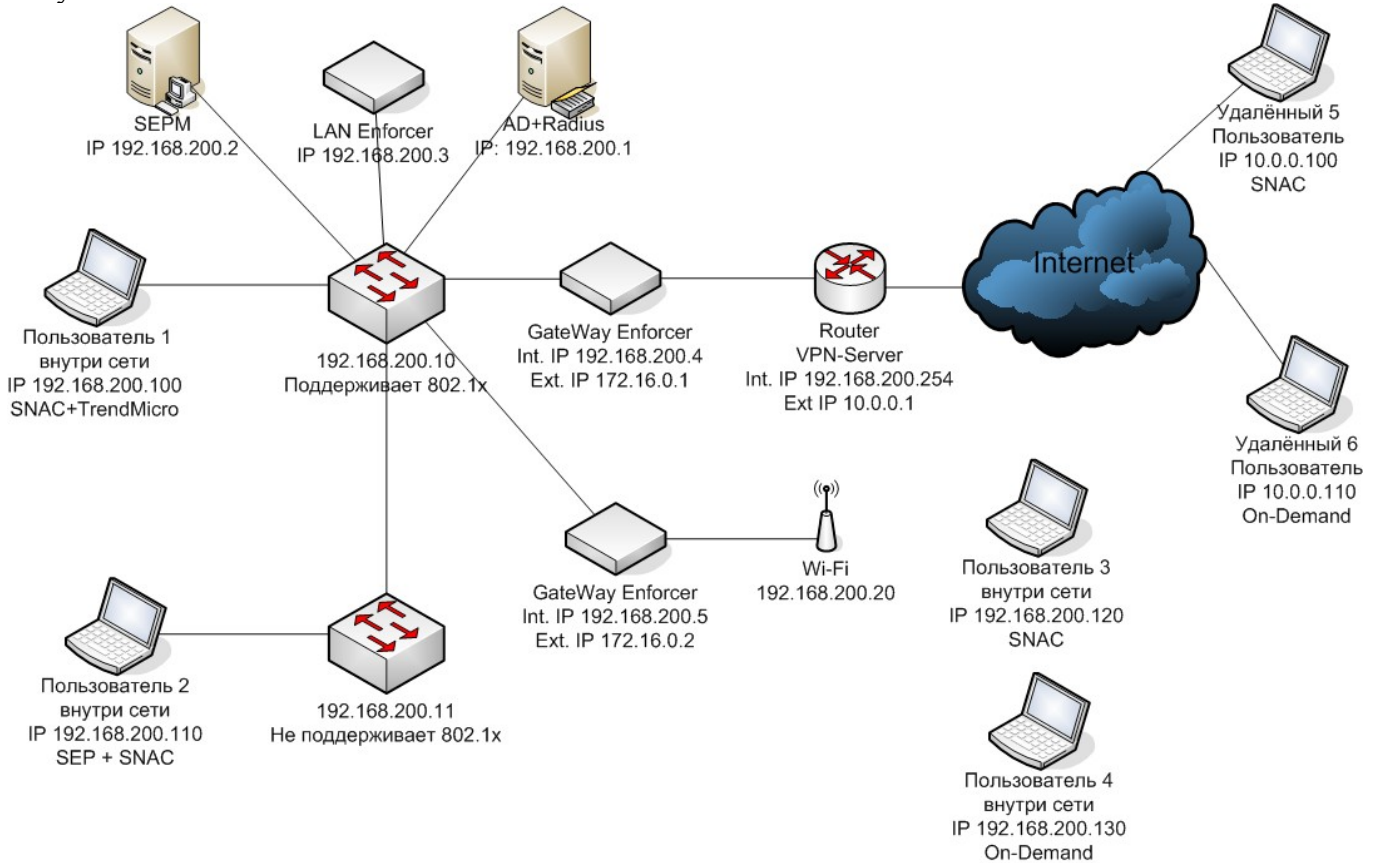


# Symantec Network Access Control.

## Общее описание.

Для демонстрации SNAC соберём стенд, схема которого представлена на рисунке:  
Рисунок 1.



В качестве сетевого оборудования будем использовать оборудование компании Cisco Systems. На стенде будут задействованы 2 коммутатора и 1 маршрутизатор. В качестве коммутаторов будем использовать Cisco Catalyst 2950, который поддерживает протокол авторизации 802.1x, и Cisco Catalyst 3500, который 802.1x не поддерживает. В качестве маршрутизатора будем использовать Cisco 2611XM.

Для наглядности на Cisco Catalyst 2950 будем блокировать или разрешать порт, в зависимости от состояния компьютера.

Так как Cisco Catalyst 3500 не поддерживает протокол 802.1x, то блокирование/разрешение порта и динамическое назначение VLAN невозможно.

Cisco 2611XM в нашей схеме используется как шлюз между локальной сетью и сетью Интернет. Также этот маршрутизатор выступает в качестве VPN-сервера.

На схеме присутствует контроллер домена. Так как мы рассматриваем типовое решение, а большинство компаний у себя так или иначе использует Active Directory, на рассматриваемом стенде в качестве централизованной БД пользователей используется именно эта служба каталогов, хотя возможно и использование других продуктов. Также служба каталогов AD необходима для управления доступом в сеть при аутентификации пользователей - например, если пользователь не зарегистрирован в домене, то доступа к сети он не получит.

У нас присутствует 6 рабочих станций/ноутбуков, на каждом из которых будет обыгран отдельный сценарий доступа в сеть:

- Компьютер пользователя 1. На компьютере установлен агент SNAC и антивирус Trend Micro Office Scan, хотя можно использовать любой другой антивирус. Данный пользователь подключается к коммутатору Catalyst 2950, и за доступ компьютера в сеть будет отвечать

порт коммутатора. В терминологии Symantec данное решение называется LAN -Enforcement.

- Компьютер пользователя 2. На компьютере установлен агент SNAC + SEP. В данном варианте может использоваться любой неуправляемый коммутатор. За доступ компьютера в сеть будет отвечать межсетевой экран, который входит в пакет SEP - то есть доступ компьютера в сеть будет регулироваться правилами МСЭ, который установлен на самом компьютере. В терминологии Symantec данное решение называется Self-Enforcement.
- Компьютер пользователя 3. На компьютере установлен агент SNAC. Доступ в сеть осуществляется посредством WiFi. Если есть «умная» точка доступа, которая поддерживает протокол 802.1x, то технология доступа будет такая же как и в случае с «умным» коммутатором. Однако, в нашем распоряжении есть обычная WiFi точка D-Link AP 2100, по этому мы реализуем схему доступа через Gateway Enforcer (про реализацию и настройку поговорим чуть позднее). В данном варианте подключения к сети за доступ в сеть отвечает как раз Gateway Enforcer, через который проходит весь трафик клиента, и, в зависимости от состояния клиента, либо пропускается, либо нет. Однако, в случае с Gateway Enforcer, доступ к серверу SEPM (Symantec Endpoint Protection Manager) есть всегда для любых компьютеров. В терминологии Symantec данное решение называется Gateway Enforcement.
- Компьютер пользователя 4. Данный компьютер так же подключается к сети через WiFi. Однако, на нём не установлено никакого ПО от Symantec. Однако, если да доступ к сети отвечает Gateway Enforcer, то существует возможность скачать и запустить (не устанавливая) временного агента SNAC, после чего компьютер может быть проверен на соответствие политикам и принято решение о предоставлении доступа в сеть. За доступ в сеть - так же, как и в предыдущем случае - отвечает Gateway Enforcer. В терминологии Symantec данное решение называется On-Demand Checking.
- Компьютер пользователя 5. Данный вариант подключения аналогичен компьютеру 3, только подключение к сети происходит не через WiFi, а посредством VPN. Между компьютером и маршрутизатором Cisco 2611XM устанавливается VPN канал, после чего компьютер попадает в локальную сеть. Весь трафик клиента проходит через Gateway Enforcer, который и принимает решение о разрешении или блокировке трафика.
- Компьютер пользователя 6. Данный вариант аналогичен компьютеру 4, только подключение происходит посредством VPN. На компьютере отсутствует агент SNAC, однако данный агент может быть установлен с Gateway Enforcer.

Выше уже упоминался Symantec Endpoint Protection Manager (SEPM) – это единая консоль управления политиками антивируса, фаервола, IPS и SNAC. Так же SEPM является сервером обновлений.

### ***Установка и настройка Symantec Endpoint Protection Manager.***

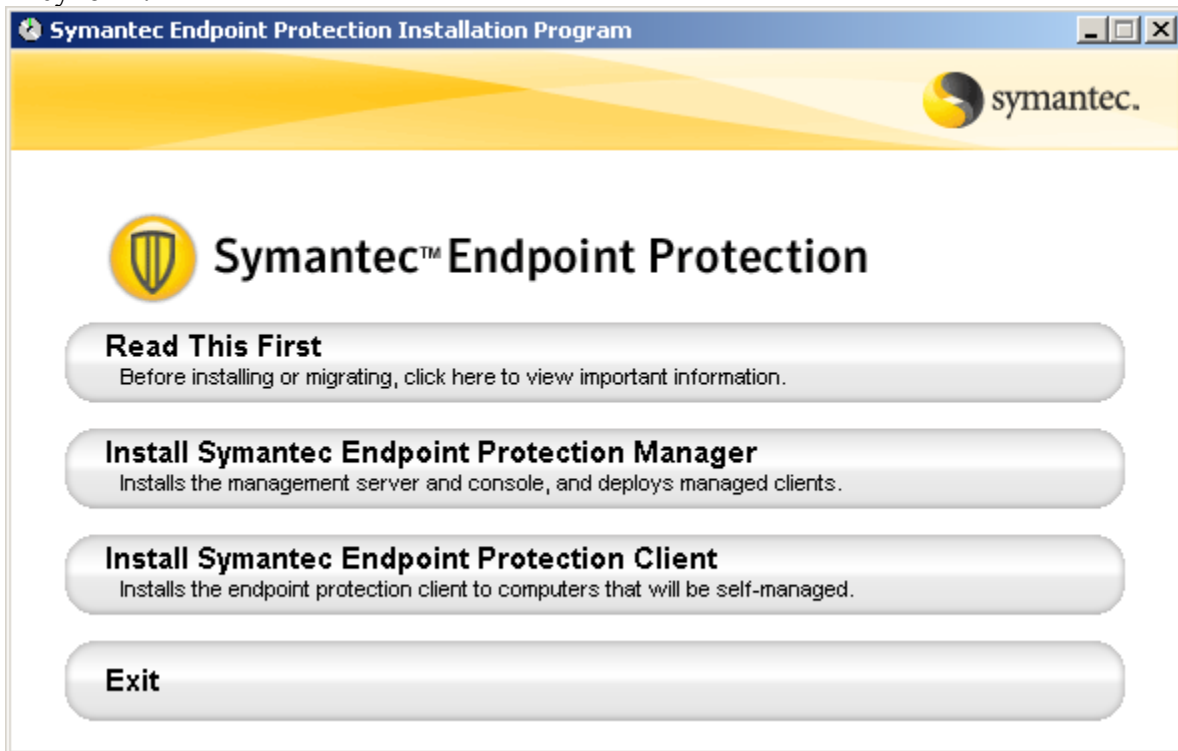
Установку и настройку службы каталогов Active Directory рассматривать не будем, так как эта стандартная процедура не имеет прямого отношения к стенду. На стенде развёрнут домен Symantec.demo. Единственным контроллером домена является сервер с именем DC1 под управлением операционной системы Windows Server 2003 Ent R2. Никакие дополнительные службы не используются.

Второй сервер так же работает под управлением Windows Server 2003 Ent R2 и является членом домена. Имя сервера SEPM.symantec.demo. На данном сервере развёрнуты службы IIS с настройками по умолчанию, установлен .NET Framework 3.0 и установлен SQL Server 2005 SP2.

Теперь приступим к установке Symantec Endpoint Protection Manager.

Запускаем установку, и из предложенного меню выбираем пункт «Install Symantec Endpoint Protection Manager».

Рисунок 2.

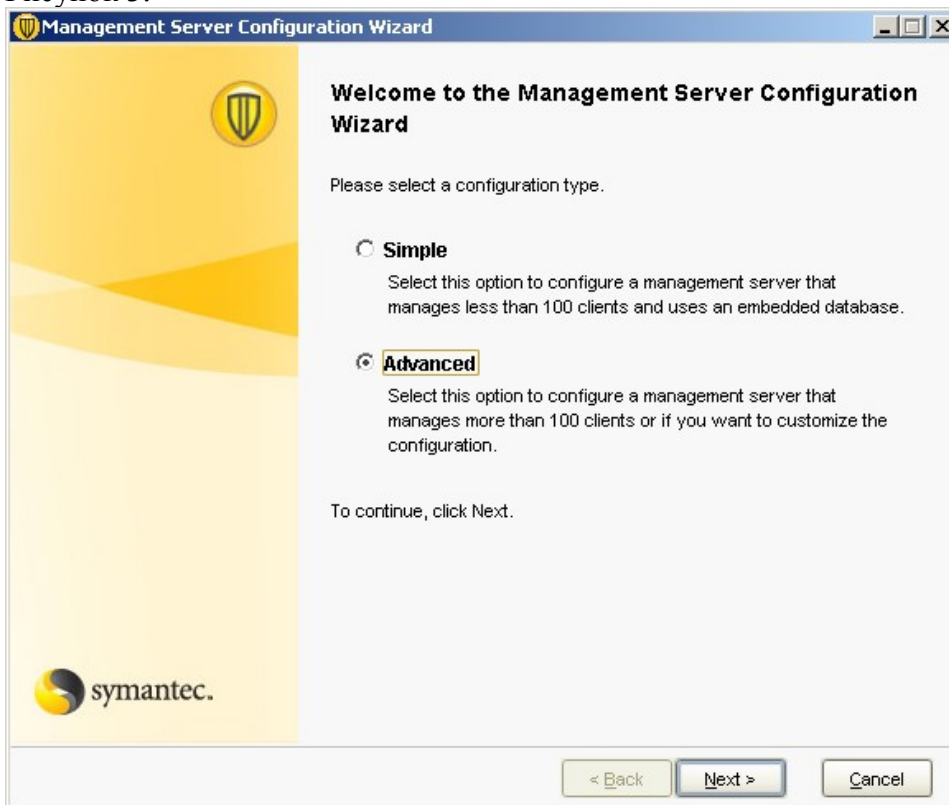


Установку производим с настройками по умолчанию, не изменяя никаких параметров. Дожидаемся окончания установки и нажимаем кнопку «Finish».

После завершения установки запустится программа конфигурирования Symantec Endpoint Protection Manager.

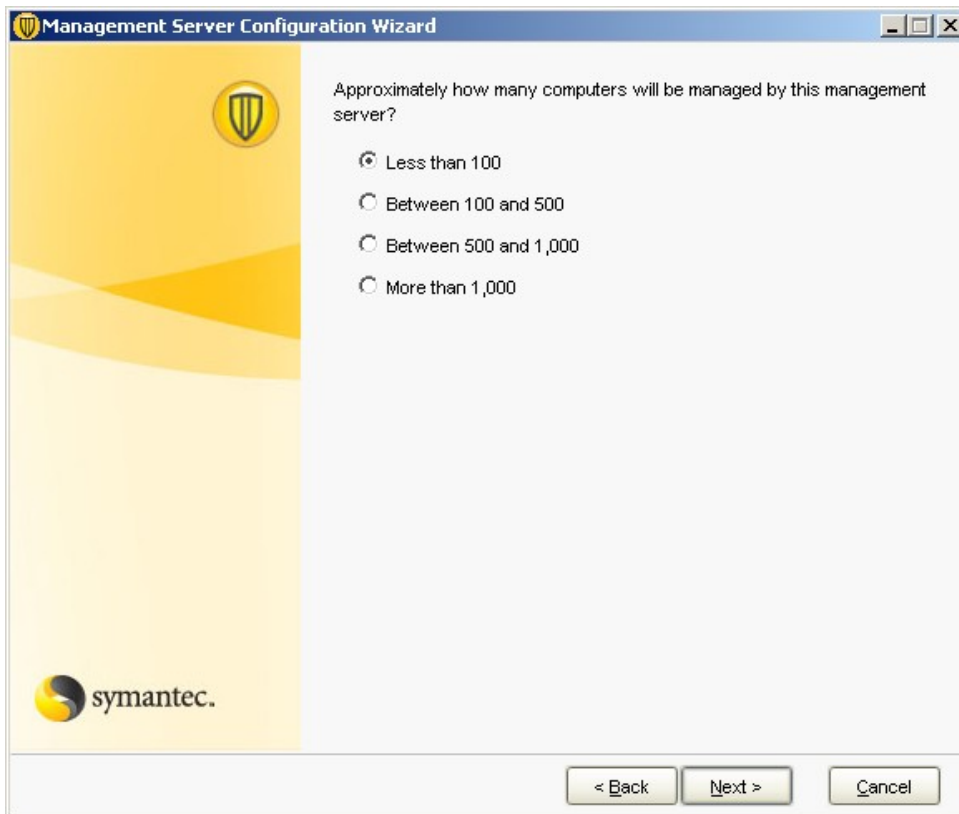
В окне Wellcome to the Management Server Configuration Wizard выбираем пункт Advanced для расширенной настройки:

Рисунок 3.



Указываем количество пользователей, которые будут управляться данным сервером Symantec Endpoint Protection Manager.

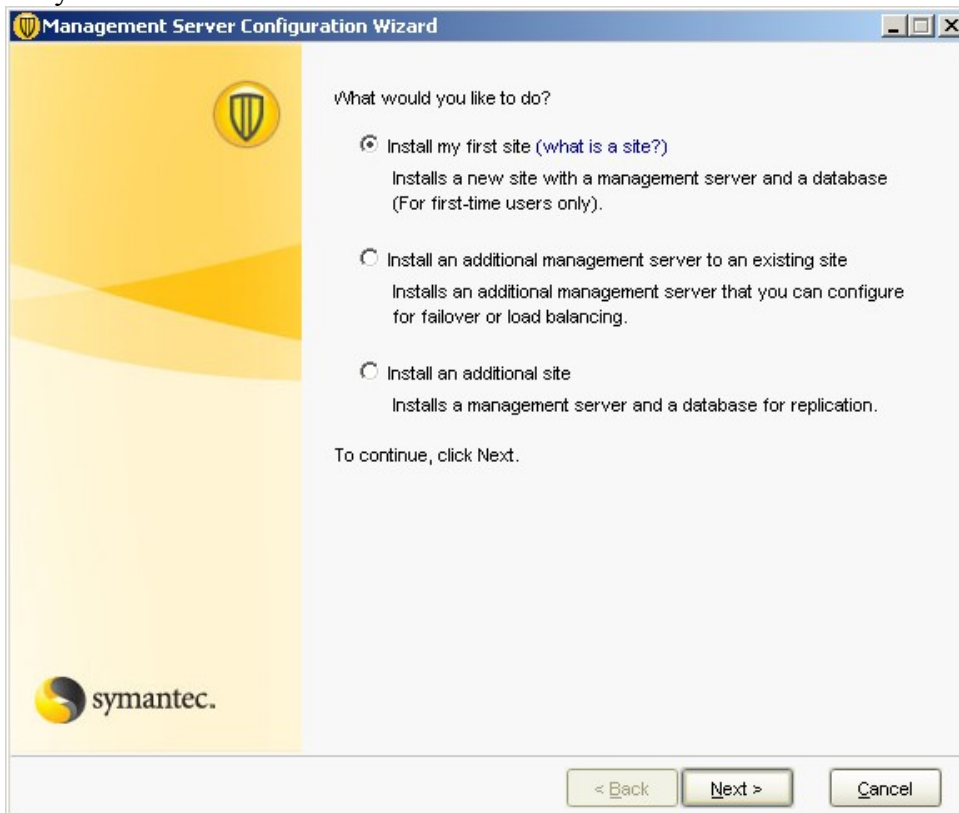
Рисунок 4.



