ID 정책

연결에서 사용자 ID 정보를 수집하기 위해 ID 정책을 사용할 수 있습니다. 그런 다음 대시보드에서 사용자 ID를 기준으로 사용량을 보고 사용자 또는 사용자 그룹을 기준으로 액세스 제어를 구성할 수 있습니다.

ID 정책 개요

ID 정책을 사용하여 연결과 연계된 사용자를 탐지할 수 있습니다. 사용자를 식별하면 위협, 엔드포인트 및 네트워크 인텔리전스를 사용자 ID 정보와 연결할 수 있습니다. 시스템에서 네트워크 행동, 트래픽 및 이벤트를 개별 사용자와 직접 연결하므로 정책 위반, 공격 또는 네트워크 취약점의 소스를 손쉽게 식별할 수 있습니다.

예를 들어 침입 이벤트의 대상인 호스트를 소유한 사용자와 내부 공격 또는 포트 스캔을 시작한 사용자를 식별할 수 있습니다. 부적절한 웹 사이트 또는 애플리케이션에 액세스하는 사용자 및 대역폭을 많이 사용하는 사용자도 식별할 수 있습니다.

사용자 탐지에서는 분석용 데이터 수집 이외의 작업도 수행할 수 있습니다. 사용자 이름 또는 사용자 그룹 이름을 기준으로 액세스 규칙을 작성하여 사용자 ID를 기준으로 리소스에 대한 액세스를 선택적으로 허용하거나 차단할 수도 있습니다.

다음 방법을 통해 사용자 ID를 획득할 수 있습니다.

- 패시브 인증 - 모든 유형의 연결에 대해, 사용자 이름과 비밀번호를 입력하라는 메시지를 표시하지 않고 다른 인증 서비스를 통해 사용자 ID를 획득합니다.
- 액티브 인증 - HTTP 연결에만 사용자 이름과 비밀번호를 입력하라는 메시지를 표시하고, 소스 IP 주소의 사용자 ID를 획득하기 위해 지정된 ID 소스를 통해 인증을 수행합니다.

다음 주제에서는 사용자 ID에 대해 자세히 설명합니다.

패시브 인증을 통한 사용자 ID 설정

패시브 인증은 사용자에게 사용자 이름 및 비밀번호를 요구하지 않고 사용자 ID를 수집합니다. 시스템은 지정된 ID 소스에서 매핑을 가져옵니다.

다음 소스에서 패시브 방식으로 사용자-IP 주소 매핑을 획득할 수 있습니다.

- 원격 액세스 VPN 로그인. 패시브 ID에 대해 지원되는 사용자 유형은 다음과 같습니다.
  - 외부 인증 서버에 정의된 사용자 어카운트.
  - device manager에 정의된 로컬 사용자 어카운트.
- Cisco ISE(Identity Services Engine), Cisco ISE PIC(Identity Services Engine Passive Identity Connector)

지정된 사용자가 둘 이상의 소스를 통해 식별되는 경우에는 RA VPN ID가 우선적으로 사용됩니다.

활성 인증을 통한 사용자 ID 설정

인증은 사용자의 ID를 확인하는 작업입니다.

활성 인증을 사용하는 경우, 시스템에 사용자-ID 매핑이 없는 IP 주소에서 HTTP 트래픽 흐름이 유입되는 경우 시스템에 구성된 디렉터리에 대해 트래픽 흐름을 시작한 사용자를 인증할지를 결정할 수 있습니다. 사용자가 정상적으로 인증하면 해당 IP 주소는 인증된 사용자의 ID를 포함하는 것으로 간주됩니다.

인증이 실패해도 사용자의 네트워크 액세스는 차단되지 않습니다. 최종적으로는 액세스 규칙에 따라 이러한 사용자에게 제공할 액세스 권한이 결정됩니다.

알 수 없는 사용자 처리

ID 정책에 대해 디렉터리 서버를 구성할 때 시스템은 디렉터리 서버에서 사용자 및 그룹 멤버십 정보를 다운로드합니다. 이 정보는 24시간마다 자정에 또는 디렉터리 컨피그레이션을 수정하고 저장할 때마다 새로 고침됩니다. 정보를 변경하지 않는 경우에도 마찬가지입니다.

사용자가 활성 인증 ID 규칙에 따라 인증에 성공했으나 사용자 이름이 다운로드된 사용자 ID 정보에 없으면 해당 사용자는 알 수 없음으로 표시됩니다. 사용자 ID와 사용자 일치 그룹 규칙은 ID 관련 대시보드에 표시되지 않습니다.

그러나 알 수 없음 사용자에 대한 모든 액세스 제어 규칙은 적용됩니다. 예를 들어 알 수 없음 사용자에 대한 연결을 차단하는 경우, 해당 사용자는 인증에 성공하더라도(즉, 디렉터리 서버에서 사용자와 비밀번호를 유효한 것으로 인식하더라도) 차단됩니다.

그러므로 사용자를 추가 또는 삭제하거나 그룹 멤버십을 변경하는 등 디렉터리 서버를 변경하면 시스템이 디렉터리에서 업데이트를 다운로드할 때까지는 해당 변경 사항이 정책 시행에 반영되지 않습니다.

매일 자정 업데이트가 수행될 때까지 기다리지 않으려면 디렉터리 영역 정보를 수정하여(**Objects(**개체**)** > **Identity Sources(ID** 소스**)**에서 해당 영역 수정) 업데이트를 강제로 수행할 수 있습니다. **Save(**저장**)**를 클릭한 다음 변경 사항을 구축합니다. 그러면 시스템이 업데이트를 즉시 다운로드합니다.

참고 **Policies(**정책**)** > **Access Control(**액세스 제어**)**로 이동하여 **Add Rule (+)(**규칙 추가**(+))** 버튼을 클릭하고 **Users(**사용자**)** 탭에서 사용자 목록을 확인하여 새 사용자 정보 또는 삭제된 사용자 정보가 시스템에 있는지를 확인할 수 있습니다. 새 사용자를 찾을 수 없거나 삭제된 사용자를 찾을 수 있으면 시스템의 정보는 오래된 것입니다.

