사용자 ID 정책

다음 주제는 ID 규칙과 ID 정책을 만들고 관리하는 방법을 설명합니다.

ID 정책 정보

ID 정책에는 ID 규칙이 포함됩니다. ID 규칙은 트래픽 집합을 영역 및 인증 방법(패시브 인증, 활성 인증, 인증 없음)과 연결합니다.

다음 단락에서 언급하는 예외 사항이 아닌 이상, 사용하려는 영역과 인증 방법을 먼저 설정해야 ID 규칙에서 이를 호출할 수 있습니다.

- ID 정책 외부, **System(**시스템**)** > **Integration(**통합**)** > **Realms(**영역**)**에서 영역을 설정합니다. 자세한 내용은 Active Directory 영역 및 영역 디렉터리 생성를 참고하십시오.
- **System(**시스템**)** > **Integration(**통합**)** > **Identity Sources(ID** 소스**)**에서 패시브 인증 ID 소스인 ISE/ISE-PIC를 구성합니다. 자세한 내용은 사용자 제어를 위한 ISE/ISE-PIC 설정를 참고하십시오.
- Firepower System 외부에서 패시브 인증 ID 소스인 TS 에이전트를 설정합니다. 자세한 내용은 *Cisco TS(Terminal Services)* 에이전트 가이드를 참조하십시오.
- ID 정책 내에서 액티브 인증 ID 소스인 캡티브 포털을 설정합니다. 자세한 내용은 사용자 제어에 대한 캡티브 포털 설정 방법를 참고하십시오.

- Remote Access VPN 정책에서 액티브 인증 ID 소스인 Remote Access VPN을 설정합니다. 자세한 내용은 Remote Access VPN 인증를 참고하십시오.

여러 ID 규칙을 단일 ID 정책에 추가한 후, 규칙 순서를 지정합니다. 시스템은 오름차순 규칙 번호에 따라 하향식 순서로 트래픽이 규칙과 일치하는지를 확인합니다. 트래픽에 일치하는 첫 번째 규칙이 트래픽을 처리하는 규칙입니다.

선택적으로 ID 개체를 설정하여 네트워크 개체별로 트래픽을 필터링할 수 있습니다. 그러면 디바이스가 메모리 제한에 도달하거나 메모리 제한에 근접할 경우 각 디바이스가 모니터링하는 네트워크가 제한됩니다. 디바이스에서 네트워크 필터링을 적용하려면 threat defense 버전 6.7 이상을 실행해야 합니다.

하나 이상의 ID 정책을 설정한 후에는 ID 정책 하나를 액세스 컨트롤 정책에 연결해야 합니다. 네트워크의 트래픽이 ID 규칙의 조건과 일치하면, 시스템은 트래픽을 지정된 영역과 연결하며 지정한 ID 소스를 사용하여 트래픽의 사용자를 인증합니다.

ID 정책을 구성하지 않으면 시스템은 사용자 인증을 수행하지 않습니다.

ID 정책 생성 예외 사항

ID 정책은 다음이 모두 참인 경우 필요하지 않습니다.

- ISE/ISE-PIC ID 소스를 사용합니다.
- 액세스 제어 정책에서 사용자 또는 그룹을 사용하지 않습니다.
- 액세스 제어 정책에서 SGT(Security Group Tag)를 사용합니다. 자세한 내용은 ISE SGT 및 맞춤형 SGT 규칙 조건 비교를 참고하십시오.

관련 항목

ID 정책 설정 방법

ID 정책 라이선스 요구 사항

Threat Defense 라이선스

모두

기본 라이선스

제어

ID 정책 요구 사항 및 사전 요건

모델 지원

모두

지원되는 도메인

모든

사용자 역할

- 관리자
- 액세스 관리자
- 네트워크 관리자

ID 정책 생성

시작하기 전에

액세스 컨트롤 정책의 영역에서 사용자와 그룹을 사용하려면 ID 정책이 있어야 합니다. Active Directory 영역 및 영역 디렉터리 생성에 설명된 대로 하나 이상의 영역을 생성하고 활성화합니다.

(선택 사항). 특정 매니지드 디바이스가 많은 사용자 그룹을 모니터링하는 경우 시스템은 매니지드 디바이스 메모리 제한으로 인해 그룹을 기준으로 사용자 매핑을 삭제할 수 있습니다. 그 결과, 영역이 있는 규칙 또는 사용자 조건이 정상적으로 수행되지 않을 수 있습니다. 디바이스가 버전 6.7 이상에서 실행되는 경우 하나의 네트워크 또는 네트워크 그룹 개체에 의한 트래픽 만 모니터링하도록 ID 규칙을 설정할 수 있습니다. 네트워크 개체를 생성하려면 네트워크 개체 생성의 내용을 참조하십시오.

ID 정책은 다음이 모두 참인 경우 필요하지 않습니다.

- ISE/ISE-PIC ID 소스를 사용합니다.
- 액세스 제어 정책에서 사용자 또는 그룹을 사용하지 않습니다.
- 액세스 제어 정책에서 SGT(Security Group Tag)를 사용합니다. 자세한 내용은 ISE SGT 및 맞춤형 SGT 규칙 조건 비교를 참고하십시오.

프로시저

단계 **1** management center에 로그인합니다.