Выбираем режим установки:

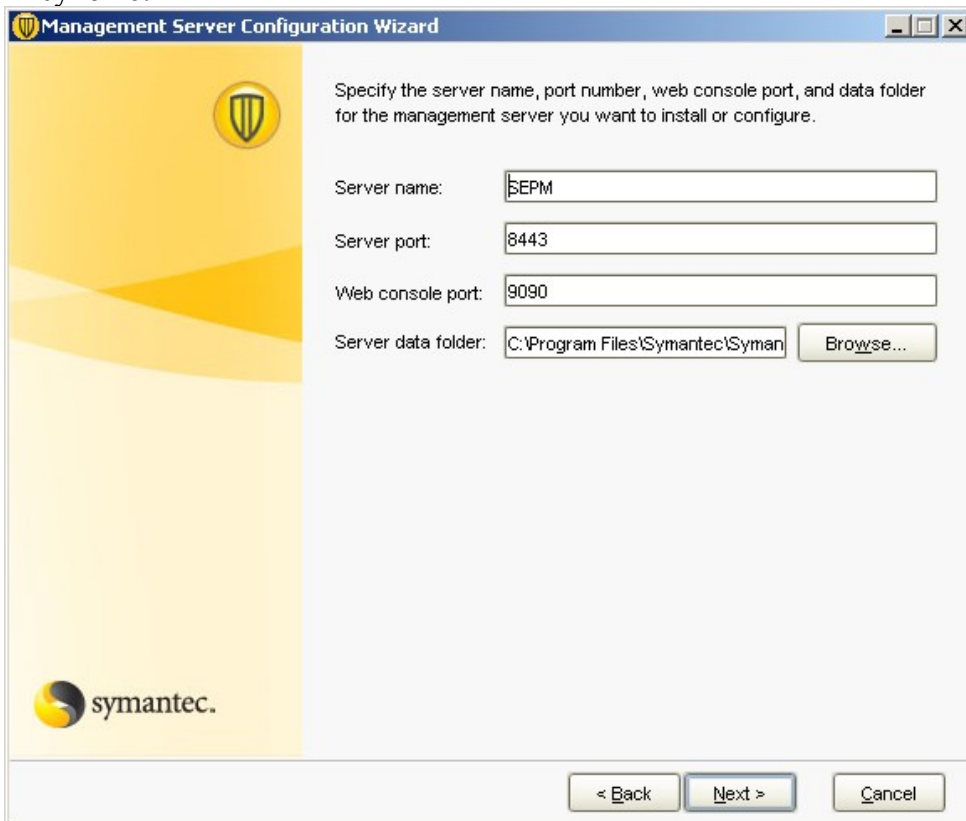
- Установка нового сайта
- Установка нового сервера в существующий сайт
- Установка дополнительного сайта

Так как у нас это первый сервер, то мы выбираем пункт: «Install my first site»  
Рисунок 5.



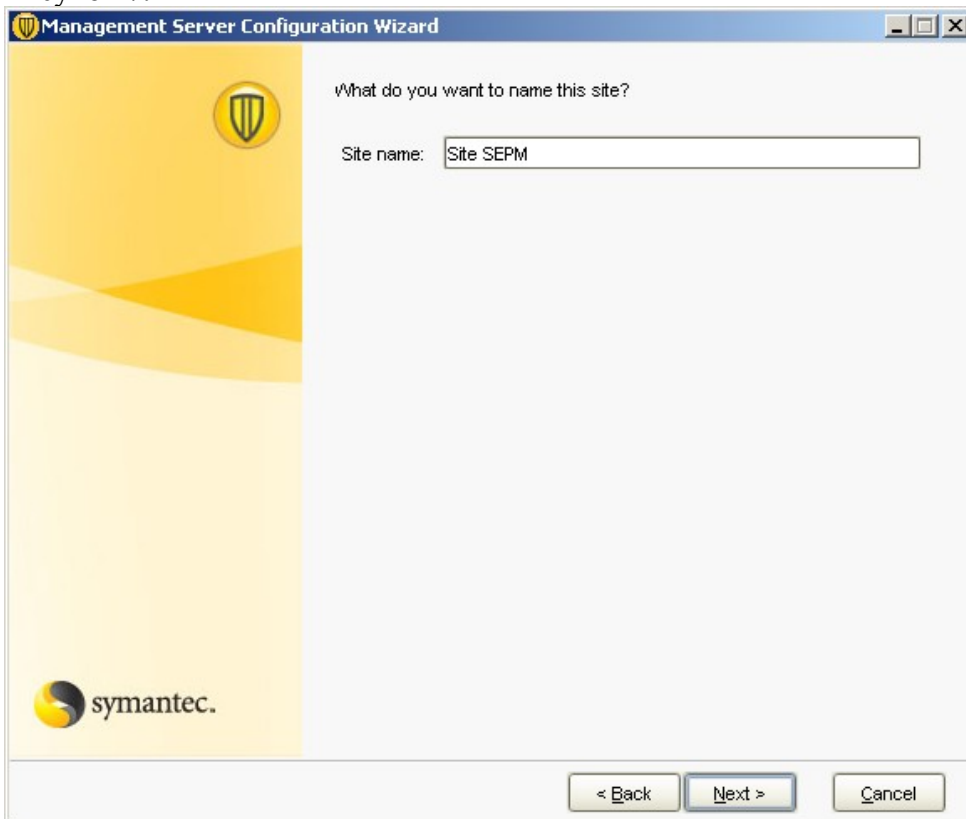
Далее нас просят указать некоторые настройки, такие как - имя сервера, порты, папку данных сервера Symantec End Point Protection Manager, который мы настраиваем. Все настройки оставляем по умолчанию.

Рисунок 6.



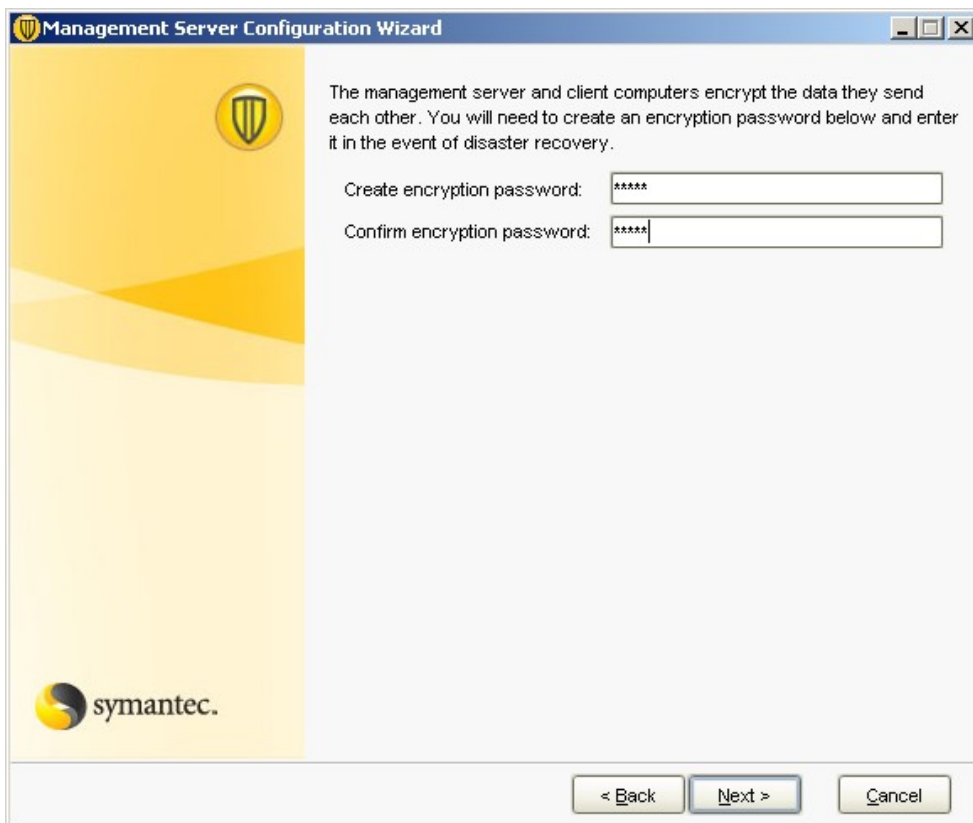
Вводим имя для нашего создаваемого сайта: «Symantec.demo»

Рисунок 7.



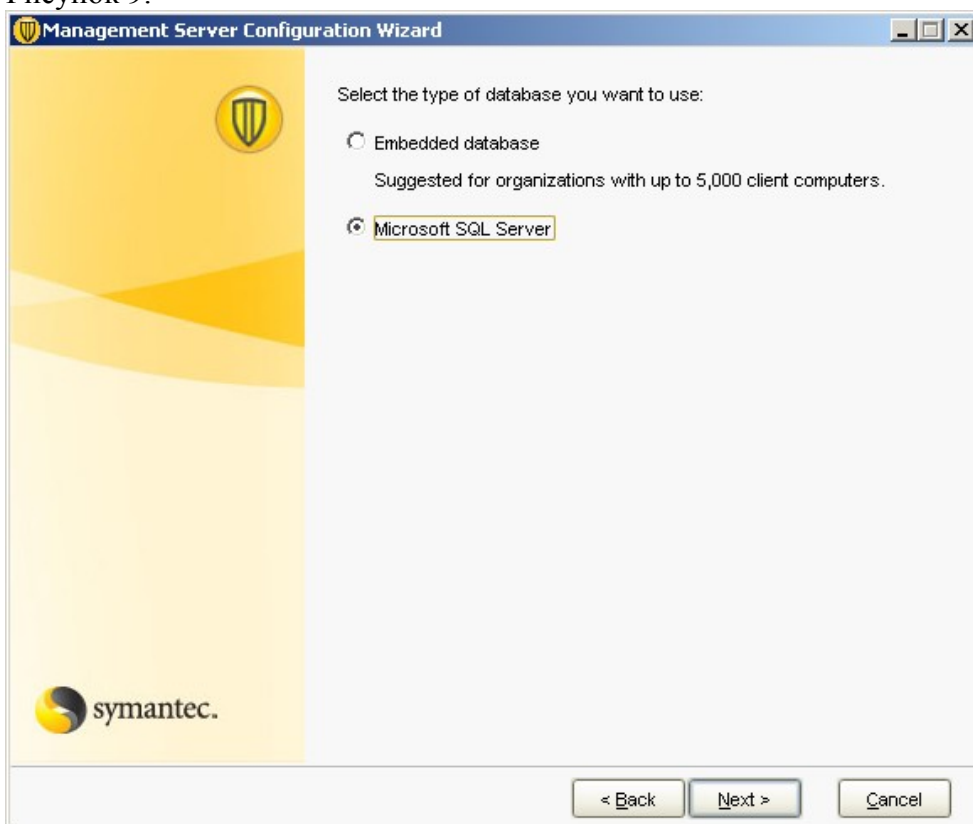
Затем нас просят указать пароль шифрования, используемый для связи между клиентами и сервером. Мы вводим пароль и запоминаем его. Далее этот пароль пригодиться нам, когда мы будем подключать Enforcer'ы к серверу Symantec Endpoint Protection Manager. По-этому не забывайте этот пароль. В дальнейшем изменить данный пароль возможно только заново запустив мастер настройки.

Рисунок 8.



Выбираем, какую базу данных будет использовать Symantec Endpoint Protection Manager для хранения своих данных. Так как у нас на сервер стоит Microsoft SQL Server 2005, то мы выбираем установку с использованием «Microsoft SQL Server».

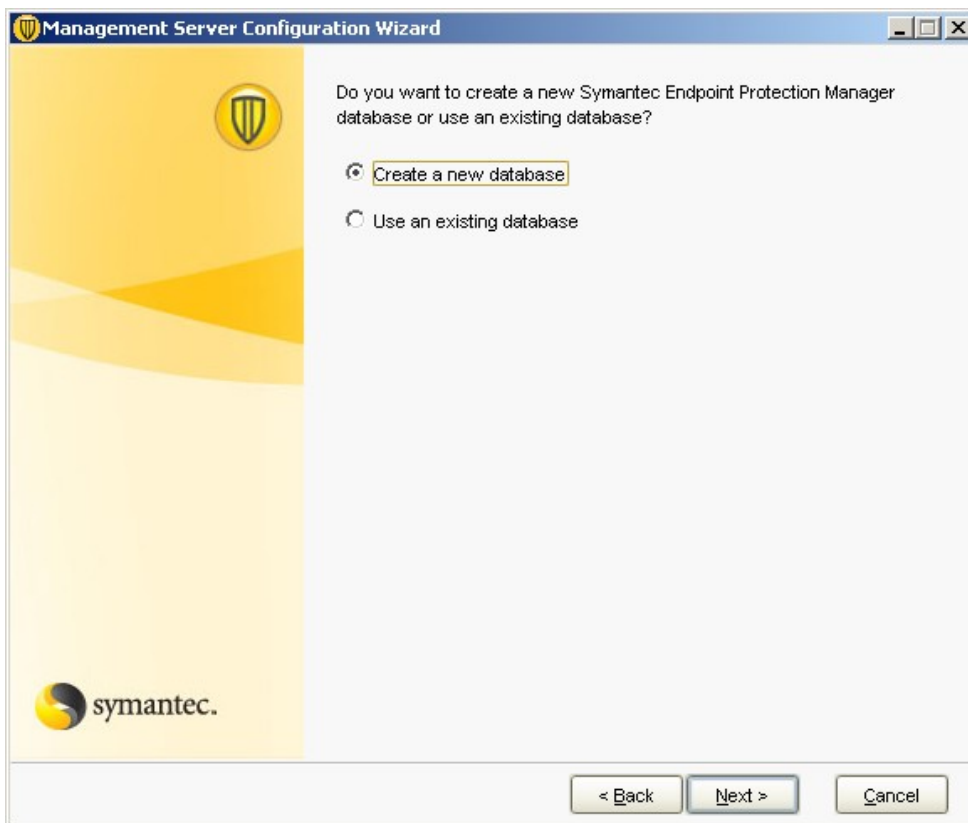
Рисунок 9.



Выбираем, будем ли мы создавать новую базу данных, или будем использовать существующую. Так как мы производим установку первого сервера, выбираем пункт «Create a new database».

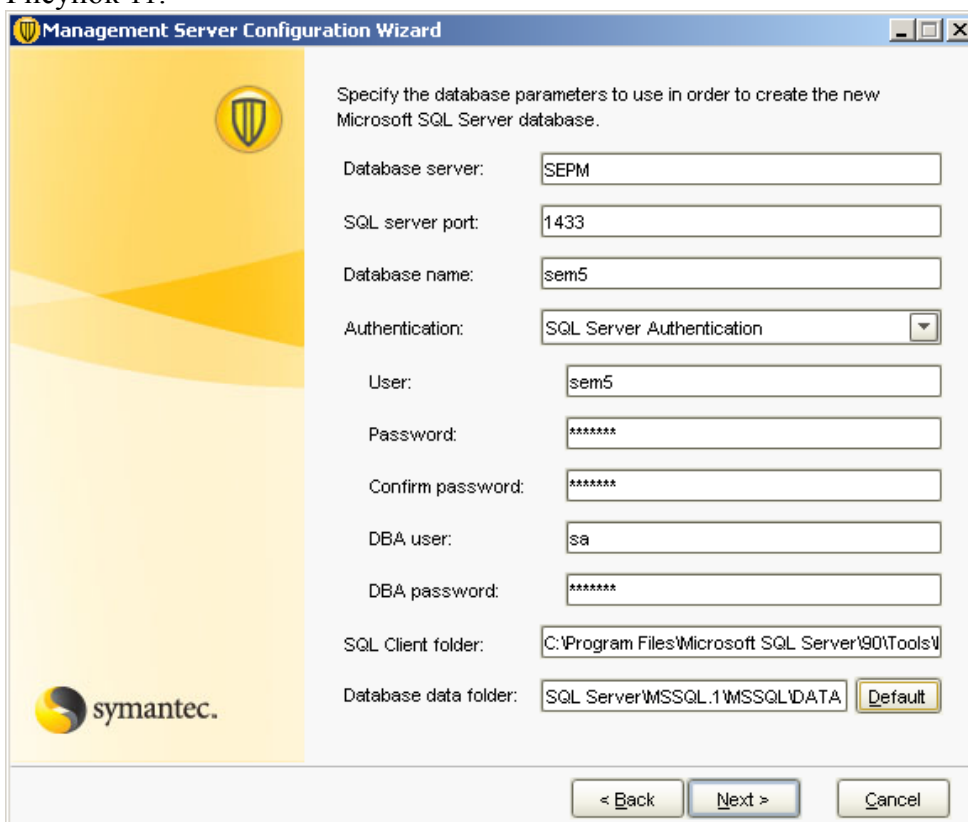
Рисунок 10.





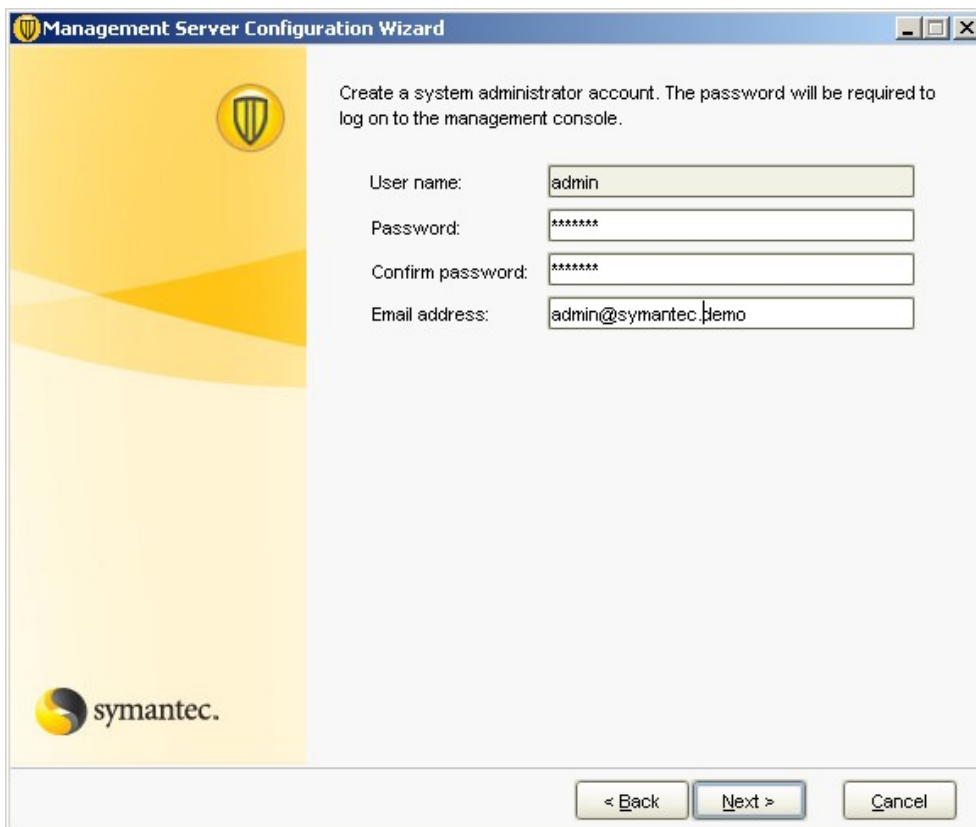
В следующем окне все заполненные поля оставляем по умолчанию. Заполняем поля Password / Confirm password, DBA password, и поле Database data folder – для заполнения этого поля автоматически нажимаем кнопку Default, расположенную справа от этого поля.

