Настройка Windows Server 2008 R2 в качестве RADIUS сервера для Cisco ASA

Недавно я работал надо проектом внедрения VPN доступа через Cisco ASA для нашей компании. В данном случае существует 3 способа аутентификации клиентов – это локальная база ASA, LDAP и RADIUS.

Из описанных методов я остановился на использовании RADIUS для аутентификации VPN запросов. В данной серии статей я опишу необходимые шаги для настройки VPN аутентификации между Cisco ASA 5510 и Windows Server 2008 R2 с помощью ASDM 6.0:

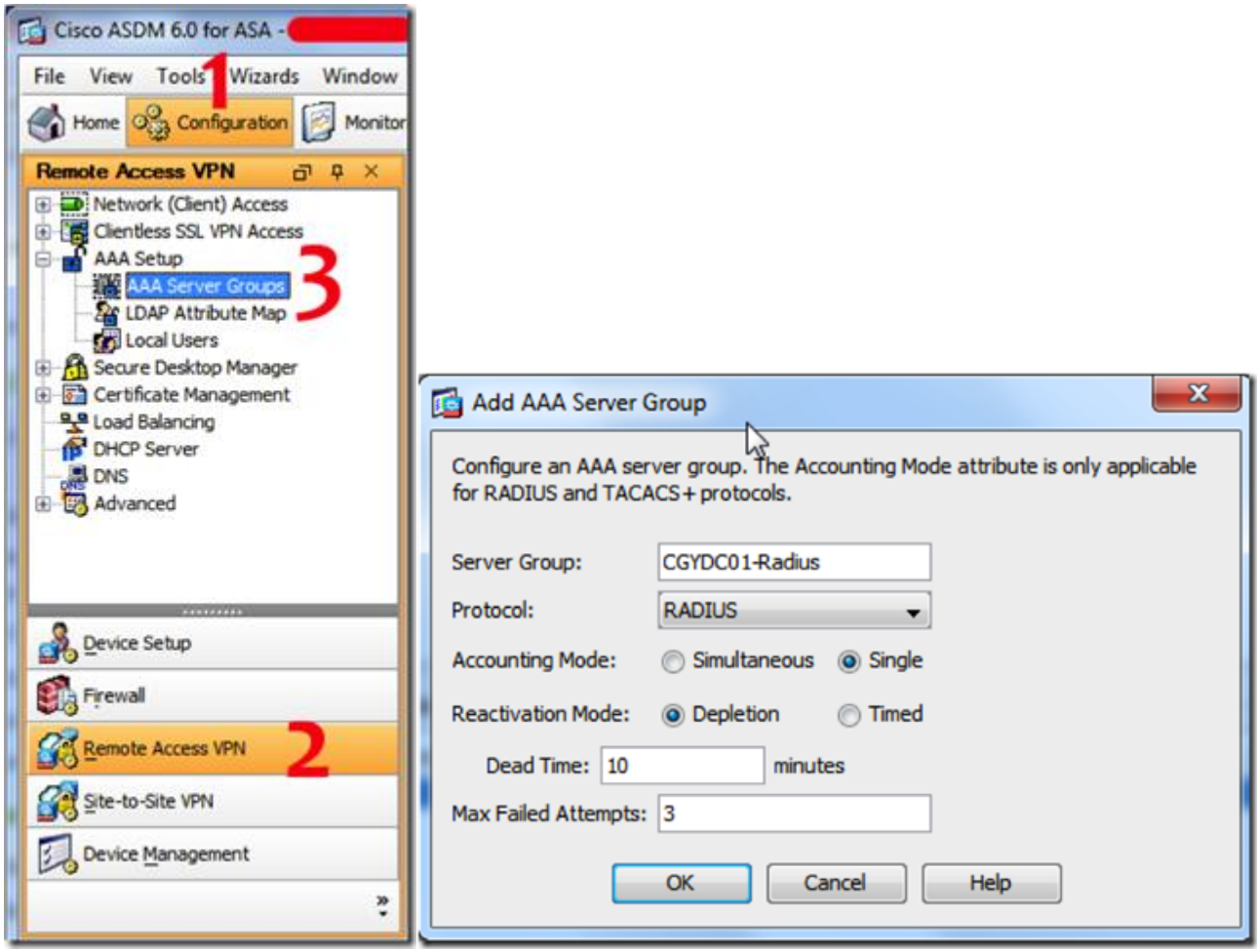
Используемые компоненты:

