Stuart Wheeler
Swheele001
Original submission

Securing the mobile client with Symantec Client Security

Introduction

This paper will discuss how to protect the mobile client with Symantec Client Security from the current dangers caused by blended threats. It will look at the various components that can be implemented with this software and at the benefits of implementing an integrated client security solution as opposed to using point products. This paper will not advise on the best way to implement Symantec Client Security as this will differ for every organization.

What is Symantec Client Security?

Symantec Client Security is a manageable, integrated security solution for the client that provides more effective protection against complex Internet threats than traditional installations of independent products. Symantec Client Security includes client firewall, intrusion detection, content filtering, and anti-virus technologies. Short response times are provided via a single update mechanism, which combines virus definitions, intrusion detection signatures, and firewall rules for distribution to clients. These integrated products can all be managed from a single console, the Symantec Systems Console.
Symantec Client Security is suitable for protecting Windows 98/ME/NT/2000 and XP clients.

The need for mobile client protection

Corporate networks can no longer be described as having a clearly defined perimeter that can be protected at specific points. With the increase of mobile users and remote clients the corporate network has expanded beyond the protection of the corporate firewall and therefore has created new challenges to protect mobile clients.
It is no longer sufficient just to protect clients with an anti-virus solution as the latest blended threats have been designed to find and exploit system vulnerabilities. This increased client protection brings with it an increased cost of ownership which is also multiplied if the client is protected using point products from different vendors. To overcome this increased cost of ownership it is necessary to implement an integrated solution that can be easily managed from a central location.

Information on blended threats can be found at :-

http://www.fedcirc.gov/docs/ses_btcsac_wp.pdf
http://enterprisesecurity.symantec.com/flashfiles/BlendedThreats/blendedthreatsdemo.cfm?EID=0

What are we protecting against?

The threats that the mobile client faces are the same as the threats that are aimed at any company that is connected to the internet the only difference being is that the mobile/standalone client does not have the protection of the company firewall.
One of the biggest dangers is that an unprotected mobile client will be used from a home office or outside of the company to connect to the internet. It is possible that this client may unwittingly download some sort of malicious code of become infected with a virus while being used via an unprotected internet connection. This infected machine will then at some time be taken into the company whereby it could either infect other machines within the company or could provide a backdoor point of entry via an unwittingly downloaded Trojan Horse.

Components of Symantec Client Security

This section briefly describes the components of Symantec Client Security and their function.