Рисунок 11.

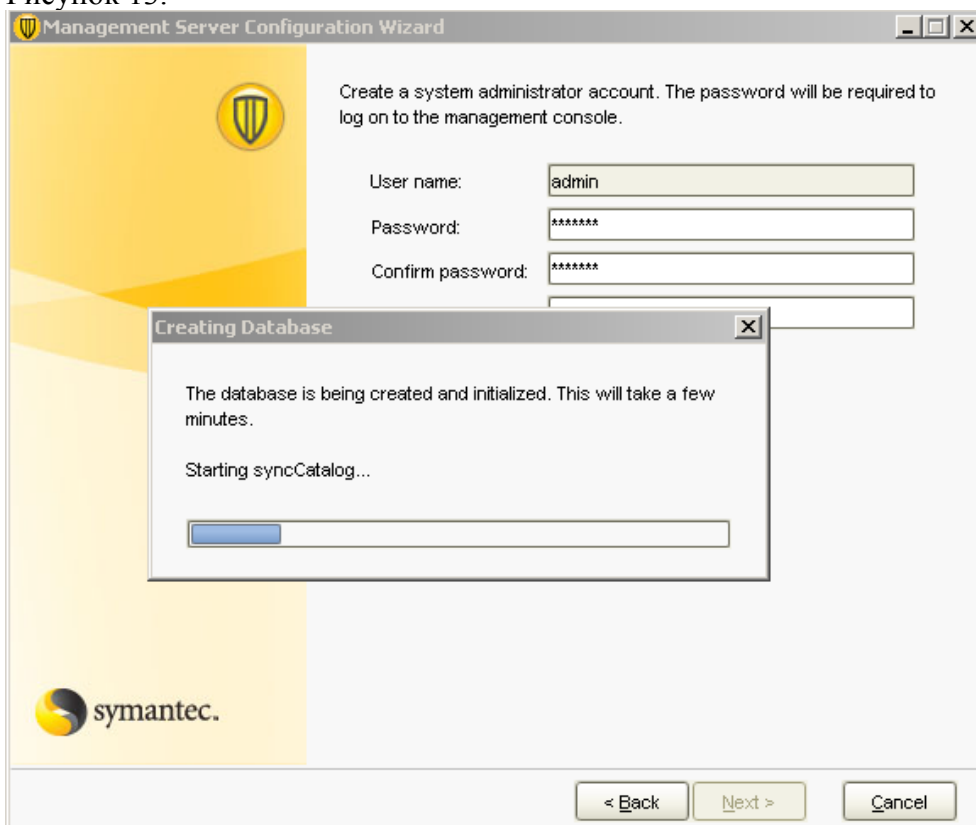


Вводим пароль администратора для доступа к консоли управления Symantec Endpoint Protection Manager.

Рисунок 12.



Стартуют процессы по созданию базы данных. У нас это длилось примерно 2 минуты.  
Рисунок 13.



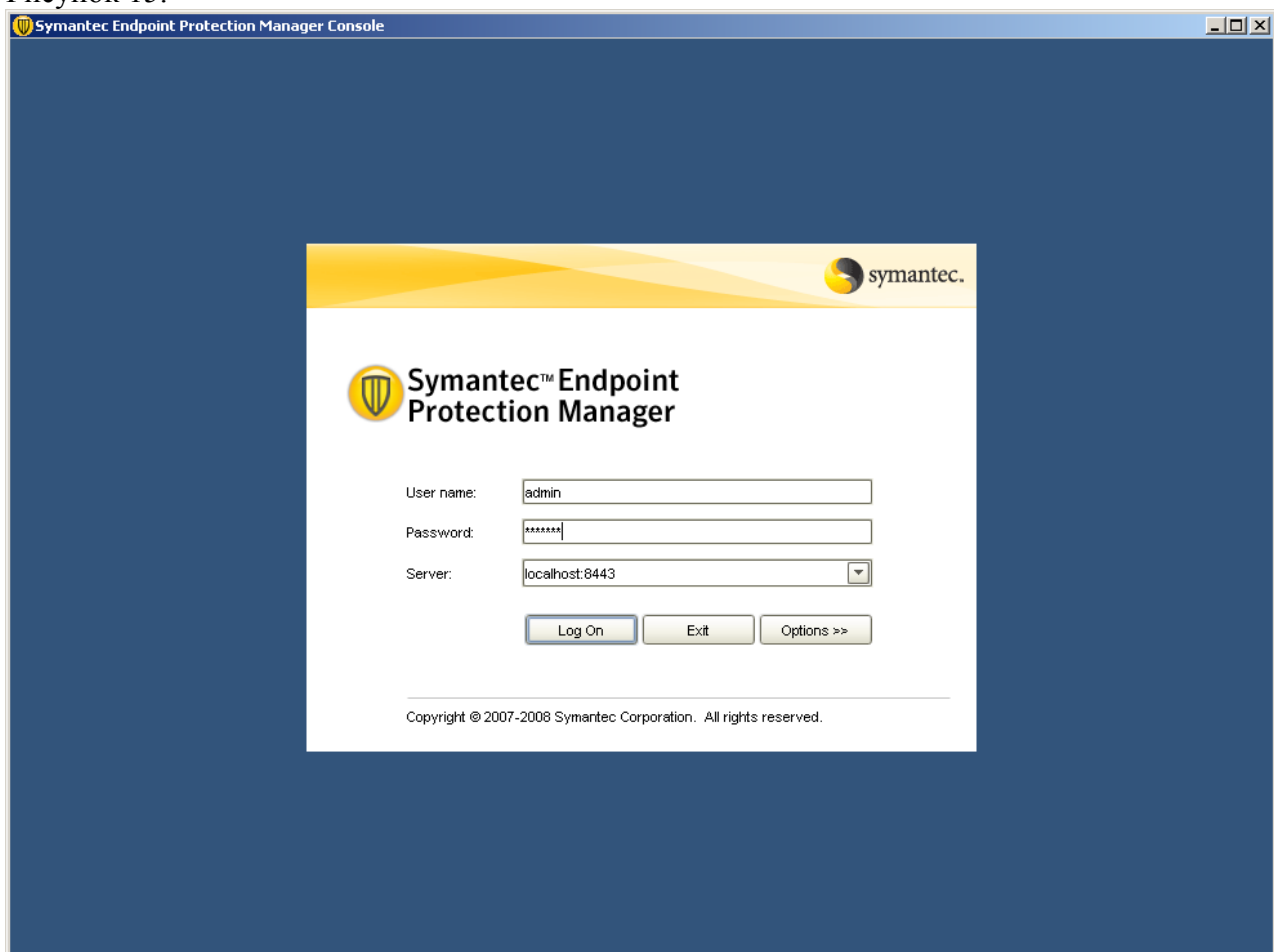
Далее нас спросят хотим ли мы запустить мастер миграции и распространения. Так как в рамках стенда используется только один сервер SEPМ, отказываемся от запуска мастера и завершаем процесс настройки Symantec End Point Protection Manager.

Рисунок 14.

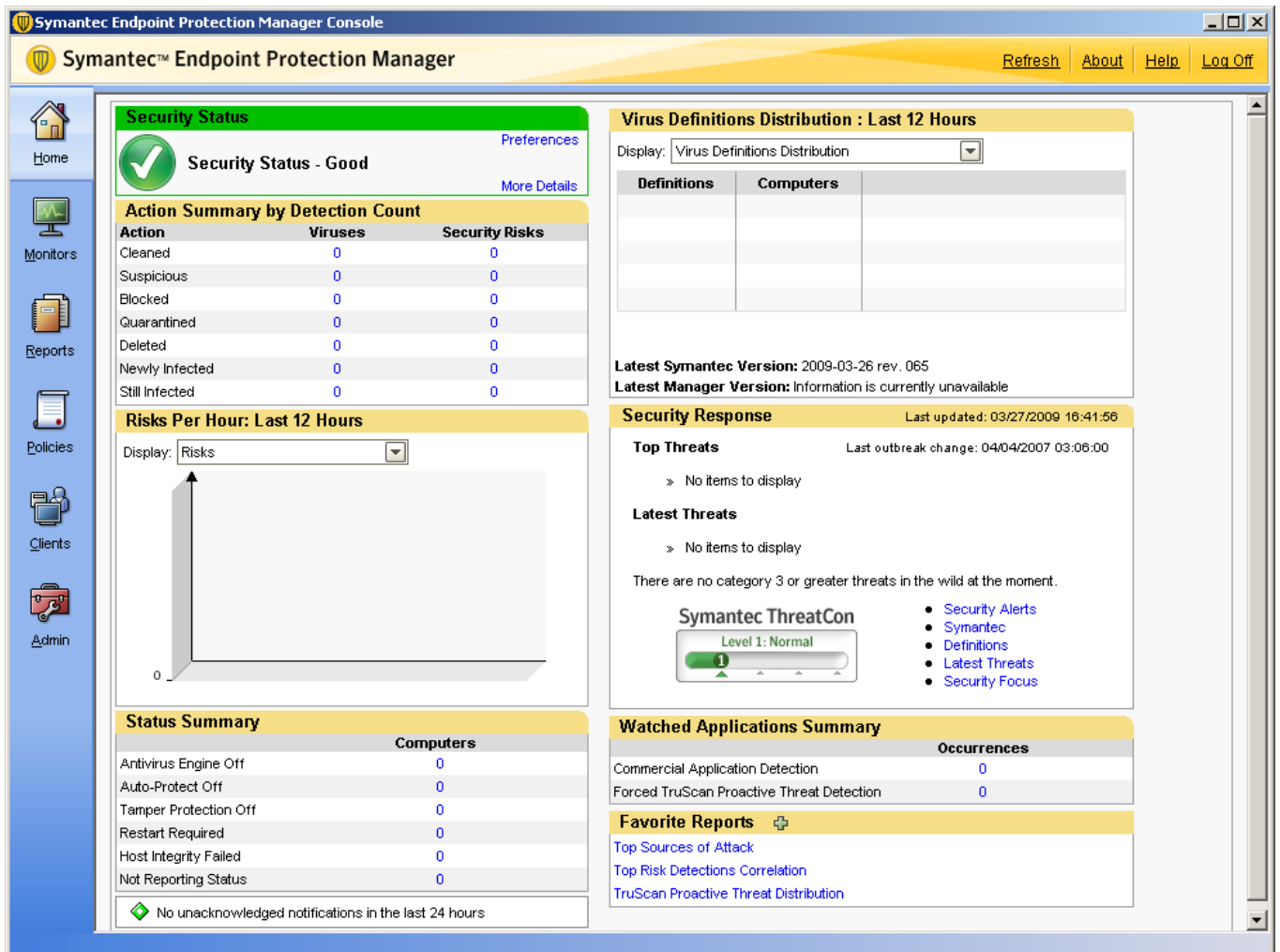




После завершения работы мастера настройки запустится консоль управления.  
Рисунок 15.



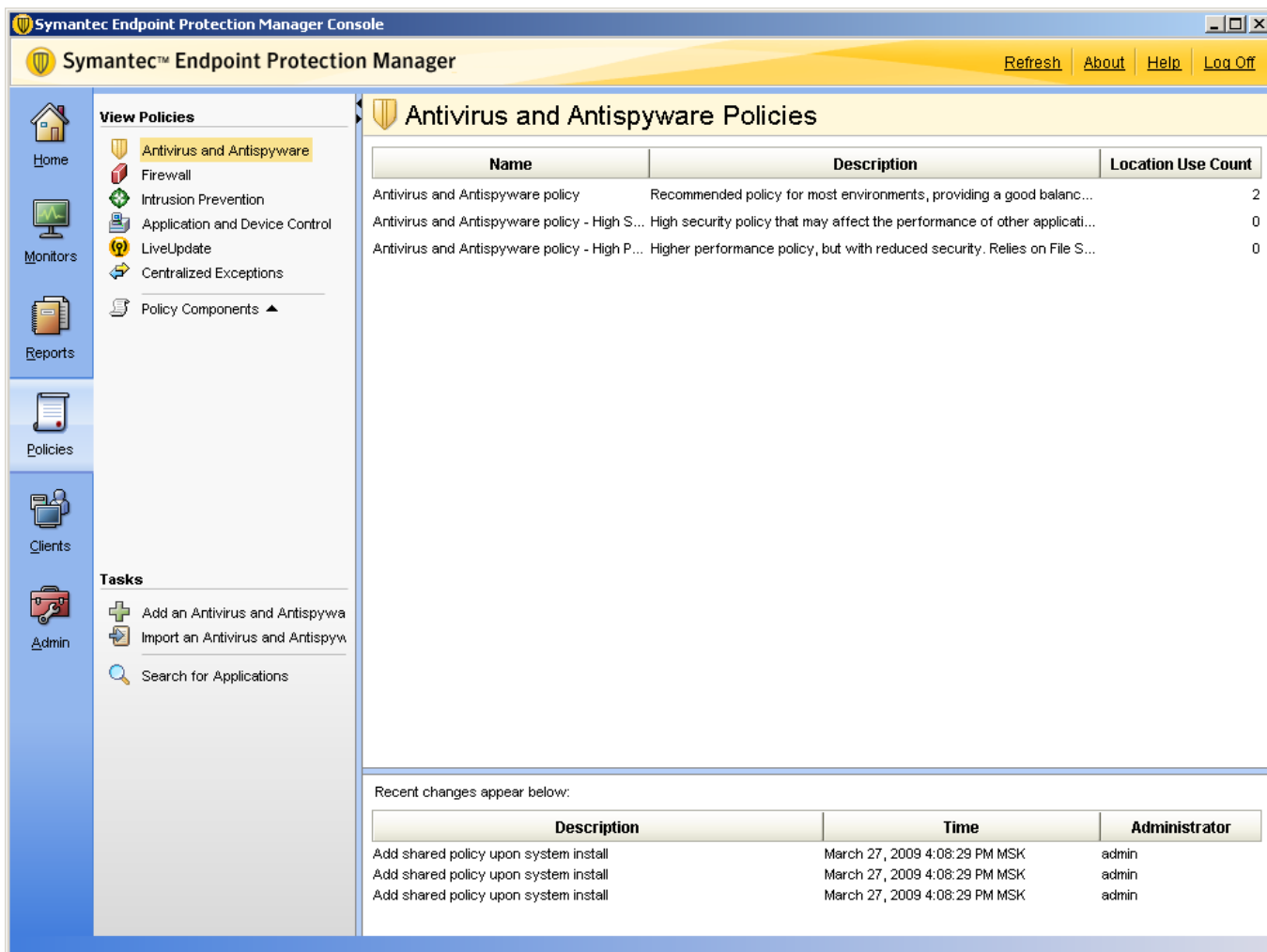
Вводим логин и пароль и попадаем в консоль Symantec Endpoint Protection Manager.  
Рисунок 16.



## *Обновление Symantec Endpoint Protection до Symantec Endpoint Protection + Symantec Network Access Control*

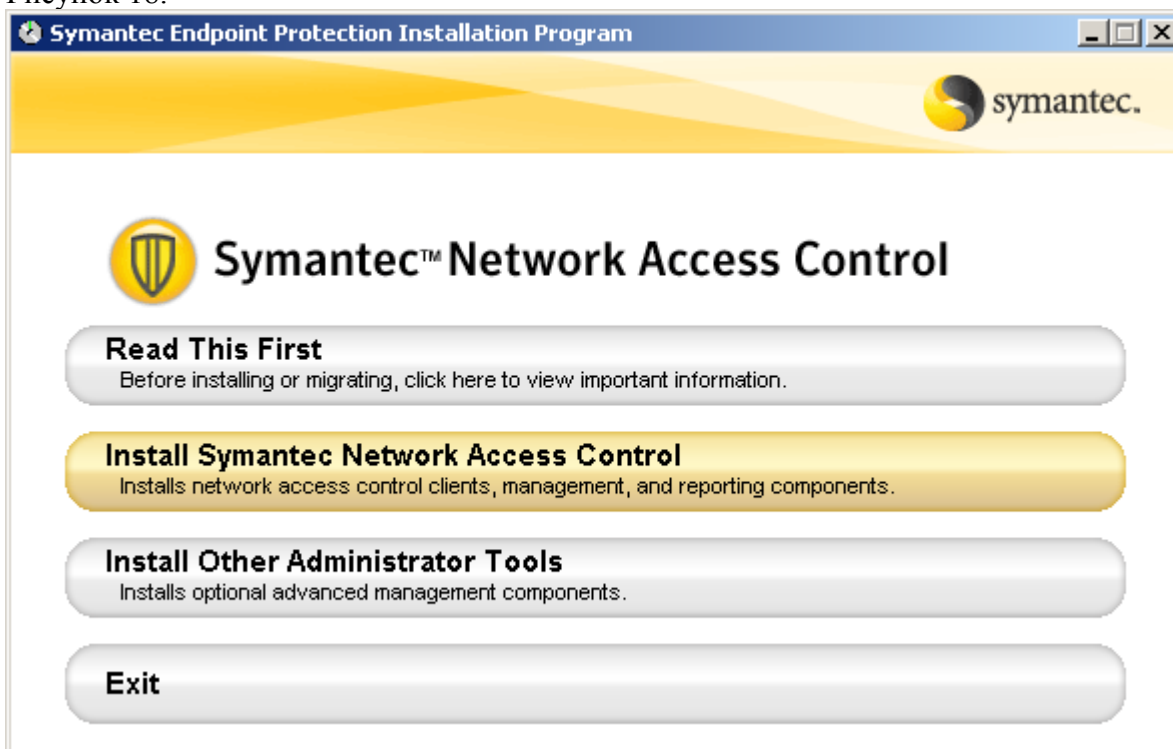
У нас есть установленный Symantec End Point Protection, однако функционал Symantec NAC пока отсутствует. В этом можно убедиться, перейдя в раздел «Policies» и в списке доступных политик попробовать найти Host Integrity. Она там будет отсутствовать:

Рисунок 17.

