CS 3.x: Настройка пользовательских прав и ролей

Содержание

Введение
Предварительные условия
Требования
Используемые компоненты
Условные обозначения
Установите права пользователя
Разрешения менеджера безопасности
Обзорные разрешения
Модифицируйте разрешения
Назначьте разрешения
Утвердите разрешения
Понимание ролей CiscoWorks
Роли CiscoWorks Common Services по умолчанию
Присвоение ролей пользователям в CiscoWorks Common Services
Понимание ролей Cisco Secure ACS
Роли Cisco Secure ACS по умолчанию
Настройка ролей Cisco Secure ACS
Ассоциации по умолчанию между разрешениями и ролями в менеджере безопасности
Дополнительные сведения

Введение

Этот документ описывает, как установить разрешения и роли пользователям в Cisco Security Manager (CSM).

Предварительные условия

Требования

Этот документ предполагает, что CSM установлен и работает должным образом.

Используемые компоненты

Сведения в этом документе основываются на CSM 3.1.

Сведения, представленные в этом документе, были получены от устройств, работающих в

специальной лабораторной среде. Все устройства, описанные в этом документе, были запущены с чистой (стандартной) конфигурацией. В рабочей сети необходимо изучить потенциальное воздействие всех команд до их использования.

Условные обозначения

Дополнительные сведения об условных обозначениях см. в документе Условные обозначения технических терминов Cisco.

Установите права пользователя

Cisco Security Manager аутентифицирует ваше имя пользователя и пароль, прежде чем можно будет войти. После того, как они будут аутентифицироваться, Менеджер безопасности устанавливает вашу роль в рамках приложения. Эта роль определяет ваши разрешения (также названный привилегиями), которые являются набором задач или операций, которые вы авторизуетесь выполнить. Если вы не авторизуетесь для определенных задач или устройств, связанных элементов меню, элементов TOC, и кнопки скрыты или отключены. Кроме того, сообщение говорит вам, что у вас нет разрешений, чтобы просмотреть выбранную информацию или выполнить выбранную операцию.

Проверкой подлинности и авторизация для Менеджера безопасности управляют или Сервер CiscoWorks или сервер Cisco Secure Access Control Server (ACS). По умолчанию CiscoWorks управляет проверкой подлинности и авторизация, но можно измениться на Cisco Secure ACS при помощи Страницы настройки Режима AAA в CiscoWorks Common Services.

Главные преимущества использования Cisco Secure ACS являются способностью создать очень гранулированные роли пользователя со специализированными наборами разрешений (например, позволяя пользователю настроить определенные типы политики, но не других) и способность ограничить пользователей определенными устройствами путем настройки сетевых групп устройств (NDGs).

Следующие темы описывают права пользователя:

- Разрешения менеджера безопасности
- Понимание ролей CiscoWorks
- Понимание ролей Cisco Secure ACS
- Ассоциации по умолчанию между разрешениями и ролями в менеджере безопасности

Разрешения менеджера безопасности

Менеджер безопасности классифицирует разрешения в категории как показано:

1. **View** — Позволяет вам просматривать текущие параметры. Для получения дополнительной информации см. Обзорные Разрешения.
2. **Модифицируйте** — Позволяет вам изменять текущие параметры. Для получения дополнительной информации посмотрите, Модифицируют Разрешения.
3. **Назначьте** — Позволяет вам назначать политику на устройства и топологии VPN. Для получения дополнительной информации посмотрите, Назначают Разрешения
4. **Утвердите** — Позволяет вам утверждать задания развертываний и изменения

политики. Для получения дополнительной информации посмотрите, Утверждают Разрешения.

5. **Импорт** — Позволяет вам импортировать конфигурации, которые уже развернуты на устройствах в Менеджера безопасности.
6. **Развернитесь** — Позволяет вам развертывать изменения конфигурации на устройствах в вашей сети и выполнять откат для возврата к ранее развернутой конфигурации.
7. **Контроль** — Позволяет вам выполнять команды к устройствам, таким как эхо-запрос.
8. **Подвергнитесь** — Позволяет вам отправлять свои изменения конфигурации для утверждения.

- Когда вы выбираете, модифицируют, назначают, утверждают, импортируют, управляют или развертывают разрешения, необходимо также выбрать соответствующие обзорные разрешения; иначе, Менеджер безопасности не будет функционировать должным образом.
- Когда вы выбираете, модифицируют разрешения политики, необходимо также выбрать соответствие, назначают и просматривают разрешения политики.
- Когда вы разрешаете политику, которая использует объекты политики в качестве части ее определения, необходимо также дать обзорные разрешения к этим типам объекта. Например, при выборе разрешений для изменения политики маршрутизации необходимо также выбрать разрешения для просмотра сетевых объектов и интерфейсных ролей, которые являются типами объекта, требуемыми политикой маршрутизации.
- То же сохраняется при разрешении объекта, который использует другие объекты в качестве части его определения. Например, при выборе разрешений для изменения групп пользователей необходимо также выбрать разрешения для просмотра сетевых объектов, объектов ACL и групп AAA-серверов.

Обзорные разрешения

Обзорные разрешения (только для чтения) в Менеджере безопасности разделены на категории как показано:

- Обзорные разрешения политики
- Разрешения объектов View
- Дополнительные обзорные разрешения

Обзорные разрешения политики

Менеджер безопасности включает следующие обзорные разрешения для политики:

1. **Представление> Политика> Межсетевой экран.** Позволяет вам просматривать политику сервиса межсетевого экрана (расположенный в Селекторе политики под Межсетевым экраном) на устройствах PIX/ASA/FWSM, маршрутизаторах IOS и Catalyst 6500/7600 устройства. Примеры политики сервиса межсетевого экрана включают правила доступа, правила AAA и инспекционные правила.
2. **Представление> Политика> Система предотвращения вторжений.** Позволяет вам просматривать политику IPS (расположенный в Селекторе политики под IPS), включая

политику для IPS, работающего на маршрутизаторах IOS.

3. **Представление> Политика> Образ.** Позволяет вам выбирать пакет обновления подписи в Применять мастере Обновлений IPS (расположенный под Программными средствами>, Применяют Обновление IPS), но не позволяет вам назначать пакет на определенные устройства, пока у вас также нет Модифицирования> Политика> разрешения Образа.
4. **Представление> Политика> NAT**. Позволяет вам просматривать политику трансляции сетевых адресов по устройствам PIX/ASA/FWSM и маршрутизаторам IOS. Примеры политики NAT включают статические правила и динамические правила.
5. **Представление> Политика> Сквозной VPN-соединение**. Позволяет вам просматривать сквозную VPN-соединение политику по устройствам PIX/ASA/FWSM, маршрутизаторам IOS и Catalyst 6500/7600 устройства. Примеры сквозной VPN-соединение политики включают Предложения ike, предложения по Ipsec и общие ключи.
6. **Представление> Политика> VPN для удаленного доступа**. Позволяет вам просматривать политику VPN для удаленного доступа по устройствам PIX/ASA/FWSM, маршрутизаторам IOS и Catalyst 6500/7600 устройства. Примеры политики VPN для удаленного доступа включают Предложения ike, предложения по Ipsec и политику PKI.
7. **Представление> Политика> VPN SSL**. Позволяет вам просматривать политику VPN SSL на устройствах PIX/ASA/FWSM и маршрутизаторах IOS, таких как мастер VPN SSL.
8. **Представление> Политика> Интерфейсы**. Позволяет вам просматривать интерфейсную политику (расположенный в Селекторе политики под Интерфейсами) на устройствах PIX/ASA/FWSM, маршрутизаторах IOS, сенсорах IPS и Catalyst 6500/7600 устройства.На устройствах PIX/ASA/FWSM эти разрешения касаются аппаратных портов и интерфейсных параметров настройки.На маршрутизаторах IOS эти разрешения касаются основных и усовершенствованных интерфейсных параметров настройки, а также другой связанной с интерфейсом политики, такой как DSL, PVC, PPP и политика номеронабирателя.На сенсорах IPS эти разрешения касаются физических интерфейсов и итоговых карт.На Catalyst 6500/7600 устройства, эти разрешения касаются интерфейсов и Параметров VLAN.
9. **Представление> Политика> Мостовое соединение**. Позволяет вам просматривать политику таблицы ARP (расположенный в Селекторе политики под Платформой> Соединяющий) на устройствах PIX/ASA/FWSM.
10. **Представление> Политика> Администрирование устройств**. Позволяет вам просматривать политику администрирования устройств (расположенный в Селекторе политики под Платформой> Admin Устройства) на устройствах PIX/ASA/FWSM, маршрутизаторах IOS и Catalyst 6500/7600 устройства:На устройствах PIX/ASA/FWSM примеры включают полицейских доступа к устройству, политику доступа сервера и политику аварийного переключения.На маршрутизаторах IOS примеры включают доступ к устройству (включая доступ линии) полицейские, политика доступа сервера, AAA, и Защищают Инициализацию Устройства.На сенсорах IPS эти разрешения касаются политики доступа к устройству и политики доступа сервера.На Catalyst 6500/7600 устройства, эти разрешения касаются параметров настройки IDSM и списков Доступа к VLAN.
11. **Представление> Политика> Идентичность**. Позволяет вам просматривать политики идентификации (расположенный в Селекторе политики под Платформой> Идентичность) на маршрутизаторах Cisco IOS, включая политику Network Admission Control (NAC) и 802.1x.

