# 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 802.1х, 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 происходить 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».

ymantec Endpoint Protection Installation Program	
	Symantec.
Symantec <sup>™</sup> Endpoint Protection     Symantec <sup>™</sup> Endpoint     Symantec <sup>™</sup> Endpoint	n
Read This First Before installing or migrating, click here to view important information.	
Install Symantec Endpoint Protection Manager Installs the management server and console, and deploys managed clients.	
Install Symantec Endpoint Protection Client	

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

После завершения установки запуститься программа конфигурирования Symantec Endpoint Protection Manager.

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



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

Рисунок 4.

Management Server Configu	iration Wizard
Symantec.	Approximately how many computers will be managed by this management server? <ul> <li>Less than 100</li> <li>Between 100 and 500</li> <li>Between 500 and 1,000</li> <li>More than 1,000</li> </ul>
	< Back Next > Cancel

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.

Management Server Configu	iration Wizard
	<ul> <li>What would you like to do?</li> <li>Install my first site (what is a site?) Installs a new site with a management server and a database (For first-time users only).</li> <li>Install an additional management server to an existing site Installs an additional management server that you can configure for failover or load balancing.</li> <li>Install an additional site Installs a management server and a database for replication.</li> <li>To continue, click Next.</li> </ul>
Symantec.	
	< Back Next > Cancel

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.			
🔘 Management Server Configu	ration Wizard		
	Specify the server for the management	name, port number, web console port, a t server you want to install or configure	ınd data folder
	Server name:	БЕРМ	
	Server port:	8443	
	Web console port:	9090	
	Server data folder:	C:\Program Files\Symantec\Syman	Bro <u>w</u> se
Symantec.			
		< Back Next >	Cancel

Вводим имя для нашего создаваемого сайта: «Symantec.demo» Рисунок 7.

🔘 Management Server Configu	uration Wizar	d			
	What do you	u want to name	this site?		
V	Site name:	Site SEPM			
Symantec.					
			<u> </u>		
8			< <u>B</u> ack	<u>N</u> ext >	Cancel

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.

Management Server Configu	iration Wizard		
symantec.	The management server and clier each other. You will need to crea it in the event of disaster recover Create encryption password: Confirm encryption password:	nt computers encrypt the data t ate an encryption password bel y. ******	hey send ow and enter
		< Back Next >	Cancel

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».

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.

Management Server Configu	iration Wizard
symantec.	Do you want to create a new Symantec Endpoint Protection Manager database or use an existing database? © Create a new database © Use an existing database
<u> </u>	
	< Back Next > Cancel

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.	•	
🛑 Management Server Config	uration Wizard	
	Specify the database pa Microsoft SQL Server da	arameters to use in order to create the new atabase.
	SQL server port:	1433
	Database name:	sem5
	Authentication:	SQL Server Authentication
	User:	sem5
	Password:	*****
	Confirm password:	******
	DBA user:	sa
	DBA password:	*****
	SQL Client folder:	C:\Program Files\Microsoft SQL Server\90\Tools\
Symantec.	Database data folder:	SQL Server/MSSQL.1/MSSQL/DATA
		< Back Next > Cancel

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

Рисунок 12.

Management Server Configu	ration Wizard		
Management Server Configu	rration Wizard Create a system adminis log on to the managemen User name: Password: Confirm password: Email address:	trator account. The password will nt console. admin ******* ****** admin@symantec.jiemo	pe required to
Symantec.			
		< <u>B</u> ack <u>N</u> ext >	Cancel

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

I NCYHOK 15.			
💭 Management Server Config	uration Wizard		
	Create a system adminis log on to the managemer	trator account. The password will b nt console.	e required to
	User name:	admin	
	Password:	*****	
	Confirm password:	*****	
Creating Databa		× –	
The database i minutes. Starting syncC	s being created and initialize atalog	d. This will take a few	
Symantec.			
		< <u>B</u> ack <u>N</u> ext >	Cancel

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

Рисунок 14.