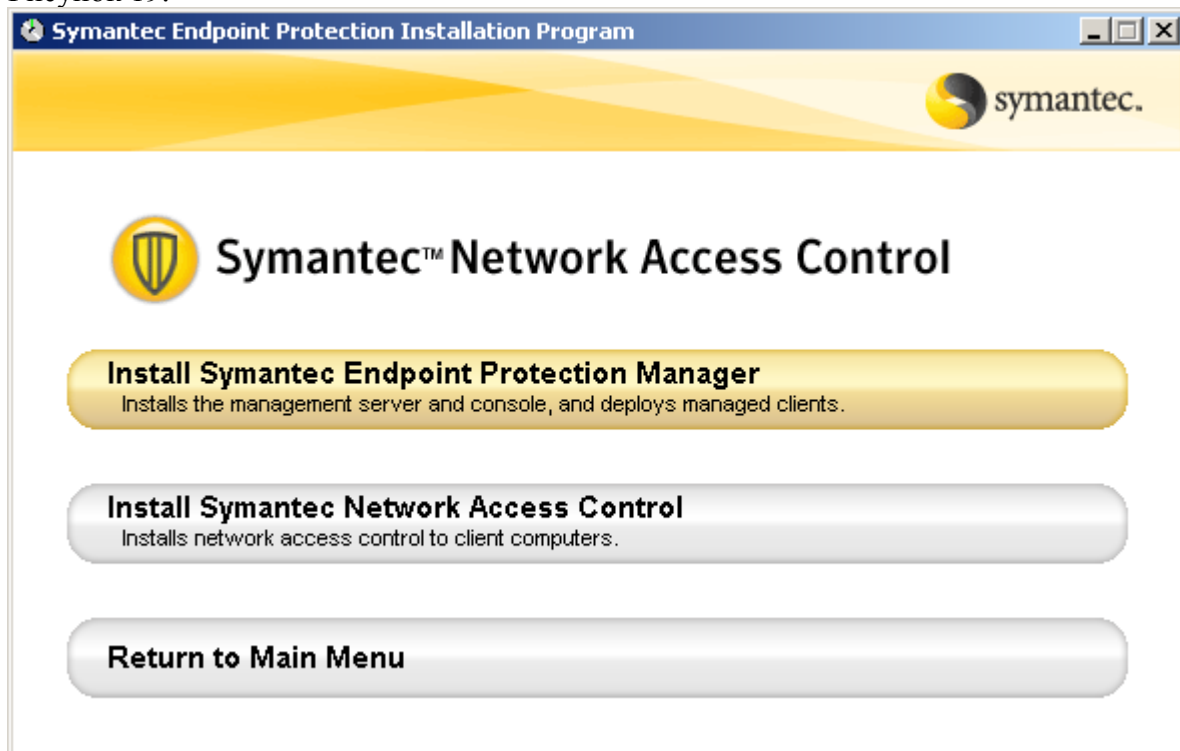


Для того, чтобы добавить в Symantec Endpoint Protection Manager функционал Symantec NAC, необходимо установить соответствующие компоненты. Для этого запускаем установку Symantec NAC, предварительно закрыв консоль Symantec Endpoint Protection Manager. Из предложенного меню выбираем пункт Install Symantec Network Access Control.

Рисунок 18.

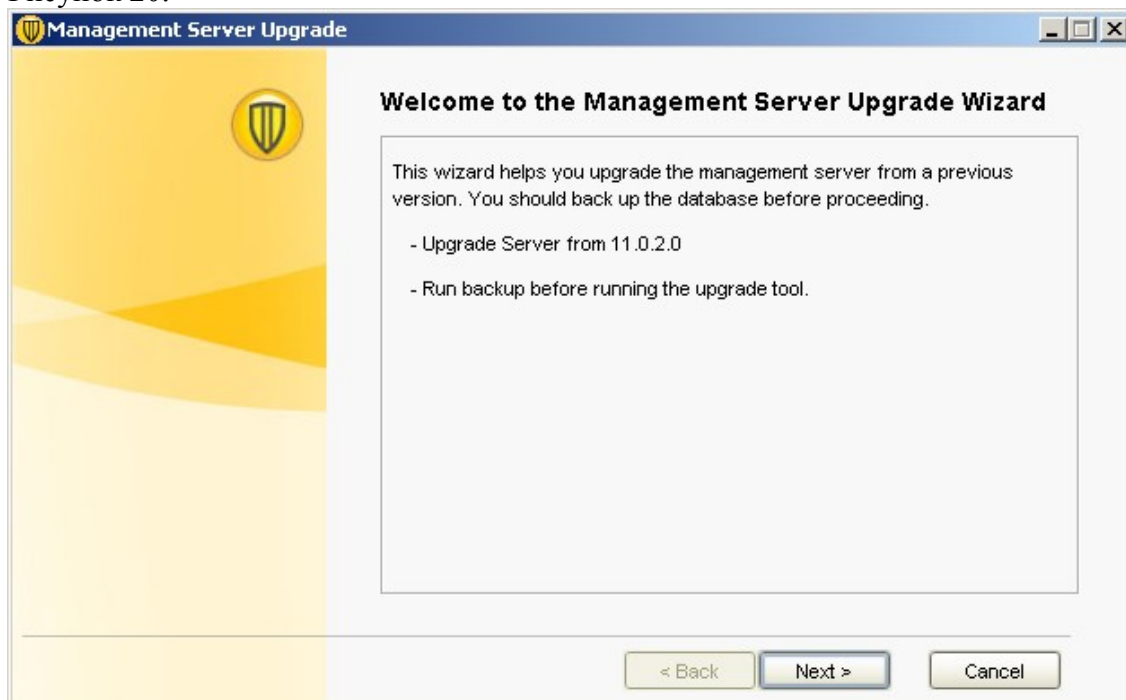


Далее выбираем пункт Install Symantec Endpoint Protection Manager:  
Рисунок 19.



Будет запущен установщик, который обнаружит уже установленный Symantec Endpoint Protection Manager и предложит обновить существующий сервер:

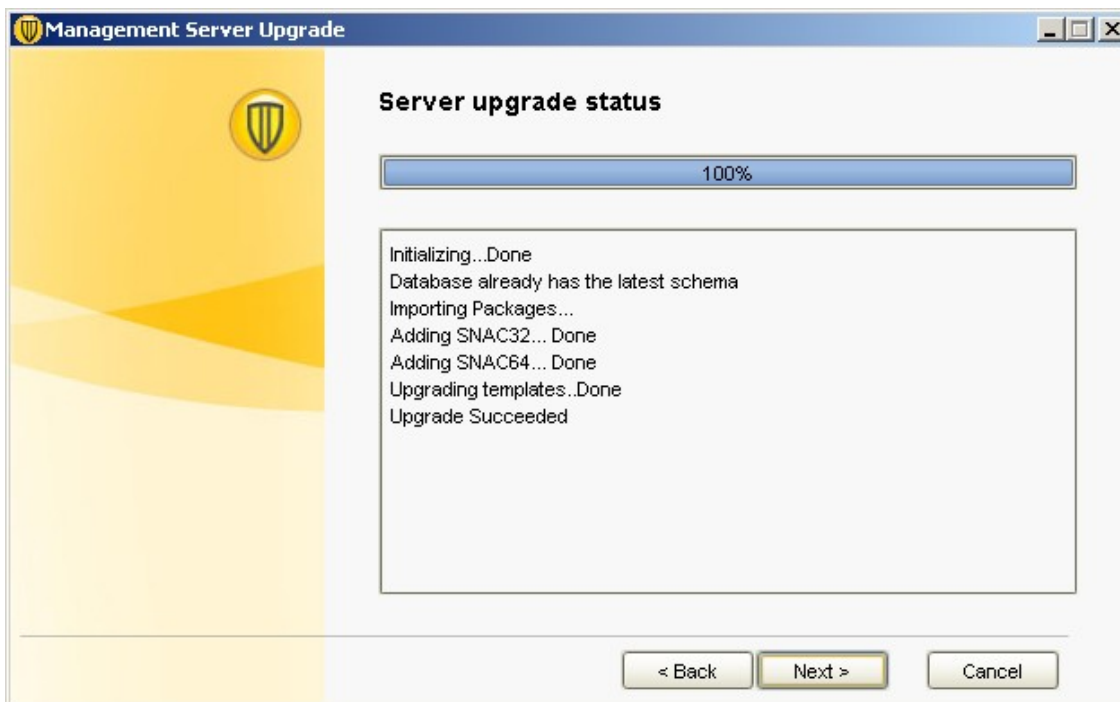
Рисунок 20.



Вы получите предупреждение о необходимости остановки всех управляющих серверов в сайте. Так как у нас только один сервер, то смело нажимаем «Continue» и продолжаем установку.

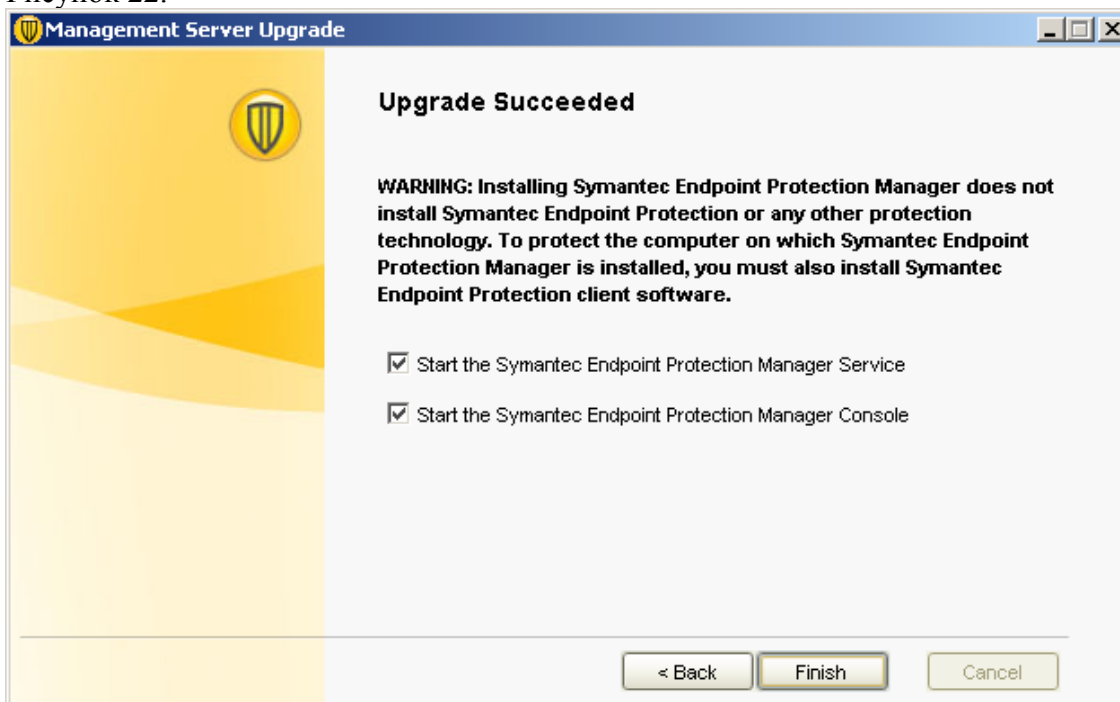
Обновление сервера займёт несколько минут. После завершения процесса обновления, в окне статуса появиться сообщение «Upgrade Succeeded». Нажимаем кнопку «Next».

Рисунок 21.



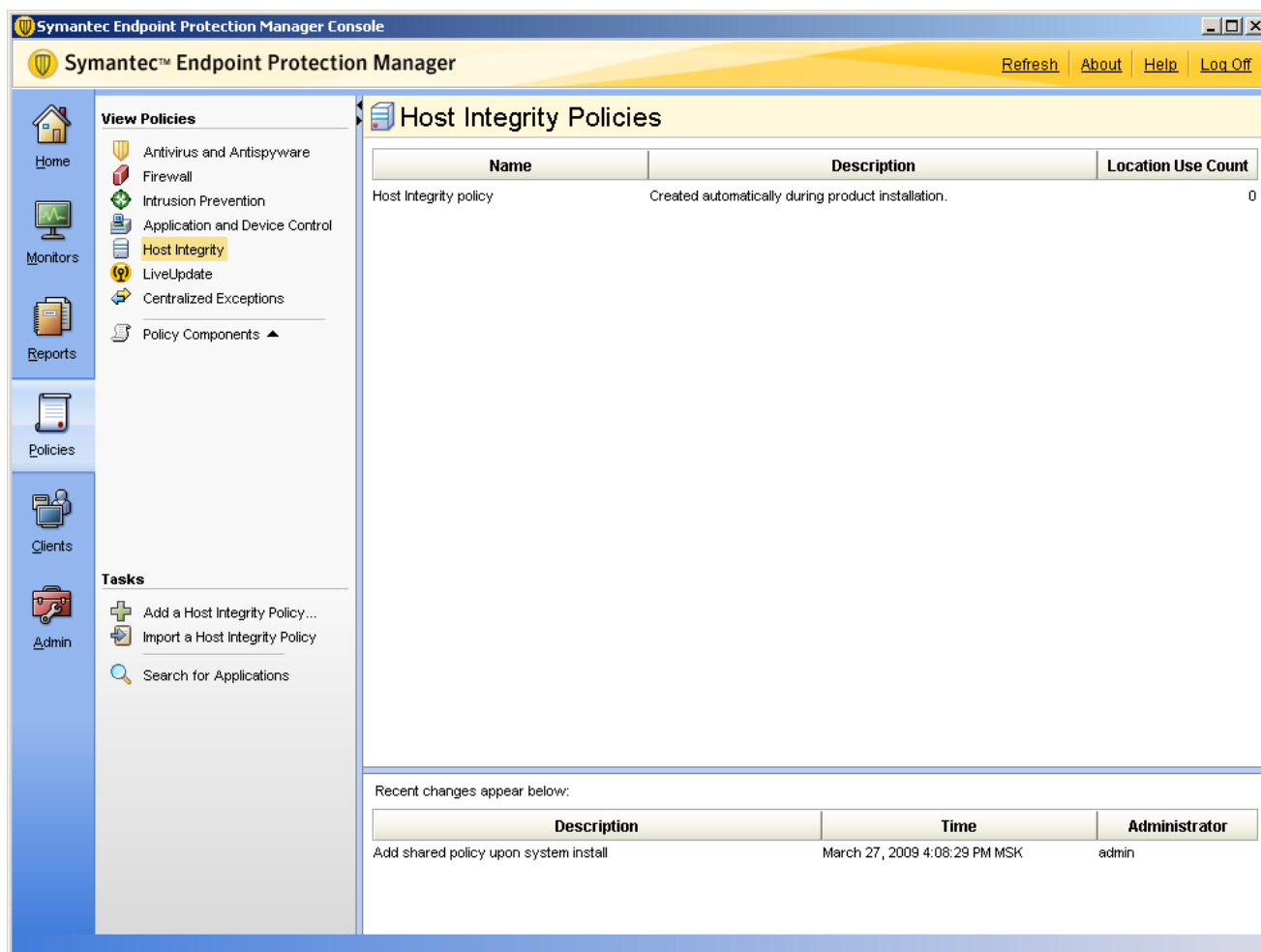
В следующем окне нажимаем «Finish» и завершаем установку:

Рисунок 22.



После завершения обновления, запуститься консоль управления Symantec Endpoint Protection Manager. Вводим логин и пароль, переходим в раздел «Policies» и убеждаемся, что в списке политик появился пункт «Host Integrity», который как раз и отвечает за реализацию Symantec Network Admission Control в консоли Symantec Endpoint Protection Manager:

Рисунок 23.



### *Немного о структуре Symantec NAC.*

Из описания технологии NAC (не привязываясь к конкретной реализации) мы знаем, что NAC состоит из 3-х частей:

1. Устройство, запрашивающее доступ к сети
2. Среда применения политик
3. Точка принятия решения.

Рассмотрим, каждую из этих частей в реализации Symantec NAC. Начнём с конца.

**Точка принятия решения.** В реализации Symantec, точкой принятия решения выступает Symantec Endpoint Protection Manager. В консоли задаются политики, которым должны удовлетворять сетевые устройства, а так же действия, которые необходимо совершить над сетевыми устройствами. Symantec Endpoint Protection Manager может обращаться к сторонним RADIUS серверам, например для проверки аутентификации пользователей, или для проверки аутентификации сетевых устройств.

**Среда применения политик.** В реализации Symantec NAC существует 4 варианта среды применения политик:

1. Self-Enforcement – «самозащита» - применение политики происходит на самом устройстве запрашивающем доступ, например на ноутбуке пользователя. Данный вариант может быть реализован, если у клиента установлен SEP и агент SNAC, так как применение политики осуществляется за счёт таких компонентов SEP как, например firewall и IPS. Self-Enforcement самый простой и быстрореализуемый вариант внедрения Symantec NAC в сети организации.
2. DHCP-Enforcement – применение политики происходит на уровне сети в момент получения устройством IP-адреса. В зависимости от состояния устройства, запрашивающего доступ к



сети, ему может быть выдан IP-адрес из различных подсетей. Относительно простой вариант для внедрения в сети, но требует некоторой модификации в схеме DHCP.

3. Gateway-Enforcement – можно назвать контролем на шлюзе. То есть применение политики происходит на уровне сети, при прохождении трафика через Gateway-Enforcer. Данный вариант уместен при контроле доступа устройств из отдельного небольшого сегмента сети, например такой как гостевой WiFi, или VPN-шлюз. Это обусловлено тем, что весь трафик проходит и обрабатывается на Gateway-Enforcer, что может стать узким местом в сети. Так же Gateway-Enforcer не контролирует трафик, который не проходит через него, например, при общении устройств внутри сегмента, такого как гостевой WiFi. По-этому данный вариант уместнее применять на границе сегментов сети. При внедрении необходимо чётко представлять работу сети, потоки трафика, и возможности самого Gateway-Enforcer, иногда требуется пересмотр и модернизация существующей схемы сети.
4. LAN-Enforcement – применение политики на уровне сетевых устройств поддерживающих протокол 802.1x, например таких как коммутаторы, маршрутизаторы, WiFi-точки доступа. Точка принятия решений определяет какие действия необходимо совершить с данным сетевым устройством и даёт команду сетевому оборудованию, например переместить устройство в специализированный VLAN или поместить устройство в рабочий VLAN, или наложить определённый список контроля доступа на порт, к которому подключилось устройство. Данный вариант самый сложный в реализации и требовательный как к структуре сети, так и к сетевому оборудованию, на котором построена сеть, однако данный вариант обладает наибольшим функционалом.

При внедрении Symantec NAC возможно использовать различные варианты совмещения и дополнения сред применения политик, как это было сделано на описываемом в данной статье стенде.

**Устройство, запрашивающее доступ к сети.** В качестве устройства, запрашивающего доступ к сети, может быть любое устройство имеющее MAC-адрес. Устройства, запрашивающие доступ к сети можно разделить на управляемые и неуправляемые. Управляемые устройства – это устройства на которых установлен или может быть установлен агент SNAC, который может предоставить запрашиваемую точкой принятия решений информацию. Неуправляемые устройства – это устройства, на которые агент SNAC не может быть установлен (например, принтеры).