12. **Представление> Политика> Регистрация**. Позволяет вам просматривать политику регистрации (расположенный в Селекторе политики под Платформой> Регистрация) на устройствах PIX/ASA/FWSM, маршрутизаторах IOS и сенсорах IPS. Примеры регистрации политики включают настройку регистрации, установку сервера и политику сервера системного журнала.
13. **Представление> Политика> Групповая адресация**. Позволяет вам просматривать политику групповой адресации (расположенный в Селекторе политики под Платформой> Групповая адресация) на устройствах PIX/ASA/FWSM. Примеры политики групповой адресации включают политика IGMP и многоадресная маршрутизация.
14. **Представление> Политика> QoS**. Позволяет вам просматривать политики QoS (расположенный в Селекторе политики под Платформой> Качество обслуживания) на маршрутизаторах Cisco IOS.
15. **Представление> Политика> Маршрутизация**. Позволяет вам просматривать политику маршрутизации (расположенный в Селекторе политики под Платформой> Направляющий) на устройствах PIX/ASA/FWSM и маршрутизаторах IOS. Примеры политики маршрутизации включают OSPF, RIP и политику статичной маршрутизации.
16. **Представление>> Security Политики**. Позволяет вам просматривать политику безопасности (расположенный в Селекторе политики в соответствии с> Security Платформы) на устройствах PIX/ASA/FWSM и сенсорах IPS:На устройствах PIX/ASA/FWSM политика безопасности включает антиспуфинг, фрагмент и настройки времени ожидания.На сенсорах IPS политика безопасности включает блокирующиеся параметры настройки.
17. **Представление> Политика> Правила Политики обслуживания**. Позволяет вам просматривать политику правила политики обслуживания (расположенный в Селекторе политики под Платформой> Правила Политики обслуживания) на PIX 7.x/ASA устройства. Примеры включают очереди с приоритетами и IPS, QoS и правила соединения.
18. **Представление> Политика> Предпочтения пользователя**. Позволяет вам просматривать политику Развертываний (расположенный в Селекторе политики под Платформой> Предпочтения пользователя) на устройствах PIX/ASA/FWSM. Эта политика содержит опцию для очистки всех преобразований NAT на развертываниях.
19. **Представление> Политика> Виртуальное устройство**. Позволяет вам просматривать действительную политику датчика по устройствам IPS. Эта политика используется для создания действительных датчиков.
20. **Представление> Политика> FlexConfig**. Позволяет вам просматривать FlexConfigs, которые являются дополнительными командами CLI и инструкциями, которые могут быть развернуты на устройствах PIX/ASA/FWSM, маршрутизаторах IOS и Catalyst 6500/7600 устройства.

Разрешения объектов View

Менеджер безопасности включает следующие обзорные разрешения для объектов:

1. **Представление> Объекты> Группы AAA-серверов**. Позволяет вам просматривать объекты группы AAA-серверов. Эти объекты используются в политике, которая требует сервисов AAA (аутентификация, авторизация и учет).
2. **Представление> Объекты> AAA-серверы**. Позволяет вам просматривать объекты AAA-

сервера. Эти объекты представляют отдельные AAA-серверы, которые определены как часть группы AAA-серверов.

3. **Представление> Объекты> Списки контроля доступа - Стандартный/Расширенный**. Позволяет вам просматривать объекты расширенного списка ACL и стандарт. Объекты Расширенного списка ACL используются для множества политики, такой как NAT и NAC, и для установления доступа VPN. Стандартные объекты ACL используются для такой политики как OSPF и SNMP, а также для установления доступа VPN.
4. **Представление> Объекты> Списки контроля доступа** - сеть. Позволяет вам просматривать веб-объекты ACL. Веб-объекты ACL используются для выполнения фильтрации содержимого в политике VPN SSL.
5. **Представление> Объекты> Группы пользователей ASA**. Позволяет вам просматривать объекты группы пользователей ASA. Эти объекты настроены на Устройствах обеспечения безопасности ASA в Легкой VPN, VPN для удаленного доступа и конфигурациях VPN SSL.
6. **Представление> Объекты> Категории**. Позволяет вам просматривать объекты категории. Эти объекты помогают вам легко определять правила и объекты в таблицах правил с помощью цвета.
7. **Представление> Объекты> Учетные данные**. Позволяет вам просматривать учетные объекты. Эти объекты используются в Конфигурации Easy VPN во время Протокола XAUTH.
8. **Представление> Объекты> FlexConfigs**. Позволяет вам просматривать объекты FlexConfig. Эти объекты, которые содержат команды настройки с дополнительными инструкциями по языку сценария, могут использоваться к командам настройки, которые не поддерживаются интерфейсом пользователя Менеджера безопасности.
9. **Представление> Объекты> Предложения ike**. Позволяет вам просматривать объекты Предложения ike. Эти объекты содержат параметры, требуемые для Предложений ike в политике VPN для удаленного доступа.
10. **Представление> Объекты> Осматривает - Карты классов** - DNS. Позволяет вам просматривать объекты карты классов DNS. Эти объекты совпадают с трафиком DNS с определенными критериями так, чтобы действия могли быть выполнены на том трафике.
11. **Представление> Объекты> Осматривает - Карты классов - FTP**. Позволяет вам просматривать объекты карты классов FTP. Эти объекты совпадают с трафиком FTP с определенными критериями так, чтобы действия могли быть выполнены на том трафике.
12. **Представление> Объекты> Осматривает - Карты классов - HTTP**. Позволяет вам просматривать объекты карты классов HTTP. Эти объекты совпадают с трафиком HTTP с определенными критериями так, чтобы действия могли быть выполнены на том трафике.
13. **Представление> Объекты> Осматривает - Карты классов - IM**. Позволяет вам просматривать объекты карты классов IM. Эти объекты совпадают с трафиком IM с определенными критериями так, чтобы действия могли быть выполнены на том трафике.
14. **Представление> Объекты> Осматривает - Карты классов - SIP**. Позволяет вам просматривать объекты карты классов SIP. Эти объекты совпадают с трафиком SIP с определенными критериями так, чтобы действия могли быть выполнены на том трафике.
15. **Представление> Объекты> Осматривает - Карты политик - DNS.** Позволяет вам

просматривать объекты карты политик DNS. Эти объекты используются для создания инспекционных карт для трафика DNS.

