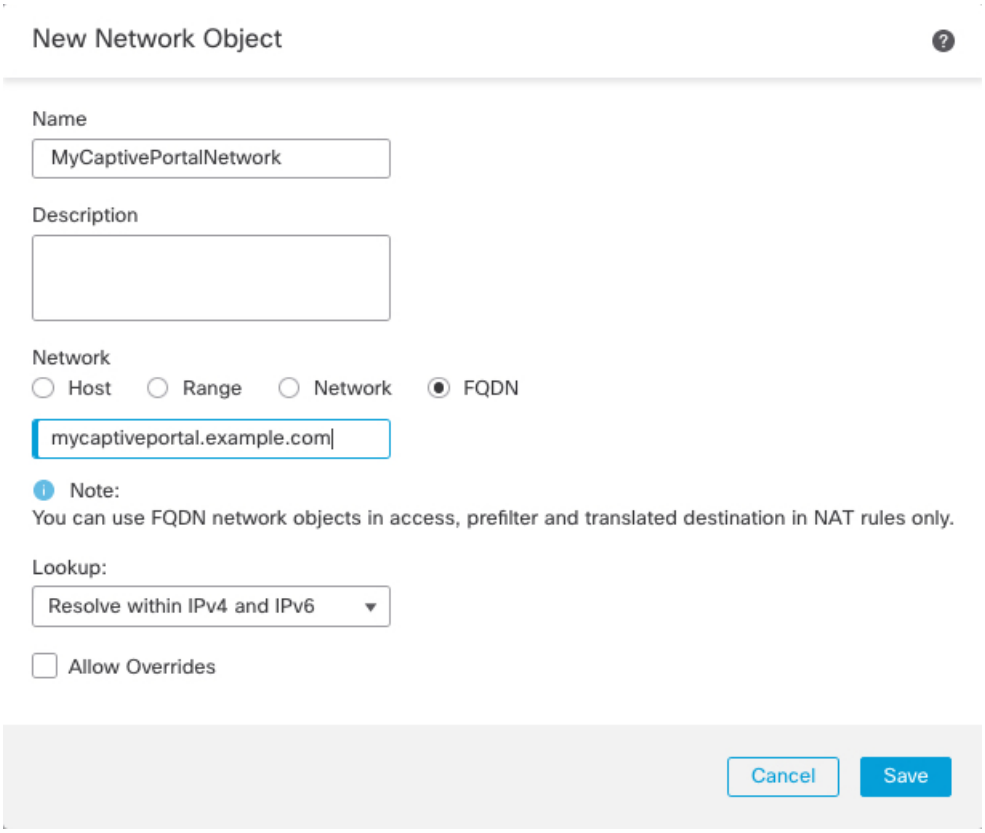
단계 12 페이지 상단의 목록에서 **Add Object(**개체 추가**)**를 클릭합니다.

단계 13 **Name(**이름**)** 필드에 개체를 식별하는 이름을 입력합니다(예: **`MyCaptivePortalNetwork`**).

단계 14 **FQDN**을 클릭하고 필드에 캡티브 포털의 FQDN 이름을 입력합니다.

단계 15 **Lookup(**조회**)** 옵션을 클릭합니다.

다음 그림은 예를 보여줍니다.



단계 16 **Save(**저장**)**를 클릭합니다.

다음에 수행할 작업

캡티브 포털 설정 2부: ID 정책 생성, 9 페이지

캡티브 포털 설정 2부: ID 정책 생성

시작하기 전에

이 여러 단계 절차는 캡티브 포털과 TLS/SSL 암호 해독 모두에 대해 기본 TCP 포트 885와 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, 5 페이지에서 확인할 수 있습니다.

프로시저

단계 **1** 아직 하지 않았다면 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 **Add(**추가**)** (+)를 클릭하여 인증서를 추가합니다.

