Визитка

СЕРГЕЙ ЦЫМБАЛЮК, *ИТ-специалист в ИНГ Банк Украина, Cisco Certified Network Professional*

Authentication Authorization Accounting

Интеграция Cisco с Microsoft Active Directory

Привязываем аутентификацию администраторов сетевых устройств Cisco к единой базе MS Active Directory

Многие системные администраторы рано или поздно сталкиваются с проблемой аутентификации на сетевых устройствах. Если руководствоваться best-practices, то учетные записи должны быть персонифицированными, пароли – отвечать критериям устойчивости, время жизни паролей – ограничено.

Также не будем забывать о разграничении уровней доступа в соответствии с выполняемыми задачами и поддержке актуальности базы пользователей, связанной с изменениями в штате сотрудников. При соблюдении этих требований ведение базы пользователей разрозненно, на каждом устройстве, становится трудоемкой и нетривиальной задачей, а на практике часто просто игнорируется, администраторы ограничиваются заданием паролей на физическую и виртуальную консоль и заданием пароля суперпользователя (enable). Логичным решением этой проблемы является ведение единой базы пользователей с контролем выдвигаемых к учетным записям требований.

Если у нас есть Active Directory, почему бы не использовать его? Все не так просто – устройства Cisco не предоставляют механизма для аутентификации средствами LDAP, коим является MS Active Directory, напрямую. Для решения этой задачи Cisco в своих решениях предоставляет механизм Authentication Authorization Accounting (AAA). Дабы не растягивать статью, за деталями отсылаю к первоисточнику [1], также неплохая статья, которая описывает основные возможности [2].

Вкратце: клиент AAA отправляет учетные данные к серверу аутентификации и, основываясь на его ответе (либо отсутствии ответа), принимает решение об отказе или предоставлении запрашиваемого доступа.

В качестве сервера аутентификации AAA позволяет использовать сервер RADIUS либо TACAS+. На первый взгляд по описанию возможностей предпочтительнее TACAS+, но основной его недостаток в том, что это закрытое решение от Cisco и его реализация существует только для *nix-систем [3]. Протокол же RADIUS является открытым промышленным стандартом, для которого существует множество реализаций, в том числе и встроенная в Windows Server 2000/2003 служба IAS (Internet Authentication Service). В Windows Server 2008 вместо службы IAS поставляется служба Network Policy Server [4].

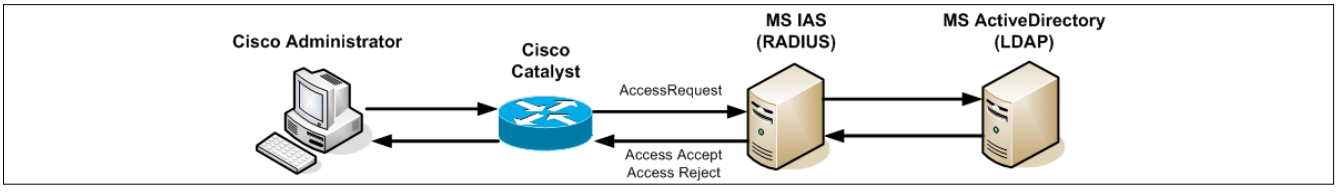
Топология

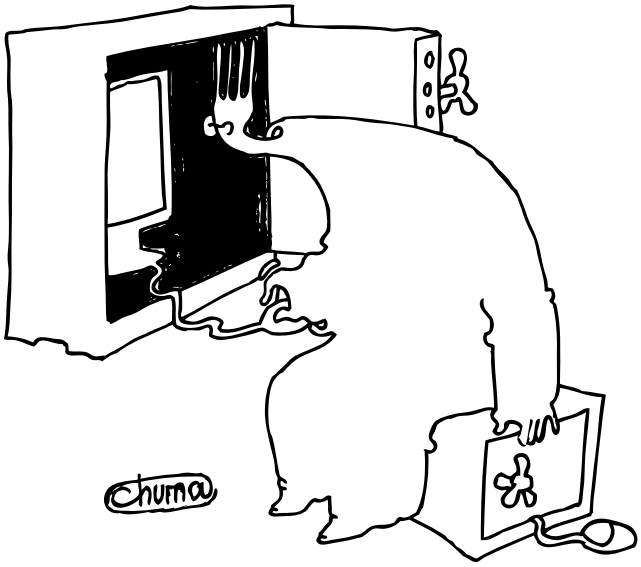
Система аутентификации сетевых устройств Cisco средствами LDAP домена Active Directory в простейшем случае имеет топологию, изображенную на рис. 1.