16. **Представление> Объекты> Осматривает - Карты политик - FTP.** Позволяет вам просматривать объекты карты политик FTP. Эти объекты используются для создания инспекционных карт для трафика FTP.
17. **Представление> Объекты> Осматривает - Карты политик - GTP**. Позволяет вам просматривать объекты карты политик GTP. Эти объекты используются для создания инспекционных карт для трафика GTP.
18. **Представление> Объекты> Осматривает - Карты политик - HTTP (ASA7.1.x/PIX7.1.x/IOS)**. Позволяет вам просматривать объекты карты политики HTTP, созданные для ASA/PIX 7.1.x устройства и маршрутизаторы IOS. Эти объекты используются для создания инспекционных карт для трафика HTTP.
19. **Представление> Объекты> Осматривает - Карты политик - HTTP (ASA7.2/PIX7.2)**. Позволяет вам просматривать объекты карты политики HTTP, созданные для ASA 7.2/PIX 7.2 устройств. Эти объекты используются для создания инспекционных карт для трафика HTTP.
20. **Представление> Объекты> Осматривает - Карты политик - IM (ASA7.2/PIX7.2)**. Позволяет вам просматривать объекты карты политик IM, созданные для ASA 7.2/PIX 7.2 устройств. Эти объекты используются для создания инспекционных карт для трафика IM.
21. **Представление> Объекты> Осматривает - Карты политик - IM (IOS)**. Позволяет вам просматривать объекты карты политик IM, созданные для устройств IOS. Эти объекты используются для создания инспекционных карт для трафика IM.
22. **Представление> Объекты> Осматривает - Карты политик - SIP**. Позволяет вам просматривать объекты карты политик SIP. Эти объекты используются для создания инспекционных карт для трафика SIP.
23. **Представление> Объекты> Осматривает - Регулярные выражения**. Позволяет вам просматривать объекты регулярного выражения. Эти объекты представляют отдельные регулярные выражения, которые определены как часть группы регулярного выражения.
24. **Представление> Объекты> Осматривает - Regular Expressions Groups**. Позволяет вам просматривать объекты группы регулярного выражения. Эти объекты используются определенными картами классов и осматривают карты для соответствия с текстом в пакете.
25. **Представление> Объекты> Осматривает - Карты TCP**. Позволяет вам просматривать объекты карты TCP. Эти объекты настраивают контроль на потоке TCP в обоих направлениях.
26. **Представление> Объекты> Интерфейсные Роли**. Позволяет вам просматривать интерфейсные объекты role. Эти объекты определяют шаблоны именования, которые могут представлять несколько интерфейсов на различных типах устройств. Интерфейсные роли позволяют вам применить политику к определенным интерфейсам на составных устройствах, не имея необходимость вручную определять название каждого интерфейса.
27. **Представление> Объекты> Команды IPsec transform set**. Позволяет вам просматривать объекты команды IPsec transform set. Эти объекты включают комбинацию протоколов безопасности, алгоритмов и других параметров настройки, которые задают точно, как данные в Туннеле IPSec будут шифроваться и аутентифицироваться.

28. **Представление> Объекты> Карты атрибутов LDAP**. Позволяет вам просматривать объекты Карты атрибутов LDAP. Эти объекты используются для сопоставления пользовательских (определяемых пользователем) названий атрибута с названиями атрибута LDAP Cisco.
29. **Представление> Объекты> Сети/Хосты**. Позволяет вам сети/объектам хоста view. Эти объекты являются логическими объединениями IP-адресов, которые представляют сети, хосты или обоих. Сеть/объекты хоста enable вы для определения политики, не задавая каждую сеть или узел индивидуально.
30. **Представление> Объекты> Регистрации PKI**. Позволяет вам просматривать объекты enrollment PKI. Эти объекты определяют серверы Центра сертификации (CA), которые работают в инфраструктуре открытых ключей.
31. **Представление> Объекты> Списки Переадресации портов**. Позволяет вам просматривать объекты списка переадресации портов. Эти объекты определяют сопоставления номеров портов на удаленном клиенте к IP-адресу приложения и порту позади Шлюза VPN SSL.
32. **Представление> Объекты> Конфигурации Защищенной настольной системы**. Позволяет вам просматривать объекты конфигурации защищенной настольной системы. Эти объекты являются допускающими повторное использование, названными компонентами, на которые может сослаться политика VPN SSL для обеспечения надежного средства устранения всех трассировок уязвимых данных, которые разделены на время сеанса VPN SSL.
33. **Представление>> Services Объектов - Списки портов**. Позволяет вам просматривать объекты списка портов. Эти объекты, которые содержат один или несколько номеров диапазонов портов, используются для оптимизации процесса создания объектов службы.
34. **Представление>> Services Объектов / Группы сервисов** Позволяет вам просматривать объекты группы сервисов и сервис. Эти объекты являются определенными сопоставлениями протокола и определений порта, которые описывают сетевые сервисы, используемые политикой, такой как Kerberos, SSH и POP3.
35. **Представление> Объекты> Серверы Единой точки входа**. Позволяет вам просматривать серверный объекты единой точки входа. Единая точка входа (SSO) позволяет пользователям VPN SSL ввести имя пользователя и пароль однажды и быть в состоянии обратиться ко множественным защищенным сервисам и Web-серверам.
36. **Представление> Объекты> Мониторы SLA**. Позволяет вам просматривать объекты монитора SLA. Эти объекты используются рабочей версией 7.2 устройств безопасности PIX/ASA или позже выполнить отслеживание маршрута. Если основной маршрут отказывает, эта функция предоставляет метод, чтобы отследить доступность основного маршрута и установить резервный маршрут.
37. **Представление> Объекты> Кастомизации VPN SSL**. Позволяет вам просматривать объекты кастомизации VPN SSL. Эти объекты определяют, как изменить появление страниц SSL VPN, которые отображены пользователям, таким как Вход в систему/Выход из системы и Домашние страницы.
38. **Представление> Объекты> Шлюзы VPN SSL**. Позволяет вам просматривать объекты Шлюза VPN SSL. Эти объекты определяют параметры, которые позволяют шлюзу использоваться в качестве прокси для соединений с защищенными ресурсами в вашей VPN SSL.

39. **Представление> Объекты> Объекты стиля**. Позволяет вам просматривать объекты стиля. Эти объекты позволяют вам настроить элементы стиля, такие как характеристики шрифта и цвета, настроить появление страницы SSL VPN, которая появляется пользователям VPN SSL, когда они соединяются с устройством безопасности.
40. **Представление> Объекты> Текстовые объекты**. Позволяет вам просматривать текстовые объекты произвольной формы. Эти объекты включают название и пару значения, где значение может быть одиночной строкой, списком строк или таблицей строк.
41. **Представление> Объекты> Временные диапазоны.** Позволяет вам просматривать объекты временного диапазона. Эти объекты используются при создании списков управления доступом (ACL) с временным критерием и инспекционных правил. Они также используются при определении групп пользователей ASA для ограничения доступа VPN к специфическим временам в течение недели.
42. **Представление> Объекты> Трафики**. Позволяет вам просматривать объекты трафика. Эти объекты определяют определенные трафики для использования PIX 7.x/ASA 7.x устройства.
43. **Представление> Объекты> Списки URL - адресов**. Позволяет вам просматривать объекты Списка URL - адресов. Эти объекты определяют URL, которые отображены на странице портала после успешной регистрации в системе. Это позволяет пользователям обратиться к ресурсам, доступным на веб-сайтах VPN SSL при работе в Безклиентом режиме доступа.
44. **Представление> Объекты> Группы пользователей**. Позволяет вам просматривать объекты группы пользователей. Эти объекты определяют группы удаленных клиентов, которые используются в Легких топологиях VPN, VPN для удаленного доступа и VPN SSL.
45. **Представление> Объекты> Списки серверов WINS**. Позволяет вам просматривать объекты списка серверов WINS. Эти объекты представляют серверы WINS, которые используются VPN SSL, чтобы обратиться или совместно использовать файлы на удаленных системах.
46. **Представление> Объекты> Внутренний - Правила DN**. Позволяет вам просматривать правила DN, используемые политикой DN. Это - внутренний объект, используемый Менеджером безопасности, который не появляется в Менеджере Объекта политики.
47. **Представление> Объекты> Внутренний - Обновления клиента**. Это - внутренний объект, требуемый объектами группы пользователей, который не появляется в Менеджере Объекта политики.
48. **Представление> Объекты> Внутренний - Стандартные ACE**. Это - внутренний объект для управляющих записей стандартного доступа, которые используются объектами ACL.
49. **Представление> Объекты> Внутренний - Расширенные ACE.** Это - внутренний объект для расширенных записей управления доступом, которые используются объектами ACL.