### ***Установка и настройка Enforcer.***

Как было написано выше, у Symantec существует 4 варианта применения политик. Вариант Self-Enforcement реализуется только программными средствами, остальные 3 варианта реализуются с помощью программно-аппаратных комплексов (appliance), в терминологии Symantec, называемых Enforcer. Вариант с DHCP-Enforcer мы рассматривать не будем, хотя установка и первичная настройка аналогична для всех трёх вариантов.

Итак, перед нами Enforcer – сервер, со специализированным ПО. Включаем его, и через консоль получаем доступ к командной строке. Нас попросят ввести login и password, если первичная настройка не выполнялась, то есть Enforcer имеет заводские настройки, то для первого входа в систему используем следующие учётные данные:

*Login: root*

*Password: symantec*

Сразу же запустится процесс первичной настройки Enforcer, который разделён на 8 шагов.

1. Вас попросят выбрать в каком из трёх возможных режимов будет работать Enforcer.

Рисунок 24.

```
Welcome to the Symantec Enforcer Appliance Console.

=====
Welcome to the Symantec Enforcer Appliance
=====

Step 1 of 8: Set the Enforcer mode
Specify the Enforcer mode:

[Gateway Enforcer  [DHCP Enforcer  [LAN Enforcer: _
```

2. Необходимо указать имя нашего Enforcer:
3. Укажем IP-адреса DNS серверов
4. Нас попросят сменить пароль для пользователя root
5. Нас попросят сменить пароль для пользователя admin
6. Затем нас спросят, хотим ли мы сменить временную зону, и если мы ответим «yes», то спросят в какой временной зоне мы находимся.
7. Нас попросят ввести текущую дату и время.
8. На последнем шаге нас попросят указать сетевые настройки.

После завершения процесса настройки, нас спросят, хотим ли мы применить данные настройки, отвечаем «yes», после чего сделанные нами настройки применятся – это займёт несколько секунд. Для дальнейшей работы нам необходимо будет повторно зайти в консоль Enforcer'a, но уже с указанными на этапе первичной настройки учётными данными.

Следующим этапом настройки Enforcer будет подключение его к Symantec Endpoint Protection Manager. Для этого в командной строке Enforcer вводим следующие команды:

```
Enforcer# configure – переходим в контекст конфигурирования;
```

```
Enforcer(configure)# spm ip IP_АДРЕС_SEPM_СЕРВЕРА – указываем IP-адрес сервера SEPM
```

```
Enforcer(configure)# spm name DNS_ИМЯ_SEPM_СЕРВЕРА – указываем DNS имя сервера SEPM (опционально)
```

```
Enforcer(configure)# spm http 8014 – указываем протокол и порт, по которым Enforcer будет общаться с Symantec Endpoint Protection Manager.
```

```
Enforcer(configure)# smp group ИМЯ_ГРУППЫ_B_SEPM – указываем имя группы, в которую будет помещён данный Enforcer, если такой группы в SEPM не существует, то она будет автоматически создана.
```

```
Enforcer(configure)# spm key КЛЮЧ – указываем ключ шифрования, который будет использоваться при обмене данными между SEPM и Enforcer. Это тот самый ключ, который мы задавали на этапе настройки SEPM когда указывали encryption key, и который Вы должны помнить.
```

На этом настройка Enforcer завершена. Если всё сделано правильно, то Enforcer должен появиться в дереве серверов в разделе Admin->Servers. Теперь все дальнейшие настройки будут производиться из консоли Symantec Endpoint Protection Manager. Далее мы подробнее рассмотрим настройку LAN Enforcer и Gateway Enforcer в соответствии с нашим стендом.

### ***Создание и настройка политик доступа в сеть.***

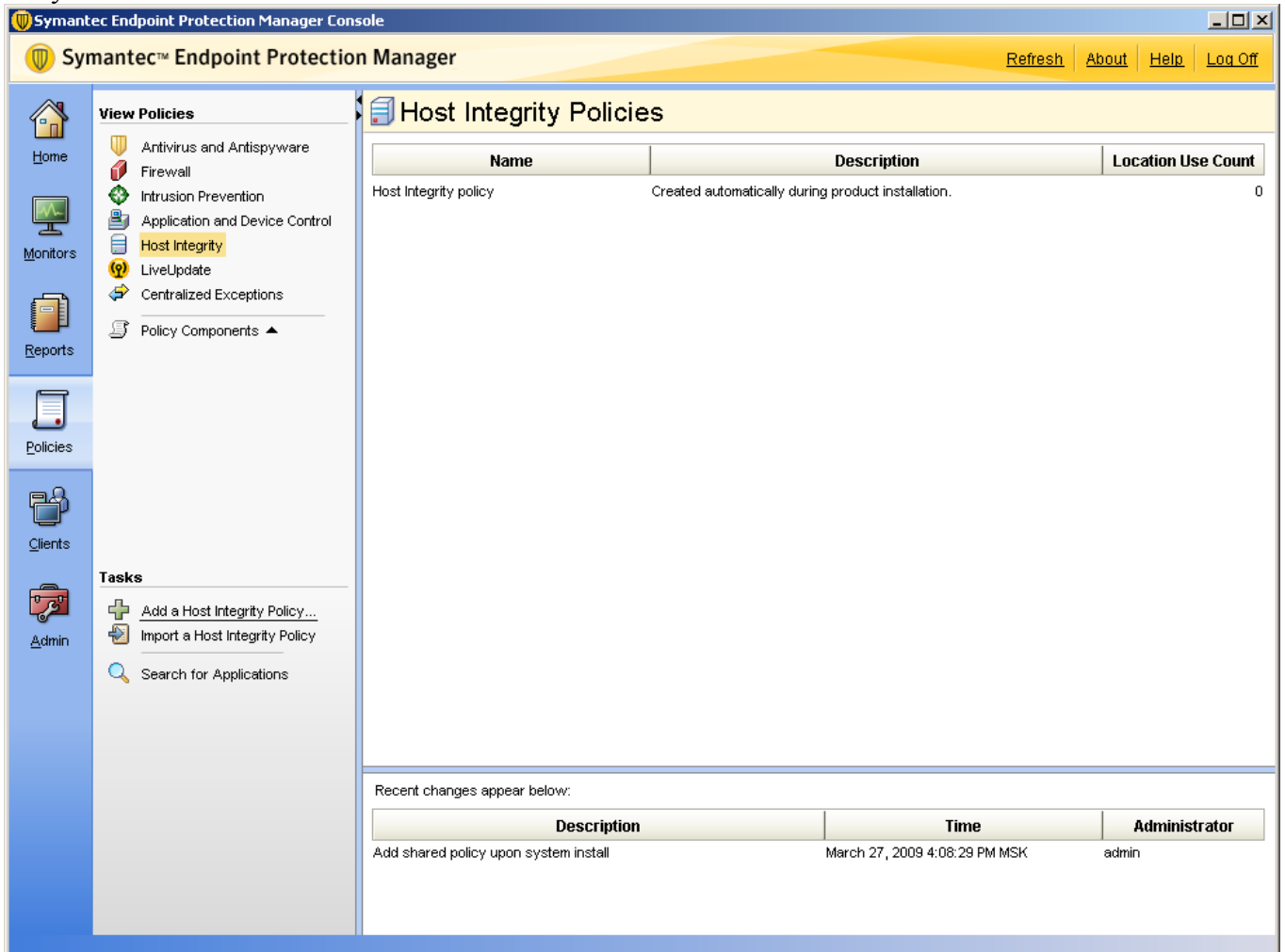
Вернёмся к нашему стенду. Для начала нам необходимо создать политики доступа в сеть, на основе которых мы будем определять, какие действия необходимо совершить с сетевыми устройствами.

При подготовки стенда нам показалось неинтересным проверять установлен ли и запущен ли антивирус, обновлены ли антивирусные базы, по-этому мы решили проверять, запущен ли на компьютере блокнот. То есть, перефразировав политику на человеческий язык, получим: «Для работы в сети нельзя запускать Блокнот». Если блокнот запущен, то мы или запрещаем доступ в

сеть (для варианта Self-Enforcement и Gateway-Enforcement), или помещаем устройство в карантинный VLAN (для варианта LAN-Enforcement).

Итак, создадим политику Host Integrity-, которая будет проверять, запущен ли блокнот и, в случае, если он запущен, возвращать несоответствие политикам - или, если блокнот не запущен, возвращать соответствие требуемым политикам. Для создания политики открываем консоль Symantec Endpoint Manager, вводим логин и пароль, переходим в раздел Policies и из списка политик выбираем Host Integrity. Ниже, в разделе «Tasks», выбираем пункт «Add a Host Integrity Polisy»...

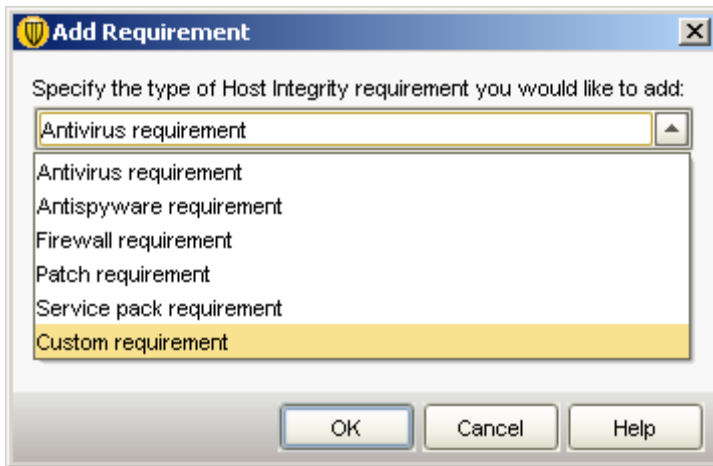
Рисунок 25.



Откроется окно создания новой политики. В разделе Overview зададим имя политики и её описание.

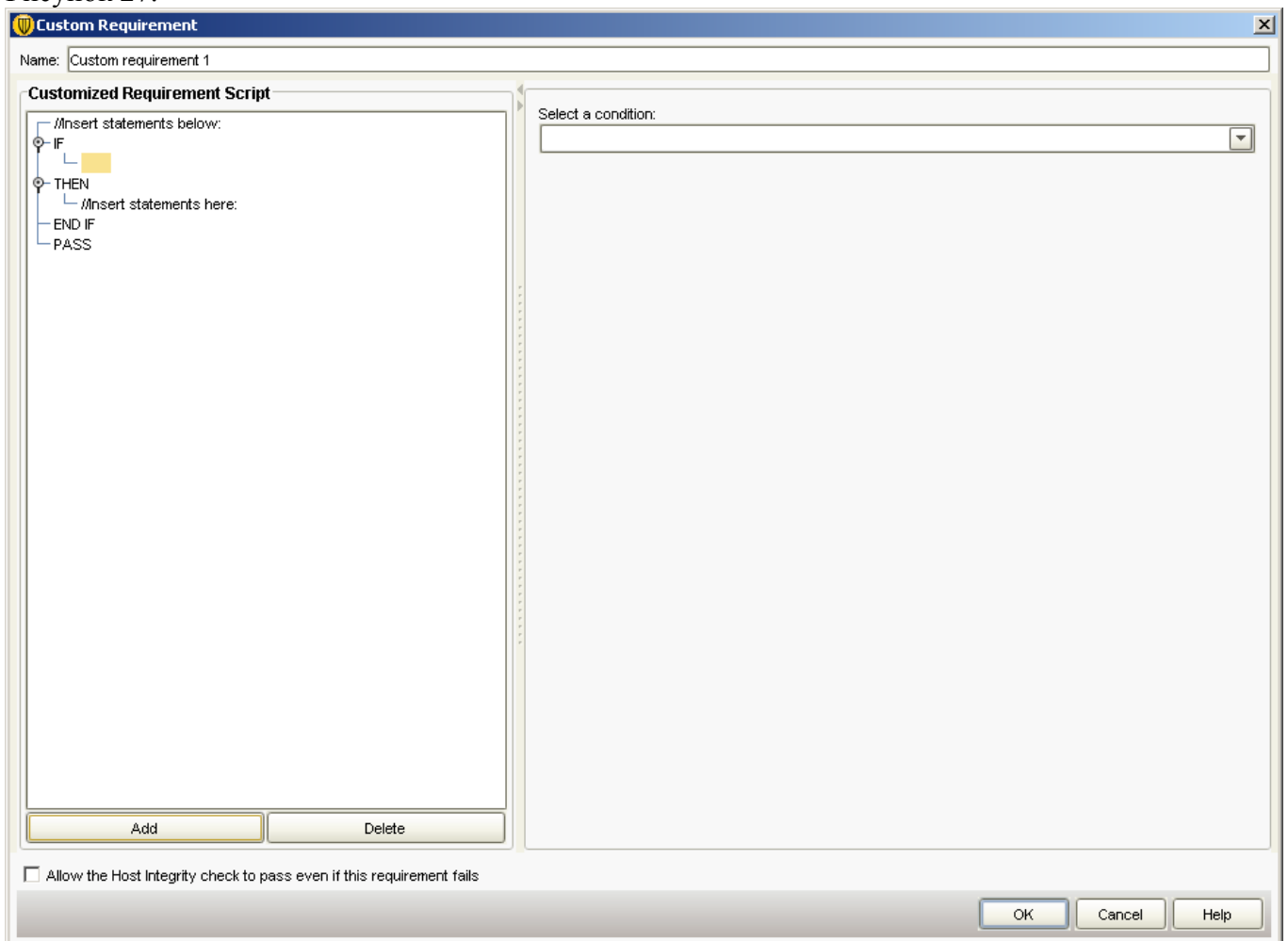
В разделе Requirements укажем параметры проверки и зададим требования, которым должны удовлетворять устройства, подключающиеся к сети. Для добавления требования нажимаем кнопку «Add», расположенную внизу окна. Из списка доступных требований, выбираем пункт «Custom requirement».

Рисунок 26.



В окне настройки требования нажимаем кнопку «Add» расположенную внизу, из открывшегося списка выбираем пункт IF..THEN .. , после чего в поле Customized Requirement Script появится следующее:

Рисунок 27.

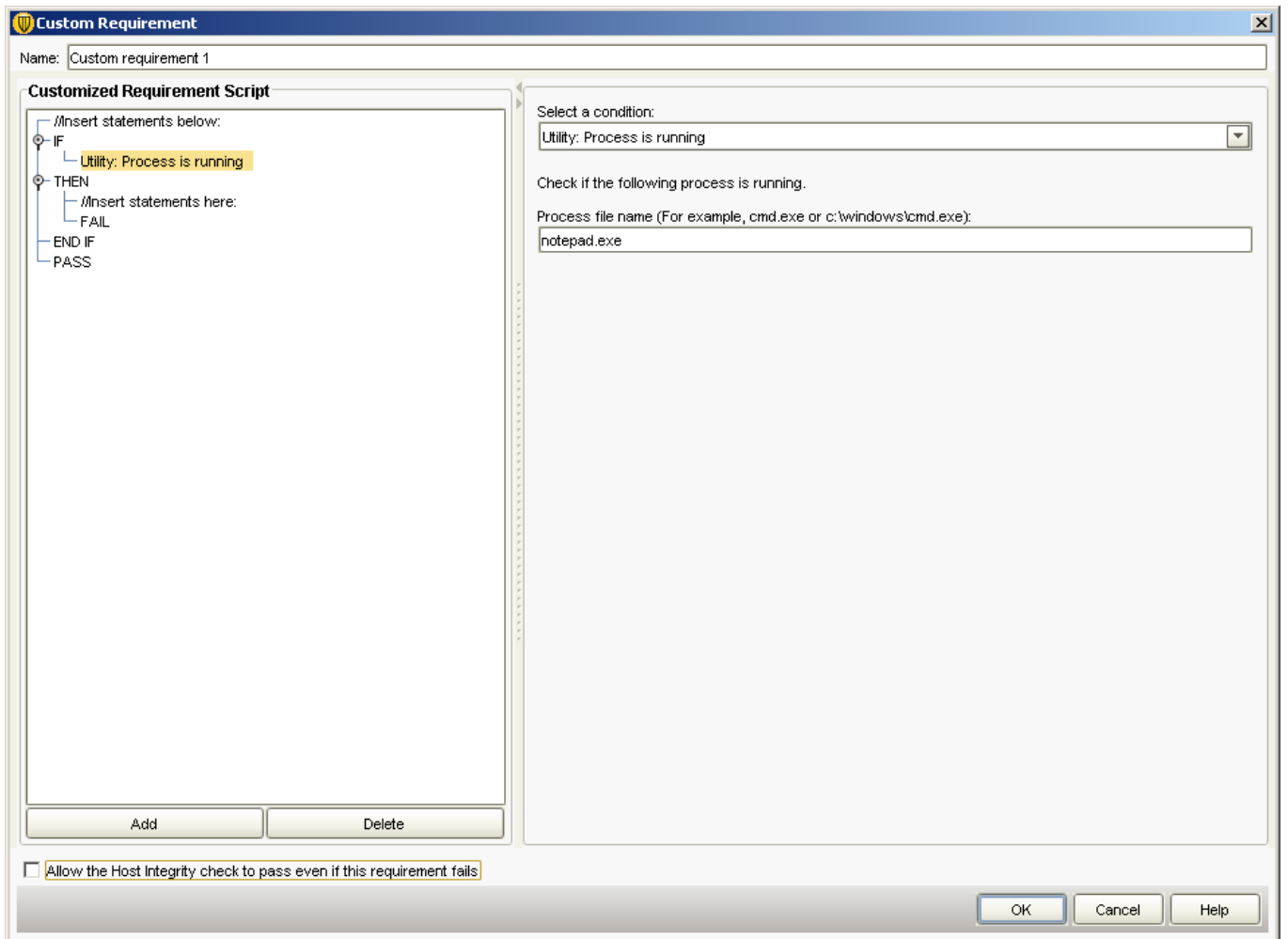


В правой части, из выпадающего списка выбираем Utility: Process is running. Затем в окне Process file name вводим значение notepad.exe.