단계 **2** **Policies(**정책**)** > **Access Control(**액세스 제어**)** > **Identity(ID)** 을(를) 클릭하고 **New Policy(**새로운 정책**)**를 클릭합니다.

단계 **3** **Name(**이름**)**을 입력하고 필요한 경우, **Description(**설명**)**을 입력합니다.

단계 **4** **Save(**저장**)**를 클릭합니다.

단계 **5** 정책에 규칙을 추가하려면 ID 규칙 생성, 12 페이지에 설명된 대로 **Add Rule(**규칙 추가**)**을 클릭합니다.

단계 **6** 규칙 카테고리를 생성하려면 **Add Category(**카테고리 추가**)**를 클릭합니다.

단계 **7** 캡티브 포털 활성 인증을 설정하려면 **Active Authentication(**활성 인증**)**을 클릭하고 캡티브 포털 설정 2부: ID 정책 생성 항목을 참고하십시오.

단계 **8** (선택 사항). 네트워크 개체별로 트래픽을 필터링하려면 **Identity Source(ID** 소스**)** 탭을 클릭합니다. 목록에서 이 ID 정책에 대한 트래픽을 필터링하는 데 사용할 네트워크 개체를 클릭합니다. 새 네트워크 개체를 생성하기 위해 **Add(**추가**)** (+)을 클릭합니다.

단계 **9** **Save(**저장**)**를 클릭하여 ID 정책을 저장합니다.

다음에 수행할 작업

- 일치시킬 사용자를 지정하는 ID 정책과 기타 옵션을 규칙에 추가합니다(ID 규칙 생성, 12 페이지 참조).
- ID 정책을 액세스 컨트롤 정책에 연결해 선택한 사용자가 지정된 리소스에 액세스하도록 허용하거나 액세스하지 못하게 합니다(액세스 제어에 다른 정책 연결 참조).
- 매니지드 디바이스에 설정 변경사항을 구축합니다(구성 변경 사항 구축 참조).

문제가 발생하는 경우에는 사용자 제어 문제 해결, 15 페이지 섹션을 참조하십시오.

관련 항목

캡티브 포털 설정 2부: ID 정책 생성
ID 매핑 필터 생성, 4 페이지
캡티브 포털(captive portal) 필드
사용자 제어 문제 해결, 15 페이지

ID 매핑 필터 생성

ID 매핑 필터는 ID 규칙이 적용되는 네트워크를 제한하는 데 사용할 수 있습니다. 예를 들어, management center가 제한된 양의 메모리가 있는 FTD를 관리하는 경우 모니터링하는 네트워크를 제한할 수 있습니다.

또한 선택적으로 ISE에서 사용자-IP 및 SGT(Security Group Tag)-IP 매핑을 수신하는 서브넷을 제외할 수 있습니다. 일반적으로 Snort ID 상태 모니터 메모리 오류를 방지하기 위해 메모리 부족 관리 디바이스에 대해 이 작업을 수행해야 합니다.

시작하기 전에

다음 작업을 수행 합니다.

1. ID 정책에 필요한 영역을 생성합니다. Active Directory 영역 및 영역 디렉터리 생성의 내용을 참조하십시오.
2. ID 정책을 생성합니다. ID 정책 생성, 3 페이지의 내용을 참조하십시오.
3. (선택 사항). 네트워크 개체 생성에 설명된 대로 네트워크 개체 또는 네트워크 그룹 개체를 생성합니다. 생성하는 네트워크 개체 또는 그룹은 ID 정책에서 관리되는 디바이스가 모니터링할 네트워크를 정의해야 합니다.

ID 매핑 필터를 구성할 때 생성할 수 있으므로 이 단계는 선택 사항입니다.

프로시저

단계 **1** management center에 로그인합니다.

단계 **2** **Policies(**정책**)** > **Identity(ID)**를 클릭합니다.

단계 **3** **Edit(**수정**)** ( ) 버튼을 클릭합니다.

단계 **4** **Identity Sources(ID** 소스**)** 탭을 클릭합니다.

단계 **5** **Identity Mapping Filter(ID** 매핑 필터**)** 목록에서 필터로 사용할 네트워크 개체의 이름을 선택하거나 새 개체를 생성하려면 **Plus(**더하기**)** ( )를 클릭합니다.

새 네트워크 개체를 생성하려면 네트워크 개체 생성의 내용을 참조하십시오.

단계 **6** **Save(**저장**)**를 클릭합니다.

단계 **7** 매니지드 디바이스에 설정 변경사항을 구축합니다(구성 변경 사항 구축 참조).

다음에 수행할 작업

액세스 제어에 다른 정책 연결에 설명된 대로 ID 정책을 액세스 제어 정책과 연결합니다.

ISE ID 매핑 필터(서브넷 필터라고도 함)를 확인하거나 변경하려면 다음 명령을 사용합니다.

```
show identity-subnet-filter
configure identity-subnet-filter { add | remove } subnet
```

ID 규칙 조건

규칙 조건을 사용하면 제어하려는 사용자 및 네트워크를 대상으로 ID 정책을 미세 조정할 수 있습니다. 자세한 내용은 다음 섹션 중 하나를 참조하십시오.

관련 항목

보안 영역 규칙 조건
네트워크 규칙 조건
VLAN 태그 규칙 조건
포트 규칙 조건
영역 및 설정 규칙 조건, 10 페이지

보안 영역 규칙 조건

보안 영역은 네트워크를 세그멘테이션화하여 여러 디바이스에 걸쳐 인터페이스를 그룹화하는 방법을 통해 트래픽 흐름을 관리하고 분류할 수 있도록 지원합니다.