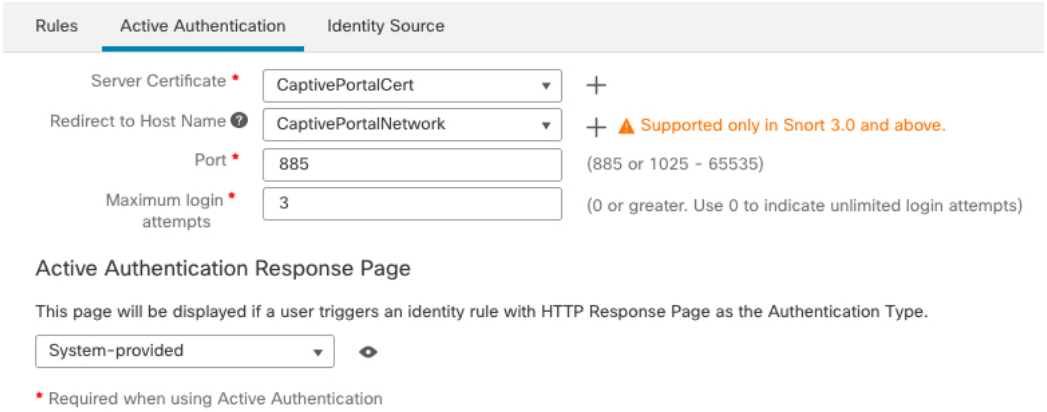
참고 캡티브 포털은 DSA(Digital Signature Algorithm) 또는 ECDSA(Elliptic Curve Digital Signature Algorithm) 인증서 사용을 지원하지 않습니다.

단계 **6** **Redirect to Host Name(**호스트 이름으로 리디렉션**)** 필드에서 이전에 생성한 네트워크 개체를 클릭합니다.

단계 **7** **885**을(를) **Port(**포트**)** 필드에 입력하고 **Maximum login attempts(**최도 로그인 시도 횟수**)**를 지정합니다.

단계 **8** (선택 사항). 캡티브 포털(captive portal) 필드, 15 페이지에 설명된 대로 **Active Authentication Response Page(**액티브 인증 응답 페이지**)**를 선택합니다.

다음 그림은 예를 보여줍니다.



단계 **9** **Save**(저장)를 클릭합니다.

단계 **10** **Rules**(규칙)를 클릭합니다.

단계 **11** **Add Rule**(규칙 추가)를 클릭하여 새 캡티브 포털 ID 정책 규칙을 추가하거나 **Edit**(수정) (✎)을 클릭하여 기존 규칙을 편집합니다.

단계 **12** 규칙의 **Name**(이름)을 입력합니다.

단계 **13** **Action**(작업) 목록에서 **Active Authentication**(액티브 인증)을 선택합니다.

단계 **14** **Realm & Settings**(영역 및 설정)를 클릭합니다.

단계 **15** **Realms**(영역) 목록에서 사용자 인증에 사용할 영역 를 선택합니다.

영역 시퀀스는 지원되지 않습니다.

단계 **16** (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, 15 페이지를 참고하십시오.

단계 **17** 목록에서 **Authentication Protocol**(인증 프로토콜)을 선택합니다.

단계 **18** (선택 사항). 특정 애플리케이션 트래픽을 캡티브 포털에서 제외하는 방법은 캡티브 포털에서 애플리케이션 제외, 16 페이지 섹션을 참조하십시오.

단계 **19** ID 규칙 조건에 설명된 대로 조건을 규칙(포트, 네트워크 등)에 추가합니다.

단계 **20** **Add**(추가)를 클릭합니다.

단계 **21** 페이지 상단에서 **Save**(저장)를 클릭합니다.

다음에 수행할 작업

캡티브 포털 3부 설정: TCP 포트 액세스 컨트롤 규칙 생성, 10 페이지를 계속 진행합니다.

캡티브 포털 3부 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 2부: ID 정책 생성, 9 페이지에서 선택한 포트여야 합니다.

시작하기 전에

전체 캡티브 포털 설정에 대한 개요는 사용자 제어에 대한 캡티브 포털 설정 방법, 5 페이지에서 확인할 수 있습니다.

프로시저

단계 1 아직 하지 않았다면 management center에 로그인합니다.

단계 2 아직 하지 않았다면, PKI에 설명된 대로 캡티브 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.