🖤 Management Server Configuration Wizard		
	Management Server Configuration Wizard Completed	
	This management server has been successfully configured.	
	Note that installing Symantec Endpoint Protection Manager does not install the Symantec Endpoint Protection client on this computer. You should also install the Symantec Endpoint Protection client.	
	The Migration and Deployment Wizard will walk you through the steps to migrate from Symantec AntiVirus. It will also assist in deploying the client software, whether you are migrating or not.	
	You can run this wizard at a later time by selecting it from the Start menu.	
	Do you want to run the Migration and Deployment Wizard now?	
	O <u>Y</u> es	
	© <u>No</u>	
Symantec.		
	< Back Einish Cancel	

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

Symantec Endpoint Protection Manager Console	
	Symantec.
<b>Operation Symantec™Endpoint</b> Protection Manager	
User name: admin	
Password: ******	
Server: localhost:8443	<b>T</b>
Log On Exit Option	< < 2
Copyright © 2007-2008 Symantec Corporation. All rights reserved.	

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

ntec™ Endpoint	Protection Mana	ger			Refresh	About
Security Status		Preferences	Virus Definitio	ns Distribution	: Last 12 Hours	
	Status - Good	Freierences	Display: Virus Defi	initions Distribution		
U Security :	510103 - 000u	More Details	Definitions	Computers		
Action Summary	by Detection Count					
Action	Viruses	Security Risks				
Cleaned	0	0				
Suspicious	0	0				
Blocked	0	0				
Quarantined	0	0				
Deleted	0	0				
Newly Infected	0	0	Latest Symantec	Version: 2009-03	3-26 rev. 065	
Still Infected	0	0	Latest Manager V	rersion: Informatio	on is currently unavailable	
<b>Risks Per Hour: L</b>	ast 12 Hours		Security Resp	onse	Last updated: 03/27/2009-16:	41:56
Display: Risks	-		Top Threats	L	_ast outbreak change: 04/04/2007 03:0	8:00
0			Latest Threats » Noitems There are no cat Syman Le	e to display egory 3 or greater <b>tec ThreatCor</b> vel 1: Normal	threats in the wild at the moment. Security Alerts Symantec Definitions Latest Threats Security Focus	
Status Summary	Com	nuters	Watched Appl	ications Sumn	nary	
Antivirus Engine Off	Com	0	Commercial Applicat	tion Detection	Occurrences	
Auto-Protect Off		0	Forced TruScep Pro	active Threat Dete	ection 0	
Tamper Protection Off		0	F Sicca Hassairrie	A The Car Dele	0	
Restart Required		0	Favorite Repo	rts 🜵		
Host Integrity Failed		0	Top Sources of Atta	ack		
Not Reporting Status		0	Top Risk Detections	Correlation		
			TruScan Proactive 1	Fhreat Distribution		

# 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 отсутсвовать: Рисунок 17.

🔘 Symant	ec Endpoint Protection Manager Cons	ole				_ 🗆 X
🔘 Syı	mantec™ Endpoint Protection	n Manager		Refresh	About Help	Log Off
	View Policies	U Antivirus and Antisp	yware Policies			
Home	Antivirus and Antispyware	Name		Description	Location U	lse Count
	Intrusion Prevention	Antivirus and Antispyware policy	Recommended policy for m	ost environments, providing a good balan	·	2
<u> </u>	Application and Device Control	Antivirus and Antispyware policy - High S	High security policy that ma	y affect the performance of other applica	ti	0
<u>M</u> onitors	<ul> <li>Q LiveUpdate</li> <li></li></ul>	Antivirus and Antispyware policy - High P	Higher performance policy,	but with reduced security. Relies on File	S	0
Reports	Policy Components					
Policies						
Clients						
	Tasks					
لکی	Add an Antivirus and Antispywa					
<u>A</u> dmin	Mimport an Antivirus and Antispyw					
	🔍 Search for Applications					
		Recent changes appear below:				
		Description		Time	Adminis	strator
		Add shared policy upon system install		March 27, 2009 4:08:29 PM MSK	admin	
		Add shared policy upon system install Add shared policy upon system install		March 27, 2009 4:08:29 PM MSK March 27, 2009 4:08:29 PM MSK	admin admin	
		The shared policy upon system install		march 21, 2000 4.00.201 m molt	Jan	

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.

🍪 Symantec Endpoint Protection Installation Program	_ 🗆 X
S S	mantec.
Symantec <sup>™</sup> Network Access Control	
Read This First	
Before installing or migrating, click here to view important information.	
Install Symantec Network Access Control	
Installs network access control clients, management, and reporting components.	
Install Other Administrator Tools	
Installs optional advanced management components.	
Exit	

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

mantec Endpoint Protection Installation Program	
	symantec.
Symantec <sup>™</sup> Network Access Control	
Install Symantec Endpoint Protection Manager Installs the management server and console, and deploys managed clients.	
Install Symantec Network Access Control Installs network access control to client computers.	
Return to Main Menu	

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

Рисунок 20.