ID 정책을 구현하는 방법

IP 주소와 연결된 사용자를 알 수 있도록 사용자 ID 획득을 활성화하려면 여러 항목을 구성해야 합니다. 이러한 항목을 정확하게 구성하면 모니터링 대시보드 및 이벤트에서 사용자 이름을 확인할 수 있습니다. 또한 액세스 제어 및 SSL 암호 해독 규칙에서 사용자 ID를 트래픽 일치 기준으로 사용할 수도 있습니다.

다음 절차에서는 ID 정책이 작동하도록 하려면 구성해야 하는 항목의 개요를 제공합니다.

프로시저

단계 **1** AD ID 영역을 구성합니다.

사용자 인증 프롬프트를 표시하여 사용자 ID를 활성 방식으로 수집하든 아니면 패시브 방식으로 수집하든 관계없이 사용자 ID 정보가 포함된 AD(Active Directory) 서버를 구성해야 합니다. AD ID 영역 구성의 내용을 참조하십시오.

패시브 ID를 구성하는 경우, 두 개 이상의 AD 영역에 있는 ID에서 시스템을 가져올 수 있는 AD 영역 시퀀스를 생성할 수 있습니다. 이는 네트워크에 여러 AD 도메인이 있는 경우 유용합니다.

단계 **2** 패시브 인증 ID 규칙을 사용하려는 경우 패시브 ID 소스를 구성합니다.

디바이스에서 구현하는 서비스와 네트워크에서 사용 가능한 서비스를 기준으로 하여 다음 중 원하는 소스를 구성할 수 있습니다.

- 원격 액세스 VPN - 디바이스에 대한 원격 액세스 VPN 연결을 지원하려는 경우 사용자 로그인은 device manager 내에 정의된 로컬 사용자 또는 AD 서버를 기준으로 하여 ID를 제공할 수 있습니다. RA VPN 구성에 대한 정보는 원격 액세스 VPN 구성의 내용을 참조하십시오.
- Cisco ISE(Identity Services Engine) 또는 Cisco ISE PIC(Identity Services Engine Passive Identity Connector) - 이러한 제품을 사용하는 경우에는 디바이스를 pxGrid 서브스크라이버로 구성하고 ISE에서 사용자 ID를 획득할 수 있습니다. ISE(Identity Services Engine) 구성의 내용을 참조하십시오.

단계 **3** **Policies(**정책**)** > **Identity(ID)**를 선택하고 ID 정책을 활성화합니다. ID 정책 구성, 5 페이지의 내용을 참조하십시오.

단계 **4** ID 정책 설정 구성, 6 페이지.

패시브 ID 소스는 시스템에서 구성한 소스를 기준으로 하여 자동으로 선택됩니다. 활성 인증을 구성하려는 경우 종속 포털 및 SSL 재서명 암호 해독(SSL 암호 해독 정책을 아직 활성화하지 않은 경우)용 인증서를 구성해야 합니다.

단계 **5** ID 정책 기본 작업 구성, 8 페이지.

패시브 인증만 사용하려는 경우에는 기본 작업을 패시브 인증으로 설정할 수 있으며, 구체적인 규칙을 생성할 필요가 없습니다.

단계 **6** ID 규칙 구성, 8 페이지.

관련 네트워크에서 패시브 또는 액티브 사용자 ID를 수집할 규칙을 생성합니다.

활성 인증 모범 사례

ID 규칙에서 사용자에 대한 액티브 인증을 요구하는 경우 사용자는 연결 시에 사용한 인터페이스의 캡티브 포털 포트로 리디렉션되며, 그리고 나면 인증하라는 메시지가 표시됩니다.

이 리디렉션은 인터페이스 IP 주소에 대한 것이므로 ID 정책 인증서가 정확하게 일치하지 않으며, 사용자에게 신뢰할 수 없는 인증서 오류가 발생합니다. 사용자가 인증서를 수락해야 디바이스를 계속 인증할 수 있습니다. 이 동작은 중간자(man-in-the-middle) 공격과 유사하므로 사용자는 신뢰할 수 없는 인증서를 수락하지 않습니다.

이 문제를 방지하기 위해 디바이스에서 한 인터페이스의 정규화된 도메인 이름(FQDN)을 사용하도록 활성 인증을 구성할 수 있습니다. 올바르게 구성된 인증서를 사용하면 신뢰할 수 없는 인증서 오류가 발생하지 않으며, 인증이 더 원활하고 안전해집니다.

시작하기 전에

활성 인증은 HTTP 트래픽에 대해서만 발생하며, 디바이스에 사용자의 워크스테이션 또는 다른 클라이언트 디바이스에 대한 현재 사용자 매핑이 없는 경우 최종 사용자에게 중단이 발생합니다. 수동 인증을 대신 구현하여 중단을 방지할 수 있습니다.

프로시저

단계 **1** DNS 서버에서 활성 인증 수집에 사용할 인터페이스의 인터페이스 IP 주소에 대한 정규화된 도메인 이름(FQDN)을 정의합니다.

종속 포털이라고도 하는 이 인터페이스는 라우팅 인터페이스여야 합니다.

단계 **2** CA(Certificate Authority)를 사용하여 이 FQDN에 대한 인증서를 가져옵니다.

ftd1.captive-port.example.com과 같은 특정 FQDN에 대한 인증서를 생성할 수 있습니다. 또는 다음을 수행할 수 있습니다.

- 여러 디바이스의 종속 포털 인터페이스에 적용할 수 있는 와일드카드 인증서를 가져옵니다(예: *.captive-port.example.com). 와일드카드는 더 광범위할 수 있으며, 넓은 범위의 엔드포인트 클래스에 적용할 수 있습니다(예: *.eng.example.com 또는 even *.example.com).
- 인증서에 여러 SAN(Subject Alternate Name)을 포함합니다.

단계 **3** **Objects(**개체**)** > **Certificates(**인증서**)**를 선택하고 인증서를 업로드합니다.

단계 **4** **Objects(**개체**)** > **Network(**네트워크**)**를 선택하고 DNS 이름에 대한 FQDN 네트워크 개체를 생성합니다.

