Управление доступом на основе ролей и с помощью SDM Cisco IOS: Разделение разрешений на настройку между операционными группами

Содержание

Введение

Функциональность маршрутизации и безопасности традиционно поддерживается в отдельных устройствах, который предлагает ясное подразделение ответственности управления между сетевой инфраструктурой и сервисами безопасности. Конвергенция безопасности и возможностей маршрутизации в Cisco ISR не предлагает, это очищается, разделение мультиустройства. Некоторым организациям нужна сегрегация возможности конфигурации ограничить клиентов или группы управления службами вдоль функциональных границ. Представления CLI, функция программного обеспечения Cisco IOS, стремятся обратиться к этой потребности с Основанным на роли доступом CLI. Этот документ описывает конфигурацию, определенную поддержкой SDM Cisco IOS Основанное на роли Управление доступом, и предлагает общие сведения в возможности Представлений CLI от Интерфейса командной строки Cisco IOS.

Предварительные условия

Требования

Для этого документа отсутствуют особые требования.

Используемые компоненты

Настоящий документ не имеет жесткой привязки к каким-либо конкретным версиям программного обеспечения и оборудования.

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

Более подробную информацию о применяемых в документе обозначениях см. в описании условных обозначений, используемых в технической документации Cisco.

Общие сведения

Много организаций делегируют ответственность за обслуживание маршрутизации и инфраструктурного подключения группе функционирований сети, и ответственность за обслуживание межсетевого экрана, VPN и функциональности предотвращения вторжений группе операций по обеспечению безопасности. Представления CLI могут ограничить конфигурацию функциональности безопасности и функции мониторинга secops группе, и с другой стороны ограничить сетевое подключение, маршрутизацию и другие инфраструктурные задачи группе неттопов.

Некоторые поставщики услуг хотят предложить ограниченную конфигурацию или контролирующую способность клиентам, но не позволить клиентам настраивать или просматривать другие настройки устройства. Еще раз Представления CLI предлагают гранулированный контроль над возможностью CLI ограничить пользователей или группы пользователей для выполнения только авторизовавших команд.

Программное обеспечение Cisco IOS предложило возможность ограничить команды CLI с TACACS + сервер для авторизации для permit or deny возможности выполнить команды CLI на основе членства группы пользователей или имени пользователя. Представления CLI предлагают подобную возможность, но правило управления политиками применено локальным устройством после того, как указанное представление пользователя получено от AAA-сервера. Когда Авторизация для выполнения команд AAA используется, каждая команда должна индивидуально авторизоваться AAA-сервером, который вызывает частый диалог между устройством и AAA-сервером. Представления CLI позволяют правило управления политиками CLI для каждого устройства, тогда как Авторизация для выполнения команд AAA применяет ту же политику авторизации для выполнения команд ко всем

устройствам, к которым обращается пользователь.

Настройка

В этом разделе содержатся сведения о настройке функций, описанных в этом документе.

Примечание: Используйте инструмент Command Lookup (только для зарегистрированных пользователей) для того, чтобы получить более подробную информацию о командах, использованных в этом разделе.

Ассоциированные пользователи с целью

Пользователи могут быть привязаны к локальному Представлению CLI атрибутом return от AAA или в конфигурации локальной проверки подлинности. Для локальной конфигурации имя пользователя настроено с дополнительной **опцией view**, которая совпадает с настроенным названием **parser view**. Эти пользователи в качестве примера настроены для Представлений SDM по умолчанию:

```
username fw-user privilege [privilege-level] view SDM_Firewall
username monitor-user privilege [privilege-level] view SDM_Monitor
username vpn-user privilege [privilege-level] view SDM_EasyVPN_Remote
username sdm-root privilege [privilege-level] view root
```

Пользователи, которые назначены на высказанное мнение, могут временно переключиться к другому представлению, если у них есть пароль для представления, что они хотят войти. Выполните эту команду exec для изменения представлений:

```
enable view view-name
```