Overview of Symantec Client Security

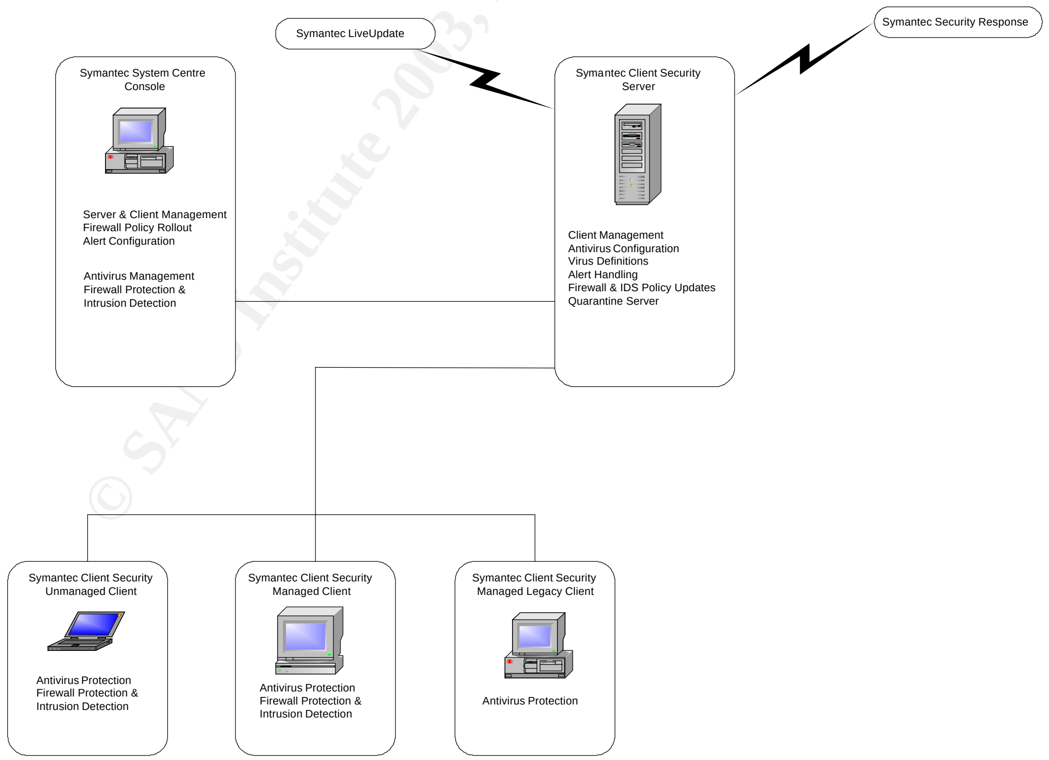


Figure 1

1. The Symantec System Centre Console

The Symantec System Center Console is used for management operations. If so wished the console can be used to for installing Symantec Client Security to workstations and network servers (Windows 2000/XP/NT and Netware). The primary function is however to update virus definitions, and manage network servers and workstations running Symantec Client Security
Symantec System Center management console runs on Windows NT/2000/XP Professional computers.

2. The Symantec Client Security server

The Symantec Client Security Server is used for pushing configuration and virus definitions file updates to Symantec Client Security clients.
It is also possible to push firewall and intrusion detection policies to Symantec Client Security firewall clients.
The machine on which it runs is also protected against viruses.

3. The Symantec Client Security client

Antivirus, firewall and intrusion protection is provided by the Symantec Client Security client for all networked (managed) and standalone (unmanaged) computers that are running Windows NT/2000/XP/98/ME

4. LiveUpdate

All clients or servers running Symantec Client Security can pull virus definitions and product updates from an internal LiveUpdate server or from the Symantec LiveUpdate server using LiveUpdate.

5. Alert Management Server

During the installation of the Symantec Client Security server the Alert Management Server is installed by default. The Alert Management Server can process various notifications sent by clients or servers and then initialize the following actions :-

- Start a program
- Send an SNMP trap
- Start a Netware NLM
- Message box
- Broadcast
- Send message to pager
- Send an SMTP mail
- Write to the Windows event log

6. Quarantine Server

If an infected file cannot be repaired by the current set of virus definitions it is moved to the local quarantine which is available on the client or server where Symantec Client Security is installed. It is possible to configure the client so that the virus can be forwarded to a central quarantine area (Quarantine Server). From here it can be automatically forwarded to Symantec Security Response for further analysis and repair.
There are two methods available for submitting viruses to Symantec Security Response :-

- Via HTTPS (fully automated submission)
- Email based (semi-automated submission)

7. Symantec Client Firewall Administrator

A tool for creating and modifying firewall and intrusion detection rules that can be deployed from a central location.

How to protect against threats

This section will deal with how to best guard against the various threats that a mobile client is confronted with and how to keep protection at its highest level with the various Symantec Client Security components that were described in the section "**Components of Symantec Client Security**". It is presumed that Symantec Client Security client has been correctly installed and that the Symantec System Centre Console and a Symantec Client Security Server have also been installed on their respective machines.

Protecting from Viruses

The most important aspect of protecting a computer against viruses is to have the most recent virus definitions installed. Symantec Client Security provides four methods of updating virus definitions but here we will deal with the two most important and widely used methods:-

a) Virus Definition Update Method
b) LiveUpdate

Virus Definition Update Method

This is method of distributing virus definitions is the default configuration for all clients after installation.
The primary server starts a push operation after it has received new definitions and distributes these definitions to all secondary servers and clients within its group. The primary server can be updated automatically or scheduled to download definitions from the Symantec LiveUpdate Server.

Some of the advantages of using this method are:-

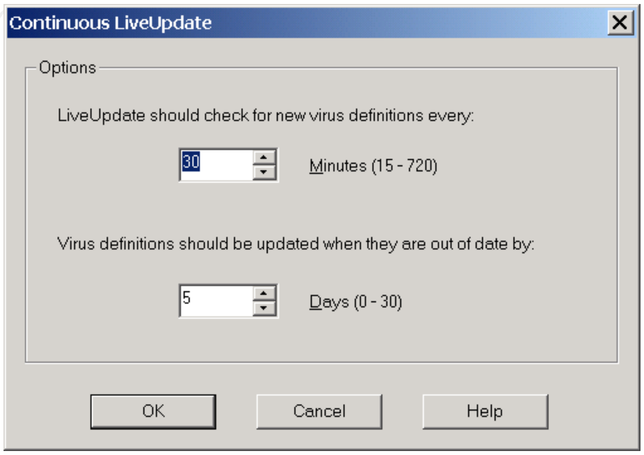
- It is only necessary to update one server to update all machines in the network.
- Minimal configuration required.
- Only the portion of the file that contains new data (microdefs 50 - 70K in size) is retrieved by the computer.
- VDTM can also distribute microdefs.