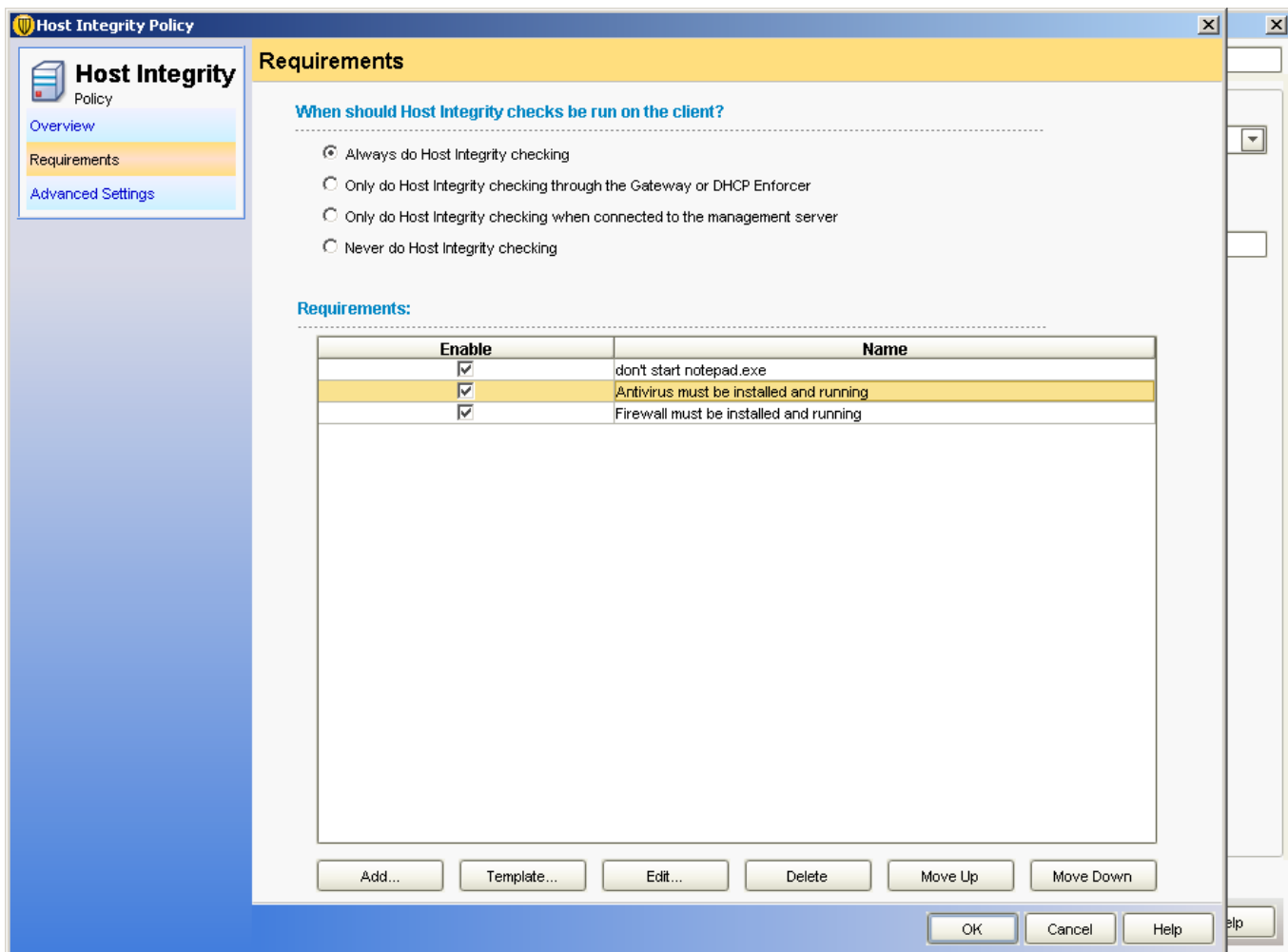
Перемещаем фокус на строку между операторами THEN и END IF. Нажимаем на кнопку «Add», из открывшегося меню выбираем пункт «return» и в правой части окна ставим переключатель в положение Fail.

Должно получиться следующее:

Рисунок 28.



Требование создано, для его сохранения и закрытия окна; нажимаем «Ok».  
При необходимости, аналогичным образом можно добавить другие требования.  
Рисунок 29.

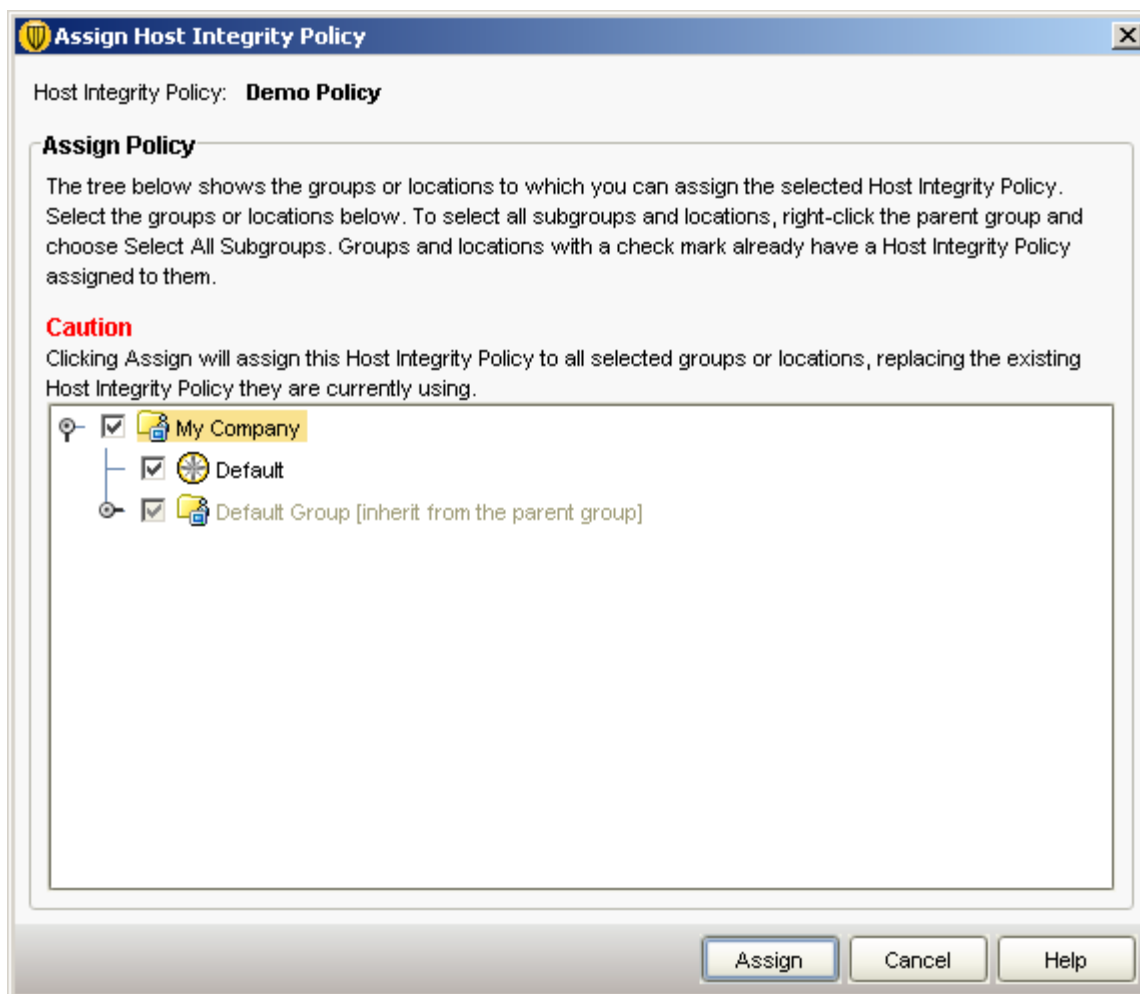


В разделе Advanced Settings, при необходимости, можно сделать дополнительные настройки - например, выводить сообщения пользователю.

После задания всех требований и дополнительных настроек, нажимаем «Ok». Политика будет создана и будет выведено окно с уведомлением о том, что она не привязана ни к какой из групп, и предложением привязать созданную политику к группе. Привяжем политику к группе My Company:

Рисунок 30.





При необходимости, аналогичным образом создаются другие политики.

### *Настройка Self-Enforcement*

Поговорим поподробнее про Self-Enforcement. Данный вариант реализации технологии NAC подразумевает применение политик к сетевому устройству на самом устройстве. То есть, у нас есть компьютер, с установленным SEP 11 и агентом SNAC, есть политики доступа в сеть, и есть политики карантина, например, карантинная политика МСЭ, в которой запрещен доступ в сеть. Карантинная политика может включать правила не только для МСЭ, но и для серверов обновлений, для антивируса, IPS.

Ключевым моментом Self-Enforcement является то, что для его реализации не требуется никакого дополнительного оборудования в виде SNAC Appliance, не важна архитектура сети и не важно, на каком оборудовании построена сеть. Данный вариант SNAC можно легко развернуть практически в любой сети.

Итак, в нашем примере мы создадим одну политику для МСЭ, в которой будут два правила:

1. Разрешить доступ к серверу, на котором установлен SEPМ - это правило позволит обмениваться данными между клиентским SEP и сервером SEPМ.
2. Заблокировать весь трафик.

Таким образом, если наш компьютер не пройдет проверку на соответствие политикам и ему будет присвоен статус «помещён в карантин», МСЭ загрузит и применит вышеуказанные правила. Следовательно, компьютер не получит доступ в сеть, кроме доступа к серверу, на котором установлен SEPМ.

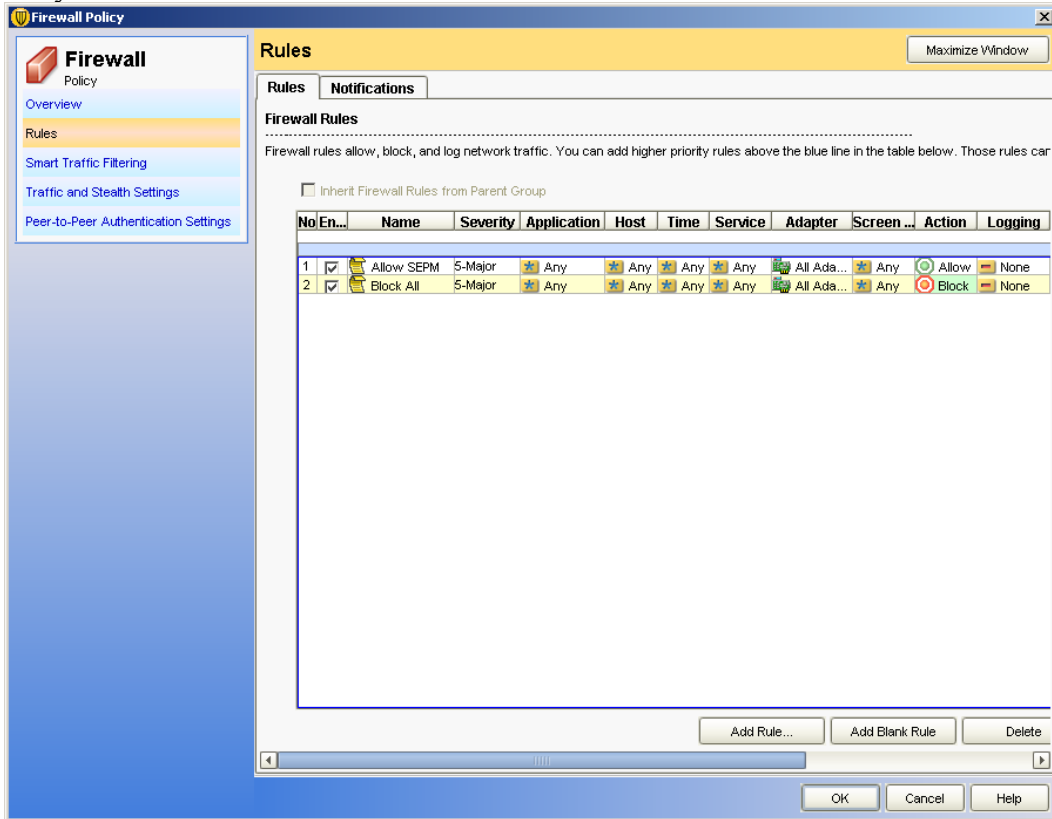
Для создания политики, заходим в консоль управления SEPМ, переходим в раздел «Clients», затем переключаемся на вкладку «Policies» и напротив надписи «Quarantine Policies when Host Integrity Fails:» нажимаем «Add a policy...». Появится окно с перечнем доступных политик, из

которого выбираем политику Quarantine Firewall Policy. В следующем окне перемещаем указатель в положение «Create a new policy».

В мастере создания политики МСЭ в разделе Overview задаём имя и описание политики.

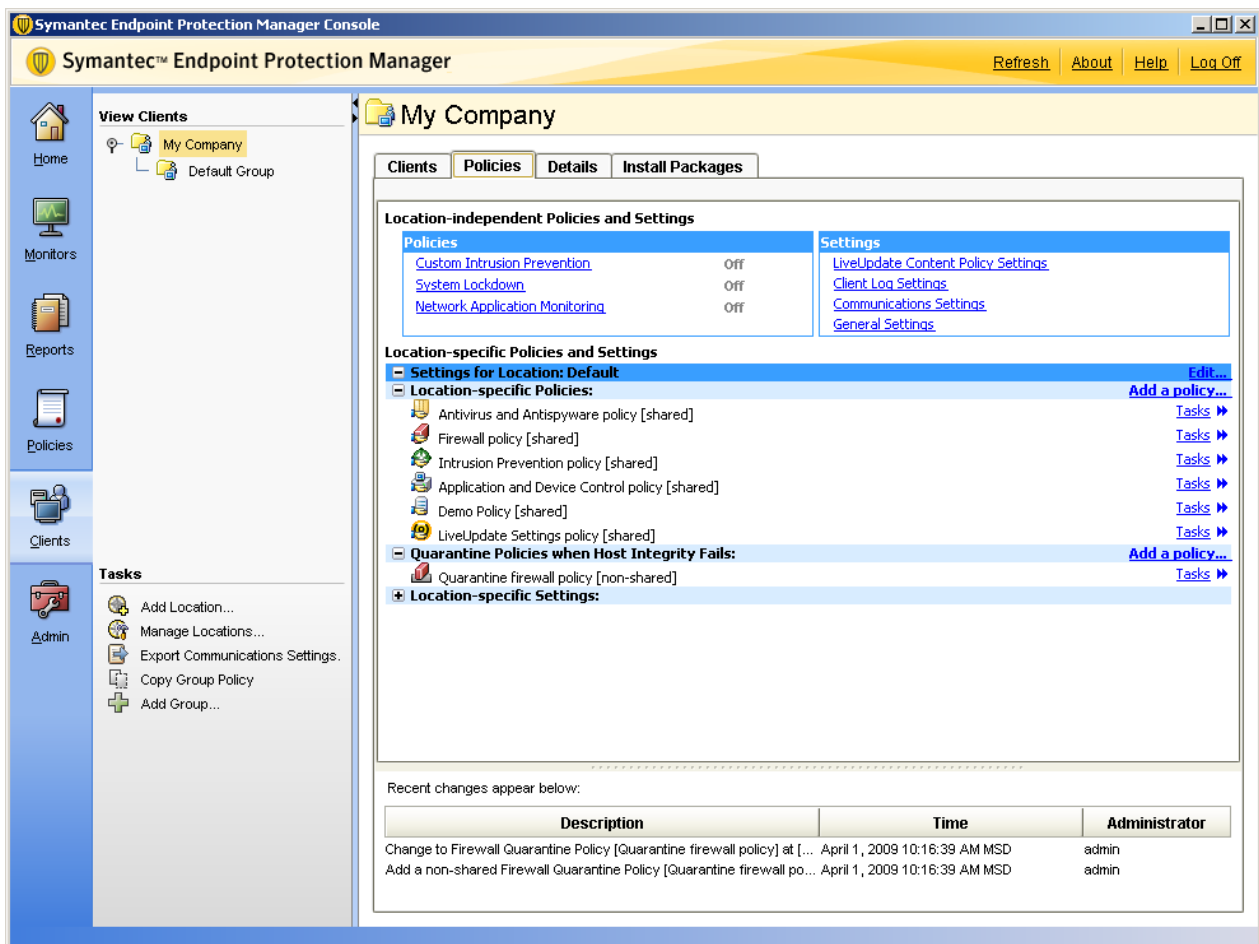
В разделе Rules, удаляем все существующие правила, и добавляем два правила, которые мы описали выше - тут останавливаться подробнее не будем, так как интерфейс интуитивно понятен. У Вас должно получиться примерно следующее:

Рисунок 31.



После создания политики, в консоли SEPM у Вас должно появиться созданное правило в разделе «Quarantine Policies when Host Integrity Fails»:

Рисунок 32.



На этом настройка политик и действий для Self-Enforcement завершена.

## *Gateway-Enforcement*

Общую настройку SNAC Enforcer рассматривали Выше. Ниже мы приведём настройки для двух Gateway-Enforcer, используемых в описываемом стенде.

По схеме (Рис.1) видно, что мы используем два Gateway-Enforcer: один для контроля устройств, подключающихся к нашей сети с помощью WiFi, второй – для контроля устройств, подключающихся к нашей сети через VPN. Оба Gateway Enforcer имеют одинаковые настройки, отличаются только имена и IP-адреса устройств.

Итак, при первом входе на устройства, выбираем, что они будут работать в режиме Gateway Enforcer.

Задаём имена: GW\_Enforcer – устройству, которое будет контролировать подключающихся через VPN, GW\_Enforcer\_WiFi – устройству, которое будет контролировать подключающихся через WiFi.

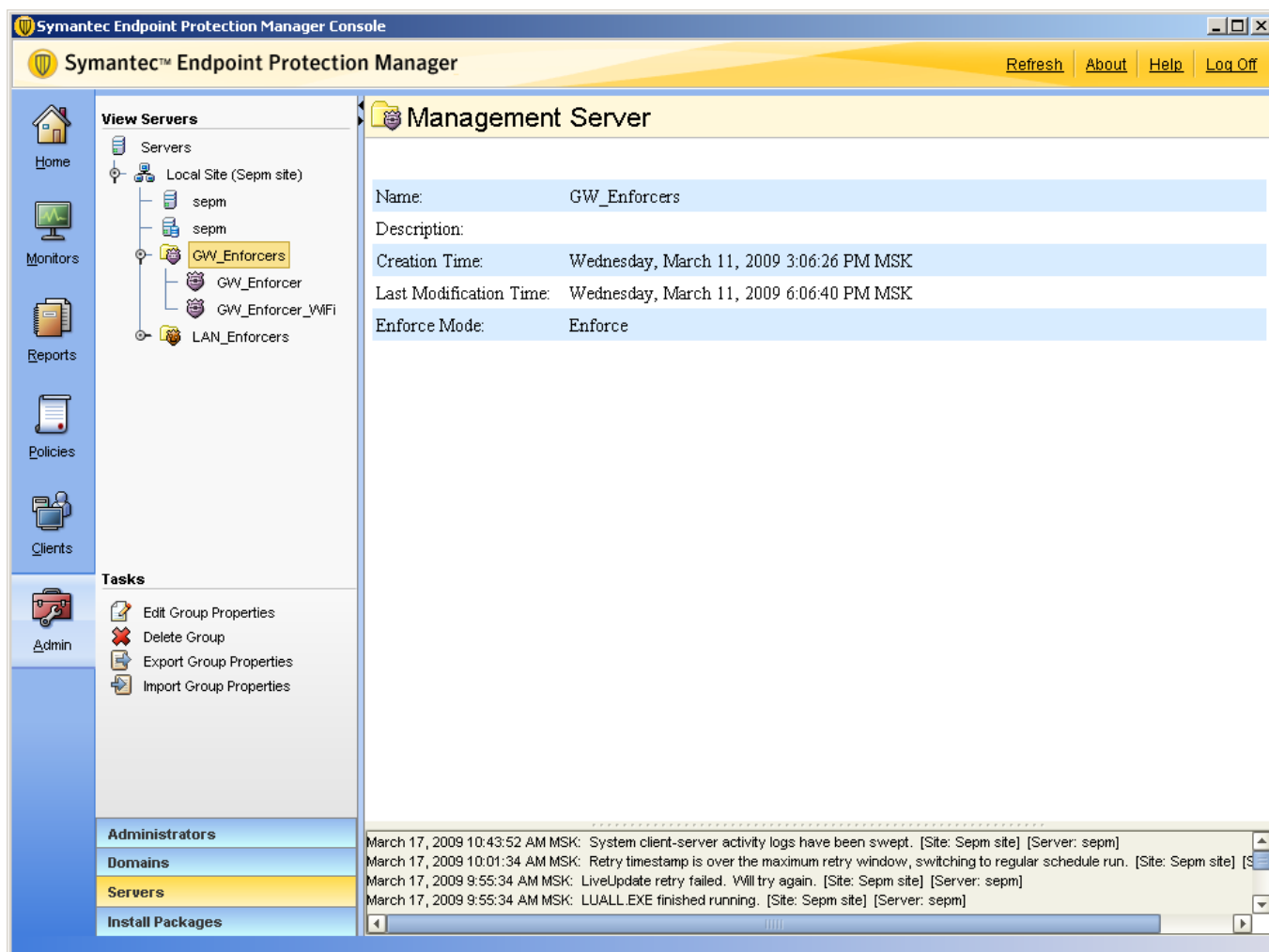
Зададим IP-адреса для Enforcer-устройств согласно схеме (Рис.1.).