Конфигурация Parser View

Представления CLI могут быть настроены от CLI маршрутизатора, или через SDM. SDM Оказывает статическую поддержку для четырех представлений, как обсуждено в Разделе поддержки Представлений CLI SDM. Для настройки Представления CLI от Интерфейса командной строки пользователь должен быть определен как **корневой** обзорный пользователь, или они должны принадлежать представлению с доступом к конфигурации **parser view**. Пользователи, которые не привязаны с целью и кто пытается настроить представления, получают это сообщение:

```
router(config#parser view test-view
No view Active! Switch to View Context
```

Представления CLI позволяют включение или исключение завершенных иерархий команд и для руководителя и для режимов конфигурации, или только делит на части этого. Три опции доступны, чтобы позволить или запретить иерархию команд или иерархию команд в высказанном мнении:

```
router(config-view)#commands configure ?
  exclude            Exclude the command from the view
  include            Add command to the view
  include-exclusive  Include in this view but exclude from others
```

Представления CLI усекают running-config, таким образом, не отображена конфигурация Parser View. Однако конфигурация Parser View видима в startup-config.

См. Основанный на роли доступ CLI для получения дополнительной информации об

определении представления.

Проверка ассоциации Parser View

Пользователи, которые назначены на Parser View, могут определить, какое представление они назначены на то, когда в них входят к маршрутизатору. Если **команда show parser view** позволена для пользовательских представлений, они могут выполнить **команду show parser view** для определения их представления:

```
router#sh parser view
Current view is 'SDM_Firewall'
```

Поддержка представлений CLI SDM

SDM предлагает три стандартных экрана, два для конфигурации и мониторинга Межсетевого экрана и компонентов VPN и одного ограниченного представления только для мониторинга. Дополнительное **корневое** представление по умолчанию доступно в SDM также.

SDM не предоставляет способность модифицировать команды, включенные в или исключенный из каждого стандартного экрана, и не предлагает возможности определить дополнительные представления. Если дополнительные представления определены от CLI, SDM не открывает дополнительный вид в своей **Пользовательской** панели конфигурации **Учетных записей/Представлений**.

Эти представления и соответствующие разрешения команды предустановлены для SDM:

Представление SDM_Firewall

```
parser view SDM_Firewall
 secret 5 $1$w/cD$T1ryjKM8aGCnIaKSm.Cx9/
 commands interface include all ip inspect
 commands interface include all ip verify
 commands interface include all ip access-group
 commands interface include ip
 commands interface include description
 commands interface include all no ip inspect
 commands interface include all no ip verify
 commands interface include all no ip access-group
 commands interface include no ip
 commands interface include no description
 commands interface include no
 commands configure include end
 commands configure include all access-list
 commands configure include all ip access-list
 commands configure include all interface
 commands configure include all zone-pair
 commands configure include all zone
 commands configure include all policy-map
 commands configure include all class-map
 commands configure include all parameter-map
 commands configure include all appfw
 commands configure include all ip urlfilter
 commands configure include all ip inspect
 commands configure include all ip port-map
 commands configure include ip cef
 commands configure include ip
```

```
 commands configure include all crypto
 commands configure include no end
 commands configure include all no access-list
 commands configure include all no ip access-list
 commands configure include all no interface
 commands configure include all no zone-pair
 commands configure include all no zone
 commands configure include all no policy-map
 commands configure include all no class-map
 commands configure include all no parameter-map
 commands configure include all no appfw
 commands configure include all no ip urlfilter
 commands configure include all no ip inspect
 commands configure include all no ip port-map
 commands configure include no ip cef
 commands configure include no ip
 commands configure include all no crypto
 commands configure include no
 commands exec include all vlan
 commands exec include dir all-filesystems
 commands exec include dir
 commands exec include crypto ipsec client ezvpn connect
 commands exec include crypto ipsec client ezvpn xauth
 commands exec include crypto ipsec client ezvpn
 commands exec include crypto ipsec client
 commands exec include crypto ipsec
 commands exec include crypto
 commands exec include write memory
 commands exec include write
 commands exec include all ping ip
 commands exec include ping
 commands exec include configure terminal
 commands exec include configure
 commands exec include all show
 commands exec include all debug appfw
 commands exec include all debug ip inspect
 commands exec include debug ip
 commands exec include debug
 commands exec include all clear
```