- Cisco ASA 5510
- Адрес внутреннего интерфейса ASA – 192.168.1.1
- Windows Server 2008 R2 в качестве контроллера домена
- IP адрес сервера 192.168.1.11
- Аккаунты администратора на ASA и контроллере домена

Давайте начнем с настройки Cisco ASA

Шаг 1: Создадим новую группу серверов AAA

1. Залогиньтесь в ASDM и нажмите на “Configuration” –> “Remote Access VPN” –> “AAA Setup” –> “AAA Server Groups
2. С правой стороны нажмите кнопку “Add”
3. Введите имя группы серверов и выберите протокол “Radius”. Все остальное оставьте без изменений и нажмите “OK”.

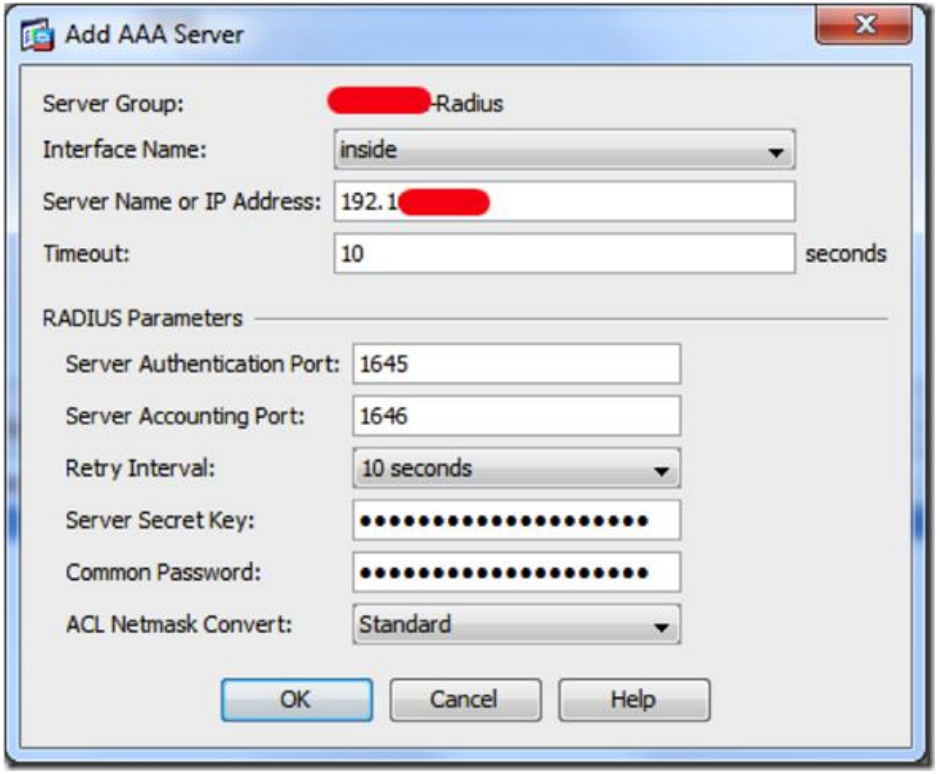


Шаг 2: Добавим сервер RADIUS

Теперь нам необходимо добавить RADIUS сервер в группу, созданную в шаге 1

1. Нажмите на созданную группу. В нашем примере это “CGYDC01-Radius”.

2. Нажмите на кнопку “Add” выбрав предварительно узел “Servers in the Selected Group”.
3. В качестве интерфейса выберите внутренний интерфейс ASA
4. Введите DNS имя или IP адрес сервера RADIUS. В нашем случае это “192.168.1.11″
5. Важно: Теперь нам необходимо указать “Server Secret Key”. Введите его и запишите себе. Он нам пригодится в будущем при настройке RADIUS сервера.
6. Повторите ключ в поле “Common Password”.



7. Нажмите “OK”.
8. Не забудьте нажать кнопку “Apply”

Во второй части данной серии статей первое что мы сделаем это добавим роль RADIUS сервера на наш Server 2008 R2. Перед этим убедитесь что у вас есть права доменного администратора.

