CSM 3.x:사용자 권한 및 역할 설정

목차

소개

이 문서에서는 CSM(Cisco Security Manager)의 사용자에게 권한 및 역할을 설정하는 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

이 문서에서는 CSM이 설치되어 제대로 작동한다고 가정합니다.

사용되는 구성 요소

이 문서의 정보는 CSM 3.1을 기반으로 합니다.

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다.이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다.현재 네트워크가 작동 중인 경우, 모든 명령어의 잠재적인 영향을 미리 숙지하시기 바랍니다.

표기 규칙

문서 규칙에 대한 자세한 내용은 Cisco 기술 팁 표기 규칙을 참고하십시오.

사용자 권한 설정

Cisco Security Manager는 사용자 이름과 비밀번호를 인증한 후 로그인할 수 있습니다.인증된 후 Security Manager는 응용 프로그램 내에서 사용자의 역할을 설정합니다.이 역할은 수행 권한이 있는 작업 또는 작업의 집합인 권한(권한이라고도 함)을 정의합니다.특정 작업 또는 장치에 대한 권한이 없는 경우 관련 메뉴 항목, 목차 항목 및 단추가 숨겨지거나 비활성화됩니다.또한 선택한 정보를 보거나 선택한 작업을 수행할 권한이 없다는 메시지가 표시됩니다.

Security Manager에 대한 인증 및 권한 부여는 CiscoWorks 서버 또는 Cisco ACS(Secure Access Control Server)에서 관리합니다. 기본적으로 CiscoWorks는 인증 및 권한 부여를 관리하지만 CiscoWorks Common Services의 AAA Mode Setup 페이지를 사용하여 Cisco Secure ACS로 변경할 수 있습니다.

Cisco Secure ACS를 사용할 때의 주요 장점은 특화된 권한 집합(예: 사용자가 특정 정책 유형을 구성하되 다른 정책 유형은 구성하지 못하도록 허용)을 사용하여 매우 세분화된 사용자 역할을 생성할 수 있고, NDG(네트워크 장치 그룹)를 구성하여 사용자를 특정 장치로 제한할 수 있는 기능입니다.

다음 항목에서는 사용자 권한에 대해 설명합니다.

- 보안 관리자 권한
- CiscoWorks 역할 이해
- Cisco Secure ACS 역할 이해
- Security Manager의 권한과 역할 간의 기본 연결

보안 관리자 권한

Security Manager는 다음과 같이 권한을 카테고리로 분류합니다.

1. **보기** - 현재 설정을 볼 수 있습니다.자세한 내용은 사용 권한 보기를 참조하십시오.
2. **Modify**(수정) - 현재 설정을 변경할 수 있습니다.자세한 내용은 사용 권한 수정을 참조하십시오.
3. **Assign**(할당) - 디바이스 및 VPN 토폴로지에 정책을 할당할 수 있습니다.자세한 내용은 사용 권한 할당을 참조하십시오.
4. **승인** - 정책 변경 및 배포 작업을 승인할 수 있습니다.자세한 내용은 사용 권한 승인을 참조하십시오.
5. **Import**(가져오기) - 디바이스에 이미 구축된 컨피그레이션을 Security Manager로 가져올 수 있습니다.
6. **Deploy**(구축) - 네트워크의 디바이스에 컨피그레이션 변경 사항을 구축하고 롤백을 수행하여 이전에 구축된 컨피그레이션으로 돌아갈 수 있습니다.
7. **Control**(제어) - ping과 같은 디바이스에 명령을 실행할 수 있습니다.
8. **Submit**(제출) - 승인을 위해 구성 변경 사항을 제출할 수 있습니다.

- 수정, 할당, 승인, 가져오기, 제어 또는 배포 권한을 선택할 때 해당 보기 권한도 선택해야 합니다.그렇지 않으면 Security Manager가 제대로 작동하지 않습니다.

- 정책 권한 수정을 선택할 때 해당 할당 및 정책 권한 보기를 선택해야 합니다.
- 정책 객체를 정의의 일부로 사용하는 정책을 허용할 경우 이러한 객체 유형에 대한 보기 권한도 부여해야 합니다.예를 들어 라우팅 정책을 수정할 수 있는 권한을 선택하는 경우 라우팅 정책에 필요한 객체 유형인 네트워크 객체 및 인터페이스 역할을 볼 수 있는 권한도 선택해야 합니다.
- 다른 개체를 정의의 일부로 사용하는 개체를 허용하는 경우에도 마찬가지입니다.예를 들어, 사용자 그룹 수정 권한을 선택하는 경우 네트워크 객체, ACL 객체 및 AAA 서버 그룹을 보기 위한 권한도 선택해야 합니다.

권한 보기

Security Manager의 보기(읽기 전용) 권한은 다음과 같이 범주로 구분됩니다.

- 정책 권한 보기
- 개체 사용 권한 보기
- 추가 보기 권한

정책 권한 보기

Security Manager에는 정책에 대한 다음 보기 권한이 포함됩니다.

1. **보기 > 정책 > 방화벽.**PIX/ASA/FWSM 디바이스, IOS 라우터 및 Catalyst 6500/7600 디바이스의 방화벽 서비스 정책(방화벽 아래의 정책 선택기에 있음)을 볼 수 있습니다.방화벽 서비스 정책의 예로는 액세스 규칙, AAA 규칙, 검사 규칙이 있습니다.
2. **View(보기) > Policies(정책) > Intrusion Prevention System(침입 방지 시스템).**IOS 라우터에서 실행되는 IPS에 대한 정책을 포함하여 IPS 정책(IPS 아래의 Policy 선택기에 있음)을 볼 수 있습니다.
3. **보기 > 정책 > 이미지.**Apply IPS Updates(IPS 업데이트 적용) 마법사(Tools(툴) > Apply IPS Update(IPS 업데이트 적용)에서 시그니처 업데이트 패키지를 선택할 수 있지만, Modify(수정) > Policies(정책) > Image(이미지) 권한도 없는 경우 특정 디바이스에 패키지를 할당할 수는 없습니다.
4. **View(보기) > Policies(정책) > NAT.**PIX/ASA/FWSM 디바이스 및 IOS 라우터에 대한 네트워크 주소 변환 정책을 볼 수 있습니다.NAT 정책의 예로는 고정 규칙 및 동적 규칙이 있습니다.
5. **View(보기) > Policies(정책) > Site-to-Site VPN.**PIX/ASA/FWSM 디바이스, IOS 라우터 및 Catalyst 6500/7600 디바이스에 대한 사이트 간 VPN 정책을 볼 수 있습니다.사이트 간 VPN 정책의 예로는 IKE 제안, IPsec 제안, 사전 공유 키가 있습니다.
6. **View(보기) > Policies(정책) > Remote Access VPN(원격 액세스 VPN)**PIX/ASA/FWSM 디바이스, IOS 라우터 및 Catalyst 6500/7600 디바이스에서 원격 액세스 VPN 정책을 볼 수 있습니다.원격 액세스 VPN 정책의 예로는 IKE 제안서, IPsec 제안서, PKI 정책이 있습니다.
7. **View(보기) > Policies(정책) > SSL VPN.**PIX/ASA/FWSM 디바이스 및 IOS 라우터(예: SSL VPN 마법사)에서 SSL VPN 정책을 볼 수 있습니다.
8. **보기 > 정책 > 인터페이스.**PIX/ASA/FWSM 디바이스, IOS 라우터, IPS 센서 및 Catalyst 6500/7600 디바이스의 인터페이스 정책(인터페이스 아래의 정책 선택기에 있음)을 볼 수 있습니다.PIX/ASA/FWSM 디바이스에서 이 권한은 하드웨어 포트 및 인터페이스 설정을 포함합니다.IOS 라우터에서 이 권한은 기본 및 고급 인터페이스 설정뿐만 아니라 DSL, PVC, PPP, 다이얼러 정책 등의 기타 인터페이스 관련 정책을 다룹니다.IPS 센서에서 이 권한은 물리적 인터페이스와 요약 맵을 포함합니다.Catalyst 6500/7600 디바이스에서 이 권한은 인터페이스 및 VLAN 설정을 다룹니다.
9. **보기 > 정책 > 브리징.**PIX/ASA/FWSM 디바이스의 ARP 테이블 정책(Platform > Bridging 아래

의 Policy 선택기에 있음)을 볼 수 있습니다.