Представление SDM_EasyVPN_Remote

```
parser view SDM_EasyVPN_Remote
 secret 5 $1$UnC3$ienYd0L7Q/9xfCNkBQ4Uu.
 commands interface include all crypto
 commands interface include all no crypto
 commands interface include no
 commands configure include end
 commands configure include all access-list
 commands configure include ip radius source-interface
 commands configure include ip radius
 commands configure include all ip nat
 commands configure include ip dns server
 commands configure include ip dns
 commands configure include all interface
 commands configure include all dot1x
 commands configure include all identity policy
 commands configure include identity profile
 commands configure include identity
 commands configure include all ip domain lookup
 commands configure include ip domain
 commands configure include ip
 commands configure include all crypto
 commands configure include all aaa
```

```
 commands configure include default end
 commands configure include all default access-list
 commands configure include default ip radius source-interface
 commands configure include default ip radius
 commands configure include all default ip nat
 commands configure include default ip dns server
 commands configure include default ip dns
 commands configure include all default interface
 commands configure include all default dot1x
 commands configure include all default identity policy
 commands configure include default identity profile
 commands configure include default identity
 commands configure include all default ip domain lookup
 commands configure include default ip domain
 commands configure include default ip
 commands configure include all default crypto
 commands configure include all default aaa
 commands configure include default
 commands configure include no end
 commands configure include all no access-list
 commands configure include no ip radius source-interface
 commands configure include no ip radius
 commands configure include all no ip nat
 commands configure include no ip dns server
 commands configure include no ip dns
 commands configure include all no interface
 commands configure include all no dot1x
 commands configure include all no identity policy
 commands configure include no identity profile
 commands configure include no identity
 commands configure include all no ip domain lookup
 commands configure include no ip domain
 commands configure include no ip
 commands configure include all no crypto
 commands configure include all no aaa
 commands configure include no
 commands exec include dir all-filesystems
 commands exec include dir
 commands exec include crypto ipsec client ezvpn connect
 commands exec include crypto ipsec client ezvpn xauth
 commands exec include crypto ipsec client ezvpn
 commands exec include crypto ipsec client
 commands exec include crypto ipsec
 commands exec include crypto
 commands exec include write memory
 commands exec include write
 commands exec include all ping ip
 commands exec include ping
 commands exec include configure terminal
 commands exec include configure
 commands exec include all show
 commands exec include no
 commands exec include all debug appfw
 commands exec include all debug ip inspect
 commands exec include debug ip
 commands exec include debug
 commands exec include all clear
```

Представление SDM_Monitor

```
parser view SDM_Monitor
 secret 5 $1$RDYW$OABbxSgtx1kOozLlkBeJ9/
 commands configure include end
 commands configure include all interface
```

```
commands configure include no end
commands configure include all no interface
commands exec include dir all-filesystems
commands exec include dir
commands exec include all crypto ipsec client ezvpn
commands exec include crypto ipsec client
commands exec include crypto ipsec
commands exec include crypto
commands exec include all ping ip
commands exec include ping
commands exec include configure terminal
commands exec include configure
commands exec include all show
commands exec include all debug appfw
commands exec include all debug ip inspect
commands exec include debug ip
commands exec include debug
commands exec include all clear
```

Проверка

В настоящее время для этой конфигурации нет процедуры проверки.

Устранение неполадок

Для этой конфигурации в настоящее время нет сведений об устранении проблем.

Дополнительные сведения

- Основанный на роли доступ CLI
- Cisco Systems – техническая поддержка и документация