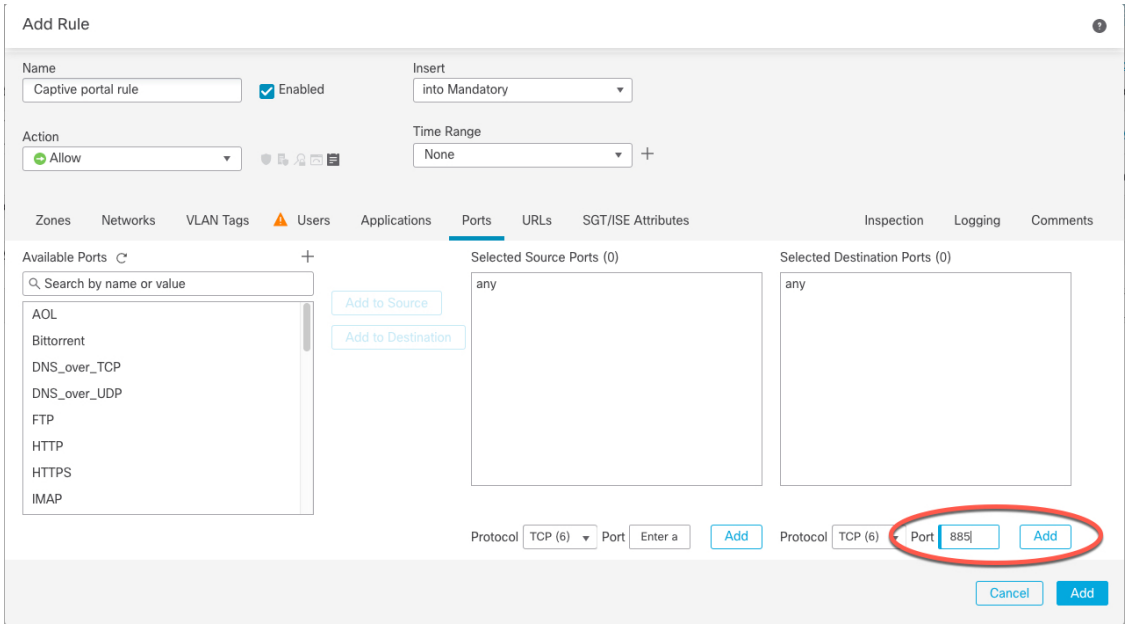
단계 6 **Action(**작업**)** 목록에서 **Allow(**허용**)**를 선택합니다.

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 보여줍니다.



단계 11 페이지 하단의 **Add(**추가**)**를 클릭합니다.

다음에 수행할 작업

캡티브 포털 설정 4부: 사용자 액세스 컨트롤 규칙 생성, 12 페이지를 계속 진행합니다.

캡티브 포털 설정 4부: 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, 5 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 **Refresh(**새로 고침**)**( )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). ID 규칙 조건에 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 5부: TLS/SSL 암호 해독 생성-정책 재서명, 12 페이지를 계속 진행합니다.

캡티브 포털 설정 5부: TLS/SSL 암호 해독 생성-정책 재서명

절차의 이 부분은 트래픽이 캡티브 포털에 도달하기 전에 트래픽을 해독하고 재서명하는 해독 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, 5 페이지에서 확인할 수 있습니다.

프로시저

단계 1 아직 로그인하지 않았다면 management center에 로그인합니다.

단계 2 아직 하지 않았다면, PKI에 설명된 대로 TLS/SSL 트래픽을 해독하는 인증서 개체를 만듭니다.

단계 3 **Policies(**정책**)** > **Access Control(**액세스 제어**)** > **Decryption(**해독**)Policies(**정책**)** > **Access Control(**액세스 컨트롤**)** > **SSL**을 클릭합니다.

단계 4 **New Policy(**새로운 정책**)**를 클릭합니다.

단계 5 **Name(**이름**)**을 입력하고 정책에 대한 **Default Action(**기본 작업**)**을 선택합니다. 기본 작업은 해독 정책 기본 작업에서 설명합니다.

단계 6 **Save(**저장**)**를 클릭합니다.

단계 7 **Add Rule(**규칙 추가**)**을 클릭합니다.

단계 8 규칙의 **Name(**이름**)**을 입력합니다.

단계 9 **Action(**작업**)** 목록에서 **Decrypt - Resign(**암호 해독 **-** 재서명**)**을 선택합니다.

단계 10 **with** 목록에서 PKI 개체를 선택합니다.