Дополнительные обзорные разрешения

Менеджер безопасности включает следующие дополнительные обзорные разрешения:

1. **Представление> Admin**. Позволяет вам просматривать Менеджера безопасности

административные параметры настройки.
2. **Представление> CLI**. Позволяет вам просматривать команды CLI, настроенные на устройстве и предварительно просматривать команды, которые собираются быть развернутыми.
3. **Представление> Архив конфигураций**. Позволяет вам просматривать список конфигураций, содержавшихся в архивной конфигурации. Вы не можете просмотреть конфигурацию устройства или любые команды CLI.
4. **Представление> Устройства**. Позволяет вам просматривать устройства в Просмотре устройств и всех дополнительных сведениях, включая их настройки устройства, свойства, присвоения, и так далее.
5. **Представление> Менеджеры устройств**. Позволяет вам запускать версии только для чтения менеджеров устройств для отдельных устройств, таких как Cisco Router and Security Device Manager (SDM) для маршрутизаторов Cisco IOS.
6. **Представление> Топология**. Позволяет вам просматривать карты, настроенные в представлении Карты.

Модифицируйте разрешения

Модифицируйте (чтение-запись), разрешения в Менеджере безопасности разделены на категории как показано:

- Модифицируйте разрешения политики
- Модифицируйте разрешения объектов
- Дополнительный модифицируют разрешения

Модифицируйте разрешения политики

Примечание: Когда вы задаете, модифицируют разрешения политики, удостоверьтесь, что вы выбрали соответствие, назначают и просматривают разрешения политики также.

Менеджер безопасности включает придерживающееся, модифицируют разрешения для политики:

1. **Модифицируйте> Политика> Межсетевой экран**. Позволяет вам модифицировать политику сервиса межсетевого экрана (расположенный в Селекторе политики под Межсетевым экраном) на устройствах PIX/ASA/FWSM, маршрутизаторах IOS и Catalyst 6500/7600 устройства. Примеры политики сервиса межсетевого экрана включают правила доступа, правила AAA и инспекционные правила.
2. **Модифицируйте> Политика> Система предотвращения вторжений**. Позволяет вам модифицировать политику IPS (расположенный в Селекторе политики под IPS), включая политику для IPS, работающего на маршрутизаторах IOS. Эти разрешения также позволяют вам настраиваться, подписи в мастере Обновления подписи (расположенный под Программными средствами> Применяют Обновление IPS).
3. **Модифицируйте> Политика> Образ**. Позволяет вам назначать пакет обновления подписи на устройства в Применять мастере Обновлений IPS (расположенный под Программными средствами>, Применяют Обновление IPS). Эти разрешения также позволяют вам назначать параметры настройки автоматического обновления на определенные устройства (расположенный под Администратором Tools> Security>

Обновления IPS).

4. **Модифицируйте> Политика> NAT**. Позволяет вам модифицировать политику трансляции сетевых адресов по устройствам PIX/ASA/FWSM и маршрутизаторам IOS. Примеры политики NAT включают статические правила и динамические правила.
5. **Модифицируйте> Политика> Сквозной VPN-соединение**. Позволяет вам модифицировать сквозную VPN-соединение политику по устройствам PIX/ASA/FWSM, маршрутизаторам IOS и Catalyst 6500/7600 устройства. Примеры сквозной VPN-соединение политики включают Предложения ike, предложения по Ipsec и общие ключи.
6. **Модифицируйте> Политика> VPN для удаленного доступа**. Позволяет вам модифицировать политику VPN для удаленного доступа по устройствам PIX/ASA/FWSM, маршрутизаторам IOS и Catalyst 6500/7600 устройства. Примеры политики VPN для удаленного доступа включают Предложения ike, предложения по Ipsec и политику PKI.
7. **Модифицируйте> Политика> VPN SSL**. Позволяет вам модифицировать политику VPN SSL на устройствах PIX/ASA/FWSM и маршрутизаторах IOS, таких как мастер VPN SSL.
8. **Модифицируйте> Политика> Интерфейсы**. Позволяет вам модифицировать интерфейсную политику (расположенный в Селекторе политики под Интерфейсами) на устройствах PIX/ASA/FWSM, маршрутизаторах IOS, сенсорах IPS и Catalyst 6500/7600 устройства:На устройствах PIX/ASA/FWSM эти разрешения касаются аппаратных портов и интерфейсных параметров настройки.На маршрутизаторах IOS эти разрешения касаются основных и усовершенствованных интерфейсных параметров настройки, а также другой связанной с интерфейсом политики, такой как DSL, PVC, PPP и политика номеронабирателя.На сенсорах IPS эти разрешения касаются физических интерфейсов и итоговых карт.На Catalyst 6500/7600 устройства, эти разрешения касаются интерфейсов и Параметров VLAN.
9. **Модифицируйте> Политика> Мостовое соединение**. Позволяет вам модифицировать политику таблицы ARP (расположенный в Селекторе политики под Платформой> Соединяющий) на устройствах PIX/ASA/FWSM.
10. **Модифицируйте> Политика> Администрирование устройств**. Позволяет вам модифицировать политику администрирования устройств (расположенный в Селекторе политики под Платформой> Admin Устройства) на устройствах PIX/ASA/FWSM, маршрутизаторах IOS и Catalyst 6500/7600 устройства:На устройствах PIX/ASA/FWSM примеры включают полицейских доступа к устройству, политику доступа сервера и политику аварийного переключения.На маршрутизаторах IOS примеры включают доступ к устройству (включая доступ линии) полицейские, политика доступа сервера, AAA, и Защищают Инициализацию Устройства.На сенсорах IPS эти разрешения касаются политики доступа к устройству и политики доступа сервера.На Catalyst 6500/7600 устройства, эти разрешения касаются параметров настройки IDSM и списка Доступа к VLAN.
11. **Модифицируйте> Политика> Идентичность**. Позволяет вам модифицировать политики идентификации (расположенный в Селекторе политики под Платформой> Идентичность) на маршрутизаторах Cisco IOS, включая политику Network Admission Control (NAC) и 802.1x.
12. **Модифицируйте> Политика> Регистрация**. Позволяет вам модифицировать политику регистрации (расположенный в Селекторе политики под Платформой> Регистрация) на устройствах PIX/ASA/FWSM, маршрутизаторах IOS и сенсорах IPS. Примеры

регистрации политики включают настройку регистрации, установку сервера и политику сервера системного журнала.

13. **Модифицируйте> Политика> Групповая адресация**. Позволяет вам модифицировать политику групповой адресации (расположенный в Селекторе политики под Платформой> Групповая адресация) на устройствах PIX/ASA/FWSM. Примеры политики групповой адресации включают политика IGMP и многоадресная маршрутизация.
14. **Модифицируйте> Политика> QoS**. Позволяет вам модифицировать политики QoS (расположенный в Селекторе политики под Платформой> Качество обслуживания) на маршрутизаторах Cisco IOS.
15. **Модифицируйте> Политика> Маршрутизация**. Позволяет вам модифицировать политику маршрутизации (расположенный в Селекторе политики под Платформой> Направляющий) на устройствах PIX/ASA/FWSM и маршрутизаторах IOS. Примеры политики маршрутизации включают OSPF, RIP и политику статичной маршрутизации.
16. **Модифицируйте>> Security Политики**. Позволяет вам модифицировать политику безопасности (расположенный в Селекторе политики в соответствии с> Security Платформы) на устройствах PIX/ASA/FWSM и сенсорах IPS:На устройствах PIX/ASA/FWSM политика безопасности включает антиспуфинг, фрагмент и настройки времени ожидания.На сенсорах IPS политика безопасности включает блокирующиеся параметры настройки.
17. **Модифицируйте> Политика> Правила Политики обслуживания**. Позволяет вам модифицировать политику правила политики обслуживания (расположенный в Селекторе политики под Платформой> Правила Политики обслуживания) на PIX 7.x/ASA устройства. Примеры включают очереди с приоритетами и IPS, QoS и правила соединения.
18. **Модифицируйте> Политика> Предпочтения пользователя**. Позволяет вам модифицировать политику Развертываний (расположенный в Селекторе политики под Платформой> Предпочтения пользователя) на устройствах PIX/ASA/FWSM. Эта политика содержит опцию для очистки всех преобразований NAT на развертываниях.
19. **Модифицируйте> Политика> Виртуальное устройство**. Позволяет вам модифицировать действительную политику датчика по устройствам IPS. Используйте эту политику для создания действительных датчиков.
20. **Модифицируйте> Политика> FlexConfig**. Позволяет вам модифицировать FlexConfigs, которые являются дополнительными командами CLI и инструкциями, которые могут быть развернуты на устройствах PIX/ASA/FWSM, маршрутизаторах IOS и Catalyst 6500/7600 устройства.