10. **보기 > 정책 > 장치 관리**.PIX/ASA/FWSM 디바이스, IOS 라우터 및 Catalyst 6500/7600 디바이스의 디바이스 관리 정책(Platform > Device Admin 아래의 Policy 선택기에 있음)을 볼 수 있습니다.PIX/ASA/FWSM 디바이스의 예로는 디바이스 액세스 정책, 서버 액세스 정책 및 장애 조치 정책이 있습니다.IOS 라우터의 예로는 디바이스 액세스(라인 액세스 포함) 정책, 서버 액세스 정책, AAA 및 Secure Device Provisioning 등이 있습니다.IPS 센서에서 이 권한은 디바이스 액세스 정책 및 서버 액세스 정책을 다룹니다.Catalyst 6500/7600 디바이스에서 이 권한은 IDSM 설정 및 VLAN 액세스 목록을 다룹니다.
11. **보기 > 정책 > ID를 선택합니다**.802.1x 및 NAC(Network Admission Control) 정책을 포함하여 Cisco IOS 라우터의 ID 정책(Platform > Identity 아래의 Policy 선택기에 있음)를 볼 수 있습니다.
12. **보기 > 정책 > 로깅을 참조하십시오**.PIX/ASA/FWSM 디바이스, IOS 라우터 및 IPS 센서에서 Platform(플랫폼) > Logging(로깅) 아래의 Policy(정책) 선택기에 있는 로깅 정책을 볼 수 있습니다.로깅 정책의 예로는 로깅 설정, 서버 설정 및 syslog 서버 정책이 있습니다.
13. **보기 > 정책 > 멀티캐스트**.PIX/ASA/FWSM 디바이스의 Policy selector(Platform(플랫폼) > Multicast(멀티캐스트) 아래의 Policy(정책) 선택기에 있음)를 볼 수 있습니다.멀티캐스트 정책의 예로는 멀티캐스트 라우팅 및 IGMP 정책이 있습니다.
14. **보기 > 정책 > QoS를 선택합니다**.Cisco IOS 라우터에서 QoS 정책(Platform > QoS(서비스 품질) 아래의 Policy 선택기에 있음)을 볼 수 있습니다.
15. **보기 > 정책 > 라우팅**.PIX/ASA/FWSM 디바이스 및 IOS 라우터의 라우팅 정책(플랫폼 > 라우팅 아래의 정책 선택기에 있음)을 볼 수 있습니다.라우팅 정책의 예로는 OSPF, RIP 및 고정 라우팅 정책이 있습니다.
16. **보기 > 정책 > 보안**.PIX/ASA/FWSM 디바이스 및 IPS 센서에서 Platform(플랫폼) > Security(보안) 아래의 Policy(정책) 선택기에 있는 보안 정책을 볼 수 있습니다 .PIX/ASA/FWSM 디바이스에서 보안 정책에는 안티스푸핑, 프래그먼트 및 시간 초과 설정이 포함됩니다.IPS 센서에서 보안 정책에는 차단 설정이 포함됩니다.
17. **보기 > 정책 > 서비스 정책 규칙**.PIX 7.x/ASA 디바이스에서 서비스 정책 규칙 정책 정책 정책 정책(Platform > Service Policy Rules 아래의 Policy Selector)을 볼 수 있습니다.우선 순위 큐와 IPS, QoS, 연결 규칙을 예로 들 수 있습니다.
18. **보기 > 정책 > 사용자 환경 설정**.PIX/ASA/FWSM 디바이스의 구축 정책(Platform(플랫폼) > User Preferences(사용자 환경 설정) 아래의 Policy(정책) 선택기에 있음)을 볼 수 있습니다 .이 정책에는 구축의 모든 NAT 변환을 지우는 옵션이 포함되어 있습니다.
19. **보기 > 정책 > 가상 장치**.IPS 디바이스에서 가상 센서 정책을 볼 수 있습니다.이 정책은 가상 센서를 생성하는 데 사용됩니다.
20. **보기 > 정책 > FlexConfig를 선택합니다**.PIX/ASA/FWSM 디바이스, IOS 라우터 및 Catalyst 6500/7600 디바이스에 구축할 수 있는 추가 CLI 명령 및 지침인 FlexConfigs를 볼 수 있습니다.

개체 사용 권한 보기

Security Manager에는 객체에 대한 다음 보기 권한이 포함됩니다.

1. **View(보기) > Objects(개체) > AAA Server Groups(AAA 서버 그룹)**.AAA 서버 그룹 객체를 볼 수 있습니다.이러한 객체는 AAA 서비스(인증, 권한 부여 및 계정 관리)가 필요한 정책에서 사용됩니다.
2. **View(보기) > Objects(개체) > AAA Servers(AAA 서버)**.AAA 서버 객체를 볼 수 있습니다.이러한 객체는 AAA 서버 그룹의 일부로 정의된 개별 AAA 서버를 나타냅니다.
3. **보기 > 객체 > 액세스 제어 목록 - 표준/확장**.표준 및 확장 ACL 객체를 볼 수 있습니다.확장

ACL 객체는 NAT 및 NAC와 같은 다양한 정책과 VPN 액세스 설정에 사용됩니다.표준 ACL 객체는 OSPF 및 SNMP와 같은 정책과 VPN 액세스 설정에 사용됩니다.

4. **보기 > 객체 > 액세스 제어 목록** - 웹웹 ACL 객체를 볼 수 있습니다.웹 ACL 객체는 SSL VPN 정책에서 콘텐츠 필터링을 수행하는 데 사용됩니다.
5. **View(보기) > Objects(개체) > ASA User Groups(ASA 사용자 그룹)**.ASA 사용자 그룹 객체를 볼 수 있습니다.이러한 객체는 Easy VPN, 원격 액세스 VPN 및 SSL VPN 컨피그레이션의 ASA 보안 어플라이언스에 구성됩니다.
6. **보기(View) > 개체(Objects) > 카테고리(Categories)**.범주 객체를 볼 수 있습니다.이러한 객체는 색상을 사용하여 규칙 테이블의 규칙과 객체를 쉽게 식별할 수 있도록 도와줍니다.
7. **보기 > 객체 > 자격 증명**.자격 증명 객체를 볼 수 있습니다.이러한 객체는 IKE Extended Authentication(Xauth) 중에 Easy VPN 컨피그레이션에서 사용됩니다.
8. **보기 > 객체 > FlexConfigs를 선택합니다**.FlexConfig 객체를 볼 수 있습니다.추가 스크립팅 언어 지침이 있는 구성 명령을 포함하는 이러한 개체를 사용하여 Security Manager 사용자 인터페이스에서 지원하지 않는 명령을 구성할 수 있습니다.
9. **View(보기) > Objects(개체) > IKE Proposals(IKE 제안)**.IKE 제안 객체를 볼 수 있습니다.이러한 개체에는 원격 액세스 VPN 정책의 IKE 제안서에 필요한 매개변수가 포함되어 있습니다.
10. **View(보기) > Objects(개체) > Inspect(검사) - Class Maps(클래스 맵)** - DNS.DNS 클래스 맵 개체를 볼 수 있습니다.이러한 객체는 DNS 트래픽과 특정 기준을 일치하므로 해당 트래픽에 대해 작업을 수행할 수 있습니다.
11. **보기 > 객체 > 검사 - 클래스 맵 - FTP**.FTP 클래스 맵 객체를 볼 수 있습니다.이러한 객체는 FTP 트래픽과 특정 기준을 일치하므로 해당 트래픽에 대해 작업을 수행할 수 있습니다.
12. **보기 > 객체 > 검사 - 클래스 맵 - HTTP**.HTTP 클래스 맵 객체를 볼 수 있습니다.이러한 객체는 HTTP 트래픽과 특정 기준을 일치하므로 해당 트래픽에 대해 작업을 수행할 수 있습니다.
13. **보기 > 객체 > 검사 - 클래스 맵 - IM**.IM 클래스 맵 개체를 볼 수 있습니다.이러한 객체는 IM 트래픽과 특정 기준을 일치하므로 해당 트래픽에 대해 작업을 수행할 수 있습니다.
14. **View > Objects > Inspect - Class Maps - SIP**.SIP 클래스 맵 개체를 볼 수 있습니다.이러한 객체는 SIP 트래픽과 특정 기준을 일치하므로 해당 트래픽에 대해 작업을 수행할 수 있습니다.
15. **View(보기) > Objects(개체) > Inspect(검사) - Policy Maps(정책 맵) - DNS.**DNS 정책 맵 객체를 볼 수 있습니다.이러한 개체는 DNS 트래픽에 대한 검사 맵을 만드는 데 사용됩니다.
16. **View(보기) > Objects(개체) > Inspect(검사) - Policy Maps(정책 맵) - FTP입니다.**FTP 정책 맵 객체를 볼 수 있습니다.이러한 객체는 FTP 트래픽에 대한 검사 맵을 만드는 데 사용됩니다.
17. **View > Objects > Inspect - Policy Maps - GTP**.GTP 정책 맵 객체를 볼 수 있습니다.이러한 객체는 GTP 트래픽에 대한 검사 맵을 생성하는 데 사용됩니다.
18. **View(보기) > Objects(개체) > Inspect - Policy Maps(검사 - 정책 맵) - HTTP(ASA7.1.x/PIX7.1.x/IOS)**. ASA/PIX 7.1.x 디바이스 및 IOS 라우터에 대해 생성된 HTTP 정책 맵 객체를 볼 수 있습니다.이러한 객체는 HTTP 트래픽에 대한 검사 맵을 만드는 데 사용됩니다.
19. **View(보기) > Objects(개체) > Inspect - Policy Maps(검사 - 정책 맵) - HTTP(ASA7.2/PIX7.2)**. ASA 7.2/PIX 7.2 디바이스에 대해 생성된 HTTP 정책 맵 객체를 볼 수 있습니다.이러한 객체는 HTTP 트래픽에 대한 검사 맵을 만드는 데 사용됩니다.
20. **View(보기) > Objects(개체) > Inspect - Policy Maps(검사 - 정책 맵) - IM(ASA7.2/PIX7.2)**. ASA 7.2/PIX 7.2 디바이스에 대해 생성된 IM 정책 맵 객체를 볼 수 있습니다.이러한 객체는 IM 트래픽에 대한 검사 맵을 만드는 데 사용됩니다.
21. **View(보기) > Objects(개체) > Inspect(검사) - Policy Maps(정책 맵) - IM(IOS)**. IOS 디바이스에 대해 생성된 IM 정책 맵 객체를 볼 수 있습니다.이러한 객체는 IM 트래픽에 대한 검사 맵을 만드는 데 사용됩니다.