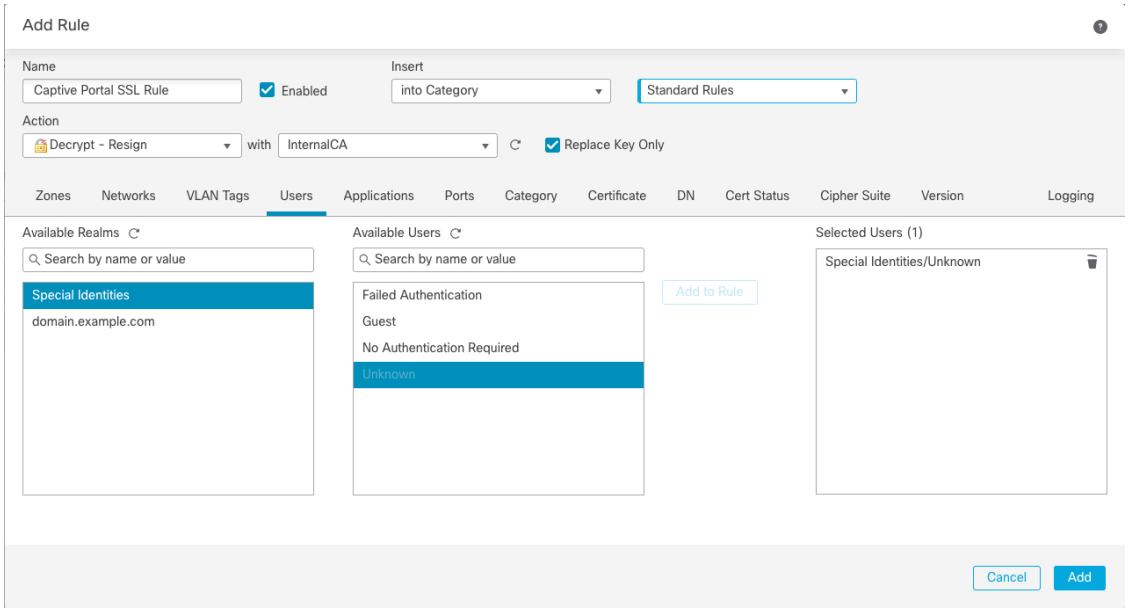
단계 11 **Users(**사용자**)**를 클릭합니다.

단계 12 **Available Realms(**사용 가능한 영역**)** 목록 위에 있는 **Refresh(**새로 고침**)**( )을(를) 클릭합니다.

단계 13 **Available Realms(**사용 가능한 영역**)** 목록에서 **Special Identities(** 특수 **ID)**를 클릭합니다.

단계 14 **Available Users(**사용 가능한 사용자**)** 목록에서 **Unknown(**알 수 없음**)**을 클릭합니다.

단계 15 **Add to Rule(**규칙에 추가**)**을 클릭합니다.
다음 그림은 예를 보여줍니다.



단계 16 (선택 사항). 해독 규칙 조건에 설명된 대로 다른 옵션을 설정합니다.

단계 17 **Add(추가)**를 클릭합니다.

단계 18 페이지 상단에서 **Save(저장)**를 클릭합니다.

다음에 수행할 작업

캡티브 포털 설정 6부: ID 및 해독 정책과 액세스 컨트롤 정책 연결, 14 페이지를 계속 진행합니다.

캡티브 포털 설정 6부: ID 및 해독 정책과 액세스 컨트롤 정책 연결

절차의 이 부분은 ID 정책과 TLS/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, 5 페이지에서 확인할 수 있습니다.

프로시저

단계 1 **Policies(정책)** > **Access Control(액세스 컨트롤)** > **Access Control(액세스 컨트롤)**을 클릭하고 캡티브 포털 3부 설정: TCP 포트 액세스 컨트롤 규칙 생성, 10 페이지에서 설명한 방법에 따라 생성한 액세스 컨트롤 정책을 편집합니다. **View(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 해독 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

- 구성 변경 사항 구축에 설명된 대로 관리되는 디바이스에 ID 및 액세스 제어 정책을 구축합니다.
- Cisco Secure Firewall Management Center 관리 가이드의 워크플로우 사용에 설명된 대로 사용자 활동을 모니터링합니다.