단계 **5** **Policies(**정책**)** > **Identity(ID)** 페이지에서 인증서 및 FQDN 개체로 ID 정책 설정을 업데이트합니다.

단계 **6** 활성 인증을 사용하는 ID 정책에서 규칙을 생성합니다.

ID 정책 구성

연결에서 사용자 ID 정보를 수집하기 위해 ID 정책을 사용할 수 있습니다. 그런 다음 대시보드에서 사용자 ID를 기준으로 사용량을 보고 사용자 또는 사용자 그룹을 기준으로 액세스 제어를 구성할 수 있습니다.

아래에서는 ID 정책을 통해 사용자 ID를 가져오는 데 필요한 요소를 구성하는 방법을 간략하게 설명합니다.

프로시저

단계 **1** **Policies(**정책**)** > **Identity(ID)**를 선택합니다.

ID 정책을 아직 정의하지 않은 경우 **ID** 정책 활성화를 클릭하여 ID 정책 설정 구성, 6 페이지에서 설명하는 대로 설정을 구성합니다.

단계 **2** ID 정책을 관리합니다.

ID 설정을 구성하고 나면 이 페이지에 모든 규칙이 순서대로 나열됩니다. 목록의 맨 위에서부터 규칙과 트래픽의 일치 여부를 확인하며, 첫 번째로 일치하는 규칙에 따라 적용할 작업이 결정됩니다. 이 페이지에서는 다음을 수행할 수 있습니다.

- ID 정책을 활성화하거나 비활성화하려면 **ID** 정책 토글을 클릭합니다.
- ID 정책 설정을 변경하려면 **Identity Policy Configuration(ID** 정책 컨피그레이션**)** 버튼()을 클릭하십시오.
- **Default Action(**기본 작업**)**을 변경하려면 작업을 클릭하고 원하는 작업을 선택합니다. ID 정책 기본 작업 구성, 8 페이지의 내용을 참조하십시오.
- 규칙을 이동하려면 규칙을 수정하고 **Order(**순서**)** 드롭다운 목록에서 새 위치를 선택합니다.
- 규칙을 구성하려면 다음을 수행합니다.

- 새 규칙을 생성하려면 + 버튼을 클릭합니다.
- 기존 규칙을 수정하려면 Actions(작업) 열에서 해당 규칙의 수정 아이콘()을 클릭합니다. 테이블에서 속성을 클릭하여 규칙 속성을 선택적으로 수정할 수도 있습니다.
- 더 이상 필요하지 않은 규칙을 삭제하려면 Actions(작업) 열에서 해당 규칙의 삭제 아이콘()을 클릭합니다.

ID 규칙 생성 및 수정에 대한 자세한 내용은 ID 규칙 구성, 8 페이지를 참조하십시오.

ID 정책 설정 구성

ID 정책이 작동하려면 사용자 ID 정보를 제공하는 소스를 구성해야 합니다. 구성해야 하는 설정은 구성할 규칙의 유형(패시브, 액티브 또는 모두)에 따라 다릅니다.

Settings(설정) 대화 상자에서는 이러한 설정이 개별 섹션에 표시됩니다. 대화 상자에 액세스하는 방법에 따라 두 섹션이 모두 표시될 수도 있고 한 섹션만 표시될 수도 있습니다. 필수 설정을 사전에 구성하지 않은 상태로 인증 유형에 대한 규칙을 생성하려고 하면 대화 상자가 자동으로 나타납니다.

다음 절차에서는 전체 대화 상자에 대해 설명합니다.

시작하기 전에

디렉터리 서버, threat defense 디바이스 및 클라이언트에서 시간 설정이 서로 일치하는지 확인합니다. 이러한 디바이스 간에 시간이 바뀌면 사용자가 정상적으로 인증하지 못할 수 있습니다. 여기서 "일치"란 여러 표준 시간대를 사용할 수는 있지만 이러한 표준 시간대를 기준으로 할 때 시간이 동일해야 한다는 의미입니다. 예를 들어 PST로 오전 10시는 EST로 오후 1시에 해당합니다.

프로시저

단계 **1** **Policies(**정책**)** > **Identity(ID)**를 선택합니다.

단계 **2** **Identity Policy Configuration(ID** 정책 컨피그레이션**)** 버튼()을 클릭하십시오.

단계 **3** **Passive Authentication(**패시브 인증**)** 옵션을 구성합니다.

대화 상자에는 이미 구성한 패시브 인증 소스가 표시됩니다.

필요한 경우 이 대화 상자를 통해 ISE를 구성할 수 있습니다. ISE 개체를 아직 구성하지 않은 경우 **Integrate ISE(ISE** 통합**)** 링크를 클릭하여 바로 ISE 개체를 생성할 수 있습니다. 개체가 있는 경우 해당 상태와 함께 나열됩니다. 상태는 Enabled(활성화됨) 또는 Disabled(비활성화됨)입니다.

패시브 인증 규칙을 생성하려면 하나 이상의 활성화된 패시브 ID 소스를 구성한 상태여야 합니다.

단계 **4** 액티브 인증 옵션을 구성합니다.

ID 규칙에서 사용자에 대한 활성 인증을 요구하는 경우 사용자는 종속 포털 포트로 리디렉션되며, 이후에는 인증하라는 메시지가 표시됩니다. 이러한 설정을 구성하기 전에 활성 인증 모범 사례, 4 페이지 항목을 읽어보십시오.

- **Server Certificate(**서버 인증서**)** — 활성 인증 중에 사용자에게 제공할 내부 인증서를 선택합니다. 필요한 인증서를 아직 생성하지 않은 경우 드롭다운 목록 하단에서 **Create New Internal Certificate(**새 내부 인증서 생성**)**를 클릭합니다.

  사용자의 브라우저에서 이미 신뢰하는 인증서를 업로드하지 않으면 사용자가 인증서를 허용해야 합니다.

- **Redirect to Host Name(**호스트 이름으로 리디렉션**)**(Snort 3.0만 해당) — 활성 인증 요청에 대한 종속 포털로 사용해야 하는 인터페이스의 정규화된 호스트 이름을 정의하는 네트워크 개체를 선택합니다. 개체가 없는 경우, **Create New Network(**새 네트워크 생성**)**를 클릭합니다.