22. **View > Objects > Inspect - Policy Maps - SIP**.SIP 정책 맵 개체를 볼 수 있습니다.이러한 개체는 SIP 트래픽에 대한 검사 맵을 만드는 데 사용됩니다.
23. **보기 > 객체 > 검사 - 정규식**.정규식 객체를 볼 수 있습니다.이러한 객체는 정규식 그룹의 일부로 정의된 개별 정규식을 나타냅니다.
24. **보기 > 객체 > 검사 - 정규식 그룹**.정규식 그룹 객체를 볼 수 있습니다.이러한 객체는 특정 클래스 맵에서 사용되고 맵을 검사하여 패킷 내의 텍스트를 확인합니다.
25. **View(보기) > Objects(개체) > Inspect(검사) - TCP Maps(TCP 맵)**.TCP 맵 객체를 볼 수 있습니다.이러한 객체는 양방향의 TCP 흐름에서 검사를 사용자 정의합니다.
26. **보기 > 객체 > 인터페이스 역할**.인터페이스 역할 객체를 볼 수 있습니다.이러한 객체는 서로 다른 유형의 디바이스에서 여러 인터페이스를 나타낼 수 있는 명명 패턴을 정의합니다.인터페이스 역할을 사용하면 각 인터페이스의 이름을 수동으로 정의하지 않고도 여러 디바이스의 특정 인터페이스에 정책을 적용할 수 있습니다.
27. **View(보기) > Objects(개체) > IPsec Transform Sets(IPsec 변형 집합)**.IPsec 변형 집합 개체를 볼 수 있습니다.이러한 객체는 보안 프로토콜, 알고리즘 및 IPsec 터널의 데이터가 암호화 및 인증되는 방식을 정확히 지정하는 기타 설정의 조합으로 구성됩니다.
28. **View(보기) > Objects(개체) > LDAP Attribute Maps(LDAP 특성 맵)**.LDAP 특성 맵 객체를 볼 수 있습니다.이러한 객체는 맞춤형(사용자 정의) 특성 이름을 Cisco LDAP 특성 이름에 매핑하는 데 사용됩니다.
29. **보기 > 객체 > 네트워크/호스트**.네트워크/호스트 객체를 볼 수 있습니다.이러한 객체는 네트워크, 호스트 또는 둘 모두를 나타내는 IP 주소의 논리적 컬렉션입니다.네트워크/호스트 객체를 사용하면 각 네트워크 또는 호스트를 개별적으로 지정하지 않고 정책을 정의할 수 있습니다.
30. **보기 > 객체 > PKI 등록**.PKI 등록 객체를 볼 수 있습니다.이러한 객체는 공개 키 인프라 내에서 작동하는 CA(인증 기관) 서버를 정의합니다.
31. **View > Objects > Port Forwarding Lists**.포트 전달 목록 객체를 볼 수 있습니다.이러한 객체는 원격 클라이언트의 포트 번호 매핑을 SSL VPN 게이트웨이 뒤에 있는 애플리케이션의 IP 주소 및 포트에 정의합니다.
32. **보기 > 객체 > 보안 데스크탑 구성**.보안 데스크톱 컨피그레이션 객체를 볼 수 있습니다.이러한 객체는 SSL VPN 정책에서 참조할 수 있는 재사용 가능한 명명된 구성 요소로, SSL VPN 세션 동안 공유되는 모든 민감한 데이터의 추적을 제거하는 안정적인 방법을 제공합니다.
33. **보기 > 객체 > 서비스 - 포트 목록**.포트 목록 객체를 볼 수 있습니다.하나 이상의 포트 번호 범위를 포함하는 이러한 객체는 서비스 객체 생성 프로세스를 간소화하는 데 사용됩니다.
34. **보기 > 객체 > 서비스/서비스 그룹** 서비스 및 서비스 그룹 객체를 볼 수 있습니다.이러한 객체는 Kerberos, SSH 및 POP3과 같은 정책에서 사용하는 네트워크 서비스를 설명하는 프로토콜 및 포트 정의의 정의된 매핑입니다.
35. **보기 > 객체 > 단일 사인온 서버**.SSO(Single Sign On) 서버 개체를 볼 수 있습니다 .SSO(Single Sign-On)를 사용하면 SSL VPN 사용자가 사용자 이름과 비밀번호를 한 번 입력할 수 있으며 여러 보호 서비스 및 웹 서버에 액세스할 수 있습니다.
36. **보기 > 객체 > SLA 모니터**.SLA 모니터 객체를 볼 수 있습니다.이러한 객체는 버전 7.2 이상을 실행하는 PIX/ASA 보안 어플라이언스에서 경로 추적을 수행하는 데 사용됩니다.이 기능은 기본 경로의 가용성을 추적하고 기본 경로가 실패할 경우 백업 경로를 설치하는 방법을 제공합니다.
37. **View(보기) > Objects(개체) > SSL VPN Customizations(SSL VPN 사용자 지정)**.SSL VPN 사용자 지정 개체를 볼 수 있습니다.이러한 객체는 사용자에게 표시되는 SSL VPN 페이지(예: 로그인/로그아웃 및 홈 페이지)의 모양을 변경하는 방법을 정의합니다.
38. **View(보기) > Objects(개체) > SSL VPN Gateway(SSL VPN 게이트웨이)**.SSL VPN 게이트웨이 개체를 볼 수 있습니다.이러한 객체는 게이트웨이를 SSL VPN에서 보호된 리소스에 대한 연결에 프록시로 사용할 수 있도록 하는 매개변수를 정의합니다.

39. **뷰(View) > 개체(Objects) > 스타일 개체(Style Objects)**.스타일 객체를 볼 수 있습니다.이러한 개체를 사용하면 글꼴 특성 및 색상과 같은 스타일 요소를 구성하여 보안 어플라이언스에 연결할 때 SSL VPN 사용자에게 표시되는 SSL VPN 페이지의 모양을 사용자 지정할 수 있습니다.
40. **보기(View) > 개체(Objects) > 텍스트 개체(Text Objects)**.자유 형식 텍스트 객체를 볼 수 있습니다.이러한 객체는 이름 및 값 쌍을 구성합니다. 여기서 값은 단일 문자열, 문자열 목록 또는 문자열 테이블이 될 수 있습니다.
41. **보기 > 객체 > 시간 범위.**시간 범위 객체를 볼 수 있습니다.이러한 객체는 시간 기반 ACL 및 검사 규칙을 생성할 때 사용됩니다.또한 ASA 사용자 그룹을 정의하여 주 중 특정 시간으로 VPN 액세스를 제한할 때도 사용됩니다.
42. **View > Objects > Traffic Flows**.트래픽 흐름 객체를 볼 수 있습니다.이러한 객체는 PIX 7.x/ASA 7.x 디바이스에서 사용할 특정 트래픽 흐름을 정의합니다.
43. **보기 > 객체 > URL 목록**.URL 목록 객체를 볼 수 있습니다.이러한 객체는 로그인 성공 후 포털 페이지에 표시되는 URL을 정의합니다.이를 통해 사용자는 클라이언트리스 액세스 모드에서 작동할 때 SSL VPN 웹 사이트에서 사용 가능한 리소스에 액세스할 수 있습니다.
44. **보기 > 객체 > 사용자 그룹**.사용자 그룹 객체를 볼 수 있습니다.이러한 객체는 Easy VPN 토폴로지, 원격 액세스 VPN 및 SSL VPN에 사용되는 원격 클라이언트 그룹을 정의합니다.
45. **보기 > 객체 > WINS 서버 목록**.WINS 서버 목록 개체를 볼 수 있습니다.이러한 객체는 SSL VPN에서 원격 시스템의 파일에 액세스하거나 공유하는 데 사용되는 WINS 서버를 나타냅니다.
46. **View(보기) > Objects(개체) > Internal - DN Rules(내부 - DN 규칙)**.DN 정책에서 사용되는 DN 규칙을 볼 수 있습니다.보안 관리자가 사용하는 내부 개체로서 정책 개체 관리자에 나타나지 않습니다.
47. **보기 > 객체 > 내부 - 클라이언트 업데이트**.이는 정책 개체 관리자에 나타나지 않는 사용자 그룹 개체에 필요한 내부 개체입니다.
48. **보기 > 객체 > 내부 - 표준 ACEs**.표준 액세스 제어 엔트리를 위한 내부 개체이며 ACL 객체에서 사용됩니다.
49. **보기 > 객체 > 내부 - 확장 ACEs**ACL 객체에서 사용하는 확장 액세스 제어 엔트리에 대한 내부 객체입니다.