При настройке соединения Enforcer-устройств с SEPМ указываем, что устройства будут находиться в группе GW\_Enforcers.

Остальные необходимые настройки описаны в разделе «Установка и настройка Enforcer».

Если Вы всё сделали правильно, то у Вас должно получиться следующее:

Рисунок 33.

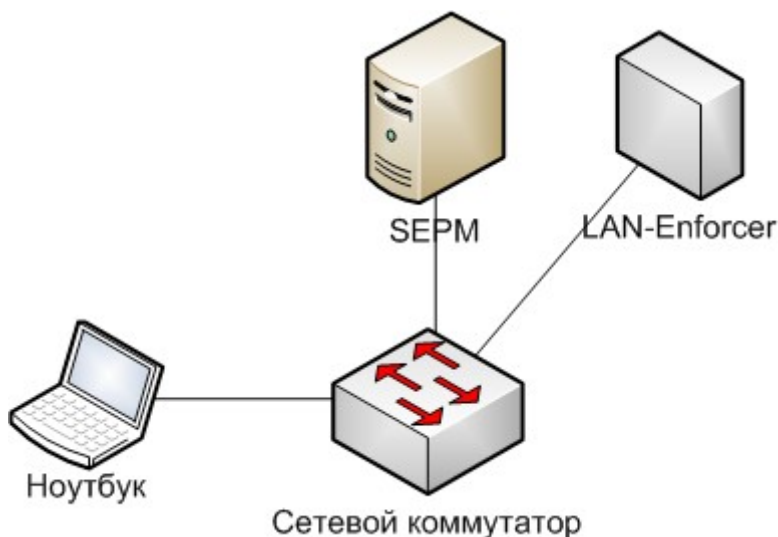


## *LAN-Enforcement*

Вот мы и подошли к самому интересному и наиболее функциональному варианту SNAC – к LAN – Enforcement. Данный вариант SNAC взаимодействует с сетевым оборудованием, что позволяет реализовывать очень сложные и в тоже время гибкие политики и действия, применяемые к сетевым устройствам, запрашивающим доступ.

Поподробнее остановимся на принципе работы LAN-Enforcement. У нас есть устройство, запрашивающее доступ в сеть – пусть это будет ноутбук сотрудника компании, и на данном ноутбуке установлен агент SNAC. Есть сетевой коммутатор, который «понимает» протокол аутентификации 802.1x - на нашем стенде мы использовали коммутатор Cisco Catalyst 2950. Есть LAN-Enforcer и есть Symantec Endpoint Protection Manager.

Рисунок 34.



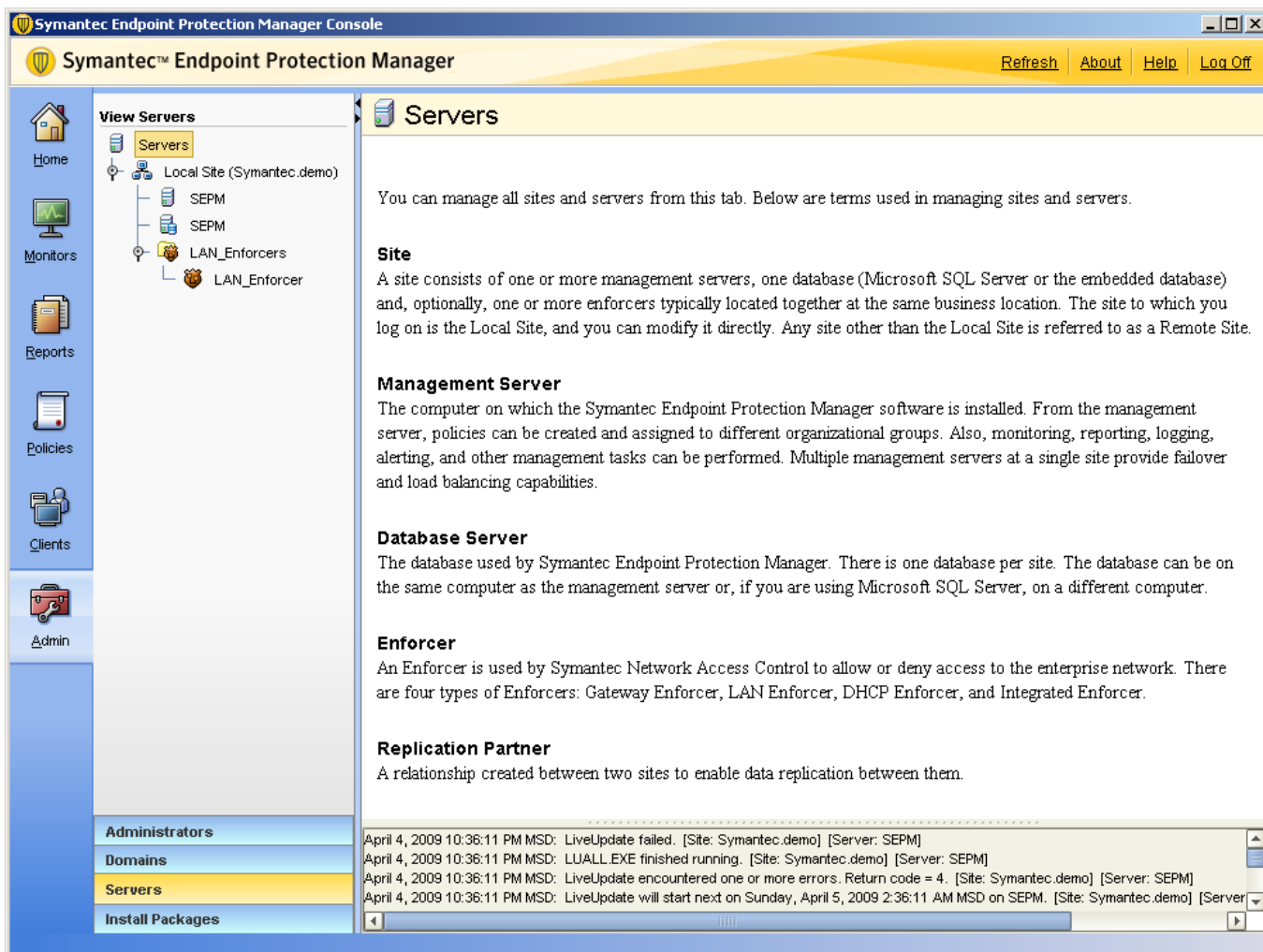
На коммутаторе, порты, к которым могут подключаться пользователи, настроены на аутентификацию по протоколу 802.1x. Как только компьютер подключается к сети, коммутатор сообщает LAN-Enforcer о появлении нового устройства. LAN-Enforcer, на основе данных, полученных от агента, установленного на ноутбуке, и на основе политик, заданных в Symantec Endpoint Protection Manager, принимает решение, что делать с подключившимся ноутбуком, и передаёт управляющие команды коммутатору. А коммутатор, соответственно, эти команды исполняет, и помещает ноутбук или в заданный VLAN или просто закрывает порт, в зависимости от политик.

Необходимо добавить, что LAN-Enforcer будет являться RADIUS-сервером для сетевых устройств, к которым подключаются пользователи.

В варианте с LAN-Enforcement, существует два режима работы: Transparent mode и Full mode. Различие между этими режимами в том, что когда мы используем Transparent mode мы можем реализовать только аутентификацию компьютера с установленным агентом и проверку на соответствие заданным политикам, но не можем реализовать проверку пользователя, который аутентифицировался на данном компьютере. При этом нам не требуется какой-либо внешний RADIUS. В режиме Full mode, помимо аутентификации компьютера и проверки на соответствие политикам мы можем так же реализовать проверку пользователя, который аутентифицировался на компьютере. Однако, для аутентификации пользователей нам потребуется внешний RADIUS-сервер.

Теперь перейдём от теории к практике. Для начала необходимо установить LAN-Enforcer и подключить его к Symantec Endpoint Protection Manager. В консоли SEPM должен появиться LAN-Enforcer, в той группе, которую Вы задали при настройке LAN-Enforcer. В нашем случае, группа называется LAN-Enforcers.

Рисунок 35.



Открываем свойства данной группы. В свойствах мы можем настроить следующие параметры:

- Вкладка **General**: здесь мы можем изменить имя группы, порт, по которому коммутаторы могут обмениваться данными с Enforcer-устройствами, входящими в группу, можем добавить описание группы.
- Вкладка **RADIUS Server Group**: на данной вкладке необходимо добавить как минимум одну запись. Если Вы работаете в Full mode, то необходимо указать хотя бы один внешний RADIUS Server, который будет отвечать за аутентификацию пользователей (например, мы использовали стандартную службу IAS, входящую в состав Windows Server). Если Вы работаете в Transparent mode, то хотя бы одну RADIUS Server Group создать придётся, а вот RADIUS-серверы можно или не указывать, или указать несуществующие, так как в Transparent mode не предусмотрена аутентификация пользователей, и к каким либо внешним серверам обращений не будет.
- Вкладка **Switch**: здесь создаются политики для коммутаторов в сети. Создание новой политики мы рассмотрим подробнее ниже.
- Вкладка **Advanced**: на данной вкладке мы можем указать два параметра, **Allow Legacy Clients** – разрешаем аутентификацию «старых» клиентов, то есть клиентов Sygate Enterprise Protection, и **Enable Local Authentication** – разрешаем локальную аутентификацию на Enforcer.
- Вкладка **Log Settings**: как Вы догадались, на данной вкладке производятся настройки журнала отчётности.

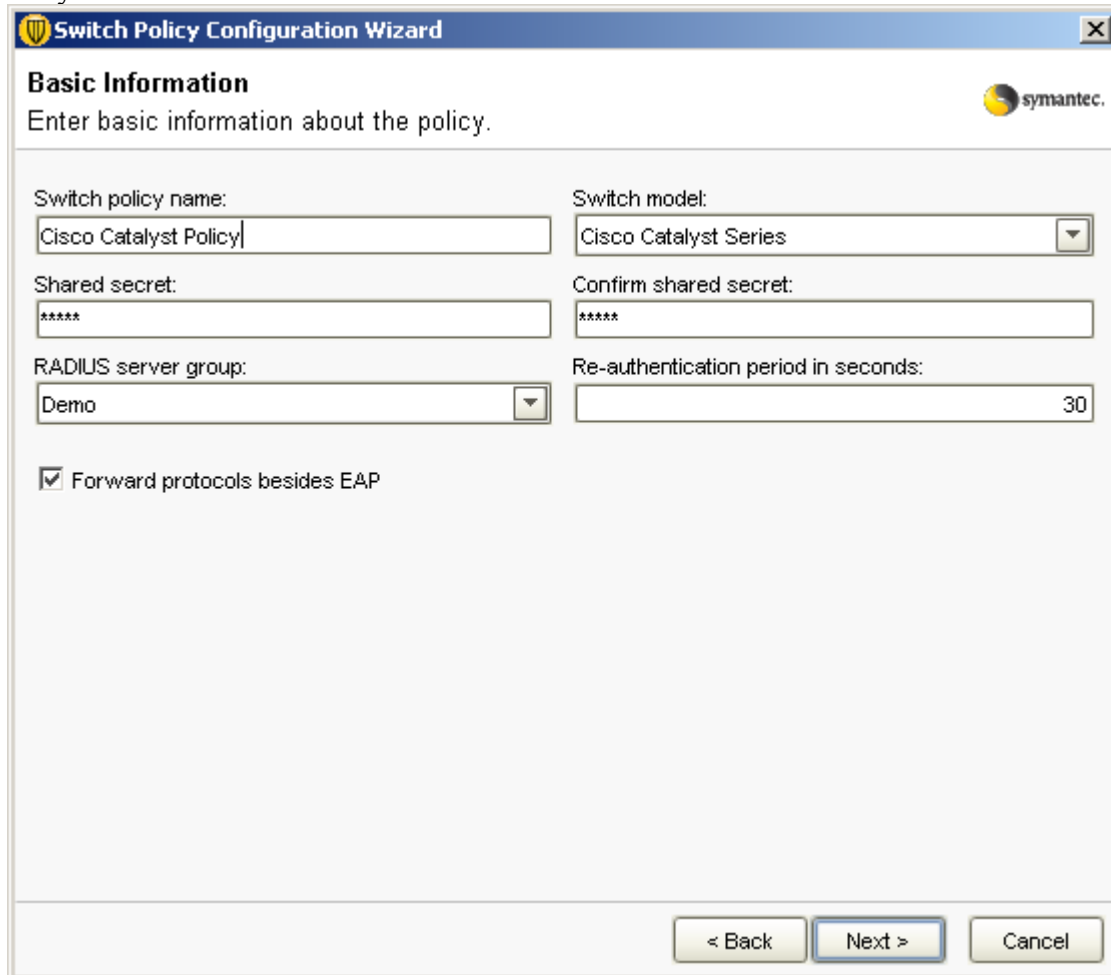
Остановимся подробнее на создании политики для коммутатора на вкладке **Switch**. Для создания новой записи, нажимаем кнопку **Add**, после чего запустится мастер настройки политики коммутаторов. Если Вы не создали ни одной RADIUS Server Group, то вместо запуска мастера, Вы



получите сообщение об ошибке, по этому перед созданием новой политики, создайте хотя бы одну RADIUS Server Group.

Итак, запустился мастер настройки политики коммутаторов. В окне Basic Information необходимо указать имя политики, модели коммутаторов, к которым данная политика будет применяться, ключ шифрования для доступа по RADIUS (RADIUS shared key), так же указать RADIUS Server Group и период реаутентификации сетевых устройств.

Рисунок 36.



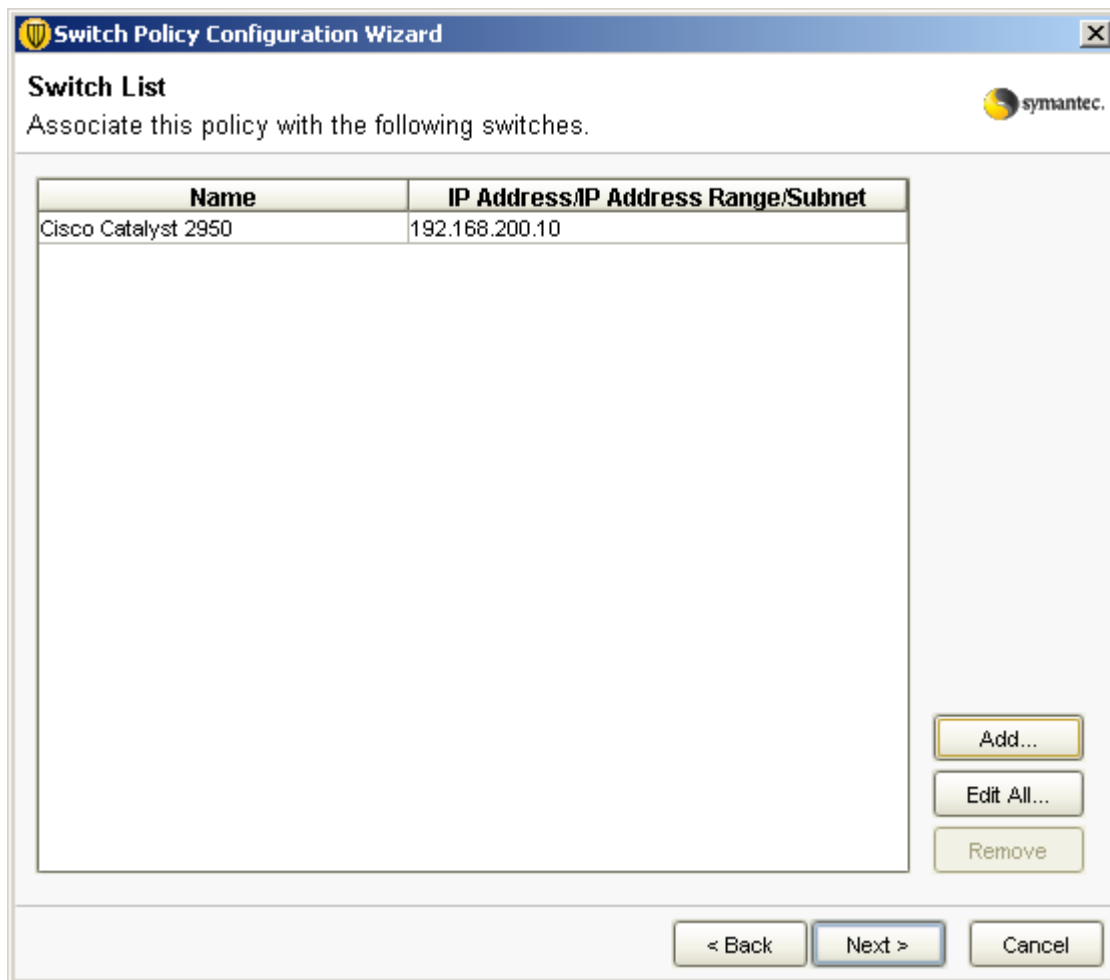
The screenshot shows the 'Switch Policy Configuration Wizard' window, specifically the 'Basic Information' step. The window title is 'Switch Policy Configuration Wizard' and it features the Symantec logo. The instructions read: 'Enter basic information about the policy.' The form contains the following fields and controls:

- Switch policy name:** Text input field containing 'Cisco Catalyst Policy'.
- Switch model:** Dropdown menu showing 'Cisco Catalyst Series'.
- Shared secret:** Password input field with six asterisks.
- Confirm shared secret:** Password input field with six asterisks.
- RADIUS server group:** Dropdown menu showing 'Demo'.
- Re-authentication period in seconds:** Text input field containing '30'.
- Forward protocols besides EAP**

At the bottom of the window, there are three buttons: '< Back', 'Next >', and 'Cancel'.