Management Server Upgrade		
	Welcome to the Management Server Upgrade Wizar This wizard helps you upgrade the management server from a previous version. You should back up the database before proceeding. - Upgrade Server from 11.0.2.0 - Run backup before running the upgrade tool.	d
	< Back Next > Cancel	

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.

Management Server Upgrade		
	Server upgrade status	
	100%	
	InitializingDone Database already has the latest schema Importing Packages Adding SNAC52Done Adding SNAC64Done Upgrading templatesDone Upgrade Succeeded	
	< Back Next > Cance	91

В следующем окне нажимаем «Finish» и завершаем установку: Рисунок 22.

🛑 Management Server Upgrade		- 🗆 🗵
	Upgrade Succeeded	
	WARNING: Installing Symantec Endpoint Protection Manager does i install Symantec Endpoint Protection or any other protection technology. To protect the computer on which Symantec Endpoint Protection Manager is installed, you must also install Symantec Endpoint Protection client software.	not
	☑ Start the Symantec Endpoint Protection Manager Service	
	☑ Start the Symantec Endpoint Protection Manager Console	
	< Back Finish Cancel	

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.

🔘 Symante	ec Endpoint Protection Manager Cons	sole					
🔘 Syn	nantec™ Endpoint Protection	n Manager		E	Refresh Abo	ut Help	Log Off
	View Policies	🗐 Host Integrity Policie	s				
<u>H</u> ome	<ul> <li>Antivirus and Antispyware</li> <li>Firewall</li> </ul>	Name Host Integrity policy	Created automatically during	Description		Location Us	se Count
Monitors	Intrusion Prevention     Application and Device Control     Host Integrity     LiveUpdate     Control LiveUpdate	Those in itegen ky policy		g product in istanialion.			
Reports	Policy Components						
Policies							
Clients							
Admin	Add a Host Integrity Policy  Add a Host Integrity Policy  Search for Applications						
		Recent changes appear below:					
		Description		Time		Administ	trator
		Add shared policy upon system install		March 27, 2009 4:08:29 PM M	SK a	dmin	

## 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 RADUIS серверам, например для проверки аутентификации пользователей, или для проверки аутентификации сетевых устройств.

<u>Среда применения политик.</u> В реализации Symantec NAC существует 4 варианта среды применения политик:

- 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-Enforcemet применение политики на уровне сетевых устройств поддерживающих протокол 802.1х, 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 входя в систему используем следующие учётные данные:

Login: root

Password: symantec

Сразу же запуститься 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: [G]ateway Enforcer [D]HCP Enforcer [L]AN 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 применяться – 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\_AДРЕС\_SEPM\_CEPBEPA – указываем IP-адрес сервера SEPM Enforcer(configure)# spm name DNS\_ИМЯ\_SEPM\_CEPBEPA – 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\_В\_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»...



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:

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.

🔍 Custom Requirement	<u>x</u>
Name: Custom requirement 1	
Name: Custom requirement 1  Customized Requirement Script  //Insert statements below:  //IF  //Insert statements here: //Insert statements here: //IL  END IF PASS	Select a condition: Utility: Process is running  Check if the following process is running.  Process file name (For example, cmd.exe or c:\windows\cmd.exe): notepad.exe
Add Delete	OK Cancel Help

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

🗐 Host Integrity	Requirements		
Policy	When should Host Integrity checks be ru	n on the client?	
	Always do Host Integrity checking		-
	O Only do Host Integrity checking through t	the Gateway or DHCP Enforcer	
Idvanced Settings	O Oply do Host Integrity checking when co	ponected to the management server	
	C Never do Host Integrity checking		
	Requirements:		
	Enable	Name	
		don't start notepad.exe	
		Antivirus must be installed and running	
	Add Template	Edit Delete Move Up Move Down	
			 1

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 Му Company:

Рисунок 30.

🔲 Assign Host Integrity Policy	×
Host Integrity Policy: Demo Policy	
Assian Policy	_
The tree below shows the groups or locations to which you can assign the selected Host Integrity Policy. Select the groups or locations below. To select all subgroups and locations, right-click the parent group and choose Select All Subgroups. Groups and locations with a check mark already have a Host Integrity Policy assigned to them.	
Caution	
Clicking Assign will assign this Host Integrity Policy to all selected groups or locations, replacing the existing Host Integrity Policy they are currently using	
P       Integrity Policy triey are currently using.         P       Image: A structure of the parent group [inherit from the parent group]         Image: A structure of the parent group [inherit from the parent group]	
Assign	

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 SEPM это правило позволит в обмениваться данными между клиентским SEP и сервером SEPM.
- 2. Заблокировать весть трафик.