추가 보기 권한

Security Manager에는 다음과 같은 추가 보기 권한이 포함됩니다.

1. **보기 > 관리자**.Security Manager 관리 설정을 볼 수 있습니다.
2. **보기 > CLI**.디바이스에 구성된 CLI 명령을 보고 구축할 명령을 미리 볼 수 있습니다.
3. **보기 > 구성 아카이브**.구성 아카이브에 포함된 구성 목록을 볼 수 있습니다.디바이스 컨피그레이션 또는 CLI 명령은 볼 수 없습니다.
4. **보기 > 디바이스**.장치 보기에서 장치 및 장치 설정, 속성, 할당 등을 포함한 모든 관련 정보를 볼 수 있습니다.
5. **보기 > 장치 관리자**.Cisco IOS 라우터용 Cisco 라우터 및 SDM(Security Device Manager)과 같은 개별 디바이스에 대한 디바이스 관리자의 읽기 전용 버전을 시작할 수 있습니다.
6. **보기 > 토폴로지**.맵 보기에서 구성된 맵을 볼 수 있습니다.

권한 수정

Security Manager에서 수정(읽기-쓰기) 권한은 다음과 같이 범주로 구분됩니다.

정책 권한 수정

참고: 수정 정책 권한을 지정할 때 해당 할당 및 보기 정책 권한도 선택했는지 확인합니다.

Security Manager에는 정책에 대한 다음 수정 권한이 포함됩니다.

1. **Modify(수정) > Policies(정책) > Firewall(방화벽)**.PIX/ASA/FWSM 디바이스, IOS 라우터 및 Catalyst 6500/7600 디바이스에서 방화벽 아래의 정책 선택기에 있는 방화벽 서비스 정책을 수정할 수 있습니다.방화벽 서비스 정책의 예로는 액세스 규칙, AAA 규칙, 검사 규칙이 있습니다.
2. **Modify > Policies > Intrusion Prevention System**.IOS 라우터에서 실행되는 IPS에 대한 정책을 포함하여 IPS 정책(IPS 아래의 Policy 선택기에 있음)을 수정할 수 있습니다.이 권한을 사용하면 Tools(툴) > Apply IPS Update(IPS 업데이트 적용)에 있는 Signature Update(서명 업데이트) 마법사에서 서명을 조정할 수도 있습니다.
3. **수정 > 정책 > 이미지**.Apply IPS Updates(IPS 업데이트 적용) 마법사(Tools(툴) > Apply IPS Update(IPS 업데이트 적용)에서 디바이스에 시그니처 업데이트 패키지를 할당할 수 있습니다. 이 권한을 사용하면 특정 장치(Tools > Security Manager Administration > IPS Updates 아래에 있음)에 자동 업데이트 설정을 할당할 수도 있습니다.
4. **Modify(수정) > Policies(정책) > NAT**.PIX/ASA/FWSM 디바이스 및 IOS 라우터에서 네트워크 주소 변환 정책을 수정할 수 있습니다.NAT 정책의 예로는 고정 규칙 및 동적 규칙이 있습니다.
5. **Modify(수정) > Policies(정책) > Site-to-Site VPN**.PIX/ASA/FWSM 디바이스, IOS 라우터 및 Catalyst 6500/7600 디바이스에서 사이트 대 사이트 VPN 정책을 수정할 수 있습니다.사이트 간 VPN 정책의 예로는 IKE 제안, IPsec 제안, 사전 공유 키가 있습니다.
6. **Modify(수정) > Policies(정책) > Remote Access VPN(원격 액세스 VPN)**PIX/ASA/FWSM 디바이스, IOS 라우터 및 Catalyst 6500/7600 디바이스에서 원격 액세스 VPN 정책을 수정할 수 있습니다.원격 액세스 VPN 정책의 예로는 IKE 제안서, IPsec 제안서, PKI 정책이 있습니다.
7. **Modify(수정) > Policies(정책) > SSL VPN**.PIX/ASA/FWSM 디바이스 및 IOS 라우터(예: SSL VPN 마법사)에서 SSL VPN 정책을 수정할 수 있습니다.
8. **Modify(수정) > Policies(정책) > Interfaces(인터페이스)**.PIX/ASA/FWSM 디바이스, IOS 라우터, IPS 센서 및 Catalyst 6500/7600 디바이스에서 인터페이스 정책(Interfaces 아래의 Policy 선택기에 있음)을 수정할 수 있습니다.PIX/ASA/FWSM 디바이스에서 이 권한은 하드웨어 포트 및 인터페이스 설정을 포함합니다.IOS 라우터에서 이 권한은 기본 및 고급 인터페이스 설정뿐만 아니라 DSL, PVC, PPP, 다이얼러 정책 등의 기타 인터페이스 관련 정책을 다룹니다.IPS 센서에서 이 권한은 물리적 인터페이스와 요약 맵을 포함합니다.Catalyst 6500/7600 디바이스에서 이 권한은 인터페이스 및 VLAN 설정을 다룹니다.
9. **수정 > 정책 > 브리징**.PIX/ASA/FWSM 디바이스에서 ARP 테이블 정책(Platform > Bridging 아래의 Policy 선택기에 있음)을 수정할 수 있습니다.
10. **Modify > Policies > Device Administration**.PIX/ASA/FWSM 디바이스, IOS 라우터 및 Catalyst 6500/7600 디바이스의 디바이스 관리 정책(Platform > Device Admin 아래의 Policy 선택기에 있음)을 수정할 수 있습니다.PIX/ASA/FWSM 디바이스의 예로는 디바이스 액세스 정책, 서버 액세스 정책 및 장애 조치 정책이 있습니다.IOS 라우터의 예로는 디바이스 액세스(라인 액세스 포함) 정책, 서버 액세스 정책, AAA 및 Secure Device Provisioning 등이 있습니다.IPS 센서에서 이 권한은 디바이스 액세스 정책 및 서버 액세스 정책을 다룹니다.Catalyst 6500/7600 디바이스에서 이 권한은 IDSM 설정 및 VLAN 액세스 목록을 다룹니다.

11. **Modify(수정) > Policies(정책) > Identity(ID)**.802.1x 및 NAC(Network Admission Control) 정책을 포함하여 Cisco IOS 라우터의 ID 정책 선택기(플랫폼 > ID 아래에 있는 정책 선택기에 있음)를 수정할 수 있습니다.
12. **Modify > Policies > Logging을 선택합니다**.PIX/ASA/FWSM 디바이스, IOS 라우터 및 IPS 센서에서 Platform(플랫폼) > Logging(로깅) 아래의 Policy(정책) 선택기에 있는 로깅 정책을 수정할 수 있습니다.로깅 정책의 예로는 로깅 설정, 서버 설정 및 syslog 서버 정책이 있습니다.
13. **Modify(수정) > Policies(정책) > Multicast(멀티캐스트)**.PIX/ASA/FWSM 디바이스의 Policy selector(Platform(플랫폼) > Multicast(멀티캐스트) 아래의 Policy(정책) 선택기에 있음)를 수정할 수 있습니다.멀티캐스트 정책의 예로는 멀티캐스트 라우팅 및 IGMP 정책이 있습니다.
14. **Modify > Policies > QoS를 선택합니다**.Cisco IOS 라우터에서 QoS 정책(Platform > QoS(서비스 품질) 아래의 Policy 선택기에 있음)을 수정할 수 있습니다.
15. **수정 > 정책 > 라우팅**.PIX/ASA/FWSM 디바이스 및 IOS 라우터의 라우팅 정책(플랫폼 > 라우팅 아래의 정책 선택기에 있음)을 수정할 수 있습니다.라우팅 정책의 예로는 OSPF, RIP 및 고정 라우팅 정책이 있습니다.
16. **수정 > 정책 > 보안**.PIX/ASA/FWSM 디바이스 및 IPS 센서에서 Platform(플랫폼) > Security(보안) 아래의 Policy(정책) 선택기에 있는 보안 정책을 수정할 수 있습니다 .PIX/ASA/FWSM 디바이스에서 보안 정책에는 안티스푸핑, 프래그먼트 및 시간 초과 설정이 포함됩니다.IPS 센서에서 보안 정책에는 차단 설정이 포함됩니다.
17. **Modify(수정) > Policies(정책) > Service Policy Rules(서비스 정책 규칙)**.PIX 7.x/ASA 디바이스에서 서비스 정책 규칙 정책 정책 정책 정책(Platform > Service Policy Rules 아래의 Policy Selector)을 수정할 수 있습니다.우선 순위 큐와 IPS, QoS, 연결 규칙을 예로 들 수 있습니다.
18. **수정 > 정책 > 사용자 환경 설정**.PIX/ASA/FWSM 디바이스의 구축 정책(Platform(플랫폼) > User Preferences(사용자 환경 설정) 아래의 Policy(정책) 선택기에 있음)을 수정할 수 있습니다.이 정책에는 구축의 모든 NAT 변환을 지우는 옵션이 포함되어 있습니다.
19. **수정 > 정책 > 가상 장치**.IPS 디바이스에서 가상 센서 정책을 수정할 수 있습니다.이 정책을 사용하여 가상 센서를 생성합니다.
20. **Modify > Policies > FlexConfig를 선택합니다**.PIX/ASA/FWSM 디바이스, IOS 라우터 및 Catalyst 6500/7600 디바이스에 구축할 수 있는 추가 CLI 명령 및 지침인 FlexConfigs를 수정할 수 있습니다.