영역 규칙의 조건은 소스 및 대상 보안 영역을 통해 트래픽을 제어합니다. 소스 및 대상 영역 모두 영역 조건에 추가할 경우 소스 영역 중 하나의 인터페이스에서 트래픽 매치를 시작하고 대상 영역 중 하나의 인터페이스에서 종료해야 합니다.

영역의 모든 인터페이스가 동일한 유형이어야 하는 것과 마찬가지로(모든 인라인, 수동, 스위칭 또는 라우팅), 영역 조건에 사용된 모든 영역도 동일한 유형이어야 합니다. 패시브 방식으로 구축된 디바이스는 트래픽을 전송하지 않으므로 패시브 인터페이스를 대상 영역으로 하면서 영역을 사용할 수 없습니다.

특히 보안 영역, 네트워크 개체 및 포트 개체에 대한 일치 기준은 가능한 경우 항상 비워 둡니다. 여러 기준을 지정하는 경우 시스템에서는 지정된 기준의 모든 콘텐츠 조합에 대해 일치시켜야 합니다.

팁 영역으로 규칙을 제한하는 것은 시스템 성능을 개선할 수 있는 가장 좋은 방법 중 하나입니다. 규칙이 디바이스의 인터페이스를 통과하는 트래픽에 적용되지 않을 경우, 해당 규칙은 해당 디바이스의 성능에 영향을 미치지 않습니다.

보안 영역 조건 및 멀티테넌시

다중 도메인 구축에서, 상위 도메인에 생성된 영역은 다른 도메인의 디바이스에 있는 인터페이스를 포함할 수 있습니다. 하위 도메인의 영역 조건을 구성할 경우, 컨피그레이션은 사용자가 볼 수 있는 인터페이스에만 적용됩니다.

네트워크 규칙 조건

네트워크 규칙 조건은 내부 헤더를 사용하여 트래픽의 소스 및 대상 IP 주소를 기준으로 삼아 트래픽을 제어합니다. 외부 헤더를 사용하는 터널 규칙에는 네트워크 조건 대신 터널 엔드포인트 조건이 있습니다.

사전 정의된 개체를 사용하여 네트워크 조건을 작성하거나, 수동으로 개별 IP 주소 또는 주소 블록을 지정할 수 있습니다.

참고 ID 규칙에서 FDQN 네트워크 개체를 사용할 수 없습니다.

참고 시스템은 각 리프 도메인에 대해 별도의 네트워크 맵을 작성합니다. 다중 도메인 구축에서 리터럴 IP 주소를 사용하여 이 컨피그레이션을 제한하면 예기치 않은 결과가 발생할 수 있습니다. 하위 도메인 관리자는 재정의가 활성화된 개체를 사용하여 로컬 환경에 맞게 글로벌 컨피그레이션을 조정할 수 있습니다.

특히 보안 영역, 네트워크 개체 및 포트 개체에 대한 일치 기준은 가능한 경우 항상 비워 둡니다. 여러 기준을 지정하는 경우 시스템에서는 지정된 기준의 모든 콘텐츠 조합에 대해 일치시켜야 합니다.

호스트네임 네트워크 규칙 조건으로 리디렉션

(Snort 3.0만 해당)—캡티브 포털에서 활성 인증 요청에 사용할 수 있는 인터페이스의 FQDN(정규화된 호스트 이름)이 포함된 네트워크 개체를 사용할 수 있습니다.

FQDN은 관리되는 디바이스에 있는 인터페이스 중 하나의 IP 주소로 확인되어야 합니다. FQDN을 사용하면 클라이언트가 인식할 활성 인증에 대한 인증서를 할당할 수 있으므로, 매니지드 디바이스 IP 주소로 리디렉션될 때 신뢰할 수 없는 인증서 경고가 표시되지 않습니다.

인증서는 인증서의 SAN(Subject Alternate Name)에 하나의 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 매니지드 디바이스 인터페이스의 캡티브 포털 포트로 리디렉션됩니다.

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.directory-server-domain-name*을 사용하여 리디렉션됩니다. 호스트 이름으로 리디렉션 FQDN 없이 HTTP 협상을 사용하려면 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.

VLAN 태그 규칙 조건

참고 액세스 규칙의 VLAN 태그는 인라인 집합에만 적용됩니다. VLAN 태그가 있는 액세스 규칙은 방화벽 인터페이스의 트래픽과 일치하지 않습니다.

VLAN 규칙 조건은 Q-in-Q(스택 VLAN) 트래픽을 포함한 VLAN 태그가 있는 트래픽을 제어합니다. 시스템은 가장 안쪽의 VLAN 태그를 사용하여 VLAN 트래픽을 필터링하며, 규칙에서 가장 바깥쪽의 VLAN 태그를 사용하는 사전 필터 정책은 예외입니다.

다음 Q-in-Q 지원에 유의하십시오.

- Firepower 4100/9300의 Threat Defense - Q-in-Q를 지원하지 않습니다(하나의 VLAN 태그만 지원).
- 다른 모든 모델의 Threat Defense:
  - 인라인 집합 및 패시브 인터페이스 - Q-in-Q를 지원합니다(최대 2개의 VLAN 태그 지원).
  - 방화벽 인터페이스 - Q-in-Q를 지원하지 않습니다(하나의 VLAN 태그만 지원).