  FQDN은 디바이스에 있는 인터페이스 중 하나의 IP 주소로 확인되어야 합니다. FQDN을 사용하면 클라이언트가 인식할 활성 인증에 대한 인증서를 할당할 수 있으므로, IP 주소로 리디렉션될 때 신뢰할 수 없는 인증서 경고가 표시되지 않습니다. 인증서는 인증서의 SAN(Subject Alternate Name)에 FQDN, 와일드카드 FQDN 또는 여러 FQDN을 지정할 수 있습니다.

  ID 규칙에서 사용자에 대한 활성 인증을 요구하지만 리디렉션 FQDN을 지정하지 않는 경우 사용자는 연결 시 사용한 인터페이스의 캡티브 포털 포트로 리디렉션됩니다.

- **Port(**포트**)** - 캡티브 포털 포트입니다. 기본값은 885(TCP)입니다. 다른 포트를 구성하는 경우에는 포트가 1025-65535 범위에 포함되어야 합니다.

  참고 호스트 이름으로 리디렉션 FQDN을 제공하지 않는 경우 HTTP 기본, HTTP 응답 페이지 및 NTLM 인증 방법에서 인터페이스의 IP 주소를 사용하여 사용자를 캡티브 포털로 리디렉션합니다. 그러나 HTTP 협상의 경우에는 사용자가 정규화된 DNS 이름 *firewall-hostname.AD-domain-name*을 사용하여 리디렉션됩니다. 호스트 이름으로 리디렉션 FQDN 없이 HTTP 협상을 사용하려는 경우에는 DNS 서버도 업데이트하여 활성 인증을 수행해야 하는 모든 내부 인터페이스의 IP 주소에 이 이름을 매핑해야 합니다. 이렇게 하지 않으면 리디렉션을 완료할 수 없으며 사용자가 인증할 수 없습니다. 인증 방법과 무관하게 일관된 동작을 보장하기 위해 항상 호스트 이름으로 리디렉션 FQDN을 제공하는 것이 좋습니다.

단계 **5** (활성 인증에만 해당됨) **Decrypt Re-Sign Certificate(**재서명 암호 해독 인증서**)**에서 재서명된 인증서를 이용하여 암호 해독을 구현하는 규칙에 사용할 내부 CA 인증서를 선택합니다.

사전 정의된 NGFW-Default-InternalCA 인증서를 사용하거나, 생성 또는 업로드한 인증서를 사용할 수 있습니다. 인증서가 아직 없으면 **Create Internal CA(**내부 **CA** 생성**)**를 클릭하여 생성합니다.

클라이언트 브라우저에서 인증서를 아직 설치하지 않은 경우, 다운로드 버튼( )을 클릭하여 복사본을 획득합니다. 인증서 설치 방법에 대한 자세한 내용은 각 브라우저에 대한 설명서를 참조하십시오. 재서명 암호 해독 규칙을 위한 CA 인증서 다운로드도 참조하십시오.

참고 SSL 암호 해독 정책을 아직 구성하지 않은 경우에만 SSL 암호 해독 설정에 대한 프롬프트가 표시됩니다. ID 정책을 활성화한 후에 이러한 설정을 변경하려면 SSL 암호 해독 정책 설정을 편집합니다.

단계 **6** **Save(**저장**)**를 클릭합니다.

ID 정책 기본 작업 구성

ID 정책은 개별 ID 규칙과 일치하지 않는 모든 연결에 대해 구현되는 기본 작업입니다.

실제로 규칙이 없는 것도 정책에 대해 유효한 컨피그레이션입니다. 모든 트래픽 소스에서 패시브 인증을 사용하려는 경우에는 기본 작업으로 패시브 인증을 구성하면 됩니다.

프로시저

단계 **1** **Policies(**정책**)** > **Identity(ID)**를 선택합니다.

단계 **2** **Default Action(**기본 작업**)**을 클릭하고 다음 중 하나를 선택합니다.

- **Passive Auth (Any Identity Source)(**패시브 인증**(**모든 **ID** 소스**))** - ID 규칙과 일치하지 않는 연결에 대해 구성된 모든 패시브 ID 소스를 사용하여 사용자 ID가 결정됩니다. 패시브 ID 소스를 구성하지 않는 경우 Passive Auth(패시브 인증)를 기본값으로 사용하는 것은 No Auth(인증 없음)를 사용하는 것과 같습니다.
- **No Auth (No Authentication Required)(**인증 없음**(**인증 필요 없음**))** - ID 규칙과 일치하지 않는 연결에 대해서는 사용자 ID가 확인되지 않습니다.

ID 규칙 구성

ID 규칙은 일치하는 트래픽에 대해 사용자 ID 정보를 수집할지 여부를 결정합니다. 일치하는 트래픽에 대해 사용자 ID 정보를 가져오지 않으려는 경우에는 인증 없음을 구성할 수 있습니다.

규칙 컨피그레이션에 관계없이 액티브 인증은 HTTP 트래픽에 대해서만 수행됩니다. 따라서 액티브 인증에서 비 HTTP 트래픽을 제외하는 규칙을 생성할 필요가 없습니다. 모든 HTTP 트래픽에 대해 사용자 ID 정보를 가져오려면 모든 소스와 대상에 대해 활성 인증 규칙만 적용하면 됩니다.

참고 인증에서 장애가 발생해도 네트워크 액세스에는 아무 영향이 없습니다. ID 정책은 사용자 ID 정보만 수집합니다. 인증 시에 장애가 발생한 사용자의 네트워크 액세스를 차단하려는 경우에는 액세스 규칙을 사용해야 합니다.

프로시저

단계 **1** **Policies(**정책**)** > **Identity(ID)**를 선택합니다.

단계 **2** 다음 중 하나를 수행합니다.

- 새 규칙을 생성하려면 + 버튼을 클릭합니다.
- 기존 규칙을 수정하려면 해당 규칙의 수정 아이콘( )을 클릭합니다.