Шаг 3: Добавляем роль Network Policy and Access Services

1. Залогиньтесь на Server 2008 R2 и откройте “Server Manager”.
2. Нажмите ссылку “Add Role” .
3. На странице “Before you Begin” нажмите кнопку “Next”.
4. Отмечаем чекбокс напротив “Network Policy and Access Services”.
5. В окне “Network Policy and Access Services” нажмите “Next”.
6. На странице “Select Role” отметьте “Network Policy Server”.
7. Нажмите “Install”
8. Перезагрузите сервер.

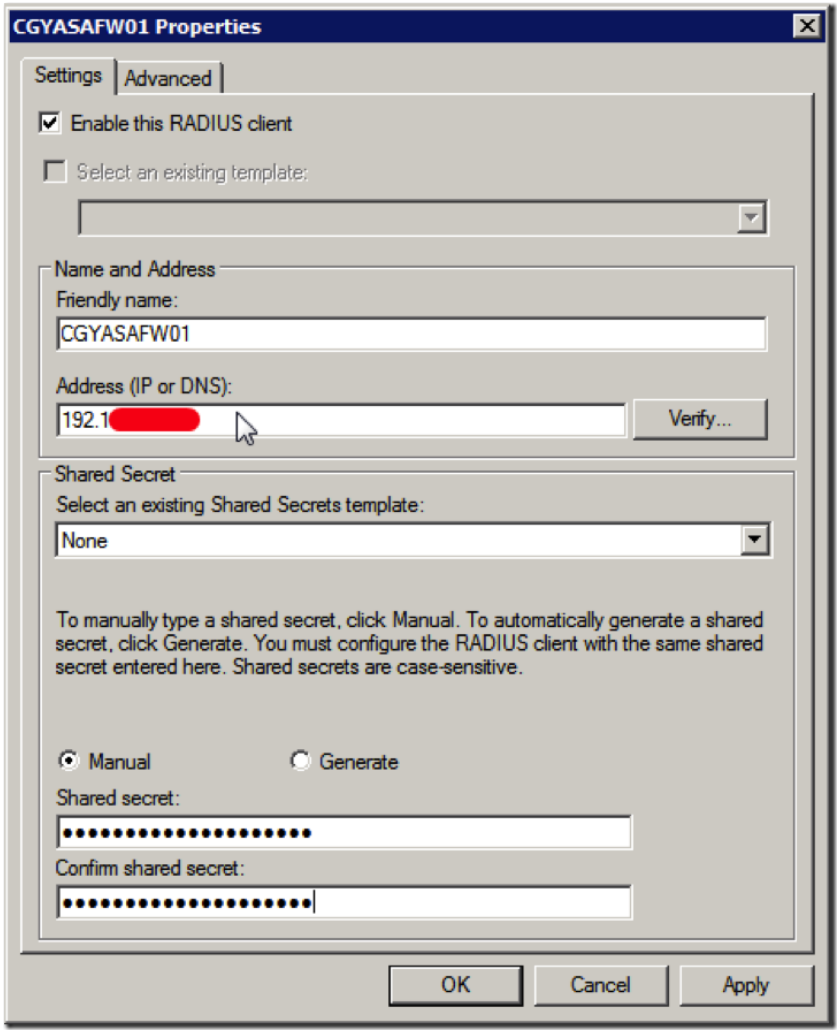
Шаг 4: Регистрация сервера RADIUS в Active Directory (AD)

1. Откройте “Server Manager”.
2. Разверните “Roles” –> “Network Policy and Access Services”.
3. Нажмите на “NPS”.
4. Теперь в правой панели нажмите на “Register Server in Active Directory”.
5. Оставьте все по умолчанию.