사전 정의된 개체를 사용하여 VLAN 조건을 작성하거나, 1에서 4094 사이의 VLAN 태그를 수동으로 입력할 수 있습니다. VLAN 태그의 범위를 지정하려면 하이픈을 사용합니다.

클러스터에서 VLAN 일치에 문제가 발생하면 액세스 제어 정책 고급 옵션인 Transport/Network Preprocessor Settings(전송/네트워크 전처리기 구성)를 편집하고 **Ignore VLAN header when tracking connections(**연결 추적 시 **VLAN** 헤더 무시**)** 옵션을 선택합니다.

참고 시스템은 각 리프 도메인에 대해 별도의 네트워크 맵을 작성합니다. 다중 도메인 구축에서 리터럴 VLAN 태그를 사용하여 이 컨피그레이션을 제한하면 예기치 않은 결과가 발생할 수 있습니다. 하위 도메인 관리자는 재정의가 활성화된 개체를 사용하여 로컬 환경에 맞게 글로벌 컨피그레이션을 조정할 수 있습니다.

포트 규칙 조건

포트 조건을 사용하면 소스 및 대상 포트를 기준으로 트래픽을 제어할 수 있습니다.

특히 보안 영역, 네트워크 개체 및 포트 개체에 대한 일치 기준은 가능한 경우 항상 비워 둡니다. 여러 기준을 지정하는 경우 시스템에서는 지정된 기준의 모든 콘텐츠 조합에 대해 일치시켜야 합니다.

포트 기반 규칙 모범 사례

포트를 지정하는 것은 애플리케이션을 대상으로 하는 기존의 방법입니다. 그러나 고유한 포트를 사용하여 액세스 제어 블록을 우회하도록 애플리케이션을 설정할 수 있습니다. 따라서 트래픽을 대상으로 지정하려면 가능한 경우 항상 포트 기준 대신 애플리케이션 필터링 기준을 사용하십시오.

FTD와 같이 제어와 데이터 흐름을 위해 별도의 채널을 동적으로 여는 애플리케이션에도 애플리케이션 필터링이 권장됩니다. 포트 기반 액세스 제어 규칙을 사용하면 이러한 종류의 애플리케이션이 올바르게 작동하지 못하게 되어 적절한 연결이 차단될 수 있습니다.

소스 및 대상 포트 제약 조건 사용

소스 및 대상 포트 제약 조건을 모두 추가할 경우 단일 전송 프로토콜(TCP 또는 UDP)을 공유하는 포트만 추가할 수 있습니다. 예를 들어, 소스 포트로 DNS over TCP를 추가한 경우, 대상 포트에 Yahoo 메신저 음성 채팅(TCP)을 추가할 수 있지만 Yahoo 메신저 음성 채팅(UDP)은 해당되지 않습니다.

소스 포트만 또는 대상 포트만 추가할 경우 다른 전송 프로토콜을 사용하는 포트를 추가할 수 있습니다. 예를 들어, DNS over TCP 및 DNS over UDP 모두를 단일 액세스 제어 규칙의 소스 포트 조건으로 추가할 수 있습니다.

포트, 프로토콜 및 ICMP 코드 규칙 조건

포트 조건은 소스 및 대상 포트를 기준으로 트래픽과 일치합니다. 규칙 유형에 따라, "포트"는 다음 중 하나를 나타낼 수 있습니다.

- TCP 및 UDP — 포트를 기준으로 TCP 및 UDP 트래픽을 제어할 수 있습니다. 시스템은 괄호 내 프로토콜 번호와 선택적으로 결합된 포트 또는 포트 범위를 사용하여 이 구성을 나타냅니다. 예: TCP(6)/22
- ICMP — 인터넷 레이어 프로토콜과 선택적 유형 및 코드에 따라 ICMP 및 ICMPv6(IPv6-ICMP) 트래픽을 제어할 수 있습니다. 예: ICMP(1):3:3

- Protocol(프로토콜) - 포트를 사용하지 않는 다른 프로토콜을 사용하여 트래픽을 제어할 수 있습니다.

특히 보안 영역, 네트워크 개체 및 포트 개체에 대한 일치 기준은 가능한 경우 항상 비워 둡니다. 여러 기준을 지정하는 경우 시스템에서는 지정된 기준의 모든 콘텐츠 조합에 대해 일치시켜야 합니다.

포트 기반 규칙 모범 사례

포트를 지정하는 것은 애플리케이션을 대상으로 하는 기존의 방법입니다. 그러나 고유한 포트를 사용하여 액세스 제어 블록을 우회하도록 애플리케이션을 설정할 수 있습니다. 따라서 트래픽을 대상으로 지정하려면 가능한 경우 항상 포트 기준 대신 애플리케이션 필터링 기준을 사용하십시오. 사전 필터 규칙에서는 애플리케이션 필터링을 사용할 수 없습니다.

FTP와 같이 제어와 데이터 흐름을 위해 별도의 채널을 동적으로 여는 애플리케이션에도 애플리케이션 필터링이 권장됩니다. 포트 기반 액세스 제어 규칙을 사용하면 이러한 종류의 애플리케이션이 올바르게 작동하지 못하게 되어 적절한 연결이 차단될 수 있습니다.