캡티브 포털(captive portal) 필드

다음 필드를 사용하여 ID 정책의 **Active Authentication(**액티브 인증**)** 탭 페이지에서 캡티브 포털(captive portal)을 설정합니다. Identity Rule Fields(ID 규칙 필드) 및 캡티브 포털에서 애플리케이션 제외, 16 페이지도 참조하십시오.

서버 인증서

캡티브 포털 데몬이 제시하는 내부 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. 캡티브 포털에 사용할 TCP 포트로 액세스 제어 규칙을 설정한 다음, ID 정책을 해당 액세스 제어 정책과 연결해야 합니다. 자세한 내용은 캡티브 포털 3부 설정: TCP 포트 액세스 컨트롤 규칙 생성, 10 페이지를 참고하십시오.

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

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

방화벽 전체에서 활성 인증 세션 공유

액세스 제어 정책이 이 ID 정책과 연결된 매니지드 디바이스 간에 세션을 공유하려면 이 체크 박스를 선택합니다.

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

캡티브 포털(captive portal) 사용자에게 표시할 시스템 제공 또는 맞춤형 HTTP 응답 페이지. ID 정책 액티브 인증 설정에서 **Active Authentication Response Page(**액티브 인증 응답 페이지**)**를 선택한 후에는 **`HTTP Response Page`(`HTTP` 응답 페이지)**가 있는 하나 이상의 ID 규칙 또한 **Authentication Protocol(**인증 프로토콜**)**로 구성해야 합니다.

시스템 제공 HTTP 응답 페이지에는 **Username(**사용자 이름**)** 및 **Password(**비밀번호**)** 필드, 그리고 사용자가 네트워크에 게스트로 액세스할 수 있는 **Login as guest(**게스트로 로그인**)** 버튼이 포함됩니다. 단일 로그인 방법을 표시하려면 맞춤형 HTTP 응답 페이지를 설정하십시오.

다음 옵션을 선택합니다.

- 일반적인 응답을 사용하려면, **System-provided(**시스템 제공**)**를 클릭합니다. 이 페이지에 대한 HTML 코드를 보려면 **View(**보기**)** ( )를 클릭합니다.
- 맞춤형 응답을 생성하려면, **Custom(**맞춤형**)**을 선택합니다. 대체하거나 수정할 수 있는 시스템 제공 코드가 표시되는 창이 나타납니다. 완료했으면 변경사항을 저장합니다. **Edit(**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** 아직 로그인하지 않았다면 management center에 로그인합니다.

단계 **2** **Policies(**정책**)** > **Access Control(**액세스 제어**)** > **Identity(ID)** 버튼을 클릭합니다.

단계 **3** 캡티브 포털 규칙을 포함하는 ID 정책을 편집합니다.

단계 **4** **Realm & Settings(**영역 및 설정**)** 탭 페이지에서 **HTTP User Agent Exclusions(HTTP** 사용자 에이전트 제외**)**를 확장합니다.

- 첫 번째 열에서 애플리케이션을 필터링할 각 항목 옆의 확인란을 선택한 다음 하나 이상의 애플리케이션을 선택하고 **Add to Rule(**규칙에 추가**)**을 클릭합니다.

  확인란은 AND로 연결됩니다.

- 표시되는 필터를 축소하려면, **Search by name(**이름으로 검색**)** 필드에 검색 문자열을 입력합니다. 이는 카테고리 및 태그에 특히 유용합니다. 검색을 지우려면 **Clear(**지우기**)** (✕) 아이콘을 클릭합니다.

- 필터 목록을 새로 고침하고 선택한 모든 필터를 지우려면 **Reload(**다시 로드**)**(↻)을 클릭합니다.

참고 목록은 한 번에 100개의 애플리케이션을 표시합니다.

단계 **5** **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 **Clear(**지우기**)** (✕) 아이콘을 클릭합니다.

- 개별 가용 애플리케이션 목록을 조회하려면 목록 하단의 페이징을 사용합니다.

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

단계 **6** 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) 매니지드 디바이스의 시간은 management center의 시간과 동기화되어야 합니다.
- DNS 확인을 구성했고 **Kerberos**(Kerberos를 옵션으로 사용하려는 경우에는 **HTTP Negotiate(HTTP** 협상**)**) 캡티브 포털(captive portal)을 수행할 ID 규칙을 생성하는 경우, 캡티브 포털(captive portal) 디바이스의 FQDN(Fully Qualified Domain Name)을 확인할 DNS 서버를 구성해야 합니다. FQDN은 DNS를 구성할 때 제공된 호스트 이름과 일치해야 합니다.