Модифицируйте разрешения объектов

Менеджер безопасности включает следующие обзорные разрешения для объектов:

1. **Модифицируйте> Объекты> Группы AAA-серверов**. Позволяет вам просматривать объекты группы AAA-серверов. Эти объекты используются в политике, которая требует сервисов AAA (аутентификация, авторизация и учет).
2. **Модифицируйте> Объекты> AAA-серверы**. Позволяет вам просматривать объекты AAA-сервера. Эти объекты представляют отдельные AAA-серверы, которые определены как часть группы AAA-серверов.
3. **Модифицируйте> Объекты> Списки контроля доступа - Стандартный/Расширенный**.

Позволяет вам просматривать объекты расширенного списка ACL и стандарт. Объекты Расширенного списка ACL используются для множества политики, такой как NAT и NAC, и для установления доступа VPN. Стандартные объекты ACL используются для такой политики как OSPF и SNMP, а также для установления доступа VPN.

4. **Модифицируйте> Объекты> Списки контроля доступа - сеть**. Позволяет вам просматривать веб-объекты ACL. Веб-объекты ACL используются для выполнения фильтрации содержимого в политике VPN SSL.
5. **Модифицируйте> Объекты>** Группы пользователей **ASA**. Позволяет вам просматривать объекты группы пользователей ASA. Эти объекты настроены на Устройствах обеспечения безопасности ASA в Легкой VPN, VPN для удаленного доступа и конфигурациях VPN SSL.
6. **Модифицируйте> Объекты> Категории**. Позволяет вам просматривать объекты категории. Эти объекты помогают вам легко определять правила и объекты в таблицах правил с помощью цвета.
7. **Модифицируйте> Объекты> Учетные данные**. Позволяет вам просматривать учетные объекты. Эти объекты используются в Конфигурации Easy VPN во время Протокола XAUTH.
8. **Модифицируйте> Объекты> FlexConfigs**. Позволяет вам просматривать объекты FlexConfig. Эти объекты, которые содержат команды настройки с дополнительными инструкциями по языку сценария, могут использоваться к командам настройки, которые не поддерживаются интерфейсом пользователя Менеджера безопасности.
9. **Модифицируйте> Объекты> Предложения ike**. Позволяет вам просматривать объекты Предложения ike. Эти объекты содержат параметры, требуемые для Предложений ike в политике VPN для удаленного доступа.
10. **Модифицируйте>, Объекты> Осматривают - Карты классов - DNS**. Позволяет вам просматривать объекты карты классов DNS. Эти объекты совпадают с трафиком DNS с определенными критериями так, чтобы действия могли быть выполнены на том трафике.
11. **Модифицируйте>, Объекты> Осматривают - Карты классов - FTP**. Позволяет вам просматривать объекты карты классов FTP. Эти объекты совпадают с трафиком FTP с определенными критериями так, чтобы действия могли быть выполнены на том трафике.
12. **Модифицируйте>, Объекты> Осматривают - Карты классов - HTTP**. Позволяет вам просматривать объекты карты классов HTTP. Эти объекты совпадают с трафиком HTTP с определенными критериями так, чтобы действия могли быть выполнены на том трафике.
13. **Модифицируйте>, Объекты> Осматривают - Карты классов - IM**. Позволяет вам просматривать объекты карты классов IM. Эти объекты совпадают с трафиком IM с определенными критериями так, чтобы действия могли быть выполнены на том трафике.
14. **Модифицируйте>, Объекты> Осматривают - Карты классов - SIP**. Позволяет вам просматривать объекты карты классов SIP. Эти объекты совпадают с трафиком SIP с определенными критериями так, чтобы действия могли быть выполнены на том трафике.
15. **Модифицируйте>, Объекты> Осматривают - Карты политик - DNS**. Позволяет вам просматривать объекты карты политик DNS. Эти объекты используются для создания инспекционных карт для трафика DNS.
16. **Модифицируйте>, Объекты> Осматривают - Карты политик - FTP**. Позволяет вам

просматривать объекты карты политик FTP. Эти объекты используются для создания инспекционных карт для трафика FTP.

17. **Модифицируйте>, Объекты> Осматривают - Карты политик - HTTP (ASA7.1.x/PIX7.1.x/IOS)**. Позволяет вам просматривать объекты карты политики HTTP, созданные для ASA/PIX 7.x устройства и маршрутизаторы IOS. Эти объекты используются для создания инспекционных карт для трафика HTTP.
18. **Модифицируйте>, Объекты> Осматривают - Карты политик - HTTP (ASA7.2/PIX7.2)**. Позволяет вам просматривать объекты карты политики HTTP, созданные для ASA 7.2/PIX 7.2 устройств. Эти объекты используются для создания инспекционных карт для трафика HTTP.
19. **Модифицируйте>, Объекты> Осматривают - Карты политик - IM (ASA7.2/PIX7.2)**. Позволяет вам просматривать объекты карты политик IM, созданные для ASA 7.2/PIX 7.2 устройств. Эти объекты используются для создания инспекционных карт для трафика IM.
20. **Модифицируйте>, Объекты> Осматривают - Карты политик - IM (IOS)**. Позволяет вам просматривать объекты карты политик IM, созданные для устройств IOS. Эти объекты используются для создания инспекционных карт для трафика IM.
21. **Модифицируйте>, Объекты> Осматривают - Карты политик - SIP**. Позволяет вам просматривать объекты карты политик SIP. Эти объекты используются для создания инспекционных карт для трафика SIP.
22. **Модифицируйте>, Объекты> Осматривают - Регулярные выражения**. Позволяет вам просматривать объекты регулярного выражения. Эти объекты представляют отдельные регулярные выражения, которые определены как часть группы регулярного выражения.
23. **Модифицируйте>, Объекты> Осматривают - Regular Expressions Groups**. Позволяет вам просматривать объекты группы регулярного выражения. Эти объекты используются определенными картами классов и осматривают карты для соответствия с текстом в пакете.
24. **Модифицируйте>, Объекты> Осматривают - Карты TCP**. Позволяет вам просматривать объекты карты TCP. Эти объекты настраивают контроль на потоке TCP в обоих направлениях.
25. **Модифицируйте> Объекты> Интерфейсные Роли**. Позволяет вам просматривать интерфейсные объекты role. Эти объекты определяют шаблоны именования, которые могут представлять несколько интерфейсов на различных типах устройств. Интерфейсные роли позволяют вам применить политику к определенным интерфейсам на составных устройствах, не имея необходимость вручную определять название каждого интерфейса.
26. **Модифицируйте> Объекты> Команды IPsec transform set**. Позволяет вам просматривать объекты команды IPsec transform set. Эти объекты включают комбинацию протоколов безопасности, алгоритмов и других параметров настройки, которые задают точно, как данные в Туннеле IPSec будут шифроваться и аутентифицироваться.
27. **Модифицируйте> Объекты> Карты атрибутов LDAP**. Позволяет вам просматривать объекты Карты атрибутов LDAP. Эти объекты используются для сопоставления пользовательских (определяемых пользователем) названий атрибута с названиями атрибута LDAP Cisco.
28. **Модифицируйте> Объекты> Сети/Хосты**. Позволяет вам сети/объектам хоста view. Эти объекты являются логическими объединениями IP-адресов, которые

представляют сети, хосты или обоих. Сеть/объекты хоста enable вы для определения политики, не задавая каждую сеть или узел индивидуально.