객체 권한 수정

Security Manager에는 객체에 대한 다음 보기 권한이 포함됩니다.

1. **Modify(수정) > Objects(개체) > AAA Server Groups(AAA 서버 그룹)**.AAA 서버 그룹 객체를 볼 수 있습니다.이러한 객체는 AAA 서비스(인증, 권한 부여 및 계정 관리)가 필요한 정책에서 사용됩니다.
2. **Modify(수정) > Objects(개체) > AAA Servers(AAA 서버)**.AAA 서버 객체를 볼 수 있습니다.이러한 객체는 AAA 서버 그룹의 일부로 정의된 개별 AAA 서버를 나타냅니다.
3. **수정 > 객체 > 액세스 제어 목록 - 표준/확장**.표준 및 확장 ACL 객체를 볼 수 있습니다.확장 ACL 객체는 NAT 및 NAC와 같은 다양한 정책과 VPN 액세스 설정에 사용됩니다.표준 ACL 객체는 OSPF 및 SNMP와 같은 정책과 VPN 액세스 설정에 사용됩니다.
4. **수정 > 객체 > 액세스 제어 목록 - 웹**.웹 ACL 객체를 볼 수 있습니다.웹 ACL 객체는 SSL VPN 정책에서 콘텐츠 필터링을 수행하는 데 사용됩니다.
5. **Modify(수정) > Objects(개체) > ASA** User Groups(ASA 사용자 그룹)를 선택합니다.ASA 사용자 그룹 객체를 볼 수 있습니다.이러한 객체는 Easy VPN, 원격 액세스 VPN 및 SSL VPN 컨피그레이션의 ASA 보안 어플라이언스에 구성됩니다.
6. **수정 > 객체 > 범주**.범주 객체를 볼 수 있습니다.이러한 객체는 색상을 사용하여 규칙 테이블

의 규칙과 객체를 쉽게 식별할 수 있도록 도와줍니다.

7. **수정 > 객체 > 자격 증명**.자격 증명 객체를 볼 수 있습니다.이러한 객체는 IKE Extended Authentication(Xauth) 중에 Easy VPN 컨피그레이션에서 사용됩니다.
8. **Modify(수정) > Objects(개체) > FlexConfigs를 선택합니다**.FlexConfig 객체를 볼 수 있습니다 .추가 스크립팅 언어 지침이 있는 구성 명령을 포함하는 이러한 개체를 사용하여 Security Manager 사용자 인터페이스에서 지원하지 않는 명령을 구성할 수 있습니다.
9. **Modify(수정) > Objects(개체) > IKE Proposals(IKE 제안)**.IKE 제안 객체를 볼 수 있습니다.이러한 개체에는 원격 액세스 VPN 정책의 IKE 제안서에 필요한 매개변수가 포함되어 있습니다.
10. **Modify > Objects > Inspect - Class Maps - DNS**.DNS 클래스 맵 개체를 볼 수 있습니다.이러한 객체는 DNS 트래픽과 특정 기준을 일치하므로 해당 트래픽에 대해 작업을 수행할 수 있습니다.
11. **Modify > Objects > Inspect - Class Maps - FTP**.FTP 클래스 맵 객체를 볼 수 있습니다.이러한 객체는 FTP 트래픽과 특정 기준을 일치하므로 해당 트래픽에 대해 작업을 수행할 수 있습니다.
12. **Modify > Objects > Inspect - Class Maps - HTTP**.HTTP 클래스 맵 객체를 볼 수 있습니다.이러한 객체는 HTTP 트래픽과 특정 기준을 일치하므로 해당 트래픽에 대해 작업을 수행할 수 있습니다.
13. **Modify > Objects > Inspect - Class Maps - IM**.IM 클래스 맵 개체를 볼 수 있습니다.이러한 객체는 IM 트래픽과 특정 기준을 일치하므로 해당 트래픽에 대해 작업을 수행할 수 있습니다.
14. **Modify > Objects > Inspect - Class Maps - SIP**.SIP 클래스 맵 개체를 볼 수 있습니다.이러한 객체는 SIP 트래픽과 특정 기준을 일치하므로 해당 트래픽에 대해 작업을 수행할 수 있습니다.
15. **Modify > Objects > Inspect - Policy Maps - DNS**.DNS 정책 맵 객체를 볼 수 있습니다.이러한 개체는 DNS 트래픽에 대한 검사 맵을 만드는 데 사용됩니다.
16. **Modify > Objects > Inspect - Policy Maps - FTP**.FTP 정책 맵 객체를 볼 수 있습니다.이러한 객체는 FTP 트래픽에 대한 검사 맵을 만드는 데 사용됩니다.
17. **Modify > Objects > Inspect - Policy Maps - HTTP(ASA7.1.x/PIX7.1.x/IOS)**. ASA/PIX 7.x 디바이스 및 IOS 라우터에 대해 생성된 HTTP 정책 맵 객체를 볼 수 있습니다.이러한 객체는 HTTP 트래픽에 대한 검사 맵을 만드는 데 사용됩니다.
18. **Modify > Objects > Inspect - Policy Maps - HTTP(ASA7.2/PIX7.2)**. ASA 7.2/PIX 7.2 디바이스에 대해 생성된 HTTP 정책 맵 객체를 볼 수 있습니다.이러한 객체는 HTTP 트래픽에 대한 검사 맵을 만드는 데 사용됩니다.
19. **Modify > Objects > Inspect - Policy Maps - IM(ASA7.2/PIX7.2)**. ASA 7.2/PIX 7.2 디바이스에 대해 생성된 IM 정책 맵 객체를 볼 수 있습니다.이러한 객체는 IM 트래픽에 대한 검사 맵을 만드는 데 사용됩니다.
20. **Modify(수정) > Objects(개체) > Inspect(검사) - Policy Maps(정책 맵) - IM(IOS)**. IOS 디바이스에 대해 생성된 IM 정책 맵 객체를 볼 수 있습니다.이러한 객체는 IM 트래픽에 대한 검사 맵을 만드는 데 사용됩니다.
21. **Modify > Objects > Inspect - Policy Maps - SIP**.SIP 정책 맵 개체를 볼 수 있습니다.이러한 개체는 SIP 트래픽에 대한 검사 맵을 만드는 데 사용됩니다.
22. **Modify > Objects > Inspect - Regular Expressions**.정규식 객체를 볼 수 있습니다.이러한 객체는 정규식 그룹의 일부로 정의된 개별 정규식을 나타냅니다.
23. **Modify > Objects > Inspect - Regular Expressions Groups**.정규식 그룹 객체를 볼 수 있습니다.이러한 객체는 특정 클래스 맵에서 사용되고 맵을 검사하여 패킷 내의 텍스트를 확인합니다.
24. **Modify > Objects > Inspect - TCP Maps**.TCP 맵 객체를 볼 수 있습니다.이러한 객체는 양방향의 TCP 흐름에서 검사를 사용자 정의합니다.
25. **수정 > 객체 > 인터페이스 역할**.인터페이스 역할 객체를 볼 수 있습니다.이러한 객체는 서로

다른 유형의 디바이스에서 여러 인터페이스를 나타낼 수 있는 명명 패턴을 정의합니다.인터페이스 역할을 사용하면 각 인터페이스의 이름을 수동으로 정의하지 않고도 여러 디바이스의 특정 인터페이스에 정책을 적용할 수 있습니다.