Information on how Symantec Client Security pushes microdefs can be found at :-

http://service1.symantec.com/SUPPORT/ent-security.nsf/docid/2002080815034048

LiveUpdate

LiveUpdate is included in almost all of Symantec's products including Symantec Client Security. This is an application which can be run to download virus definitions and program updates from either the Symantec LiveUpdate Server or from an internal LiveUpdate server and applies the updates/definitions on the machine it is running on.
Having the ability to obtain the most recent virus definitions was sometimes a problem for a mobile client.
Due to the fact that the mobile client is very often only connected to the company network periodically and only connected to the internet for a short period of time (usually for a period sufficient to replicate mail) and usually connected via a slow connection, the timeframe was not sufficient to download new virus definitions.
A workaround for this was to configure LiveUpdate to connect directly to the Symantec LiveUpdate Server and for the user to manually start LiveUpdate. The problem with this is that users are not always reliable and forget to update their definitions.
A new function of Symantec Client Security is Continuous LiveUpdate.
Continuous LiveUpdate allows for virus definitions updates for clients with an Internet connection, but infrequent or no connection to a parent server. It is possible to specify a maximum number of days after which definitions are out-of-date.
When definitions exceed the specified date, LiveUpdate is automatically initiated in silent mode when it detects an available Internet connection.


Continuous LiveUpdate

Options

LiveUpdate should check for new virus definitions every:

30 Minutes (15 - 720)

Virus definitions should be updated when they are out of date by:

5 Days (0 - 30)

Figure 2

Having the ability to obtain the most recent virus definitions was sometimes a problem for a mobile client.
Due to the fact that the mobile client is very often only connected to the company network periodically and only connected to the internet for a short period of time (usually for a period sufficient to replicate mail) and usually connected via a slow connection, the timeframe was not sufficient to download new virus definitions.
A workaround for this was to configure LiveUpdate to connect directly to the Symantec LiveUpdate Server and for the user to manually start LiveUpdate. The problem with this is that users are not always reliable and forget to update their definitions.
Continuous LiveUpdate in combination with the smaller microdefs solves the problem that mobile clients had with not always having the latest virus definitions and does away with having to rely on the user to manually update their definitions.

It is advisable to scan a computer as soon as it has received new definitions as viruses could be resident that were not detected by the Realtime Protection function with the previous definitions. If this procedure is always followed it will mean that the chances are considerably reduced that a virus remains undetected on any machine. This procedure should also be automated so that a scheduled scan is completed after newer definitions have been installed and that we again do not have to rely on the user to complete this task.

Configuring & Monitoring the Symantec Client Security Firewall

The Symantec Client Security Firewall can be configured so that the client is protected against unauthorized access when connected to the Internet, to detect hacker attacks and to protect personal information.
The task of configuring this firewall cannot be left to the user as this task is too complex for the average user to successfully complete and there is also a necessity for us to configure the client firewall to comply with our security policies which would most certainly not be the case if every user was allowed to configure their firewall independently.

Symantec Client Security offers the possibility to configure firewall policies and to distribute them from a central location. The policies are created and configured with the Symantec Client Firewall Administrator and can then be distributed from the Symantec System Console. This centralized firewall management provides a maximum of firewall protection with a minimal user involvement.