더 이상 필요하지 않은 규칙을 삭제하려면 해당 규칙의 삭제 아이콘( )을 클릭합니다.

단계 **3** **Order(**순서**)**에서 순서가 지정된 규칙 목록에 규칙을 삽입할 위치를 선택합니다.

규칙은 처음 일치하는 항목을 기준으로 적용되므로, 매우 구체적인 트래픽 일치 기준이 포함된 규칙이 보다 일반적인 기준이 포함된 정책(규칙이 일치하지 않는 경우 일치하는 트래픽에 적용됨) 위에 표시되도록 삽입해야 합니다.

기본적으로는 규칙이 목록의 끝에 추가됩니다. 나중에 규칙의 위치를 변경하려는 경우 이 옵션을 수정합니다.

단계 **4** **Tile(**제목**)**에서 규칙의 이름을 입력합니다.

단계 **5** **Action(**작업**)**을 선택하고 필요한 경우 **AD Identity Source(AD ID** 소스**)**를 선택합니다.

패시브 및 활성 인증 규칙용 사용자 어카운트를 포함하는 AD ID 영역을 선택해야 합니다. 필요한 영역이 아직 없는 경우, **Create New Identity Realm(**새 **ID** 영역 생성**)**을 클릭하여 바로 생성합니다. 패시브 인증의 경우 단일 AD 영역 개체 대신 AD 영역 시퀀스를 선택할 수 있습니다.

- **Passive Auth(**패시브 인증**)** - 패시브 인증을 통해 사용자 ID를 확인합니다. 구성된 모든 ID 소스가 표시됩니다. 규칙은 구성된 모든 소스를 자동으로 사용합니다.
- **Active Auth(**활성 인증**)** - 활성 인증을 통해 사용자 ID를 확인합니다. 액티브 인증은 HTTP 트래픽에만 적용됩니다. 다른 트래픽 유형이 액티브 인증을 요구하거나 허용하는 ID 정책과 일치하는 경우에는 액티브 인증을 시도하지 않습니다.
- **No Auth(**인증 없음**)** - 사용자 ID를 가져오지 않습니다. 이 트래픽에는 ID 기반 액세스 규칙이 적용되지 않습니다. 이러한 사용자는 인증 필요 없음으로 표시됩니다.

단계 **6** (액티브 인증에만 해당됨) 디렉터리 서버에서 지원하는 인증 방법(유형)을 선택합니다.

- **HTTP** 기본 - 암호화되지 않은 HTTP BA(기본 인증) 연결을 통해 사용자를 인증합니다. 사용자는 브라우저의 기본 인증 팝업 창을 통해 네트워크에 로그인합니다. 이는 기본값입니다.
- **NTLM** - NTLM(NT LAN Manager) 연결을 통해 사용자를 인증합니다. 이 선택 사항은 AD 영역을 선택할 때만 사용 가능합니다. 사용자가 브라우저의 기본 인증 팝업 창을 통해 네트워크에 로그인합니다. 그러나 사용자가 Windows 도메인 로그인을 통해 투명하게 인증을 하도록 IE 및 Firefox 브라우저를 구성할 수 있습니다(투명 사용자 인증 활성화, 12 페이지 참조).
- **HTTP** 협상 - 디바이스가 사용자 에이전트(사용자가 트래픽 흐름을 시작하는 데 사용 중인 애플리케이션)와 Active Directory 서버 간에 방법을 협상할 수 있도록 합니다. 협상 시에는 일반적으로 지원되는 가장 강력한 방법이 순서대로 사용됩니다(NTLM -> 기본). 사용자는 브라우저의 기본 인증 팝업 창을 통해 네트워크에 로그인합니다.
- **HTTP** 대응 페이지 - 시스템 제공 웹 페이지를 통해 인증하라는 메시지를 사용자에게 표시합니다. 이 방법은 일종의 HTTP 기본 인증입니다.

참고 호스트 이름으로 리디렉션 FQDN을 제공하지 않는 경우 HTTP 기본, HTTP 응답 페이지 및 NTLM 인증 방법에서 인터페이스의 IP 주소를 사용하여 사용자를 캡티브 포털로 리디렉션합니다. 그러나 HTTP 협상의 경우에는 사용자가 정규화된 DNS 이름 *firewall-hostname.AD-domain-name*을 사용하여 리디렉션됩니다. 호스트 이름으로 리디렉션 FQDN 없이 HTTP 협상을 사용하려는 경우에는 DNS 서버도 업데이트하여 활성 인증을 수행해야 하는 모든 내부 인터페이스의 IP 주소에 이 이름을 매핑해야 합니다. 이렇게 하지 않으면 리디렉션을 완료할 수 없으며 사용자가 인증할 수 없습니다. 인증 방법과 무관하게 일관된 동작을 보장하기 위해 항상 호스트 이름으로 리디렉션 FQDN을 제공하는 것이 좋습니다.

단계 **7** (활성 인증에만 해당됨) 활성 인증에서 장애가 발생하는 사용자에게 게스트 사용자 레이블을 지정할지를 결정하려면 **Fall Back as Guest(**게스트로 폴백**)** > **On/Off(**켜기/끄기**)**를 선택합니다.

사용자에게는 3번의 인증 기회가 제공됩니다. 인증에서 장애가 발생하면 이 옵션의 선택 여부에 따라 사용자 표시 방법이 결정됩니다. 이러한 값을 기준으로 액세스 규칙을 작성할 수 있습니다.

- **Fall Back as Guest(**게스트로 폴백**)** > **On(**켜기**)** - 사용자가 게스트로 표시됩니다.
- **Fall Back as Guest(**게스트로 폴백**)** > **Off(**끄기**)** - 사용자가 실패한 인증으로 표시됩니다.

단계 **8** **Source/Destination(**소스/대상**)** 탭에서 트래픽 일치 기준을 정의합니다.

HTTP 트래픽에 대해서만 액티브 인증을 시도합니다. 그러므로 비 HTTP 트래픽에 대해서는 인증 없음 규칙을 구성할 필요가 없으며 액티브 인증 규칙을 생성할 필요도 없습니다. 그러나 패시브 인증은 모든 유형의 트래픽에 유효합니다.