29. **Модифицируйте> Объекты> Регистрации PKI**. Позволяет вам просматривать объекты enrollment PKI. Эти объекты определяют серверы Центра сертификации (CA), которые работают в инфраструктуре открытых ключей.
30. **Модифицируйте> Объекты> Списки Переадресации портов**. Позволяет вам просматривать объекты списка переадресации портов. Эти объекты определяют сопоставления номеров портов на удаленном клиенте к IP-адресу приложения и порту позади Шлюза VPN SSL.
31. **Модифицируйте> Объекты> Конфигурации Защищенной настольной системы**. Позволяет вам просматривать объекты конфигурации защищенной настольной системы. Эти объекты являются допускающими повторное использование, названными компонентами, на которые может сослаться политика VPN SSL для обеспечения надежного средства устранения всех трассировок уязвимых данных, которые разделены на время сеанса VPN SSL.
32. **Модифицируйте>> Services Объектов - Списки портов**. Позволяет вам просматривать объекты списка портов. Эти объекты, которые содержат один или несколько номеров диапазонов портов, используются для оптимизации процесса создания объектов службы.
33. **Модифицируйте>> Services Объектов / Группы сервисов.** Позволяет вам просматривать объекты группы сервисов и сервис. Эти объекты являются определенными сопоставлениями протокола и определений порта, которые описывают сетевые сервисы, используемые политикой, такой как Kerberos, SSH и POP3.
34. **Модифицируйте> Объекты> Серверы Единой точки входа.** Позволяет вам просматривать серверный объекты единой точки входа. Единая точка входа (SSO) позволяет пользователям VPN SSL ввести имя пользователя и пароль однажды и быть в состоянии обратиться ко множественным защищенным сервисам и Web-серверам.
35. **Модифицируйте> Объекты> Мониторы SLA**. Позволяет вам просматривать объекты монитора SLA. Эти объекты используются рабочей версией 7.2 устройств безопасности PIX/ASA или позже выполнить отслеживание маршрута. Если основной маршрут отказывает, эта функция предоставляет метод, чтобы отследить доступность основного маршрута и установить резервный маршрут.
36. **Модифицируйте> Объекты> Кастомизации VPN SSL**. Позволяет вам просматривать объекты кастомизации VPN SSL. Эти объекты определяют, как изменить появление страниц SSL VPN, которые отображены пользователям, таким как Вход в систему/Выход из системы и Домашние страницы.
37. **Модифицируйте> Объекты> Шлюзы VPN SSL**. Позволяет вам просматривать объекты Шлюза VPN SSL. Эти объекты определяют параметры, которые позволяют шлюзу использоваться в качестве прокси для соединений с защищенными ресурсами в вашей VPN SSL.
38. **Модифицируйте> Объекты> Объекты стиля**. Позволяет вам просматривать объекты стиля. Эти объекты позволяют вам настроить элементы стиля, такие как характеристики шрифта и цвета, настроить появление страницы SSL VPN, которая появляется пользователям VPN SSL, когда они соединяются с устройством безопасности.
39. **Модифицируйте> Объекты> Текстовые объекты**. Позволяет вам просматривать

текстовые объекты произвольной формы. Эти объекты включают название и пару значения, где значение может быть одиночной строкой, списком строк или таблицей строк.

40. **Модифицируйте> Объекты> Временные диапазоны.** Позволяет вам просматривать объекты временного диапазона. Эти объекты используются при создании списков управления доступом (ACL) с временным критерием и инспекционных правил. Они также используются при определении групп пользователей ASA для ограничения доступа VPN к специфическим временам в течение недели.
41. **Модифицируйте> Объекты> Трафики**. Позволяет вам просматривать объекты трафика. Эти объекты определяют определенные трафики для использования PIX 7.x/ASA 7.x устройства.
42. **Модифицируйте> Объекты> Списки URL - адресов**. Позволяет вам просматривать объекты Списка URL - адресов. Эти объекты определяют URL, которые отображены на странице портала после успешной регистрации в системе. Это позволяет пользователям обратиться к ресурсам, доступным на веб-сайтах VPN SSL при работе в Безклиентом режиме доступа.
43. **Модифицируйте> Объекты> Группы пользователей**. Позволяет вам просматривать объекты группы пользователей. Эти объекты определяют группы удаленных клиентов, которые используются в Легких топологиях VPN, VPN для удаленного доступа и VPN SSL
44. **Модифицируйте> Объекты> Списки серверов WINS**. Позволяет вам просматривать объекты списка серверов WINS. Эти объекты представляют серверы WINS, которые используются VPN SSL, чтобы обратиться или совместно использовать файлы на удаленных системах.
45. **Модифицируйте> Объекты> Внутренний - Правила DN.** Позволяет вам просматривать правила DN, используемые политикой DN. Это - внутренний объект, используемый Менеджером безопасности, который не появляется в Менеджере Объекта политики.
46. **Модифицируйте> Объекты> Внутренний - Обновления клиента**. Это - внутренний объект, требуемый объектами группы пользователей, который не появляется в Менеджере Объекта политики.
47. **Модифицируйте> Объекты> Внутренний - Стандартный ACE**. Это - внутренний объект для управляющих записей стандартного доступа, которые используются объектами ACL.
48. **Модифицируйте> Объекты> Внутренний - Расширенный ACE**. Это - внутренний объект для расширенных записей управления доступом, которые используются объектами ACL.

Дополнительный модифицируют разрешения

Менеджер безопасности включает дополнительное, модифицируют разрешения как показано:

1. **Модифицируйте> Admin**. Позволяет вам модифицировать Менеджера безопасности административные параметры настройки.
2. **Модифицируйте> Архив конфигураций**. Позволяет вам модифицировать конфигурацию устройства в Архивной конфигурации. Кроме того, это позволяет вам добавлять конфигурации к архиву и настраивать программное средство Архивной конфигурации.
3. **Модифицируйте> Устройства**. Позволяет вам добавлять и удалять устройства, а также

модифицировать свойства устройства и атрибуты. Для обнаружения политики по добавляемому устройству необходимо также включить разрешения Импорта. Кроме того, при включении Модифицирования> разрешения Устройств удостоверьтесь, что вы также включаете Назначение> Политика> разрешения Интерфейсов.
4. **Модифицируйте> Иерархия**. Позволяет вам модифицировать группы устройств.
5. **Модифицируйте> Топология**. Позволяет вам модифицировать карты в представлении Карты.

Назначьте разрешения

Менеджер безопасности включает разрешения присвоения политики как показано:

1. **Назначьте> Политика> Межсетевой экран**. Позволяет вам назначать политику сервиса межсетевого экрана (расположенный в Селекторе политики под Межсетевым экраном) к устройствам PIX/ASA/FWSM, маршрутизаторам IOS и Catalyst 6500/7600 устройства. Примеры политики сервиса межсетевого экрана включают правила доступа, правила AAA и инспекционные правила.
2. **Назначьте> Политика> Система предотвращения вторжений**. Позволяет вам назначать политику IPS (расположенный в Селекторе политики под IPS), включая политику для IPS, работающего на маршрутизаторах IOS.
3. **Назначьте> Политика> Образ**. Эти разрешения в настоящее время не используются Менеджером безопасности.
4. **Назначьте> Политика> NAT**. Позволяет вам назначать политику трансляции сетевых адресов на устройства PIX/ASA/FWSM и маршрутизаторы IOS. Примеры политики NAT включают статические правила и динамические правила.
5. **Назначьте> Политика> Сквозной VPN-соединение**. Позволяет вам назначать сквозную VPN-соединение политику на устройства PIX/ASA/FWSM, маршрутизаторы IOS и Catalyst 6500/7600 устройства. Примеры сквозной VPN-соединение политики включают Предложения ike, предложения по Ipsec и общие ключи.
6. **Назначьте> Политика> VPN для удаленного доступа**. Позволяет вам назначать политику VPN для удаленного доступа на устройства PIX/ASA/FWSM, маршрутизаторы IOS и Catalyst 6500/7600 устройства. Примеры политики VPN для удаленного доступа включают Предложения ike, предложения по Ipsec и политику PKI.
7. **Назначьте> Политика> VPN SSL**. Позволяет вам назначать политику VPN SSL на устройства PIX/ASA/FWSM и маршрутизаторы IOS, такие как мастер VPN SSL.
8. **Назначьте> Политика> Интерфейсы**. Позволяет вам назначать интерфейсную политику (расположенный в Селекторе политики под Интерфейсами) к устройствам PIX/ASA/FWSM, маршрутизаторам IOS и Catalyst 6500/7600 устройства:На устройствах PIX/ASA/FWSM эти разрешения касаются аппаратных портов и интерфейсных параметров настройки.На маршрутизаторах IOS эти разрешения касаются основных и усовершенствованных интерфейсных параметров настройки, а также другой связанной с интерфейсом политики, такой как DSL, PVC, PPP и политика номеронабирателя.На Catalyst 6500/7600 устройства, эти разрешения касаются интерфейсов и Параметров VLAN.
9. **Назначьте> Политика> Мостовое соединение**. Позволяет вам назначать политику таблицы ARP (расположенный в Селекторе политики под Платформой> Соединяющий) к устройствам PIX/ASA/FWSM.
10. **Назначьте> Политика> Администрирование устройств**. Позволяет вам назначать

политику администрирования устройств (расположенный в Селекторе политики под Платформой> Admin Устройства) к устройствам PIX/ASA/FWSM, маршрутизаторам IOS и Catalyst 6500/7600 устройства:На устройствах PIX/ASA/FWSM примеры включают полицейских доступа к устройству, политику доступа сервера и политику аварийного переключения.На маршрутизаторах IOS примеры включают доступ к устройству (включая доступ линии) полицейские, политика доступа сервера, AAA, и Защищают Инициализацию Устройства.На сенсорах IPS эти разрешения касаются политики доступа к устройству и политики доступа сервера.На Catalyst 6500/7600 устройства, эти разрешения касаются параметров настройки IDSM и списков Доступа к VLAN.

11. **Назначьте> Политика> Идентичность**. Позволяет вам назначать политики идентификации (расположенный в Селекторе политики под Платформой> Идентичность) к маршрутизаторам Cisco IOS, включая политику Network Admission Control (NAC) и 802.1x.
12. **Назначьте> Политика> Регистрация**. Позволяет вам назначать политику регистрации (расположенный в Селекторе политики под Платформой> Регистрация) к устройствам PIX/ASA/FWSM и маршрутизаторам IOS. Примеры регистрации политики включают настройку регистрации, установку сервера и политику сервера системного журнала.
13. **Назначьте> Политика> Групповая адресация**. Позволяет вам назначать политику групповой адресации (расположенный в Селекторе политики под Платформой> Групповая адресация) к устройствам PIX/ASA/FWSM. Примеры политики групповой адресации включают политика IGMP и многоадресная маршрутизация.
14. **Назначьте> Политика> QoS**. Позволяет вам назначать политики QoS (расположенный в Селекторе политики под Платформой> Качество обслуживания) к маршрутизаторам Cisco IOS.
15. **Назначьте> Политика> Маршрутизация**. Позволяет вам назначать политику маршрутизации (расположенный в Селекторе политики под Платформой> Направляющий) к устройствам PIX/ASA/FWSM и маршрутизаторам IOS. Примеры политики маршрутизации включают OSPF, RIP и политику статичной маршрутизации.
16. **Назначьте>> Security Политики**. Позволяет вам назначать политику безопасности (расположенный в Селекторе политики в соответствии с> Security Платформы) к устройствам PIX/ASA/FWSM. Политика безопасности включает антиспуфинг, фрагмент и настройки времени ожидания.
17. **Назначьте> Политика> Правила Политики обслуживания**. Позволяет вам назначать политику правила политики обслуживания (расположенный в Селекторе политики под Платформой> Правила Политики обслуживания) к PIX 7.x/ASA устройства. Примеры включают очереди с приоритетами и IPS, QoS и правила соединения.
18. **Назначьте> Политика> Предпочтения пользователя**. Позволяет вам назначать политику Развертываний (расположенный в Селекторе политики под Платформой> Предпочтения пользователя) к устройствам PIX/ASA/FWSM. Эта политика содержит опцию для очистки всех преобразований NAT на развертываниях.
19. **Назначьте> Политика> Виртуальное устройство**. Позволяет вам назначать действительную политику датчика на устройства IPS. Используйте эту политику для создания действительных датчиков.
20. **Назначьте> Политика> FlexConfig**. Позволяет вам назначать FlexConfigs, которые являются дополнительными командами CLI и инструкциями, которые могут быть развернуты на устройствах PIX/ASA/FWSM, маршрутизаторах IOS и Catalyst 6500/7600 устройства.

Примечание: Когда вы задаете, назначают разрешения, удостоверьтесь, что вы выбрали соответствующие обзорные разрешения также.

Утвердите разрешения

Менеджер безопасности предоставляет утвердить разрешения как показано:

1. **Утвердите> CLI**. Позволяет вам утверждать изменения команды CLI, содержавшиеся в задании развертываний.
2. **Утвердите> Политика**. Позволяет вам утверждать изменения конфигурации, содержавшиеся в политике, которая была настроена в действии потока операций.

Понимание ролей CiscoWorks

Когда пользователи созданы в CiscoWorks Common Services, им назначают одна или более ролей. Разрешения, привязанные к каждой роли, определяют операции, которые каждый пользователь авторизуется выполнить в Менеджере безопасности.

Следующие темы описывают роли CiscoWorks:

- Роли CiscoWorks Common Services по умолчанию
- Присвоение ролей пользователям в CiscoWorks Common Services

Роли CiscoWorks Common Services по умолчанию

CiscoWorks Common Services содержит следующие роли по умолчанию:

1. **Справочный стол** — пользователи Справочного стола могут просмотреть (но не модифицировать), устройства, политика, объекты и схемы топологии.
2. **Оператор сети** — Кроме того, для просмотра разрешений операторы сети могут просмотреть команды CLI и Менеджера безопасности административные параметры настройки. Операторы сети могут также модифицировать архивную конфигурацию и выполнить команды (такие как эхо-запрос) к устройствам.
3. **Утверждающее лицо** — Кроме того, для просмотра разрешений утверждающие лица могут утвердить или отклонить задания развертываний. Они не могут выполнить развертывания.
4. **Администратор сети** — Администраторы сети имеют полное представление и модифицируют разрешения, за исключением изменения административных параметров настройки. Они могут обнаружить устройства и политику, настроенную на этих устройствах, назначить политику на устройства и выполнить команды к устройствам. Администраторы сети не могут утвердить задания развертываний или действия; однако, они могут развернуть задания, которые были утверждены другими.
5. **Системный администратор** — у Системных администраторов есть полный доступ ко всем разрешениям Менеджера безопасности, включая модификацию, присвоение политики, действие и утверждение задачи, обнаружение, развертывания и команды выдачи к устройствам.

Примечание: Если дополнительные приложения установлены на сервере, дополнительные роли, такие как данные экспорта, могли бы быть отображены в Общем обслуживании. Роль

данных экспорта для сторонних разработчиков и не используется Менеджером безопасности.

Совет: Несмотря на то, что вы не можете изменить определение ролей CiscoWorks, можно определить, какие роли назначены на каждого пользователя. Для получения дополнительной информации посмотрите Роли Присвоения Пользователям в CiscoWorks Common Services.

Присвоение ролей пользователям в CiscoWorks Common Services

CiscoWorks Common Services позволяет вам определить, какие роли назначены на каждого пользователя. Путем изменения определения роли для пользователя вы изменяете типы операций, этот пользователь авторизуется, выполняют в Менеджере безопасности. Например, если вы назначаете роль Справочного стола, пользователь ограничен для просмотра операций и не может модифицировать данные. Однако, если вы назначаете роль Оператора сети, пользователь также в состоянии модифицировать архивную конфигурацию. Можно назначить множественные роли на каждого пользователя.