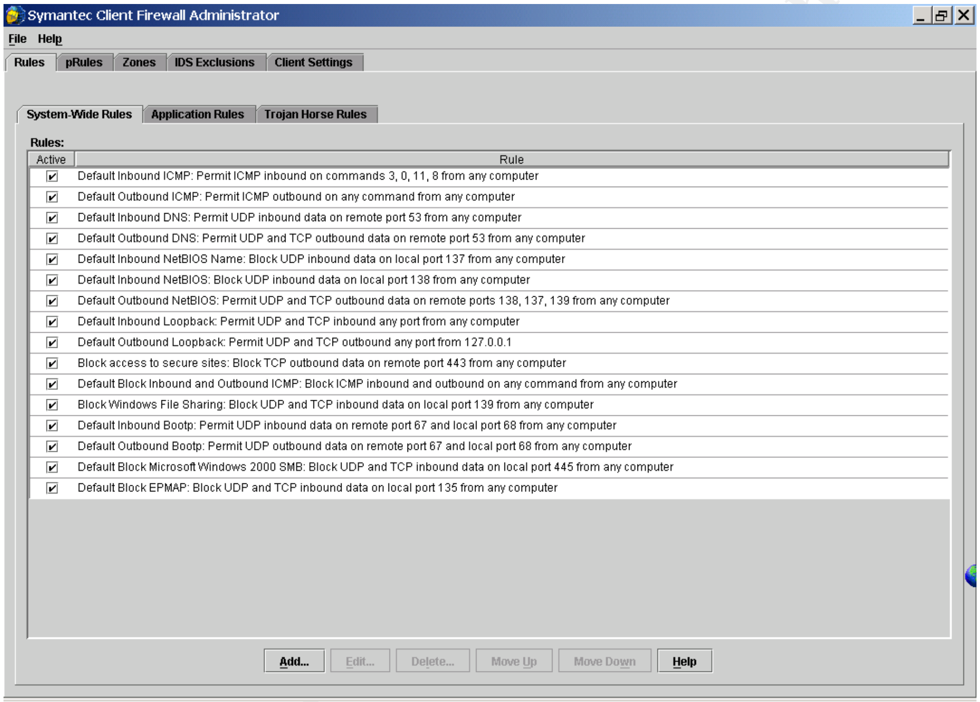
Policies

There are two types of policies files :- native .xml that do not include intrusion detection signatures or compressed .cfp (Client Firewall Policy) files, that contain all of the firewall rules, intrusion detection signatures, and configuration settings.

Policy components

The components of a firewall policy include:-

- Rules
  Firewall Rules include system wide, application and trojan horse rules. These rules apply to all of the clients network communication when it accesses the Internet. These rules are based on specific IP ports or IP addresses and all communication that relates to them.
  Figure 3 below shows examples or these rules.



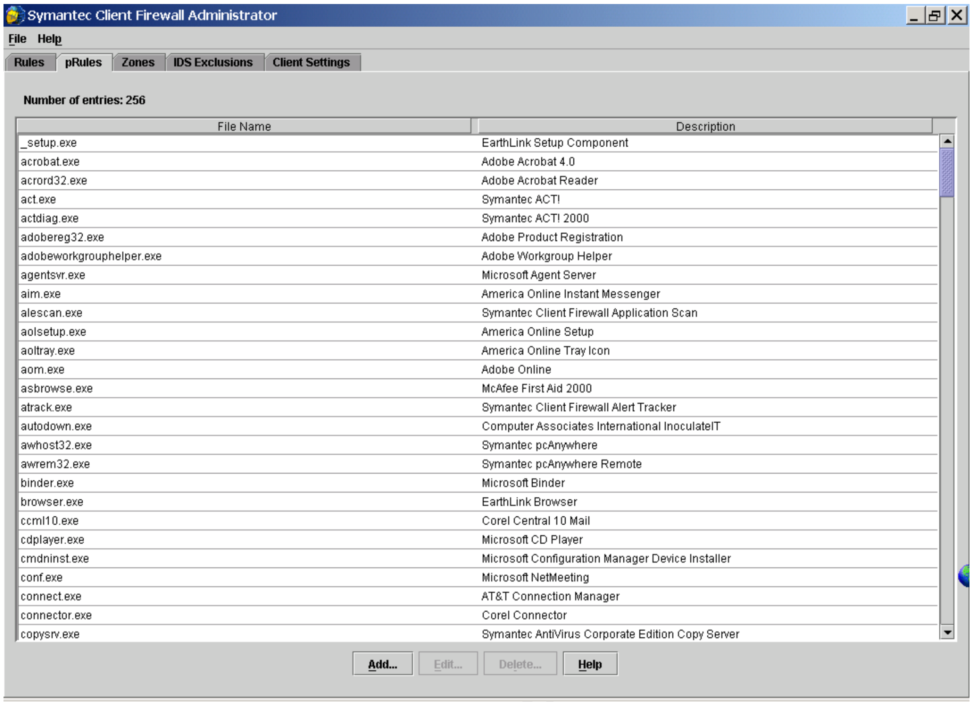
Active	Rule
☑	Default Inbound ICMP: Permit ICMP inbound on commands 3, 0, 11, 8 from any computer
☑	Default Outbound ICMP: Permit ICMP outbound on any command from any computer
☑	Default Inbound DNS: Permit UDP inbound data on remote port 53 from any computer
☑	Default Outbound DNS: Permit UDP and TCP outbound data on remote port 53 from any computer
☑	Default Inbound NetBIOS Name: Block UDP inbound data on local port 137 from any computer
☑	Default Inbound NetBIOS: Block UDP inbound data on local port 138 from any computer
☑	Default Outbound NetBIOS: Permit UDP and TCP outbound data on remote ports 138, 137, 139 from any computer
☑	Default Inbound Loopback: Permit UDP and TCP inbound any port from any computer
☑	Default Outbound Loopback: Permit UDP and TCP outbound any port from 127.0.0.1
☑	Block access to secure sites: Block TCP outbound data on remote port 443 from any computer
☑	Default Block Inbound and Outbound ICMP: Block ICMP inbound and outbound on any command from any computer
☑	Block Windows File Sharing: Block UDP and TCP inbound data on local port 139 from any computer
☑	Default Inbound Bootp: Permit UDP inbound data on remote port 67 and local port 68 from any computer
☑	Default Outbound Bootp: Permit UDP outbound data on remote port 67 and local port 68 from any computer
☑	Default Block Microsoft Windows 2000 SMB: Block UDP and TCP inbound data on local port 445 from any computer
☑	Default Block EPMAP: Block UDP and TCP inbound data on local port 135 from any computer