26. **Modify > Objects > IPsec Transform Sets**.IPsec 변형 집합 개체를 볼 수 있습니다.이러한 객체는 보안 프로토콜, 알고리즘 및 IPsec 터널의 데이터가 암호화 및 인증되는 방식을 정확히 지정하는 기타 설정의 조합으로 구성됩니다.
27. **Modify(수정) > Objects(개체) > LDAP Attribute Maps(LDAP 특성 맵)**.LDAP 특성 맵 객체를 볼 수 있습니다.이러한 객체는 맞춤형(사용자 정의) 특성 이름을 Cisco LDAP 특성 이름에 매핑하는 데 사용됩니다.
28. **Modify > Objects > Networks/Hosts를 선택합니다**.네트워크/호스트 객체를 볼 수 있습니다.이러한 객체는 네트워크, 호스트 또는 둘 모두를 나타내는 IP 주소의 논리적 컬렉션입니다.네트워크/호스트 객체를 사용하면 각 네트워크 또는 호스트를 개별적으로 지정하지 않고 정책을 정의할 수 있습니다.
29. **Modify(수정) > Objects(개체) > PKI Enrollment(PKI 등록)**.PKI 등록 객체를 볼 수 있습니다.이러한 객체는 공개 키 인프라 내에서 작동하는 CA(인증 기관) 서버를 정의합니다.
30. **Modify > Objects > Port Forwarding Lists**.포트 전달 목록 객체를 볼 수 있습니다.이러한 객체는 원격 클라이언트의 포트 번호 매핑을 SSL VPN 게이트웨이 뒤에 있는 애플리케이션의 IP 주소 및 포트에 정의합니다.
31. **수정 > 객체 > 보안 데스크탑 구성**.보안 데스크톱 컨피그레이션 객체를 볼 수 있습니다.이러한 객체는 SSL VPN 정책에서 참조할 수 있는 재사용 가능한 명명된 구성 요소로, SSL VPN 세션 동안 공유되는 모든 민감한 데이터의 추적을 제거하는 안정적인 방법을 제공합니다.
32. **Modify(수정) > Objects(개체) > Services(서비스) - Port Lists(포트 목록)**.포트 목록 객체를 볼 수 있습니다.하나 이상의 포트 번호 범위를 포함하는 이러한 객체는 서비스 객체 생성 프로세스를 간소화하는 데 사용됩니다.
33. **수정 > 객체 > 서비스/서비스 그룹.**서비스 및 서비스 그룹 객체를 볼 수 있습니다.이러한 객체는 Kerberos, SSH 및 POP3과 같은 정책에서 사용하는 네트워크 서비스를 설명하는 프로토콜 및 포트 정의의 정의된 매핑입니다.
34. **수정 > 객체 > 단일 로그인 서버.**SSO(Single Sign On) 서버 개체를 볼 수 있습니다.SSO(Single Sign-On)를 사용하면 SSL VPN 사용자가 사용자 이름과 비밀번호를 한 번 입력할 수 있으며 여러 보호 서비스 및 웹 서버에 액세스할 수 있습니다.
35. **Modify(수정) > Objects(개체) > SLA Monitor(SLA 모니터)**.SLA 모니터 객체를 볼 수 있습니다.이러한 객체는 버전 7.2 이상을 실행하는 PIX/ASA 보안 어플라이언스에서 경로 추적을 수행하는 데 사용됩니다.이 기능은 기본 경로의 가용성을 추적하고 기본 경로가 실패할 경우 백업 경로를 설치하는 방법을 제공합니다.
36. **Modify(수정) > Objects(개체) > SSL VPN Customizations(SSL VPN 사용자 지정)**.SSL VPN 사용자 지정 개체를 볼 수 있습니다.이러한 객체는 사용자에게 표시되는 SSL VPN 페이지(예: 로그인/로그아웃 및 홈 페이지)의 모양을 변경하는 방법을 정의합니다.
37. **Modify(수정) > Objects(개체) > SSL VPN Gateway(SSL VPN 게이트웨이)**.SSL VPN 게이트웨이 개체를 볼 수 있습니다.이러한 객체는 게이트웨이를 SSL VPN에서 보호된 리소스에 대한 연결에 프록시로 사용할 수 있도록 하는 매개변수를 정의합니다.
38. **수정(Modify) > 개체(Objects) > 스타일 개체(Style Objects)**.스타일 객체를 볼 수 있습니다.이러한 개체를 사용하면 글꼴 특성 및 색상과 같은 스타일 요소를 구성하여 보안 어플라이언스에 연결할 때 SSL VPN 사용자에게 표시되는 SSL VPN 페이지의 모양을 사용자 지정할 수 있습니다.
39. **수정 > 객체 > 텍스트 객체**.자유 형식 텍스트 객체를 볼 수 있습니다.이러한 객체는 이름 및 값 쌍을 구성합니다. 여기서 값은 단일 문자열, 문자열 목록 또는 문자열 테이블이 될 수 있습니다.
40. **수정 > 객체 > 시간 범위.**시간 범위 객체를 볼 수 있습니다.이러한 객체는 시간 기반 ACL 및

검사 규칙을 생성할 때 사용됩니다.또한 ASA 사용자 그룹을 정의하여 주 중 특정 시간으로 VPN 액세스를 제한할 때도 사용됩니다.

41. **Modify > Objects > Traffic Flows**.트래픽 흐름 객체를 볼 수 있습니다.이러한 객체는 PIX 7.x/ASA 7.x 디바이스에서 사용할 특정 트래픽 흐름을 정의합니다.
42. **수정 > 객체 > URL 목록**.URL 목록 객체를 볼 수 있습니다.이러한 객체는 로그인 성공 후 포털 페이지에 표시되는 URL을 정의합니다.이를 통해 사용자는 클라이언트리스 액세스 모드에서 작동할 때 SSL VPN 웹 사이트에서 사용 가능한 리소스에 액세스할 수 있습니다.
43. **수정 > 객체 > 사용자 그룹**.사용자 그룹 객체를 볼 수 있습니다.이러한 객체는 Easy VPN 토폴로지, 원격 액세스 VPN 및 SSL VPN에서 사용되는 원격 클라이언트 그룹을 정의합니다.
44. **Modify(수정) > Objects(개체) > WINS Server Lists(WINS 서버 목록)**.WINS 서버 목록 개체를 볼 수 있습니다.이러한 객체는 SSL VPN에서 원격 시스템의 파일에 액세스하거나 공유하는 데 사용되는 WINS 서버를 나타냅니다.
45. **Modify > Objects > Internal - DN Rules를 선택합니다.**DN 정책에서 사용되는 DN 규칙을 볼 수 있습니다.보안 관리자가 사용하는 내부 개체로서 정책 개체 관리자에 나타나지 않습니다.
46. **수정 > 객체 > 내부 - 클라이언트 업데이트**.이는 정책 개체 관리자에 나타나지 않는 사용자 그룹 개체에 필요한 내부 개체입니다.
47. **수정 > 객체 > 내부 - 표준 ACE**.표준 액세스 제어 엔트리를 위한 내부 개체이며 ACL 객체에서 사용됩니다.
48. **수정 > 객체 > 내부 - 확장 ACE**.ACL 객체에서 사용하는 확장 액세스 제어 엔트리에 대한 내부 객체입니다.

추가 수정 권한

Security Manager에는 다음과 같은 추가 수정 권한이 포함됩니다.

1. **수정 > 관리자**.Security Manager 관리 설정을 수정할 수 있습니다.
2. **Modify(수정) > Config Archive(컨피그레이션 아카이브)**.컨피그레이션 아카이브에서 디바이스 컨피그레이션을 수정할 수 있습니다.또한 아카이브에 컨피그레이션을 추가하고 Configuration Archive 툴을 사용자 지정할 수 있습니다.
3. **Modify(수정) > Devices(디바이스)**.디바이스를 추가 및 삭제할 뿐 아니라 디바이스 속성 및 특성을 수정할 수 있습니다.추가 중인 디바이스에서 정책을 검색하려면 가져오기 권한도 활성화해야 합니다.또한 Modify > Devices 권한을 활성화한 경우 Assign > Policies > Interfaces 권한도 활성화해야 합니다.
4. **수정 > 계층 구조**.디바이스 그룹을 수정할 수 있습니다.
5. **수정 > 토폴로지**.맵 보기에서 맵을 수정할 수 있습니다.

권한 할당

Security Manager에는 다음과 같이 정책 할당 권한이 포함됩니다.

1. **Assign(할당) > Policies(정책) > Firewall(방화벽)**.방화벽 아래의 정책 선택기에 있는 방화벽 서비스 정책을 PIX/ASA/FWSM 디바이스, IOS 라우터 및 Catalyst 6500/7600 디바이스에 할당할 수 있습니다.방화벽 서비스 정책의 예로는 액세스 규칙, AAA 규칙, 검사 규칙이 있습니다.
2. **Assign > Policies > Intrusion Prevention System**.IOS 라우터에서 실행되는 IPS에 대한 정책을 포함하여 IPS 정책(IPS 아래의 Policy 선택기에 있음)을 할당할 수 있습니다.
3. **Assign(할당) > Policies(정책) > Image(이미지)**.이 권한은 현재 보안 관리자에서 사용되지 않습니다.
4. **Assign(할당) > Policies(정책) > NAT**.PIX/ASA/FWSM 디바이스 및 IOS 라우터에 네트워크 주

소 변환 정책을 할당할 수 있습니다.NAT 정책의 예로는 고정 규칙 및 동적 규칙이 있습니다.