ID 규칙의 소스/대상 기준은 트래픽이 통과하는 보안 영역(인터페이스), IP 주소나 IP 주소의 국가나 대륙(지리적 위치) 또는 트래픽에서 사용되는 프로토콜과 포트를 정의합니다. 기본값은 모든 영역, 주소, 지리적 위치, 프로토콜 및 포트입니다.

조건을 수정하려면 해당 조건 내의 **+** 버튼을 클릭하고 필요한 개체나 요소를 선택한 후에 팝업 대화상자에서 **OK(**확인**)**를 클릭합니다. 기준에 개체가 필요한데 필요한 개체가 없는 경우에는 새 개체 생성을 클릭하면 됩니다. 개체 또는 요소의 **x**를 클릭하면 정책에서 해당 개체나 요소를 제거할 수 있습니다.

다음과 같은 트래픽 일치 기준을 구성할 수 있습니다.

소스 영역**,** 대상 영역

트래픽이 통과하는 인터페이스를 정의하는 보안 영역 개체입니다. 기준은 하나 또는 둘 다 정의할 수도 있고 둘 다 정의하지 않을 수도 있습니다. 지정되지 않은 기준은 임의 인터페이스의 트래픽에 적용됩니다.

- 영역 내 인터페이스의 디바이스에서 나가는 트래픽에 일치시키기 위해서는 대상 영역에 해당 영역을 추가합니다.
- 영역 내 인터페이스를 통해 디바이스로 들어오는 트래픽에 일치시키기 위해서는 소스 영역에 해당 영역을 추가합니다.
- 규칙에 소스와 대상 영역 조건을 모두 추가한 경우, 일치하는 트래픽은 반드시 지정된 소스 영역 중 하나에서 발생해야 하며 대상 영역 중 하나를 통해 전송되어야 합니다.

트래픽이 디바이스로 들어오거나 디바이스에서 나가는 위치를 기준으로 규칙을 적용해야 하는 경우 이 기준을 사용해야 합니다. 예를 들어 내부 네트워크에서 생성되는 모든 트래픽에서 사용자 ID를 수집하려는 경우 내부 영역을 소스 영역으로 선택하고 대상 영역은 비워 둡니다.

참고 단일 규칙에서 패시브 보안 영역과 라우팅 보안 영역을 함께 사용할 수는 없습니다. 또한 패시브 보안 영역은 소스 영역으로만 지정할 수 있으며 대상 영역으로 지정할 수는 없습니다.

소스 네트워크, 대상 네트워크

트래픽의 네트워크 주소나 위치를 정의하는 네트워크 개체 또는 지리적 위치입니다.

- 특정 IP 주소 또는 지리적 위치에서 나오는 트래픽을 일치시키려면 소스 네트워크를 구성합니다.
- 특정 IP 주소 또는 지리적 위치로 향하는 트래픽을 일치시키려면 대상 네트워크를 구성합니다.
- 규칙에 소스와 대상 네트워크 조건을 모두 추가한 경우, 일치하는 트래픽은 반드시 지정된 IP 주소 중 하나에서 발생해야 하며 그 목적지가 대상 IP 주소 중 하나여야 합니다.

이 기준을 추가할 때는 다음 탭에서 선택합니다.

- 네트워크 - 제어하려는 트래픽의 소스 또는 대상 IP 주소를 정의하는 네트워크 개체 또는 그룹을 선택합니다.
- 지리위치 - 소스 또는 대상 국가나 대륙을 기준으로 트래픽을 제어하려면 지리적 위치를 선택합니다. 대륙을 선택하면 대륙 내의 모든 국가가 선택됩니다. 규칙에서 지리적 위치를 직접 선택하는 방법 외에, 위치를 정의하기 위해 생성한 지리위치 개체를 선택할 수도 있습니다. 지리적 위치를 사용하면 특정 국가에서 사용될 수 있는 모든 IP 주소를 몰라도 해당 국가에 대한 액세스를 쉽게 제한할 수 있습니다.

  참고 최신 지리적 위치 데이터를 사용하여 트래픽을 필터링하려면 GeoDB(geolocation database)를 정기적으로 업데이트하는 것이 좋습니다.

소스 포트, 대상 포트/프로토콜

트래픽에 사용되는 프로토콜을 정의하는 포트 개체입니다. TCP/UDP의 경우 여기에는 포트가 포함될 수 있습니다.

- 특정 프로토콜이나 포트에서 나오는 트래픽을 일치시키려면 소스 포트를 구성합니다. 소스 포트는 TCP/UDP 전용일 수 있습니다.
- 특정 프로토콜이나 포트로 향하는 트래픽을 일치시키려면 대상 포트/프로토콜을 구성합니다.
- 특정 TCP/UDP 포트에서 발생하는 트래픽과 특정 TCP/UDP 포트로 향하는 트래픽을 모두 일치시키려면 두 포트를 모두 구성합니다. 조건에 소스 및 대상 포트를 모두 추가한 경우, 단일 전송 프로토콜(TCP 또는 UDP)을 공유하는 포트만 추가할 수 있습니다. 예를 들어 포트 TCP/80에서 포트 TCP/8080으로 이동하는 트래픽을 대상으로 지정할 수 있습니다.

단계 **9** **OK(**확인**)**를 클릭합니다.

투명 사용자 인증 활성화

액티브 인증을 허용하도록 ID 정책을 구성하는 경우 다음 인증 방법을 통해 사용자 ID를 가져올 수 있습니다.

HTTP 기본

HTTP 기본 인증을 사용하는 경우 사용자에게 디렉터리 사용자 이름과 비밀번호를 사용하여 인증하라는 메시지가 항상 표시됩니다. 비밀번호는 일반 텍스트로 전송됩니다. 그러므로 기본 인증은 안전한 인증 형식으로 간주되지 않습니다.

기본은 기본적으로 사용되는 인증 메커니즘입니다.

HTTP 대응 페이지

사용자에게 로그인 브라우저 페이지가 표시되는 HTTP 기본 인증 유형입니다.