Таким образом, если наш компьютер не пройдёт 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 SEPM.

Для создания политики, заходим в консоль управления SEPM, переходим в раздел «Clients», затем переключаемся на вкладку «Policies» и напротив надписи «Quarantine Policies when Host Integrity Fails:» нажимаем «Add a policy…». Появиться 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. Firewall Policy × Firewall Rules Maximize Window Policy Rules Notifications Overview Firewall Rules Rules Firewall rules allow, block, and log network traffic. You can add higher priority rules above the blue line in the table below. Those rules ca Smart Traffic Filtering Traffic and Stealth Settings Inherit Firewall Rules from Parent Group Peer-to-Peer Authentication Settings No En... Name Severity Application Host Time Service Adapter Screen ... Action Logging 1 🔽 🔚 Allow SEPM 5-Major 🐮 Any 2 🔽 🖹 Block All 5-Major 🐮 Any 12 Any 22 Any 23 Any 12 All Ada... 22 Any 10 Allow = None 12 Any 23 Any 23 Any 13 All Ada... 23 Any 10 Block = None Add Blank Rule Add Rule. Delete ► OK Cancel Help

После создания политики, в консоли SEPM у Вас должно появиться созданное правило в paзделе «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 SEPM 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.

🔘 Symant	🔍 Symantec Endpoint Protection Manager Console						
🕕 Syn	mantec™ Endpoint Protection	n Manager		<u>Refresh</u>	<u>About</u>	<u>Help</u>	<u>Loq Off</u>
	View Servers	🕞 Management	Server				
Home	🧊 Servers 🖗 🎩 Local Site (Sepmisite)						
	- 🗐 sepm	Name:	GW_Enforcers				
<u> </u>	— 🔒 sepm	Description:					
<u>M</u> onitors	P-L  GW_Enforcers	Creation Time:	Wednesday, March 11, 2009 3:06:26 PM MSK				
<b>A</b>	GVV_Enforcer	Last Modification Time:	Wednesday, March 11, 2009 6:06:40 PM MSK				
	LAN_Enforcers     Langer	Enforce Mode:	Enforce				
<u>R</u> eports	-						
F							
<u> </u>							
Policies							
eg							
Cliente							
Gients	Taeke						
	Edit Group Properties						
Admin	Delete Group						
Gamm	Export Group Properties						
	Import Group Properties						
	Administrators	March 17, 2000 40:42:52, 41444	No. Sustan aliast aguar achidu laga kara kara aguart 10% a Cara	atel Course	conml		
	Domains	March 17, 2009 10:43:52 AM M3 March 17, 2009 10:01:34 AM M3	<ul> <li>Set of the server activity logs have been swept. [Site: Seph.]</li> <li>SK: Retry timestamp is over the maximum retry window, switching to</li> </ul>	regular sched	sepmj lule run. [:	Site: Sep	m site] [S
	Servers	March 17, 2009 9:55:34 AM MS March 17, 2009 9:55:34 AM MS	K: LiveUpdate retry failed. Will try again. [Site: Sepmisite] [Server: si K: LUALL.EXE finished running. [Site: Sepmisite] [Server: sepmi]	epm]			
	Install Packages	•					Þ

## 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 802.1х - 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 802.1х. 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 RADUIS-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 RADIUSсервер.

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.