5. **Assign(할당) > Policies(정책) > Site-to-Site VPN**.PIX/ASA/FWSM 디바이스, IOS 라우터 및 Catalyst 6500/7600 디바이스에 사이트 간 VPN 정책을 할당할 수 있습니다.사이트 간 VPN 정책의 예로는 IKE 제안, IPsec 제안, 사전 공유 키가 있습니다.
6. **Assign(할당) > Policies(정책) > Remote Access VPN(원격 액세스 VPN)**PIX/ASA/FWSM 디바이스, IOS 라우터 및 Catalyst 6500/7600 디바이스에 원격 액세스 VPN 정책을 할당할 수 있습니다.원격 액세스 VPN 정책의 예로는 IKE 제안서, IPsec 제안서, PKI 정책이 있습니다.
7. **Assign(할당) > Policies(정책) > SSL VPN**.SSL VPN 마법사와 같은 PIX/ASA/FWSM 디바이스 및 IOS 라우터에 SSL VPN 정책을 할당할 수 있습니다.
8. **Assign(할당) > Policies(정책) > Interfaces(인터페이스)**.PIX/ASA/FWSM 디바이스, IOS 라우터 및 Catalyst 6500/7600 디바이스에 인터페이스 정책(인터페이스 아래의 정책 선택기에 있음)을 할당할 수 있습니다.PIX/ASA/FWSM 디바이스에서 이 권한은 하드웨어 포트 및 인터페이스 설정을 포함합니다.IOS 라우터에서 이 권한은 기본 및 고급 인터페이스 설정뿐만 아니라 DSL, PVC, PPP, 다이얼러 정책 등의 기타 인터페이스 관련 정책을 다룹니다.Catalyst 6500/7600 디바이스에서 이 권한은 인터페이스 및 VLAN 설정을 다룹니다.
9. **Assign(할당) > Policies(정책) > Bridging(브리징)**.PIX/ASA/FWSM 디바이스에 ARP 테이블 정책(Platform > Bridging 아래의 Policy 선택기에 있음)을 할당할 수 있습니다.
10. **Assign(할당) > Policies(정책) > Device Administration(디바이스 관리)**.PIX/ASA/FWSM 디바이스, IOS 라우터 및 Catalyst 6500/7600 디바이스에 디바이스 관리 정책(Platform > Device Admin 아래의 Policy 선택기에 있음)을 할당할 수 있습니다.PIX/ASA/FWSM 디바이스의 예로는 디바이스 액세스 정책, 서버 액세스 정책 및 장애 조치 정책이 있습니다.IOS 라우터의 예로는 디바이스 액세스(라인 액세스 포함) 정책, 서버 액세스 정책, AAA 및 Secure Device Provisioning 등이 있습니다.IPS 센서에서 이 권한은 디바이스 액세스 정책 및 서버 액세스 정책을 다룹니다.Catalyst 6500/7600 디바이스에서 이 권한은 IDSM 설정 및 VLAN 액세스 목록을 다룹니다.
11. **Assign(할당) > Policies(정책) > Identity(ID)**.802.1x 및 NAC(Network Admission Control) 정책을 포함하여 Cisco IOS 라우터에 ID 정책(플랫폼 > ID 아래의 정책 선택기에 있음)를 할당할 수 있습니다.
12. **Assign(할당) > Policies(정책) > Logging(로깅)**.PIX/ASA/FWSM 디바이스 및 IOS 라우터에 로깅 정책(Platform > Logging 아래의 Policy 선택기에 있음)을 할당할 수 있습니다.로깅 정책의 예로는 로깅 설정, 서버 설정 및 syslog 서버 정책이 있습니다.
13. **Assign(할당) > Policies(정책) > Multicast(멀티캐스트)**.PIX/ASA/FWSM 디바이스에 멀티캐스트 정책(Platform(플랫폼) > Multicast(멀티캐스트) 아래의 Policy(정책) 선택기에 있음)을 할당할 수 있습니다.멀티캐스트 정책의 예로는 멀티캐스트 라우팅 및 IGMP 정책이 있습니다.
14. **Assign(할당) > Policies(정책) > QoS**.Cisco IOS 라우터에 QoS 정책(Platform > Quality of Service 아래의 Policy 선택기에 있음)을 할당할 수 있습니다.
15. **Assign(할당) > Policies(정책) > Routing(라우팅)**.PIX/ASA/FWSM 디바이스 및 IOS 라우터에 라우팅 정책(플랫폼 > 라우팅 아래의 정책 선택기에 있음)을 할당할 수 있습니다.라우팅 정책의 예로는 OSPF, RIP 및 고정 라우팅 정책이 있습니다.
16. **Assign(할당) > Policies(정책) > Security(보안)**.PIX/ASA/FWSM 디바이스에 보안 정책(Platform(플랫폼) > Security(보안) 아래의 Policy(정책) 선택기에 있음)을 할당할 수 있습니다.보안 정책에는 스푸핑 방지, 프래그먼트 및 시간 초과 설정이 포함됩니다.
17. **Assign(할당) > Policies(정책) > Service Policy Rules(서비스 정책 규칙)**.PIX 7.x/ASA 디바이스에 서비스 정책 규칙 정책 정책 정책 정책 정책 정책(Platform > Service Policy Rules 아래의 Policy selector)을 할당할 수 있습니다.우선 순위 큐와 IPS, QoS, 연결 규칙을 예로 들 수 있습니다.
18. **Assign(할당) > Policies(정책) > User Preferences(사용자 환경 설정)**.PIX/ASA/FWSM 디바

이스에 구축 정책(Platform(플랫폼) > User Preferences(사용자 환경 설정) 아래의 Policy selector(정책 선택기)을 할당할 수 있습니다.이 정책에는 구축의 모든 NAT 변환을 지우는 옵션이 포함되어 있습니다.

19. **Assign(할당) > Policies(정책) > Virtual Device(가상 디바이스)**.IPS 디바이스에 가상 센서 정책을 할당할 수 있습니다.이 정책을 사용하여 가상 센서를 생성합니다.
20. **Assign(할당) > Policies(정책) > FlexConfig**.PIX/ASA/FWSM 디바이스, IOS 라우터 및 Catalyst 6500/7600 디바이스에 구축할 수 있는 추가 CLI 명령 및 지침인 FlexConfigs를 할당할 수 있습니다.

참고: 권한을 지정할 때 해당 보기 권한도 선택했는지 확인합니다.

권한 승인

Security Manager는 다음과 같이 승인 권한을 제공합니다.

1. **승인 > CLI**.구축 작업에 포함된 CLI 명령 변경 사항을 승인할 수 있습니다.
2. **승인 > 정책**.워크플로 활동에 구성된 정책에 포함된 컨피그레이션 변경 사항을 승인할 수 있습니다.

CiscoWorks 역할 이해

사용자가 CiscoWorks Common Services에서 생성되면 하나 이상의 역할이 할당됩니다.각 역할에 연결된 권한은 각 사용자가 Security Manager에서 수행할 수 있는 작업을 결정합니다.

다음 항목에서는 CiscoWorks 역할에 대해 설명합니다.

CiscoWorks Common Services 기본 역할

CiscoWorks Common Services에는 다음과 같은 기본 역할이 포함되어 있습니다.

1. **헬프 데스크** - 헬프 데스크 사용자는 디바이스, 정책, 객체 및 토폴로지 맵을 볼 수 있지만 수정할 수는 없습니다.
2. **Network Operator**(네트워크 운영자) - 권한을 볼 뿐만 아니라 네트워크 운영자가 CLI 명령 및 Security Manager 관리 설정을 볼 수 있습니다.네트워크 운영자는 구성 아카이브를 수정하고 디바이스에 ping과 같은 명령을 실행할 수도 있습니다.
3. **승인자** - 승인자는 권한을 볼 뿐만 아니라 배포 작업을 승인하거나 거부할 수 있습니다.구축을 수행할 수 없습니다.
4. **네트워크 관리자**—네트워크 관리자는 관리 설정을 수정하는 경우를 제외하고 전체 보기 및 수정 권한을 가집니다.이러한 디바이스와 이러한 디바이스에 구성된 정책을 검색하고, 디바이스에 정책을 할당하고, 디바이스에 명령을 실행할 수 있습니다.네트워크 관리자는 활동 또는 구축 작업을 승인할 수 없습니다.하지만 다른 사람이 승인한 작업을 배포할 수 있습니다.
5. **시스템 관리자**—시스템 관리자는 수정, 정책 할당, 활동 및 작업 승인, 검색, 배포, 장치에 대한 명령 실행 등 모든 Security Manager 권한에 대한 완전한 액세스 권한을 가집니다.

참고: 서버에 추가 응용 프로그램이 설치된 경우 내보내기 데이터와 같은 추가 역할이 Common Services에 표시될 수 있습니다.내보내기 데이터 역할은 서드파티 개발자를 위한 것이며 Security Manager에서 사용되지 않습니다.