NTLM, HTTP 협상**(Active Directory**용 **Windows** 통합 인증**)**

Windows 통합 인증을 사용할 때는 사용자가 워크스테이션을 사용하기 위해 도메인에 로그인하는 방식을 활용합니다. 브라우저는 서버에 액세스할 때 이 도메인 로그인 사용을 시도합니다(활성 인증 중의 위협 방어 캡티브 포털 포함). 비밀번호는 전송되지 않습니다. 인증이 성공하면 사용자는 투명 방식으로 인증되므로 인증 과정이 수행되었는지 또는 처리되었는지를 알 수 없습니다.

브라우저가 도메인 로그인 크리덴셜을 사용하여 인증 요청을 처리할 수 없으면 사용자에게 사용자 이름과 비밀번호를 입력하라는 메시지가 표시됩니다. 이러한 방식은 기본 인증과 동일한 사용자 환경입니다. 따라서 Windows 통합 인증을 구성하는 경우에는 사용자가 같은 도메인의 네트워크나 서버에 액세스할 때 크리덴셜을 입력해야 할 필요가 감소합니다.

HTTP 협상은 Active Directory 서버와 사용자 에이전트에서 모두 지원하는 가장 강력한 방법을 선택합니다. 협상에서 인증 방법으로 HTTP 기본을 선택하는 경우에는 투명 인증 기능이 제공되지 않습니다. 강도의 순서는 NTLM, 기본입니다. 투명 인증을 수행하려면 협상에서 NTLM을 선택해야 합니다.

투명 인증을 활성화하려면 클라이언트 브라우저가 Windows 통합 인증을 지원하도록 구성해야 합니다. 다음 섹션에서는 Windows 통합 인증을 지원하는 흔히 사용되는 몇 가지 브라우저에 대한 Windows 통합 인증의 일반적인 요건 및 기본 컨피그레이션에 대해 설명합니다. 사용되는 기술은 소프트웨어 릴리스 간에 변경될 수 있으므로, 사용자는 사용 중인 브라우저나 다른 사용자 에이전트의 도움말을 참조해야 합니다.

팁 모든 브라우저에서 Windows 통합 인증을 지원하는 것은 아닙니다. 예를 들어 이 문서를 작성하는 시점의 버전을 기준으로 할 때 Chrome 및 Safari와 같은 브라우저는 해당 인증을 지원하지 않습니다. 이러한 브라우저의 경우 사용자에게 사용자 이름과 비밀번호를 입력하라는 메시지가 표시됩니다. 브라우저 설명서를 참조하여 사용 중인 버전에서 지원되는지 확인하십시오.

투명 인증 요구사항

사용자는 투명 인증을 구현하도록 브라우저 또는 사용자 에이전트를 구성해야 합니다. 이 작업은 사용자가 개별적으로 수행할 수도 있고, 관리자가 사용자를 위해 브라우저 또는 사용자 에이전트를 구성한 다음 소프트웨어 배포 툴을 사용해 클라이언트 워크스테이션으로 해당 컨피그레이션을 푸시할 수도 있습니다. 사용자가 이 작업을 직접 수행하도록 하는 경우 네트워크에서 사용되는 특정 컨피그레이션 파라미터를 제공해야 합니다.

브라우저 또는 사용자 에이전트와 관계없이 다음과 같은 일반 컨피그레이션을 구현해야 합니다.

- 사용자가 네트워크에 연결하는 데 사용하는 위협 방어 리디렉션 호스트 이름 또는 인터페이스를 신뢰할 수 있는 사이트 목록에 추가합니다. 리디렉션 호스트 이름을 사용하지 않는 경우 IP 주소를 사용할 수도 있고, 사용 가능한 경우 inside.example.com과 같은 정규화된 호스트 이름(FQDN)을 사용할 수도 있습니다. 와일드카드 또는 부분 주소를 사용하여 일반화된 신뢰할 수 있는 사이트를 생성할 수도 있습니다. 예를 들어, 일반적으로 *.example.com 또는 단순히 example.com을 사용하여 모든 내부 사이트를 포함하면 네트워크의 모든 서버를 신뢰할 수 있습니다(자신의 도메인 이름을 사용). 인터페이스의 특정 주소를 추가하는 경우에는 모든 사용자 액세스 포인트가 네트워크를 가리키도록 신뢰할 수 있는 사이트에 여러 주소를 추가해야 할 수 있습니다.
- Windows 통합 인증은 프록시 서버를 통해 작동하지 않습니다. 따라서 프록시를 사용하지 않거나, 프록시를 통과하지 않도록 제외되는 주소에 위협 방어 리디렉션 호스트 이름 또는 인터페이스를 추가해야 합니다. 프록시를 사용해야 하도록 결정하는 경우에는 NTLM을 사용하더라도 사용자에게 인증하라는 메시지가 표시됩니다.

팁 투명 인증은 반드시 구성해야 하는 것은 아니며 엔드 유저의 편의를 위해 구성하는 기능입니다. 투명 인증을 구성하지 않으면 모든 인증 방법에서 사용자에게 로그인 과정이 제공됩니다.

투명 인증을 위해 **Internet Explorer** 구성

NTLM 투명 인증을 위해 Internet Explorer를 구성하려면 다음 단계를 수행합니다.

프로시저

단계 **1** **Tools(**도구**) > Internet Options(**인터넷 옵션**)**을 선택합니다.

단계 **2** **Security(**보안**)** 탭과 **Local Intranet(**로컬 인트라넷**)** 영역을 차례로 선택하고 다음을 수행합니다.

a) **Sites(**사이트**)** 버튼을 클릭하여 신뢰할 수 있는 사이트 목록을 엽니다.

b) 다음 옵션 중 하나 이상이 선택되어 있는지 확인합니다.

- **Automatically detect intranet network(**인트라넷 네트워크를 자동으로 검색**)**. 이 옵션을 선택하면 다른 옵션은 모두 비활성화됩니다.
- **Include all sites that bypass the proxy(**프록시 서버를 건너뛰는 사이트를 모두 포함**)**

c) **Advanced(**고급**)**를 클릭하여 로컬 인트라넷 사이트 대화 상자를 열고 신뢰하려는 URL을 **Add Site(**사이트 추가**)** 상자에 붙여넣은 후에 **Add(**추가**)**를 클릭합니다.