소스 및 대상 포트 제약 조건 사용

소스 및 대상 포트 제약 조건을 모두 추가할 경우 단일 전송 프로토콜(TCP 또는 UDP)을 공유하는 포트만 추가할 수 있습니다. 예를 들어, 소스 포트로 DNS over TCP를 추가한 경우, 대상 포트에 Yahoo 메신저 음성 채팅(TCP)을 추가할 수 있지만 Yahoo 메신저 음성 채팅(UDP)은 해당되지 않습니다.

소스 포트만 또는 대상 포트만 추가할 경우 다른 전송 프로토콜을 사용하는 포트를 추가할 수 있습니다. 예를 들어, DNS over TCP 및 DNS over UDP 모두를 단일 액세스 제어 규칙의 대상 포트 조건으로 추가할 수 있습니다.

비 **TCP** 트래픽을 포트 조건과 일치

비 포트 기반 프로토콜을 매칭할 수 있습니다. 기본적으로 포트 조건을 지정하지 않으면 IP 트래픽이 일치하게 됩니다. 비 TCP 트래픽과 일치하도록 포트 조건을 구성할 수 있지만, 몇 가지 제한 사항이 있습니다.

- 액세스 제어 규칙 - 기본 디바이스의 경우 GRE(47) 프로토콜을 대상 포트 조건으로 사용하는 방법으로 GRE 캡슐화 트래픽을 액세스 제어 규칙과 매치할 수 있습니다. GRE 제한 규칙에는 네트워크 기반 조건(영역, IP 주소, 포트, VLAN 태그)만 추가할 수 있습니다. 또한, 시스템은 외부 헤더를 사용하여 액세스 제어 정책의 모든 트래픽을 GRE 제한 규칙과 일치시킵니다. threat defense 디바이스의 경우, 사전 필터 정책의 터널 규칙을 사용하여 GRE 캡슐화된 트래픽을 제어합니다.
- Decryption(암호 해독) 규칙 — 이러한 규칙은 TCP 포트 조건만 지원합니다.
- IMCP 에코 - 대상 ICMP 포트의 유형이 0으로 설정되었거나 대상 ICMPv6 포트의 유형이 129로 설정된 경우 요청하지 않은 에코 응답만 매치합니다. ICMP 에코 요청에 대한 응답으로 전송된 ICMP 에코 응답은 무시됩니다. 모든 ICMP 에코에 일치하는 규칙의 경우, ICMP 유형 8 또는 ICMPv6 유형 128을 사용합니다.

영역 및 설정 규칙 조건

Realm & Settings(영역 및 설정**)** 탭 페이지에서는 ID 규칙을 적용할 영역 또는 영역 시퀀스를 선택할 수 있습니다. 캡티브 포털을 사용하는 경우 추가 옵션이 있습니다.

인증 영역

Realm(영역**)** 목록에서 영역 또는 영역 시퀀스를 클릭합니다.

지정된 **Action(**작업**)**을 수행할 사용자가 포함된 영역 또는 영역 시퀀스 . 영역 또는 영역 시퀀스를 완전히 설정해야 ID 규칙에서 이를 영역으로 선택할 수 있습니다.

참고 원격 액세스 VPN이 활성화되어 있고 구축에서 VPN 인증에 RADIUS 서버 그룹을 사용할 경우, 이 RADIUS 서버 그룹과 연결된 영역을 지정하십시오.

활성 인증에만 해당됨**:** 기타 옵션

인증 유형으로 **Active Authentication(**활성 인증**)**을 선택하거나 **Use active authentication if passive or VPN identity cannot be unable(**패시브 또는 **VPN ID**를 설정할 수 없는 경우 활성 인증 사용**)** 확인란을 선택하는 경우 다음 옵션을 사용할 수 있습니다.

수동 또는 **VPN ID**를 구축할 수 없는 경우 활성 인증을 사용합니다**.**

패시브 또는 VPN 인증이 사용자를 식별하지 못할 경우, 이 옵션을 선택하면 캡티브 포털(captive portal) 액티브 인증을 통해 사용자를 인증합니다. 이 옵션을 선택하려면 ID 정책에서 활성 인증 규칙을 구성해야 합니다. (즉, 사용자가 캡티브 포털을 이용해 인증해야 합니다.)

이 옵션을 비활성화하면 VPN ID가 없거나 패시브 인증으로 식별할 수 없는 사용자는 Unknown(알 수 없음)으로 식별됩니다.

또한 이 항목의 뒷부분에 있는 인증 영역 목록의 설명을 참고하십시오.

인증에서 사용자를 식별할 수 없는 경우 특수 **ID**/게스트로 식별함

이 옵션을 선택하면 지정된 횟수만큼 캡티브 포털(captive portal) 액티브 인증에 실패한 사용자가 네트워크에 게스트로 액세스할 수 있습니다. management center에 표시되는 이러한 사용자는 사용자 이름(사용자 이름이 AD 또는 LDAP 서버에 있는 경우) 또는 **Guest(**게스트**)**(사용자 이름을 알 수 없는 경우)로 식별됩니다. 이 영역은 ID 규칙에 지정된 영역입니다. (기본 로그인 실패 횟수는 3회입니다.)

이 필드는 **Active Authentication(**액티브 인증**)**(즉 캡티브 포털 인증)을 규칙 **Action(**작업**)**으로 설정했을 때만 표시됩니다.