Figure 3

- PRules (Potential Rules)

Contrary to application rules, pRules do not create registry entries on the client after the policy has been rolled out. PRules are used when a client has a set of applications that differ from the standard set of applications installed on the client. A pRule contains only the data to validate an application that has the capability to access the Internet and when this application accesses the Internet for the first time the pRule is processed. If the application matches the criteria in the pRule an Application Rule is then created and the corresponding entries are then created in the registry.
The advantage of using pRules is that the Symantec Client Security firewall Client can generate Application rules as they are required rather than the Administrator having to create Application rules for applications that may never be used.
The default policy already contains pRules for many commonly used applications but this list should be customized by the administrator to include additional corporate applications before rolling out the policy.

The diagram below shows examples of applications that use pRules.



Number of entries: 256

File Name	Description
_setup.exe	EarthLink Setup Component
acrobat.exe	Adobe Acrobat 4.0
acrord32.exe	Adobe Acrobat Reader
act.exe	Symantec ACT!
actdiag.exe	Symantec ACT! 2000
adobereg32.exe	Adobe Product Registration
adobeworkgrouphelper.exe	Adobe Workgroup Helper
agentsvr.exe	Microsoft Agent Server
aim.exe	America Online Instant Messenger
alescan.exe	Symantec Client Firewall Application Scan
aolsetup.exe	America Online Setup
aoltray.exe	America Online Tray Icon
aom.exe	Adobe Online
asbrowse.exe	McAfee First Aid 2000
atrack.exe	Symantec Client Firewall Alert Tracker
autodown.exe	Computer Associates International InoculateIT
awhost32.exe	Symantec pcAnywhere
awrem32.exe	Symantec pcAnywhere Remote
binder.exe	Microsoft Binder
browser.exe	EarthLink Browser
ccml10.exe	Corel Central 10 Mail
cdplayer.exe	Microsoft CD Player
cmdninst.exe	Microsoft Configuration Manager Device Installer
conf.exe	Microsoft NetMeeting
connect.exe	AT&T Connection Manager
connector.exe	Corel Connector
copysrv.exe	Symantec AntiVirus Corporate Edition Copy Server