() Symant	ec Endpoint Protection Manager Con	sole
🔘 Syr	nantec™ Endpoint Protectio	n Manager Refresh About Help Log Off
	View Servers	🗐 Servers
Home Monitors Reports	Servers - Servers - SEPM -	You can manage all sites and servers from this tab. Below are terms used in managing sites and servers. <b>Site</b> A site consists of one or more management servers, one database (Microsoft SQL Server or the embedded database) and, optionally, one or more enforcers typically located together at the same business location. The site to which you log on is the Local Site, and you can modify it directly. Any site other than the Local Site is referred to as a Remote Site. <b>Management Server</b> The computer on which the Symantec Endpoint Protection Manager software is installed. From the management
Policies		The computer on which the Synantec Endpoint Protection Manager Software is instance. From the management server, policies can be created and assigned to different organizational groups. Also, monitoring, reporting, logging, alerting, and other management tasks can be performed. Multiple management servers at a single site provide failover and load balancing capabilities. <b>Database Server</b> The database used by Symantec Endpoint Protection Manager. There is one database per site. The database can be on
Admin		the same computer as the management server or, if you are using Microsoft SQL Server, on a different computer. Enforcer An Enforcer is used by Symantec Network Access Control to allow or deny access to the enterprise network. There are four types of Enforcers: Gateway Enforcer, LAN Enforcer, DHCP Enforcer, and Integrated Enforcer.
		<b>Replication Partner</b> A relationship created between two sites to enable data replication between them.
	Administrators	April 4, 2009 10:36:11 PM MSD: LiveUpdate failed. [Site: Symantec.demo] [Server: SEPM]
	Domains	April 4, 2009 10:36:11 PM MSD: LUALL.EXE finished running. [Site: Symantec.demo] [Server: SEPM] April 4, 2009 10:36:11 PM MSD: Livel Indate encountered one or more errors. Return code = 4. [Site: Symantec.demo] [Server: SEPM]
	Servers	April 4, 2009 10:36:11 PM MSD: LiveUpdate encountered one of more encors. Neturn code = 4. [Site: Symanice: definit] [Server, Schwi]
	Install Packages	

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 RADUIS 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 запуститься 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.		
🔫 Switch Policy Configuration Wizard		×
<b>Basic Information</b> Enter basic information about the policy.		Symantec.
Switch policy name: Cisco Catalyst Policy Shared secret: ***** RADIUS server group:	Switch model: Cisco Catalyst Series Confirm shared secret: ***** Re-authentication period in seconds:	
✓ Forward protocols besides EAP		
	< Back Next >	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.

Name	IP Address/IP Address Range/Subr	net
sco Catalyst 2950	192.168.200.10	
		0 alal
		Add
		Edit All
		Lone - million

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.

👿 Switch Policy Configuration Wi	zard	×
Switch VLAN Configuration Specify switch VLAN information	n.	Symantec.
Note: For Enterasys, VLAN name sho case sensitive.	uld be role name; for most switches, VLAN nam	ne is
VLAN ID	VLAN Name	
1	Default	
2	Production	
3	Quarantine	
		Add
		Edit
		Remove
		lext > Cancel

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.

`	Loct Authon	Lloor Authon	Doligy Chook	Action	7
<u>.</u>	Passed	lanore Result	Policy Check	Switch to V-LAN Production	-
	Failed	lanore Result	lanore Result	Switch to V-LAN Default	-
	Passed	Ignore Result	Failed	Switch to V-LAN Quarantine	_
					Move Up

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 802.1х. На данном коммутаторе необходимо произвести некоторые настройки.

Перейдём в административный режим работы с коммутатором: Switch2950> enable Перейдём в контекст конфигурирования коммутатора: Switch2950# configure terminal Vкажем, что для аутентификации по 802.1x мы будем использовать RADIUS сетвер: Switch2950(config)# aaa new-model Switch2950(config)# aaa authentication dot1x default group radius Switch2950(config)# aaa authentication network default group radius Switch2950(config)# dot1x system-auth-control Vкажем настройки для связи с RADUIS 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 802.1х. 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 802.1х 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.

😈 General Settings for My Company 🛛 🛛 🔀
General Settings Security Settings Tamper Protection
Enforce Client
Display a message when a client is blocked by a Symantec Enforcer
If selected, blocked clients receive a message.
Specify additional text to be displayed: Set Additional Text
✓ Enable 802.1× authentication
✓ Use the client as an 802.1× supplicant
O Use Symantec Transparent Mode
O Allow the user to select the authentication protocol
I Maximum time to hold the Windows logon before 802.1× authentication completes: 3 seconds
Enable NAP Enforcement
Client Password Protection
Require a password to open the client user interface Password:
Require a password to stop the client service     Confirm password:
□ Require a password to import or export a policy
☐ Require a password to uninstall the client
Security Settings
☐ Block all traffic until the firewall starts and after the firewall stops
Allow initial DHCP and NetBIOS traffic
Enable secure communications between the management server and clients by using digital certificates for authentication
OK Cancel Help

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 производиться локально на клиентском компьютере. Перед ручной установки необходимо выгрузить установочный пакет на диск. Для этого перейдем в раздел Admin, далее выберем пункт Install Packages. Из списка доступных пакетов выбираем тот, который ходим 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:



#### 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.