Authentication Protocol(인증 프로토콜**)**

캡티브 포털 액티브 인증을 수행하는 데 사용할 방법입니다. 선택 사항은 영역의 유형, LDAP 또는 AD에 따라 달라집니다.

- 암호화되지 않은 HTTP BA(Basic Authentication) 연결을 사용하여 사용자를 인증하려는 경우 **HTTP Basic(HTTP** 기본**)**을 선택합니다. 사용자는 브라우저의 기본 인증 팝업 창을 통해 네트워크에 로그인합니다.

  대부분의 웹 브라우저는 **HTTP Basic(HTTP** 기본**)** 로그인의 접속 정보를 캐시하며, 접속 정보를 사용하여 기존 세션의 시간이 초과하면 새 세션을 원활하게 시작합니다.

- NTLM(NT LAN Manager) 연결을 사용하여 사용자를 인증하려는 경우 **NTLM**을 선택합니다. 이 선택 사항은 AD 영역을 선택한 경우에만 사용 가능합니다. 사용자의 브라우저에 투명 인증이 구성된 경우, 사용자는 자동으로 로그인됩니다. 투명 인증이 구성되지 않은 경우, 사용자는 브라우저의 기본 인증 팝업 창을 통해 네트워크에 로그인합니다.
- Kerberos 연결을 사용하여 사용자를 인증하려는 경우 **Kerberos**를 선택합니다. 이 선택 사항은 보안 LDAP(LDAPS)가 활성화된 서버에 대해 AD 영역을 선택한 경우에만 사용 가능합니다. 사용자의 브라우저에 투명 인증이 구성된 경우, 사용자는 자동으로 로그인됩니다. 투명 인증이 구성되지 않은 경우, 사용자는 브라우저의 기본 인증 팝업 창을 통해 네트워크에 로그인합니다.

참고 Kerberos 캡티브 포털(captive portal) 액티브 인증을 수행하려면 선택한 **Realm(**영역**)**에 **AD Join Username(AD** 조인 사용자 이름**)**과 **AD Join Password(AD** 조인 비밀번호**)**를 설정해야 합니다.

참고 Kerberos 캡티브 포털(captive portal)을 수행할 ID 규칙을 생성 중이고 DNS 확인을 구성한 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.

threat defense 디바이스의 경우 FQDN은 캡티브 포털에 사용된 라우티드 인터페이스의 IP 주소를 확인해야 합니다.

- 캡티브 포털(captive portal) 서버가 인증 연결에 HTTP Basic(HTTP 기본), Kerberos 또는 NTLM 중에서 선택할 수 있도록 하려면 **HTTP Negotiate(HTTP** 협상**)**를 선택합니다. 이 유형은 AD 영역을 선택한 경우에만 사용 가능합니다.

참고 **HTTP Negotiate(HTTP** 협상**)**가 Kerberos 캡티브 포털(captive portal) 액티브 인증을 선택하도록 하려면, 선택한 **Realm(**영역**)**에 **AD Join Username(AD** 조인 사용자 이름**)**과 **AD Join Password(AD** 조인 비밀번호**)**를 설정해야 합니다.

참고 **HTTP** 협상 캡티브 포털(captive portal)을 수행할 ID 규칙을 생성 중이고 DNS 확인을 구성한 경우, 캡티브 포털(captive portal) 디바이스의 FQDN(Fully Qualified Domain Name)을 확인할 DNS 서버를 설정해야 합니다. 캡티브 포털(captive portal)에 사용할 디바이스의 FQDN은 DNS를 구성할 때 제공된 호스트 이름과 일치해야 합니다.

ID 규칙 생성

ID 규칙의 설정 옵션에 대한 자세한 내용은 Identity Rule Fields(ID 규칙 필드), 13 페이지 섹션을 참조하십시오.

시작하기 전에

영역 또는 영역 시퀀스를 생성하고 활성화해야 합니다.

- Active Directory 영역 및 영역 디렉터리 생성에 설명된 대로 Microsoft Active Directory 영역 및 영역 디렉터리를 생성합니다.
- 사용자 및 그룹 동기화에 설명된 대로 사용자 및 그룹을 다운로드하고 영역을 활성화합니다.
- (선택 사항). 영역 시퀀스 생성에 설명된 대로 영역 시퀀스를 생성합니다.

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.

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.

프로시저

단계 **1** management center에 로그인합니다.

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

단계 **3** ID 규칙을 추가할 ID 정책 옆에 있는 **Edit(**수정**)** ( )을 클릭합니다.

View(보기**)** ( )이 대신 표시되는 경우에는 설정이 상위 도메인에 속하거나 설정을 수정할 권한이 없는 것입니다.

단계 4 **Add Rule(**규칙 추가**)**을 클릭합니다.

단계 5 **Name(**이름**)**을 입력합니다.

단계 6 Specified(지정됨) 규칙이 적용 가능한 경우 **Enabled(**활성화됨**)** 체크 박스를 선택합니다.

단계 7 기존 카테고리에 규칙을 추가하려면 규칙을 **Insert(**삽입**)**할 위치를 나타냅니다. 새 카테고리를 추가하려면 **Add Category(**카테고리 추가**)**를 클릭합니다.

단계 8 목록에서 규칙 **Action(**작업**)**을 선택합니다.