URL이 두 개 이상인 경우 이 프로세스를 반복합니다. 부분 URL을 지정하려면 와일드카드를 사용합니다. 예를 들어 **`http://*.example.com`**과 같이 입력할 수도 있고 **`*.example.com`**만 입력할 수도 있습니다.

대화 상자를 닫고 인터넷 옵션 대화 상자로 돌아옵니다.

d) **Local Intranet(**로컬 인트라넷**)**을 계속 선택한 상태로 **Custom Level(**맞춤형 레벨**)**을 클릭하여 보안 설정 대화 상자를 엽니다. **User Authentication(**사용자 인증**)** > **Logon(**로그온**)** 설정을 찾아서 인트라넷 영역에서만 자동으로 로그온을 선택합니다. **OK(**확인**)**를 클릭합니다.

단계 **3** 인터넷 옵션 대화 상자에서 **Connections(**연결**)** 탭을 클릭한 다음 **LAN Settings(LAN** 설정**)**를 클릭합니다.

Use a proxy server for your LAN(LAN에 프록시 서버 사용**)**이 선택되어 있으면 위협 방어 인터페이스가 프록시를 우회하는지 확인해야 합니다. 이렇게 하려면 다음 중 적절한 작업을 수행합니다.

- 로컬 주소에 프록시 서버 건너뛰기를 선택합니다.
- **Advanced(**고급**)**를 클릭하고 다음으로 시작하는 주소에는 프록시 서버 사용 안 함 상자에 주소를 입력합니다. **`*.example.com`**과 같은 와일드카드를 사용할 수 있습니다.

투명 인증을 위해 **Firefox** 구성

NTLM 투명 인증을 위해 Firefox를 구성하려면 다음 단계를 수행합니다.

프로시저

단계 **1** **about:config**를 엽니다. 필터 막대를 사용하여 수정해야 하는 기본 설정을 찾습니다.

단계 **2** NTLM을 지원하려면 다음 기본 설정을 수정합니다(network.automatic으로 필터링).

- **network.automatic-ntlm-auth.trusted-uris** - 기본 설정을 더블 클릭하고 URL을 입력한 후에 **OK(**확인**)**를 클릭합니다. URL이 여러 개이면 쉼표로 구분하여 입력할 수 있습니다. 프로토콜은 원하는 경우 입력하면 됩니다. 예를 들면 다음과 같습니다.

```
http://host.example.com, http://hostname, myhost.example.com
```

부분 URL을 사용할 수도 있습니다. Firefox는 임의 하위 문자열이 아닌 문자열 끝이 일치하는지를 확인합니다. 그러므로 도메인 이름만 지정하여 전체 내부 네트워크를 포함할 수 있습니다. 예를 들면 다음과 같습니다.

```
example.com
```

- **network.automatic-ntlm-auth.allow-proxies** - 값이 기본값인 **true**인지 확인합니다. 값이 현재 false인 경우 더블 클릭하여 값을 변경합니다.

단계 **3** HTTP 프록시 설정을 확인합니다. **Tools(**툴**)** > **Options(**옵션**)**를 선택한 다음 옵션 대화 상자의 **Network(**네트워크**)** 탭을 클릭하여 이러한 옵션을 찾을 수 있습니다. 연결 그룹에서 **Settings(**설정**)** 버튼을 클릭합니다.

- **No Proxy(**프록시 없음**)**이 선택되어 있으면 구성할 항목이 없는 것입니다.
- **Use System Proxy Settings(**시스템 프록시 설정 사용**)**이 선택되어 있으면 about:config에서 **network.proxy.no_proxies_on** 속성을 수정하여 **network.automatic-ntlm-auth.trusted-uris**에 포함한 신뢰할 수 있는 URI를 추가해야 합니다.
- **Manual Proxy Configuration(**수동 프록시 컨피그레이션**)**이 선택되어 있으면 이러한 신뢰할 수 있는 URI가 포함되도록 프록시 없음 목록을 업데이트합니다.
- 다른 옵션 중 하나가 선택되어 있으면 해당 컨피그레이션에 사용되는 속성에서 동일한 신뢰할 수 있는 URI가 제외되는지를 확인합니다.

ID 정책 모니터링

인증이 필요한 ID 정책이 올바르게 작동하는 경우 **Monitoring(**모니터링**)** > **Users(**사용자**)** 대시보드와 사용자 정보를 포함하는 기타 대시보드에 사용자 정보가 표시됩니다.

또한, **Monitoring(**모니터링**)** > **Events(**이벤트**)**에 표시되는 이벤트에 사용자 정보가 포함됩니다.

사용자 정보가 표시되지 않으면 디렉터리 서버가 올바르게 작동하고 있는지 확인하십시오. 연결을 확인하려면 디렉터리 서버 컨피그레이션 대화 상자의 **Test(**테스트**)** 버튼을 사용합니다.

디렉터리 서버가 작동 중이며 사용 가능한 경우 활성 인증이 필요한 ID 규칙의 트래픽 일치 기준이 사용자를 일치시키는 방식으로 작성되어 있는지 확인합니다. 예를 들어 사용자 트래픽이 디바이스에 진입하는 경로로 사용되는 인터페이스가 소스 영역에 포함되어 있는지 확인합니다. 활성 인증 ID 규칙은 HTTP 트래픽만 일치시키므로 사용자는 디바이스를 통해 이 트래픽 유형을 전송해야 합니다.

패시브 인증의 경우 해당 소스를 사용 중이라면 ISE 개체에서 **Test(**테스트**)** 버튼을 사용합니다. 원격 액세스 VPN을 사용 중이라면 서비스가 정상 작동하며 사용자가 VPN 연결을 할 수 있는지 확인합니다. 문제 파악 및 해결에 대한 자세한 정보는 이러한 기능의 트러블슈팅 주제를 참조하십시오.

ID 정책의 예시

사용 사례 장에는 ID 정책을 구현하는 예시가 포함되어 있습니다. 네트워크 트래픽을 파악하는 방법의 내용을 참조하십시오.