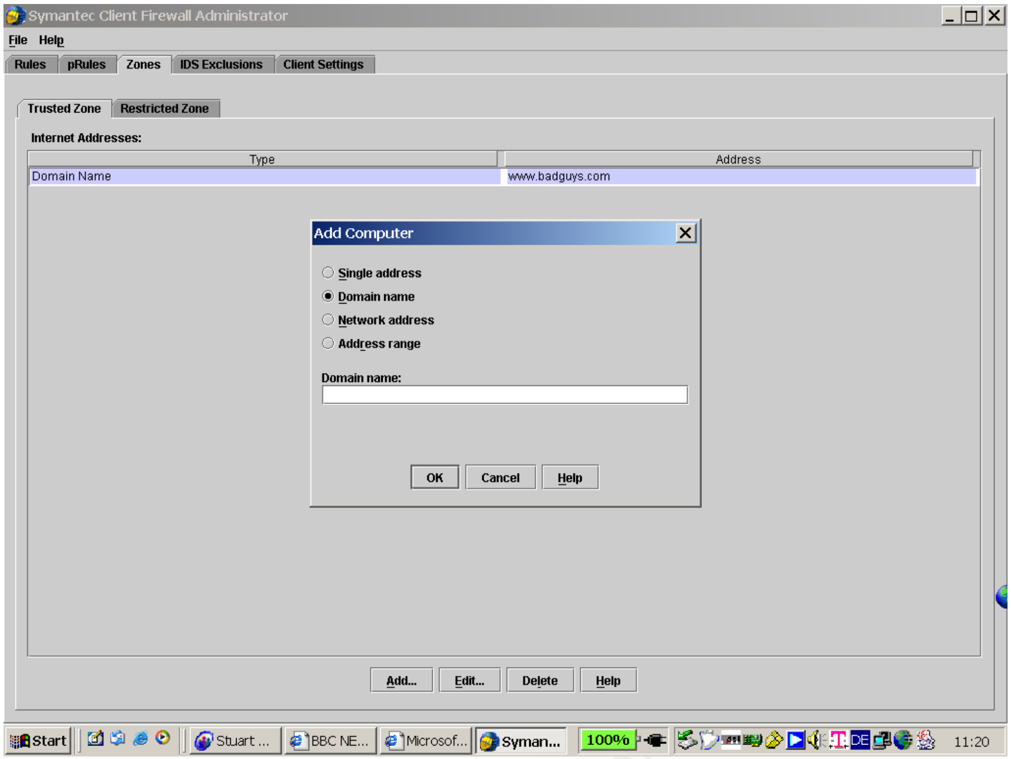
Figure 4

- Zones

It is possible to configure the client firewall so that computers or groups of computers can be placed into either a trusted or a restricted zone. The client firewall checks Zones before it processes any other rules. If a computer has been added to the restricted zone the firewall will block any communication from this computer without checking to see whether any other firewall rules are applicable.
A computer that has been added to the trusted zone is not controlled by the client firewall and has the same access to the client as if Symantec Client Firewall was not installed.

Computers can be included in either of these two zones by adding them by IP address, domain name, network address or address range (Figure 5.)

Symantec Deep Sight Threat Management System (https://tms.symantec.com) publishes the known top ten offending ISPs and IP addresses which could be added to the restricted zone.



Internet Addresses:

Type	Address
Domain Name	www.badguys.com

Add Computer

○ Single address
● Domain name
○ Network address
○ Address range

Domain name:

Figure 5

- Intrusion Detection System (IDS)

Every packet that enters or leaves the client is examined by the firewall client for attack signatures.
More information on attack signatures can be found at :-

http://www.cisco.com/warp/public/cc/pd/sqsw/sqidsz/prodlit/idssa_wp.htm

Intrusion Detection does not only examine single packets but also examines streams of packets which can identify attacks that are spread among several packets.
If attack information is matched with IDS signatures then communication with the attacking computer is blocked. As the list of attack signatures is always growing it is necessary to keep this list up to date. This can be achieved by LiveUpdate.
One of the problems with ID systems is that they sometimes recognize valid data packets as suspicious activity and block communication from these computers. If you know that these alarms are being caused by safe behavior then the corresponding signature can be excluded. This can cause problems as the client is then no longer protected by this attack and a decision must be made as to whether the risk of this sort of attack outweighs the problems caused by false alarms. If these false alarms are coming from a computer that is known to be safe then this machine could be added to the list of trusted computers.

Managing Clients with the Symantec System Centre Console

This section will briefly explain how to manage mobile clients with the Symantec System Centre Console.