팁: CiscoWorks 역할의 정의를 변경할 수는 없지만, 각 사용자에게 어떤 역할을 할당할지 정의할 수 있습니다.자세한 내용은 CiscoWorks Common Services의 사용자에게 역할 할당을 참조하십시오.

CiscoWorks Common Services의 사용자에게 역할 할당

CiscoWorks Common Services를 사용하면 각 사용자에게 어떤 역할이 할당되는지 정의할 수 있습니다.사용자에 대한 역할 정의를 변경하면 이 사용자가 Security Manager에서 수행할 수 있는 작업의 유형을 변경할 수 있습니다.예를 들어, 헬프 데스크 역할을 할당하는 경우 사용자는 보기 작업으로 제한되며 데이터를 수정할 수 없습니다.그러나 Network Operator(네트워크 운영자) 역할을 할당하는 경우 사용자는 구성 아카이브를 수정할 수도 있습니다.각 사용자에게 여러 역할을 할당할 수 있습니다.

참고: 사용자 권한을 변경한 후 Security Manager를 다시 시작해야 합니다.

절차:

1. Common Services(공통 서비스)에서 **Server(서버) > Security(보안)**를 선택한 다음 TOC에서 **Single-Server Trust Management(단일 서버 신뢰 관리) > Local User Setup(로컬 사용자 설정)을** 선택합니다.**팁:** Security Manager 내에서 Local User Setup(로컬 사용자 설정) 페이지에 액세스하려면 Tools(도구) > Security Manager Administration(보안 관리자 관리) > Server Security(서버 보안)를 선택한 다음 Local User Setup(로컬 사용자 설정)을 클릭합니다.
2. 기존 사용자 옆의 확인란을 선택한 다음 **Edit**(편집)를 클릭합니다.
3. User Information 페이지에서 확인란을 클릭하여 이 사용자에게 할당할 역할을 선택합니다.각 역할에 대한 자세한 내용은 CiscoWorks Common Services Default Roles를 참조하십시오.
4. 확인**을** 클릭하여 변경 사항을 저장합니다.
5. 보안 관리자를 다시 시작합니다.

Cisco Secure ACS 역할 이해

Cisco Secure ACS는 구성할 수 있는 애플리케이션별 역할을 지원하므로 CiscoWorks보다 Security Manager 권한을 관리할 수 있는 유연성이 향상됩니다.각 역할은 Security Manager 작업에 대한 권한 부여 수준을 결정하는 권한 집합으로 구성됩니다.Cisco Secure ACS에서는 각 사용자 그룹(그리고 선택적으로 개별 사용자에게도 역할)에 역할을 할당하여 해당 그룹의 각 사용자가 해당 역할에 대해 정의된 권한에 의해 승인된 작업을 수행할 수 있도록 합니다.

또한 이러한 역할을 Cisco Secure ACS 디바이스 그룹에 할당할 수 있으므로, 다양한 디바이스 세트에 대해 권한을 차별화할 수 있습니다.

참고: Cisco Secure ACS 디바이스 그룹은 Security Manager 디바이스 그룹과 독립적입니다.

다음 항목에서는 Cisco Secure ACS 역할에 대해 설명합니다.

- Cisco Secure ACS 기본 역할
- Cisco Secure ACS 역할 사용자 지정

Cisco Secure ACS 기본 역할

Cisco Secure ACS에는 CiscoWorks와 동일한 역할(CiscoWorks 역할 이해 참조)과 다음 추가 역할이 포함됩니다.

1. **보안 승인자** — 보안 승인자는 디바이스, 정책, 객체, 맵, CLI 명령 및 관리 설정을 볼 수 있지만 수정할 수는 없습니다.또한 보안 승인자는 활동에 포함된 구성 변경 사항을 승인하거나 거부할 수 있습니다.배포 작업을 승인하거나 거부할 수 없으며 배포를 수행할 수도 없습니다.
2. **보안 관리자**—보안 관리자는 보기 권한 외에도 디바이스, 디바이스 그룹, 정책, 객체 및 토폴로지 맵을 수정할 수 있습니다.또한 디바이스 및 VPN 토폴로지에 정책을 할당하고 검색을 수행하여 새 디바이스를 시스템으로 가져올 수 있습니다.
3. **네트워크 관리자**—네트워크 관리자는 권한을 볼 뿐만 아니라 구성 아카이브를 수정하고 구축을 수행하고 디바이스에 명령을 실행할 수 있습니다.

참고: Cisco Secure ACS 네트워크 관리자 역할에 포함된 권한은 CiscoWorks 네트워크 관리자 역할에 포함된 권한과 다릅니다.자세한 내용은 CiscoWorks 역할 이해를 참조하십시오.

CiscoWorks와 달리 Cisco Secure ACS는 각 Security Manager 역할과 관련된 권한을 사용자 지정할 수 있도록 합니다.기본 역할 수정에 대한 자세한 내용은 Cisco Secure ACS 역할 사용자 정의를 참조하십시오.

참고: Security Manager 인증을 위해 Cisco Secure ACS 3.3 이상을 설치해야 합니다.

Cisco Secure ACS 역할 사용자 지정

Cisco Secure ACS를 사용하면 각 Security Manager 역할과 관련된 권한을 수정할 수 있습니다.특정 Security Manager 작업을 대상으로 하는 권한을 가진 특수 사용자 역할을 만들어 Cisco Secure ACS를 사용자 지정할 수도 있습니다.

참고: 사용자 권한을 변경한 후 Security Manager를 다시 시작해야 합니다.

절차:

1. Cisco Secure ACS의 탐색 모음**에서 Shared Profile Components**를 클릭합니다.
2. 공유 **구성 요소** 페이지에서 **Cisco Security Manager**를 클릭합니다.보안 관리자에 대해 구성된 역할이 표시됩니다.
3. 다음 중 하나를 수행합니다.역할을 생성하려면 Add를 **클릭합니다**.4단계로 이동합니다.기존 역할을 수정하려면 역할을 클릭합니다.5단계로 이동합니다.
4. 역할 이름과 설명(선택 사항)을 입력합니다.
5. 사용 권한 트리에서 확인란을 선택하고 선택 취소하여 이 역할에 대한 사용 권한을 정의합니다.트리의 분기에 대한 확인란을 선택하면 해당 분기의 모든 권한이 선택됩니다.예를 들어 할당을 선택하면 모든 할당 권한이 선택됩니다.Security Manager 사용 권한의 전체 목록은 Security Manager 사용 권한을 참조하십시오.**참고:** 수정, 승인, 할당, 가져오기, 제어 또는 배포 권한을 선택하는 경우 해당 보기 권한도 선택해야 합니다.그렇지 않으면 Security Manager가 제대로 작동하지 않습니다.
6. Submit(**제출**)을 클릭하여 변경 사항을 저장합니다.
7. 보안 관리자를 다시 시작합니다.

Security Manager의 권한과 역할 간의 기본 연결

이 표에서는 Security Manager 권한이 CiscoWorks Common Services 역할 및 Cisco Secure ACS의 기본 역할과 연결되는 방법을 보여 줍니다.

사용 권한	역할							

	시스템관리자	보안관리자(ACS)	보안승인자(ACS)	네트워크관리자(CW)	네트워크관리자(ACS)	승인자	네트워크운영자	헬프데스크
권한 보기								
장치 보기	예	예	예	예	예	예	예	예
정책 보기	예	예	예	예	예	예	예	예
개체 보기	예	예	예	예	예	예	예	예
토폴로지 보기	예	예	예	예	예	예	예	예
CLI 보기	예	예	예	예	예	예	예	아니요
관리자 보기	예	예	예	예	예	예	예	아니요
구성 아카이브 보기	예	예	예	예	예	예	예	예
장치 관리자 보기	예	예	예	예	예	예	예	아니요
권한 수정								
디바이스 수정	예	예	아니요	예	아니요	아니요	아니요	아니요
계층 수정	예	예	아니요	예	아니요	아니요	아니요	아니요
정책 수정	예	예	아니요	예	아니요	아니요	아니요	아니요
이미지 수정	예	예	아니요	예	아니요	아니요	아니요	아니요
객체 수정	예	예	아니요	예	아니요	아니요	아니요	아니요
토폴로지 수정	예	예	아니요	예	아니요	아니요	아니요	아니요
관리자 수정	예	아니요	아니요	아니요	아니요	아니요	아니요	아니요
구성 아카이브 수정	예	예	아니요	예	예	아니요	예	아니요
추가 권한								

정책 할당	예	예	아니요	예	아니요	아니요	아니요	아니요
정책 승인	예	아니요	예	아니요	아니요	아니요	아니요	아니요
CLI 승인	예	아니요	아니요	아니요	아니요	예	아니요	아니요
검색(가져오기)	예	예	아니요	예	아니요	아니요	아니요	아니요
구축	예	아니요	아니요	예	예	아니요	아니요	아니요
제어	예	아니요	아니요	예	예	아니요	예	아니요
제출	예	예	아니요	예	아니요	아니요	아니요	아니요

관련 정보

- Cisco Security Manager 지원 페이지
- 기술 지원 및 문서 – Cisco Systems