В окне Switch List необходимо указать IP адреса сетевых устройств, которые будут управляться данной политикой. По аналогии с Microsoft IAS – нам необходимо указать IP-адреса RADIUS клиентов.

Рисунок 37.

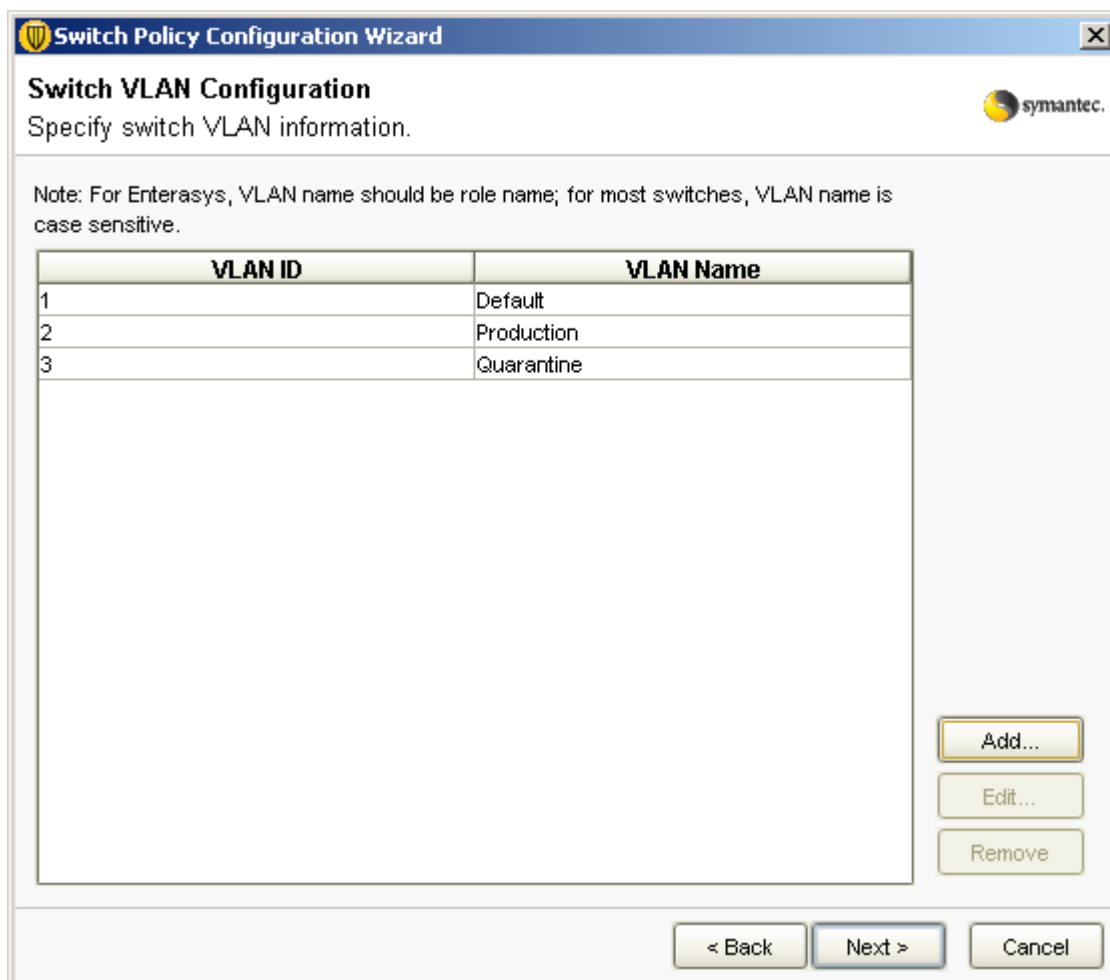


В окне Switch VLAN Configuration, указываются VLAN который присутствуют на сетевых устройствах, указанных на предыдущем шаге, и которые будут использоваться в создаваемых политиках. Например, у нас есть 3 VLAN:

- Default ID 1 все порты по умолчанию находятся в этом VLAN, доступ к каким либо сервисам в в этом VLAN отсутствует.
- Production ID 2 это VLAN, в котором находятся все сервисы, необходимые для работы - то есть, можно сказать, что это рабочий VLAN.
- Quarantine ID 3 это VLAN, в котором есть доступ только к серверам обновлений.

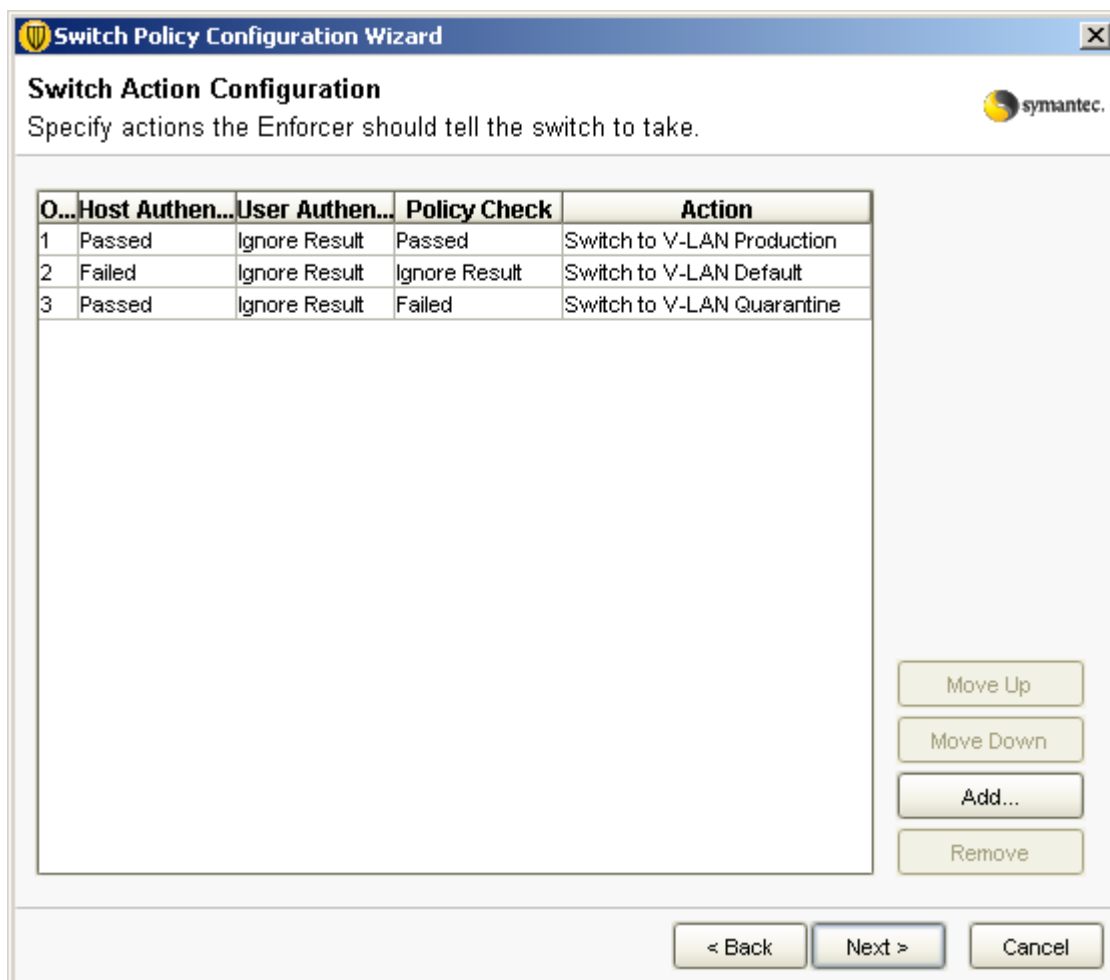
Следовательно, нам необходимо создать 3 записи, которые будут содержать имя VLAN и его ID. Имена и номера создаваемых VLAN, должны полностью совпадать с настройками сетевого оборудования.

Рисунок 38.



В окне Switch Action Configuration указываются действия, которые необходимо выполнять сетевым устройствам в зависимости от результатов проверки на соответствие корпоративным политикам. Например, если компьютер аутентифицирован и прошёл проверку соответствия корпоративным политикам, то необходимо переместить порт, к которому подключён компьютер, в Production VLAN. Аналогично создаются другие действия для остальных вариантов событий.

Рисунок 39.



Теперь все необходимые настройки выполнены. Обращаю внимание, что выше Мы рассмотрели только настройки для Transparent mode, так как не учитывали аутентификацию пользователей.

### ***Настройка коммутатора Cisco Catalyst.***

Выше мы рассмотрели настройку компонентов решения, за которые отвечает Symantec. Однако, как уже упоминалось, для реализации LAN-Enforcement нам необходимо произвести некоторые настройки на сетевом оборудовании. Итак, при сборке стенда мы использовали коммутатор Cisco Catalyst 2950, который поддерживает протокол аутентификации 802.1x. На данном коммутаторе необходимо произвести некоторые настройки.

Перейдём в административный режим работы с коммутатором:

```
Switch2950> enable
```

Перейдём в контекст конфигурирования коммутатора:

```
Switch2950# configure terminal
```

Укажем, что для аутентификации по 802.1x мы будем использовать RADIUS сервер:

```
Switch2950(config)# aaa new-model
```

```
Switch2950(config)# aaa authentication dot1x default group radius
```

```
Switch2950(config)# aaa authorization network default group radius
```

```
Switch2950(config)# dot1x system-auth-control
```

Укажем настройки для связи с RADIUS сервером, в роли которого выступает LAN-Enforcer. Из схемы (Рисунок 1.) видно, что IP-адрес LAN-Enforcer 192.168.200.3 :

```
Switch2950(config)# radius-server host 192.168.200.3 auth-port 1812 acct-port 1813
```

```
Switch2950(config)# radius-server retransmit 10
```

```
Switch2950v# radius-server key 12345
```

Теперь необходимо настроить порты коммутатора:

```
Switch2950(config)# interface FastEthernet 0/1
Switch2950(config-if)# switchport mode access
Switch2950(config-if)# dot1x port-control auto
Switch2950(config-if)# dot1x timeout reauth-period 10
Switch2950(config-if)# dot1x reauthentication
Switch2950(config-if)# spanning-tree portfast
```

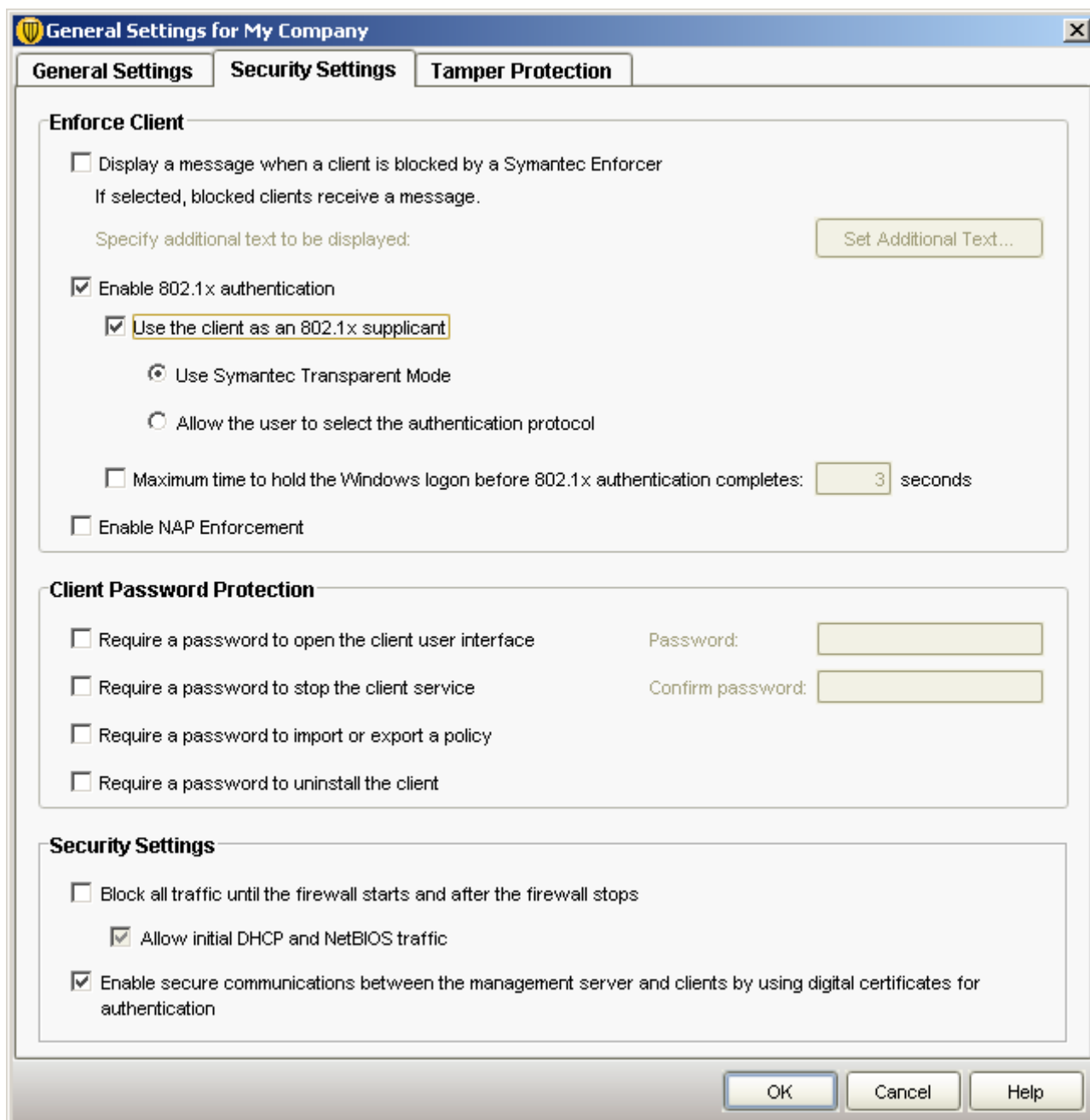
Эти настройки необходимо проделать для каждого порта, к которому могут подключаться пользовательские компьютеры.

На этом настройка коммутатора закончена.

### ***Настройки клиента.***

Основные настройки для серверной части SNAC выполнены, и теперь необходимо указать клиенту, то есть агенту SNAC, что ему необходимо проходить аутентификацию по протоколу 802.1x. Для этого перейдём в раздел Clients, далее переключаемся на вкладку Policies. На вкладке в разделе Settings нажимаем на ссылку General Settings, откроется окно «General Settings for ...». В открывшемся окне переходим на вкладку Security Settings. Ставим галочку «Enable 802.1x authentication», далее ставим галочку «Use the client as an 802.1x supplicant», выбираем пункт «Use Symantec Transparent Mode». (в случае, если мы ходим проводить аутентификацию пользователей, то нам необходимо выбрать пункт «Allow the user to select the authentication protocol», после чего нам необходимо будет сделать дополнительные настройки).

Рисунок 40.



Теперь осталось самое простое – установить SEP на клиентские компьютеры. Это можно сделать несколькими способами:

- Поиск в сети компьютеров по IP-адресам или имени. Установка производится из консоли управления Symantec Endpoint Protection Manager. Перейдём в раздел Clients, в разделе Tasks выберем пункт Find Unmanaged Computers. В открывшемся окне указываем диапазон IP-адресов для сканирования или имя компьютера и учётные данные пользователя, который обладает правами установки программного обеспечения на клиентских компьютерах. После того, как будут найдены компьютеры в указанном диапазоне, выбираем те из них на которые ходим установить SEP, и нажимаем Start Installation.
- Импорт компьютеров из Active Directory. Установка производится из консоли управления Symantec Endpoint Protection Manager. Для импорта компьютеров из Active Directory необходимо сначала настроить LDAP Server – для этого в разделе Clients, в разделе Tasks выбираем ссылку Import Active Directory or LDAP Users и производим необходимые настройки. После настройки LDAP, в разделе Tasks нажимаем на ссылку Import Organizational Unit or Container и производим импорт необходимых компьютеров.

- Ручная установка. Установка производится локально на клиентском компьютере. Перед ручной установкой необходимо выгрузить установочный пакет на диск. Для этого перейдем в раздел Admin, далее выберем пункт Install Packages. Из списка доступных пакетов выбираем тот, который хотим выгрузить, нажимаем правую кнопку мыши и из контекстного меню выбираем пункт Export. В появившемся окне указываем необходимые настройки и нажимаем Ok. После этого выгруженный пакет можно распространять на клиентов.

После установки SEP клиента на компьютер, желательно его перезагрузить. В случае успешной установки полнофункционального клиента SEP его окно должно выглядеть следующим образом:

Рисунок 41.



### *Гостевой доступ.*

Под гостевым доступом мы подразумеваем предоставление доступа к сети компьютерам, которые не управляются нашим Symantec Endpoint Protection Manager. Следовательно мы не можем проверить состояние этих компьютеров, установленное и запущенное программное обеспечение и т.д. - то есть, не можем проверить эти компьютеры на соответствие сетевым политикам, которые применяются в нашей организации.

Компания Symantec предложила для проверки гостевых компьютеров использовать загружаемый Java или ActiveX компонент, который после загрузки на компьютер может произвести его проверку и предоставить Symantec Endpoint Protection Manager требуемые данные для принятия решения о доступе в сеть. К сожалению, данный функционал реализован только на Gateway Enforcer - поэтому для реализации гостевого доступа клиент должен подключаться к сети через Gateway Enforcer. В нашем стенде данный функционал реализован для WiFi сети, и если пользователь, у которого агент SNAC не установлен, попытается получить доступ к внутренним ресурсам сети, то ему будет предложено скачать SNAC-агента, после чего будет произведена проверка компьютера и будет принято решение о предоставлении компьютеру доступа в сеть. Для настройки гостевого доступа необходимо зайти в консоль Gateway Enforcer, для перехода в контекстное меню настройки гостевого доступа в командной строке вводим:

*Enforcer# on-demand*

Затем указываем домен, с которым работает Symantec Endpoint Protection. Домен можно посмотреть в консоли Symantec Endpoint Protection, в разделе Admin, выбрать пункт меню Domains. Вы увидите перечень всех доменов, (по умолчанию в списке содержится один домен с именем *Default*). При указании домена в консоли Gateway Enforcer соблюдайте написание больших и маленьких букв в имени домена.

```
Enforcer(on-demand)# spm-domain name Default
```

Теперь необходимо указать в какую группу будут попадать гостевые пользователи - для этого необходимо ввести команду:

```
Enforcer(on-demand)# client-group "My Company/Guests"
```

Теперь можно включить гостевой доступ, для этого вводим:

```
Enforcer(on-demand)# enable
```

Гостевой доступ настроен.

### ***Небольшой итог.***

В данной статье мы постарались рассказать про подход компании Symantec к реализации технологии NAC, а также постарались описать некоторые настройки и технические подробности, которые пригодятся Вам при тестировании/внедрении SNAC.

Для того, чтобы понять, как работает SNAC и как Вы можете применить его у себя в организации, попробуйте развернуть SNAC Self-Enforcement – это не потребует никаких изменений в Вашей инфраструктуре, больших финансовых и трудовых затрат.