  자세한 내용은 호스트네임 리디렉션 정보, 2 페이지을 참고하십시오.
- Kerberos 인증을 사용하는 경우 매니지드 디바이스의 호스트 이름은 15자 미만이어야 합니다(Windows에서 설정한 NetBIOS 제한). 그렇지 않으면 캡티브 포털 인증이 실패합니다. 디바이스를 설정할 때 매니지드 디바이스 호스트 이름을 설정합니다. 자세한 내용은 Microsoft 설명서 사이트에서 컴퓨터, 도메인, 사이트 및 OU에 대한 Active Directory의 명명 규칙과 유사한 문서를 참조하십시오.
- DNS는 호스트 이름에 대해 64KB 이하의 응답을 반환해야 합니다. 그렇지 않으면 연결 테스트에서 AD 연결이 실패합니다. 이 제한은 양방향으로 적용되며 RFC 6891 섹션-6.2.5에 설명되어 있습니다.
- 캡티브 포털이 올바르게 구성되었지만 IP 주소 또는 FQDN(Fully Qualified Domain Name)에 대한 리디렉션이 실패하는 경우 엔드포인트 보안 소프트웨어를 비활성화합니다. 이러한 유형의 소프트웨어는 리디렉션을 방해할 수 있습니다.
- **Kerberos**(Kerberos를 옵션으로 사용하려는 경우에는 **HTTP Negotiate(HTTP** 협상**)**)를 ID 규칙의 **Authentication Type(**인증 유형**)**으로 선택할 경우, Kerberos 캡티브 포털 액티브 인증을 수행하려면 선택한 **Realm(**영역**)**에 **AD Join Username(AD** 조인 사용자 이름**)**과 **AD Join Password(AD** 조인 암호**)**를 설정해야 합니다.
- ID 규칙에서 **HTTP Basic(HTTP** 기본**)**을 **Authentication Type(**인증 유형**)**으로 선택한 경우, 네트워크의 사용자가 세션 시간 초과를 알지 못할 수 있습니다. 대부분의 웹 브라우저는 **HTTP Basic(HTTP** 기본**)** 로그인의 접속 정보를 캐시하며, 접속 정보를 사용하여 기존 세션의 시간이 초과하면 새 세션을 원활하게 시작합니다.
- management center와 매니지드 디바이스 간의 연결에 실패했을 때, 사용자가 이전에 확인된 적이 있고 management center에 다운로드된 경우가 아니라면 다운타임 동안에는 디바이스에서 보고된 어떤 캡티브 포털(captive portal) 로그인도 식별할 수 없습니다. 식별되지 않은 사용자는

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.
- 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 포털이 ID 규칙과 일치하는 사용자를 인증하는 경우, 다운로드되지 않은 Microsoft Active Directory 또는 LDAP 그룹의 사용자는 Unknown(알 수 없음)으로 식별됩니다. 사용자가 Unknown(알 수 없음)으로 식별되는 것을 방지하려면 캡티브 포털(captive portal)로 인증할 것으로 예상하는 모든 그룹의 사용자를 다운로드하도록 영역 를 구성합니다. 알 수 없는 사용자는 연결된 액세스 제어 정책에 따라 처리됩니다. 알 수 없는 사용자를 차단하도록 액세스 제어 정책이 구성된 경우 이러한 사용자는 차단됩니다.

  시스템이 영역의 모든 사용자를 다운로드하도록 하려면 해당 그룹이 영역 구성의 Available Groups(사용 가능한 그룹) 목록에 있는지 확인합니다.

  자세한 내용은 사용자 및 그룹 동기화를 참고하십시오.

캡티브 포털 기록

기능	버전	세부 사항
호스트네임 리디렉션	7.1.0	(Snort 3만 해당)—캡티브 포털에서 활성 인증 요청에 사용할 수 있는 인터페이스의 FQDN(정규화된 호스트 이름)이 포함된 네트워크 개체를 사용할 수 있습니다.
게스트 로그인입니다.	6.1.0	사용자는 캡티브 포털을 이용해 게스트로 로그인할 수 있습니다.
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.