단계 9 캡티브 포털을 설정하는 경우에는 사용자 제어에 대한 캡티브 포털 설정 방법 섹션을 참조하십시오.

단계 10 (선택사항) ID 규칙에 조건을 추가하려면 ID 규칙 조건, 5 페이지 섹션을 참조하십시오.

단계 11 **Add(**추가**)**를 클릭합니다.

단계 12 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.

단계 13 **Save(**저장**)**를 클릭합니다.

다음에 수행할 작업

- 구성 변경 사항을 구축합니다. 구성 변경 사항 구축의 내용을 참고하십시오.

Identity Rule Fields(ID 규칙 필드)

ID 규칙을 구성하려면 다음 필드를 사용합니다.

Enabled(활성화**)**

이 옵션을 활성화하면 ID 정책에서 ID 규칙이 활성화됩니다. 이 옵션을 선택 취소하면 ID 규칙이 비활성화됩니다.

작업

지정한 영역에 있는 사용자에 대해 실행할 인증 유형을 지정합니다. **Passive Authentication(**패시브 인증**)**(기본값), **Active Authentication(**액티브 인증**)** 또는 **No Authentication(**인증 없음**)**을 지정할 수 있습니다. 인증 방법, 즉 *ID* 소스를 완전히 구성해야 ID 규칙에서 이를 작업으로 선택할 수 있습니다.

또한 VPN이 활성화된 경우(최소 하나 이상의 매니지드 디바이스에서 구성됨) Remote Access VPN 세션은 VPN에 의해 액티브 인증됩니다. 다른 세션은 규칙 작업을 사용합니다. 즉, VPN이 활성화되면 선택한 작업에 관계없이 모든 세션에 대해 VPN ID 확인이 먼저 수행됩니다. 지정된 영역에 VPN ID가 있을 경우, 이를 ID 소스로 사용합니다. No additional captive portal active authentication is done, even if selected.

VPN ID 소스가 없는 경우, 지정된 작업에 따라 프로세스가 계속 진행됩니다. VPN ID 소스가 없는 경우 ID 정책을 VPN 인증에만 제한할 수 없으며, 선택한 작업에 따라 규칙이 적용됩니다.

주의 TLS/SSL 암호 해독이 비활성화되어 있을 때(액세스 컨트롤 정책에 SSL 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.

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.

현재 보유한 버전의 시스템에서 어떤 수동 및 활성 인증 방법을 지원하는지 알아보려면 사용자 ID 소스 정보의 내용을 참고하십시오.

ID 정책 관리

다중 도메인 구축에서 시스템은 현재 도메인에서 생성된 정책을 표시하며 이러한 정책은 수정할 수 있습니다. 상위 도메인에서 생성된 정책도 표시되지만, 이러한 정책은 수정할 수 없습니다. 하위 도메인에서 생성된 정책을 보고 수정하려면 해당 도메인으로 전환하십시오.

프로시저

단계 **1** management center에 로그인합니다.

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

단계 **3** 정책을 삭제하려면 **Delete(**삭제**)** ( )를 클릭합니다. 컨트롤이 흐리게 표시되는 경우에는 컨피그레이션이 상위 도메인에 속하거나 컨피그레이션을 수정할 권한이 없는 것입니다.

단계 **4** 정책을 편집하려면 정책 옆에 있는 **Edit(**수정**)** ( )을 클릭하고 ID 정책 생성, 3 페이지에 설명된 대로 변경합니다. **View(**보기**)** ( )이 대신 표시되는 경우에는 설정이 상위 도메인에 속하거나 설정을 수정할 권한이 없는 것입니다.

단계 **5** 정책을 복사하려면 **Copy(**복사**)** ( )을 클릭합니다.

단계 **6** 정책에 대한 보고서를 생성하려면 현재 정책 보고서 생성에 설명된 대로 **Report(**보고서**)** ( )을 클릭합니다.

단계 **7** 정책을 비교하려면 정책 비교 섹션을 참조하십시오.

단계 **8** 정책을 구성할 폴더를 생성하려면 **Add Category(**범주 추가**)**를 클릭합니다.

다음에 수행할 작업

구성 변경 사항을 구축합니다. 구성 변경 사항 구축의 내용을 참고하십시오.

ID 규칙 관리

프로시저

단계 1 management center에 로그인합니다.

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

단계 3 수정하려는 정책 옆에 있는 **Edit(**수정**)** ( )를 클릭합니다. **View(**보기**)** ( )이 대신 표시되는 경우에는 설정이 상위 도메인에 속하거나 설정을 수정할 권한이 없는 것입니다.

단계 4 ID 규칙을 수정하려면 **Edit(**수정**)** ( )을 클릭하고 ID 정책 생성, 3 페이지에 설명된 대로 규칙을 변경합니다.

단계 5 ID 규칙을 삭제하려면 **Delete(**삭제**)** ( )을 클릭합니다.

단계 6 규칙 카테고리를 생성하려면 **Add Category(**카테고리 추가**)**를 클릭하고 위치와 규칙을 선택합니다.

단계 7 **Save(**저장**)**를 클릭합니다.

다음에 수행할 작업

- 구성 변경 사항을 구축합니다. 구성 변경 사항 구축의 내용을 참고하십시오.