Шаг 5: Создадим запись клиента RADIUS для Cisco ASA

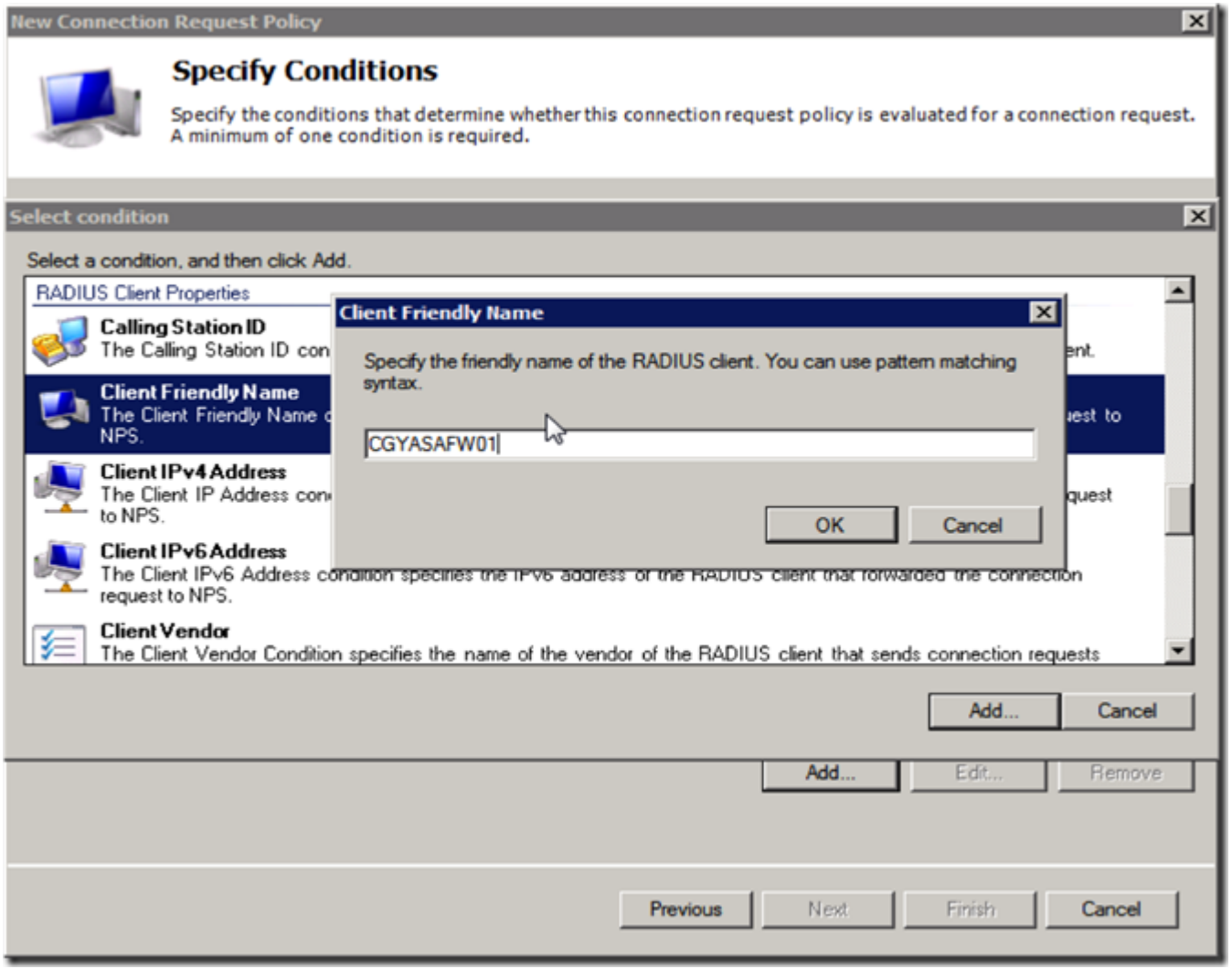
1. Разверните узел дальше до “RADIUS client and Servers”.
2. Нажмите правой кнопкой по “RADIUS Client” и выберите “New”.

3. Введите понятное имя для Cisco ASA и не забудьте документировать его. Нам понадобиться данное имя в дальнейшем.
4. Установите переключатель в “Manual” и введите ранее созданный секретный ключ.
5. Нажмите “OK”.