Server Groups

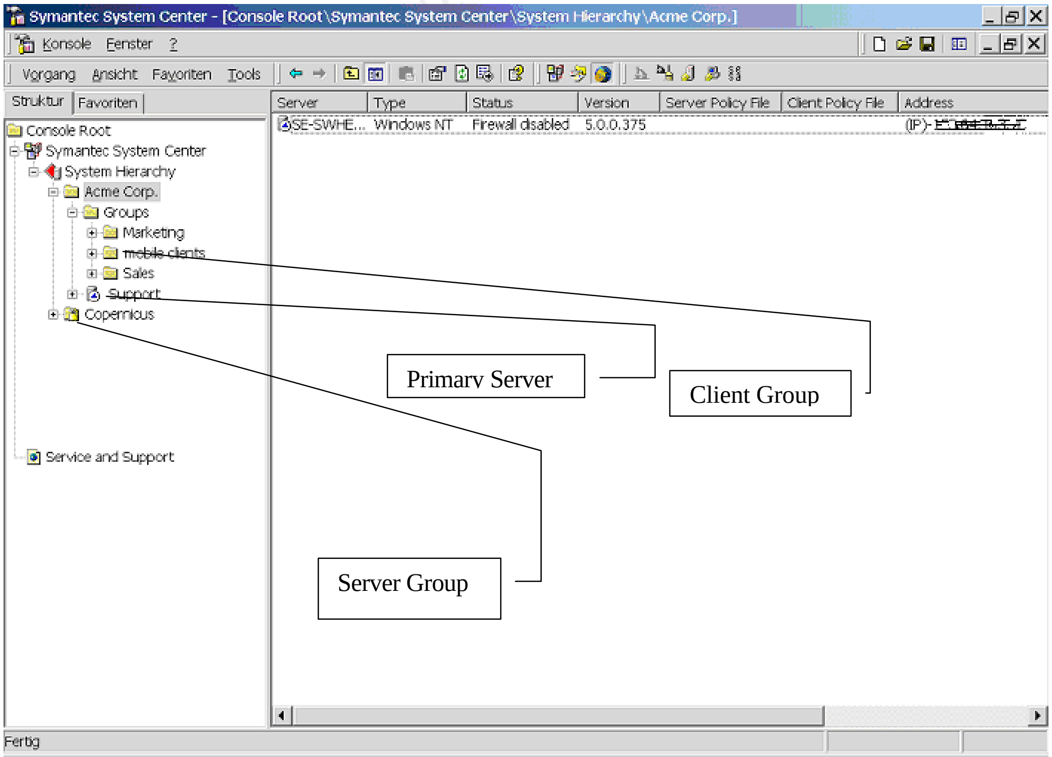
It is possible to create server groups in the console can be password protected. This means that the responsibility of administering a group of clients can be delegated to other people within the organization.

Primary Server

Each server group must contain a primary server. The primary server has the task of retrieving virus definitions and distributing them to the clients and any secondary servers within the server group.

Client Groups

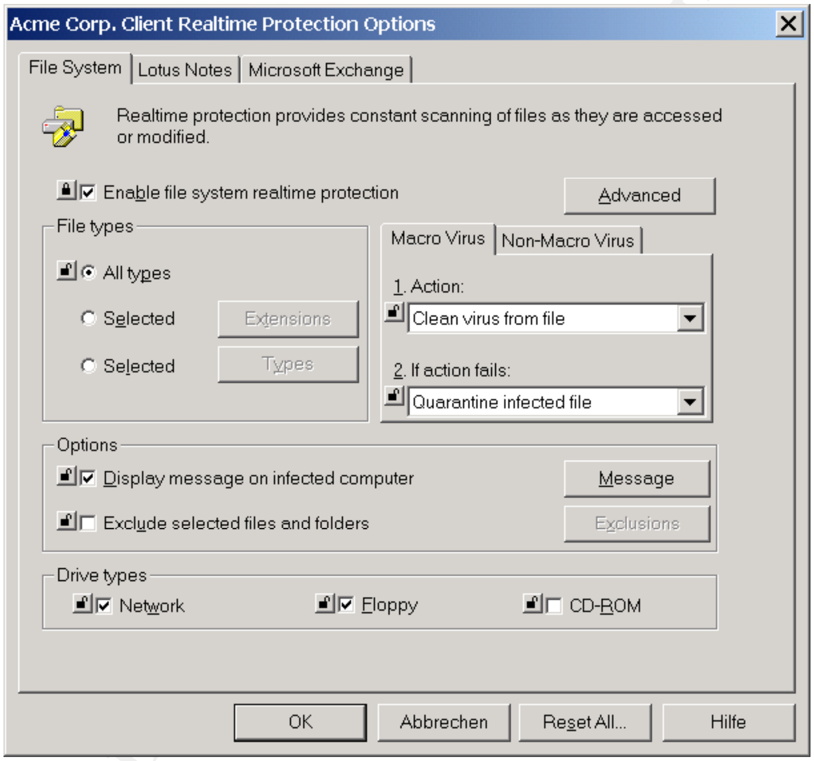
Client groups can be created within the Server Group. The reason for having more than one client group is so that different virus protection and client firewall settings can be configured for each respective group relative to its task. A group for mobile clients will almost certainly have a different configuration compared to a group of clients that are permanently situated within the company.