Примечание: Необходимо перезапустить Менеджера безопасности после внесения изменений в права пользователя.

Процедура:

1. В Общем обслуживании выберите **Server> Security**, затем выберите **Single-Server Trust Management> Local User Setup** от TOC.**Совет:** Для достижения Страницы настройки Локального пользователя из Менеджера безопасности выберите Tools> Security Manager Administration> Server Security, затем нажмите Local User Setup.
2. Установите флажок рядом с существующим пользователем, затем нажмите **Edit**.
3. На странице User Information выберите роли для присвоения на этого пользователя путем нажатия флажков.Для получения дополнительной информации о каждой роли, посмотрите Роли CiscoWorks Common Services По умолчанию.
4. Нажмите **OK** для сохранения изменений.
5. Менеджер безопасности перезапуска.

Понимание ролей Cisco Secure ACS

Cisco Secure ACS предоставляет большую гибкость для управления разрешениями Менеджера безопасности, чем делает CiscoWorks, потому что это поддерживает специализированные роли, которые можно настроить. Каждая роль составлена из ряда разрешений, которые определяют уровень авторизации к задачам Менеджера безопасности. В Cisco Secure ACS вы назначаете роль на каждую группу пользователей (и дополнительно, отдельным пользователям также), который позволяет каждому пользователю в той группе выполнить операции, авторизовавшие разрешениями, определенными для той роли.

Кроме того, можно назначить эти роли на группы устройств Cisco Secure ACS, позволив разрешениям дифференцироваться на других наборах устройств.

Примечание: Группы устройств Cisco Secure ACS независимы от групп устройств Менеджера безопасности.

Следующие темы описывают роли Cisco Secure ACS:

- Роли Cisco Secure ACS по умолчанию
- Настройка ролей Cisco Secure ACS

Роли Cisco Secure ACS по умолчанию

Cisco Secure ACS включает те же роли как CiscoWorks (см. Роли CiscoWorks Понимания), плюс эти дополнительные роли:

1. **Утверждающее лицо безопасности** — утверждающие лица Безопасности могут просмотреть (но не модифицировать), устройства, политика, объекты, карты, команды CLI и административные параметры настройки. Кроме того, утверждающие лица безопасности могут утвердить или отклонить изменения конфигурации, содержавшиеся в действии. Они не могут утвердить или отклонить задание развертываний, и при этом они не могут выполнить развертывания.
2. **Администратор безопасности** — В дополнение к наличию обзорных разрешений, администраторы безопасности могут модифицировать устройства, группы устройств, политику, объекты и схемы топологии. Они могут также назначить политику на устройства и топологии VPN, и выполнить обнаружение для импорта новых устройств в систему.
3. **Администратор сети** — Кроме того, для просмотра разрешений, администраторы сети могут модифицировать архивную конфигурацию, выполнить развертывания и выполнить команды к устройствам.

Примечание: Разрешения, содержавшиеся в роли администратора сети Cisco Secure ACS, отличаются от содержавшихся в роли администратора сети CiscoWorks. Для получения дополнительной информации посмотрите Роли CiscoWorks Понимания.

В отличие от CiscoWorks, Cisco Secure ACS позволяет вам настроить разрешения, привязанные к каждой роли Менеджера безопасности. Для получения дополнительной информации об изменении ролей по умолчанию, посмотрите Роли Cisco Secure ACS Настройки.

Примечание: Cisco Secure ACS 3.3 или позже должен быть установлен для авторизации Менеджера безопасности.

Настройка ролей Cisco Secure ACS

Cisco Secure ACS позволяет вам модифицировать разрешения, привязанные к каждой роли Менеджера безопасности. Можно также настроить Cisco Secure ACS путем создания специализированных ролей пользователя с разрешениями, которые предназначены к определенным задачам Менеджера безопасности.

Примечание: Необходимо перезапустить Менеджера безопасности после внесения изменений в права пользователя.

Процедура:

1. В Cisco Secure ACS нажмите **Shared Profile Components** на панели навигации.
2. Нажмите **Cisco Security Manager** на странице Shared Components. Роли, которые

настроены для Менеджера безопасности, отображены.
3. Выполните одно из следующих действий:Для создания роли **нажмите Add**. Перейдите к шагу 4.Для изменения существующей роли нажмите роль. Переходите к шагу 5.
4. Введите имя для роли и, дополнительно, описание.
5. Выберите и снимите флажки в дереве разрешений для определения разрешений для этой ролиУстановка флажка для ответвления дерева выбирает все разрешения в том ответвлении. Например, выбор **Assign** выбирает все назначать разрешения.Для полного списка разрешений Менеджера безопасности см. Разрешения Менеджера безопасности.**Примечание:** Когда вы выбираете, модифицируют, утверждают, назначают, импортируют, управляют или развертывают разрешения, необходимо также выбрать соответствующие обзорные разрешения; иначе, Менеджер безопасности не будет функционировать должным образом.
6. **Нажмите кнопку Submit, чтобы сохранить изменения.**
7. Менеджер безопасности перезапуска.

Ассоциации по умолчанию между разрешениями и ролями в менеджере безопасности

Эта таблица показывает, как разрешения Менеджера безопасности привязаны к ролям CiscoWorks Common Services и ролям по умолчанию в Cisco Secure ACS.

Разрешения	Роли							
	Системный администратор	Admin безопасности (ACS)	Утверждающее лицо безопасности (ACS)	Сеть Admin (CW)	Сеть Admin (ACS)	Утверждающее лицо	Оператор сети	Техническая поддержка
Обзорные разрешения								
Обзорное устройство	Да	Да	Да	Да	Да	Да	Да	Да
Обзорная политика	Да	Да	Да	Да	Да	Да	Да	Да
Объекты View	Да	Да	Да	Да	Да	Да	Да	Да
Обзорная топология	Да	Да	Да	Да	Да	Да	Да	Да
Обзорный CLI	Да	Да	Да	Да	Да	Да	Да	Нет

Обзорный Admin	Да	Да	Да	Да	Да	Да	Да	Нет
Обзорный архив конфигураций	Да	Да	Да	Да	Да	Да	Да	Да
Обзорные менеджеры устройств	Да	Да	Да	Да	Да	Да	Да	Нет
Модифицируйте разрешения								
Модифицируйте устройство	Да	Да	Нет	Да	Нет	Нет	Нет	Нет
Модифицируйте иерархию	Да	Да	Нет	Да	Нет	Нет	Нет	Нет
Модифицируйте политику	Да	Да	Нет	Да	Нет	Нет	Нет	Нет
Модифицируйте образ	Да	Да	Нет	Да	Нет	Нет	Нет	Нет
Модифицируйте объекты	Да	Да	Нет	Да	Нет	Нет	Нет	Нет
Модифицируйте топологию	Да	Да	Нет	Да	Нет	Нет	Нет	Нет
Модифицируйте Admin	Да	Нет	Нет	Нет	Нет	Нет	Нет	Нет
Модифицируйте архив конфигураций	Да	Да	Нет	Да	Да	Нет	Да	Нет
Дополнительные разрешения								
Назначьте политику	Да	Да	Нет	Да	Нет	Нет	Нет	Нет
Утвердите политику	Да	Нет	Да	Нет	Нет	Нет	Нет	Нет
Утвердите CLI	Да	Нет	Нет	Нет	Нет	Да	Нет	Нет
Обнаружьте (Импорт)	Да	Да	Нет	Да	Нет	Нет	Нет	Нет
Развернуться	Да	Нет	Нет	Да	Да	Нет	Нет	Нет

Контроль	Да	Нет	Нет	Да	Да	Нет	Да	Нет
Подвергнуться	Да	Да	Нет	Да	Нет	Нет	Нет	Нет

Дополнительные сведения

- Страница технической поддержки Cisco Security Manager
- Cisco Systems – техническая поддержка и документация