Шаг 6: Создание политики запросов на подключение

1. Разверните узел “Policies”.
2. Нажмите правой кнопкой на “Connection Request Policies” и выберите “New”.
3. Введите имя политики и нажмите “Next”.
4. В окне “Specify Conditions” нажмите “Add”.
5. Найдите и выделите опцию “ClientFriendlyName”



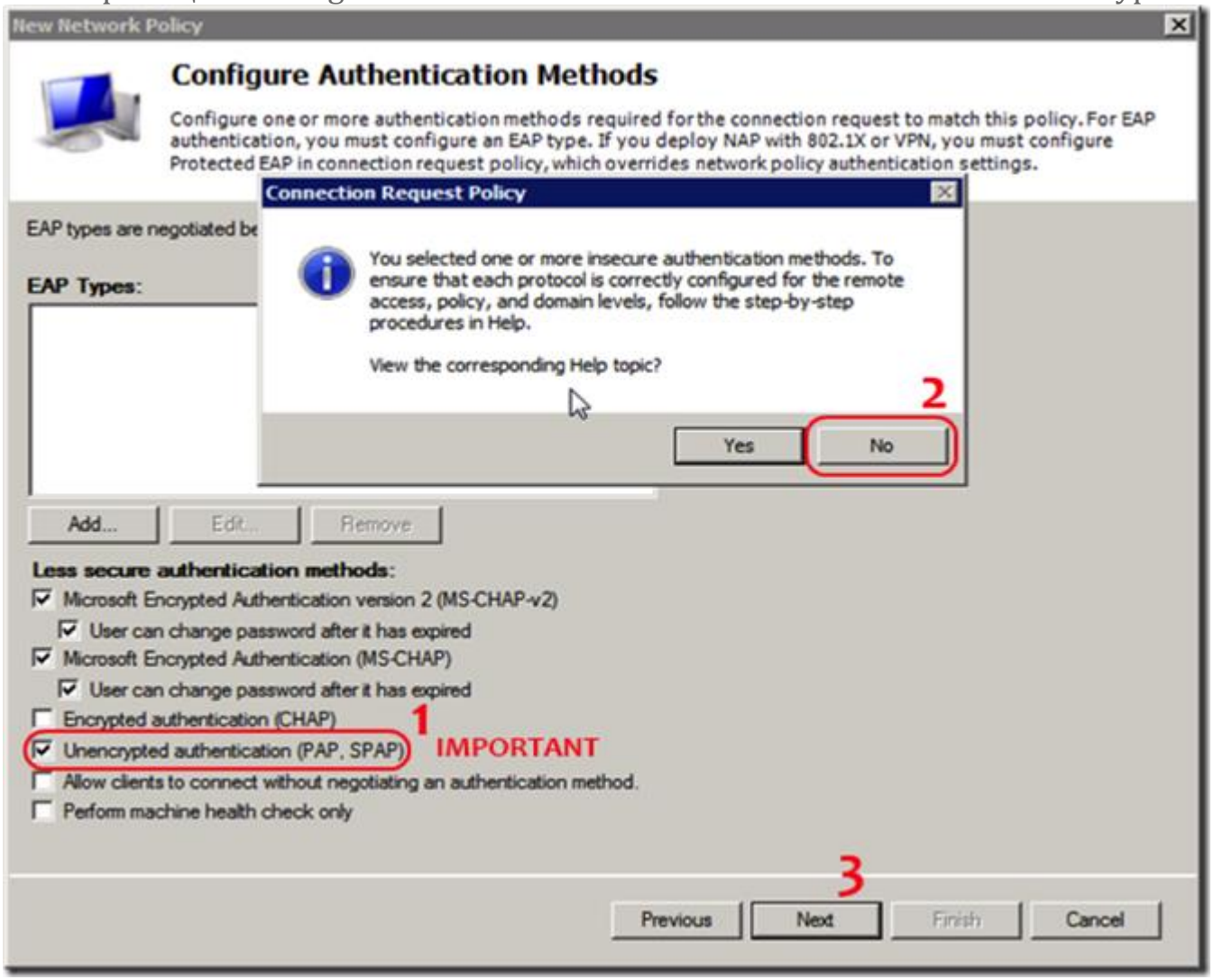
6. Нажмите “Add”
7. Укажите имя, созданное нами в шаге 5.3 во второй части данной серии статей.
8. Нажмите “OK”.