사용자 제어 문제 해결

사용자 규칙 동작이 정상적이지 않을 경우 규칙, ID 소스 또는 영역 컨피그레이션을 조정하는 방법을 고려하십시오. 기타 관련 문제 해결 정보를 보려면 다음을 참조하십시오.

- ISE/ISE-PIC 또는 Cisco TrustSec 문제 해결
- TS 에이전트 ID 소스 문제 해결
- 캡티브 포털(captive portal) ID 소스 문제 해결
- 영역 및 사용자 다운로드 문제 해결

영역, 사용자 또는 사용자 그룹을 대상으로 하는 규칙이 트래픽과 일치하지 않음

다수의 사용자 그룹을 모니터링하는 TS 에이전트 또는 ISE/ISE-PIC 디바이스를 설정하거나 네트워크의 호스트에 매우 많은 사용자가 매핑된 경우, Secure Firewall Management Center 사용자 제한으로 인해 사용자 레코드가 삭제될 수 있습니다. 그 결과, 사용자 조건이 있는 규칙은 정상적으로 트래픽과 일치하지 않을 수 있습니다.

사용자 그룹 내의 사용자 그룹 또는 사용자를 대상으로 하는 규칙이 정상적으로 트래픽과 일치하지 않음

사용자 그룹 조건이 포함된 규칙을 구성할 경우, LDAP 또는 Active Directory 서버에 사용자 그룹을 구성해야 합니다. 서버가 기본 개체 계층으로 사용자를 구성하는 경우 시스템은 사용자 그룹 제어를 수행할 수 없습니다.

보조 그룹의 사용자를 대상으로 하는 규칙이 정상적으로 트래픽과 일치하지 않음

Active Directory 서버에 있는 보조 그룹의 구성원인 사용자를 포함하거나 제외하는 사용자 그룹 조건이 포함된 규칙을 구성할 경우, 서버에서는 보고하는 사용자 수를 제한할 수 있습니다.

기본적으로 Active Directory 서버는 보조 그룹에서 보고하는 사용자 수를 제한합니다. 보조 그룹의 모든 사용자를 Secure Firewall Management Center에 보고하고 사용자 조건이 포함된 규칙에서 사용할 수 있도록 하려면 이 제한을 맞춤설정해야 합니다.

사용자가 최초로 확인된 경우 규칙이 해당 사용자와 일치하지 않음

이전에 확인되지 않은 사용자의 활동이 탐지되면 시스템은 서버에서 해당 사용자에 대한 정보를 검색합니다. 시스템이 이러한 정보를 성공적으로 검색할 때까지 해당 사용자가 보여준 활동이 일치하는 규칙으로 처리되지 않습니다. 그 대신, 일치하는 다음 규칙(또는 해당하는 경우 정책의 기본 작업)에 따라 사용자 세션이 처리됩니다.

다음과 같은 경우를 예로 들 수 있습니다.

- 사용자 그룹의 구성원인 사용자가 사용자 그룹 조건이 포함된 규칙과 일치하지 않음
- 사용자 데이터 회수에 사용된 서버가 액티브 디렉토리 서버인 경우, TS 에이전트 또는 ISE/ISE-PIC 디바이스가 보고한 사용자가 규칙과 일치하지 않습니다.

이 경우 시스템에서 이벤트 보기 및 분석 툴에 사용자 데이터를 표시하는 것이 지연될 수 있습니다.

규칙이 모든 **ISE** 사용자와 일치하지 않음

이는 정상적인 동작입니다. Active Directory 도메인 컨트롤러에서 인증된 ISE 사용자에 대해 사용자 제어를 수행할 수 있습니다. LDAP, RADIUS 또는 RSA 도메인 컨트롤러에서 인증된 ISE 사용자에 대해서는 사용자 제어를 수행할 수 없습니다.

규칙이 모든 **ISE/ISE-PIC** 사용자와 일치하지 않음

이는 정상적인 동작입니다. Active Directory 도메인 컨트롤러에서 인증된 ISE/ISE-PIC 사용자에 대해 사용자 제어를 수행할 수 있습니다. LDAP, RADIUS 또는 RSA 도메인 컨트롤러에서 인증된 ISE/ISE-PIC 사용자에 대해서는 사용자 제어를 수행할 수 없습니다.

너무 많은 메모리를 사용하는 사용자 및 그룹

처리 중인 사용자 및 그룹이 너무 많은 메모리를 사용하는 경우 상태 알림이 표시됩니다. 모든 사용자 세션은 management center에서 관리하는 모든 디바이스로 전파됩니다. management center가 메모리가 다른 디바이스를 관리하는 경우, 메모리가 가장 적은 디바이스가 시스템이 오류 없이 처리할 수 있는 사용자 세션 수를 결정합니다.

문제가 지속되는 경우 다음 옵션 중 하나를 선택합니다.

- 서브넷에서 저용량 관리 디바이스를 분리하고 패시브 인증 데이터를 해당 서브넷에 보고하지 않도록 ISE/ISE-PIC를 설정합니다.

  Cisco ISE(Identity Services Engine) 관리자 설명서의 네트워크 디바이스 관리 장을 참조하십시오.

- SGT(Security Group Tag)에서 구독을 취소합니다.

  자세한 내용은 사용자 제어를 위한 ISE/ISE-PIC 설정를 참고하십시오.

- 더 많은 메모리를 사용하여 매니지드 디바이스를 모델로 업그레이드합니다.