Администратор со своего рабочего места подключается к виртуальному терминалу сетевого устройства. Согласно настроенным политикам AAA устройство запрашивает логин и пароль, после чего передает логин и хеш пароля RADIUS-серверу. RADIUS-сервер средствами Active Directory аутентифицирует пользователя и проверяет, является ли он членом административной группы.

Если пользователь успешно прошел аутентификацию, сетевое устройство Cisco получает от RADIUS-сервера подтверждение об успехе аутентификации и авторизации и разрешает пользователю подключение, в противном слу-

Рисунок 1. Топология системы





Централизуя учетные записи, мы экономим время и снижаем риск их компрометации

чае сообщает о неуспешной аутентификации и закрывает соединение.

Аутентификация пользователей на сетевом оборудовании будет происходить средствами Active Directory посредством RADIUS, авторизация доступа – на основе принадлежности к одной из двух групп, соответственно разрешающих непривилегированный (User exec mode) и привилегированный (Privilege exec mode) доступ к устройству. В дальнейшем можно разделить доступ по ролям, сконфигурировав на устройствах профили с разрешением запускать необходимые команды и связав каждый профиль с соответствующей группой AD.

Настройка MS Active Directory

Предполагаем, что политики безопасности для длины, сложности паролей, времени их жизни и пр. уже внедрены. Итак, для начала создадим две группы безопасности (Security group) gsgrCiscoUserEXEC и gsgrCiscoPrivEXEC:

Теперь создадим учетные записи администраторов PetrovI и IvanovP, сделав их членами групп gsgrCiscoUserEXEC и gsgrCiscoPrivEXEC соответственно. Таким образом, видим, что PetrovI будет непривилегированным пользователем, а IvanovP – привилегированным.

На этом с Active Directory все.

Настройка MS Internet Authentication Service

Если на сервере еще не установлена служба IAS, то ее необходимо установить. Для этого нужно в панели управления выбрать: Add/Remove Programs → Add/Remove Windows Components → Network Services, нажать кнопку Details («Дополнительно»), выбрать пункт Internet Information Service (IIS) и нажать Details, выбрать Internet Authentication Service.

Открываем оснастку Internet Authentication Service и создаем новую политику удаленного доступа (Remote Access Policies → RClick → New Remote Access Policy) с названием CiscoAAA_AD. В открывшемся окне Select Attribute выбираем Authentication Type и добавляем CHAP, критерий – принадлежность пользователей к ранее созданной группе gsgrCiscoUserEXEC. Выбираем пункт Windows-Groups, добавляем gsgrCiscoUserEXEC.

И самое главное, выбираем атрибут Service-Type = Login для пользовательского и Administrative – для привилегированного доступа (см. рис. 2).

В завершение мастера выбираем пункт Grant remote access permission.

Теперь необходимо создать учетные записи для устройств, к которым будет выдаваться доступ. Для этого в оснастке IAS выбираем пункт RADIUS Clients → RClick → New RADIUS Client (см. рис. 3).

Рисунок 2. Выбираем атрибут Service Type

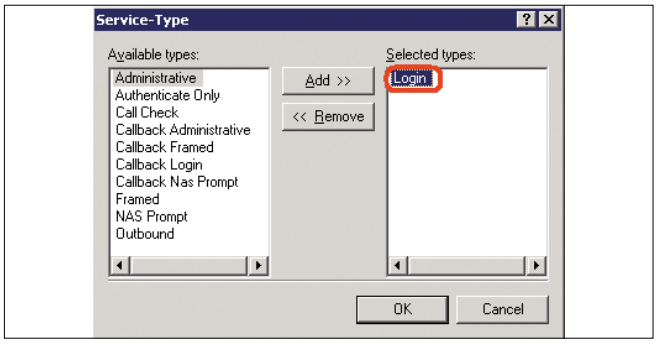
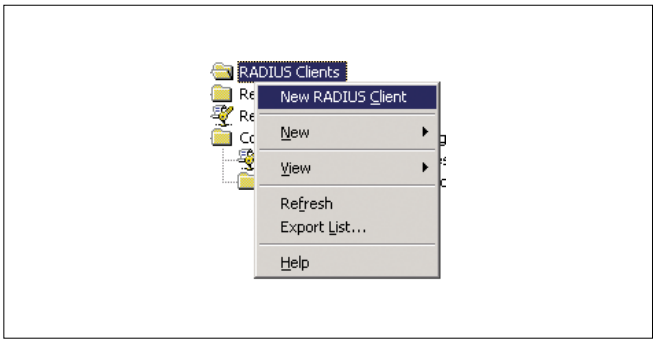


Рисунок 3. Создаем учетную запись устройства



В появившемся окне вводим дружественное имя, например Switch1, и IP-адрес устройства, жмем Next, выбираем Client-Vendor = Cisco, вводим ключ для аутентификации RADIUS-сервера и клиента (см. рис. 4).