9. Нажмите “Next” и примите все данные в оставшихся двух окнах без изменений.
10. В окне “Configure Settings” в секции “Specify a RealmName” выберите “Attribute”.
11. В качестве атрибута из выпадающего меню выберите “UserName”.
12. Проверьте настройки и нажмите кнопку “Finish”.

Шаг 7: Создание сетевой политики

1. Нажмите правой кнопкой на узел “Network Policy” и выберите “New”.
2. Введите имя политики и нажмите “Next”.
3. В окне “Specify Conditions” нажмите “Add”.
4. Выберите “User Groups” и нажмите “Add”.
5. Добавьте пользователей или группы, которым будет разрешен VPN вход.
6. Нажмите “OK” и затем нажмите “Next”.
7. Убедитесь что установлена опция “Access Granted” и нажмите “Next”.

8. На странице “Configure Authentication Methods” отметьте “Unencrypted Authentication (PAP, SPAP).



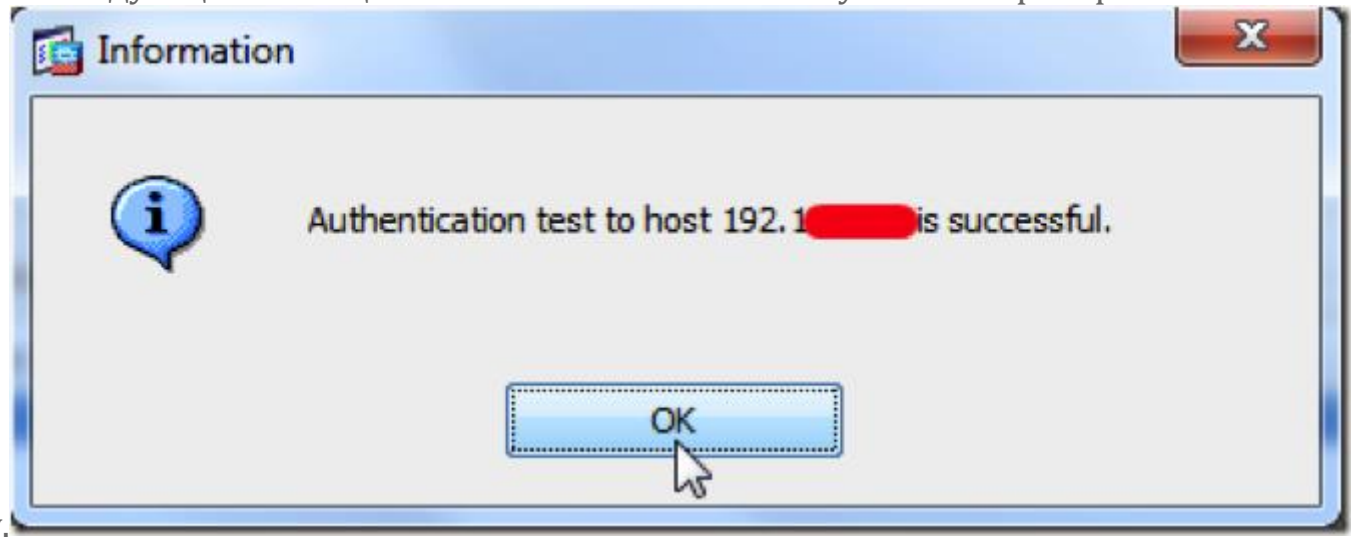
9. Примите все данные в оставшихся двух окнах без изменений.
10. Проверьте настройки и нажмите кнопку “Finish”.

Шаг 8: Тестируем аутентификацию Cisco ASA через Windows Server 2008 R2 RADIUS

1. Запустите ASDM и нажмите “Configuration” –> “Remote Access VPN” –> “AAA Setup” –> “AAA Server Groups”.
2. Выберите группу серверов созданную в шаге STEP 1.3.
3. Выберите сервер из списка “Servers in Selected Server Group”.
4. Нажмите кнопку “Test” в правой колонке.
5. Отметьте переключатель “Authentication”.

6. Введите имя пользователя и пароль

7. Вы должны увидеть следующее сообщение. Если что то не получилось проверьте свои настройки и повторите попытку.



В настоящее время вы можете использовать RADIUS аутентификацию для ваших VPN пользователей.