Server	Type	Status	Version	Server Policy File	Client Policy File	Address
SE-SWHE...	Windows NT	Firewall disabled	5.0.0.375			(IP)-[redacted]

Figure 6

Configuration settings can be implemented from different levels within the Symantec System Centre Console. The highest level from which settings can be implemented is from the server group level. These settings are then valid for all servers and clients within the server group.
Settings implemented from the client group level are valid for all clients within that client group. The lowest level at which settings can be implemented is at the client itself.
After settings have been configured they can be locked down by the administrator by closing the lock on the left side of the item that has been configured. In the following diagram (Figure 7) “Enable file system realtime protection” has been locked and this setting can no longer be changed by the client.


Acme Corp. Client Realtime Protection Options

File System | Lotus Notes | Microsoft Exchange

Realtime protection provides constant scanning of files as they are accessed or modified.

☑ Enable file system realtime protection

File types
● All types
○ Selected
○ Selected

Macro Virus | Non-Macro Virus
1. Action: Clean virus from file
2. If action fails: Quarantine infected file

Options
☑ Display message on infected computer
□ Exclude selected files and folders

Drive types
☑ Network
☑ Floppy
□ CD-ROM

Figure 7

It is recommended that all options are locked down to prevent users from tampering with these settings which could lead to the client being vulnerable to attack by viruses.
The firewall policy files that have been created with the Symantec Client Firewall Administrator can be distributed to the relevant client groups from the Symantec System Centre Console. The firewall status and which policy has been applied can be viewed in the console.

Quarantine Server

If an unknown virus is found either with realtime protection or during a manual scan it can be forwarded from the client to the quarantine server. These files that have been forwarded can no longer be accessed and are unable to spread within the network.

When newer definitions are available, the file in quarantine can be rescanned. If the virus cannot be removed after rescanning the file can be forwarded to Symantec Security Response for analysis and repair. The quarantine server can be configured so that definitions which have been created to repair the newly discovered virus are automatically distributed to all machines in the network.

Benefits of implementing Symantec Client Security

One of the major problems facing IT administrators is how to coordinate and manage multiple client security point products across the enterprise. Because of the growing number of security vulnerabilities and threats, security products require frequent upgrades and reconfigurations to be able to provide a secure defense. In the past it was always difficult to keep the mobile client up to date with the latest security updates due to the fact that most mobile clients connect to the company network over a slow WAN link. As the management of the client firewall and anti virus protection can now be managed from one place and implemented with decreased definition file updates it is possible to keep the mobile client at the latest level of protection. IT departments usually have enough work with the day to day running of the organization and require integrated security products that can be centrally managed which is provided by Symantec Client Security.
A single integrated client security solution with a central management console reduces considerably the time and effort spent to provide all clients with the latest updates against threats and results in a lowered total cost of ownership.

What the future holds

As the number and complexity of security incidents increases and the number of mobile clients, that require perhaps tighter security than company internal computers, increases, it is vital that security measures for mobile clients are developed even further.
One of the weaknesses of Symantec Client Security is that a client whose virus or firewall protection has been disabled or is not running correctly will in some cases not be visible in the console. This is also true of a client that has never had Symantec Security installed. The console does not check the client for security policy compliance with regards to anti virus and firewall protection which means that an unprotected client can still access the company network and maybe infect other computers or provide a back door for an attacker.
I believe that future developments in client security will produce some method of checking the client for security policy compliance when the client logs into the network. If the client is not compliant then it will not be granted access to the network and therefore provide one less weakness in the corporate defense against attackers and malicious code.

Research material was obtained from the following sources:-

Comprehensive Client Security across organizations
http://www.verio.com/powerplatform/library/client_security_across.pdf
An IDC White Paper by Brian Burke and Chris Christiansen

Defending the Digital frontier by Mark W. Doll, Sajay Rai and Jose Granado
ISBN 0-471-22144-9