Настройка со стороны IAS завершена, переходим к настройке сетевых устройств.

Настройка сетевого устройства Cisco на примере коммутатора Catalyst 2960

Включаем шифрование паролей:

```
service password-encryption
```

Задаем пароль для привилегированного режима:

```
enable secret *******
```

Внимание! Протокол RADIUS работает так, что, если не получен ответ от сервера, клиент предполагает аутентификацию неуспешной! Обязательно создаем локального пользователя на случай, если RADIUS-сервер недоступен по какой-либо причине, печатаем на листике, заворачиваем в конверт и прячем в сейф.

```
username recover password *********
```

Включаем AAA:

```
aaa new-model
```

Баннер о том, что это закрытая система и делать здесь нечего. Необязательно:

```
aaa authentication banner ^ Access only for persons
explicitly authorized. All rights reserved.
^
```

Сообщение на случай неуспешной аутентификации. Полезно при отладке:

```
aaa authentication fail-message ^ Authentication failed
^
```

Создаем профиль аутентификации. Не забываем как резервный указать локальный способ аутентификации:

```
aaa authentication login login-RADIUS group radius local
```

Создаем профиль авторизации:

```
aaa authorization exec auth-RADIUS-exec group radius local
```

По умолчанию клиент AAA трижды пытается авторизоваться через RADIUS. Дабы не блокировать учетные записи в Active Directory, ставим одну попытку:

```
radius-server retransmit 1
```

Указываем наш RADUIS-сервер:

```
radius-server host 10.0.0.2
```

Задаем ключ для шифрования:

```
radius-server key SupErkEy
```

Включаем созданные профили для виртуальных консолей:

```
line vty 0 15
 exec-timeout 15 0
 login authentication login-RADIUS
 authorization exec auth-RADIUS-exec
 timeout login response 180
 no password
```

Настройка завершена, переходим к тестированию. Проверяем работу (см. рис. 5).

Отладка

Не всегда все идет хорошо. На этот случай следует воспользоваться командами отладки Cisco IOS:

```
# debug radius events
# debug aaa authentication
# debug aaa authorization
# debug aaa protocols
# debug radius [authentication | elog | verbose]
```

Также не забываем смотреть в Event log AD и IAS.

***

Таким образом, потратив некоторое время на централизацию учетных записей, мы сэкономим много времени в будущем и уменьшим риск компрометации учетных записей. В случае ошибки администратора будет легко выявить виновника по его учетным данным, а также установить права доступа к устройствам, ограничив администраторов в правах согласно их обязанностям. EOF

1. Authentication, Authorization, and Accounting Overview – http://www.cisco.com/en/US/products/ps6638/products_data_sheet09186a00804fe332.html.
2. Настройка AAA на CISCO – краткий обзор – http://faq-cisco.ru/index.php?option=com_content&task=view&id=26&Itemid=30.
3. Remote Authentication Dial In User Service (RADIUS) – http://en.wikipedia.org/wiki/RADIUS.
4. Understanding the new Windows Server 2008 Network Policy Server – http://www.windowsnetworking.com/articles_tutorials/Understanding-new-Windows-Server-2008-Network-Policy-Server.html.

Рисунок 4. Данные для аутентификации RADUIS-сессии

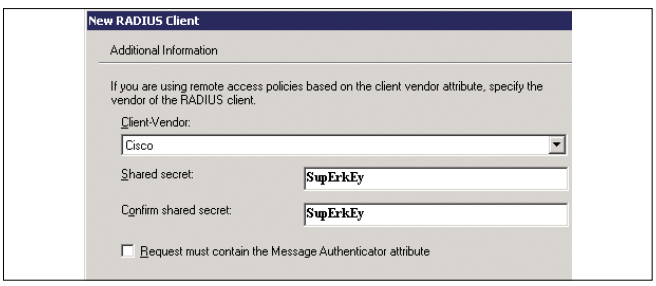


Рисунок 5. Проверка работы