Partner Client Test Plan
SecNet 5.0

(Draft 11.0)

John Bee
Managing Test Lead
ThreeBears Laboratories

Yves Boulanger
Greene Software Systems, Inc.

Robert Sabourin
Greene Software Systems, Inc.

May 23, 2004

Revision History

Date	Revision	Description	Author(s)
April 14, 2004	1.0	Initial Draft	John Bee < johnb@threebears.com>
April 15, 2004	2.0	Draft	John Bee < johnb@threebears.com>
April 16, 2004	3.0	Draft	John Bee < johnb@threebears.com>
April 17, 2004	4.0	Draft	John Bee < johnb@threebears.com>
April 18, 2004	5.0	Draft	John Bee < johnb@threebears.com>
April 21, 2004	6.0	Draft	Yves Boulanger <yvesb@greenesoftware.com>
April 22, 2004	6.1	Draft	Yves Boulanger <yvesb@greenesoftware.com>
April 26, 2004	7.0	Draft	John Bee < johnb@threebears.com>
April 27, 2004	7.1	Draft	Yves Boulanger <yvesb@greenesoftware.com>
April 30, 2004	8.0	Draft	Yves Boulanger <yvesb@greenesoftware.com>
April 30, 2004	9.0	Draft	John Bee <johnb@threebears.com>
May 1, 2004	9.1	Draft	John Bee <johnb@threebears.com>
May 2, 2004	9.2	Draft	John Bee <johnb@threebears.com>
May 4, 2004	9.3	Draft	Robert Sabourin <robs@greenesoftware.com>
May 7, 2004	10.0	Draft	John Bee <johnb@threebears.com>
May 9, 2004	10.1	Draft	John Bee <johnb@threebears.com>
May 13, 2004	10.2	Draft	Robert Sabourin <robs@greenesoftware.com>
May 19, 2004	10.3	Draft	Robert Sabourin <robs@greenesoftware.com>
May 23, 2004	11.0		John Bee <johnb@threebears.com>

Table of Contents

1. Introduction 4
   - 1.1 Overview 4
   - 1.2 Purpose 4
   - 1.3 Strategy 4

2. Test Cases 5
   - 2.1 Installation 5
   - 2.2 Main Application 19
   - 2.3 Activation 21
   - 2.4 Anti-Virus 26
   - 2.5 Firewall 54
   - 2.6 Anti-Spyware 65
   - 2.7 Pop-up / Ad Blocker 78
   - 2.8 Privacy Manager 87
   - 2.9 Parental Control 107
   - 2.10 Uninstall 118
   - 2.11 Performance 120
   - 2.12 Platform Requirements 123

1. Introduction

1.1 Overview

This document describes the test cases to be executed on SecNet 5.0 by ThreeBears Laboratories, Inc. in order to implement the SecNet 5.0 Partner Client Test.

1.2 Purpose

The purpose of this document is to provide testing staff with a set of test cases to confirm SecNet 5.0 Requirements.

1.3 Strategy

An initial set of requirements was provided to ThreeBears on 4/15/04 by Robert Sabourin of Greene Software Systems (see 2004_04_13_GSS_SecNet_5_0_Requirements.xls) and updated weekly. The test cases in this document were built to verify that those requirements were met in each release of SecNet 5.0 software that was given to ThreeBears over a period of 7 weeks.

All operating system configurations and co-resident applications defined in the SecNet 5.0 requirements document were used in implementing and running these test cases.

2. Test Cases

2.1 Installation

2.1.1 Detection of third party redundant security applications: Norton Anti-Virus 2001

Description: During installation, SecNet shall notify the user if any known 3rd-party redundant security application software is detected (as listed in the Redundant Security Applications list)			
Test Case ID: QZ115			
GSS Requirements Met: ZIN004 / ZIDAV001			
Date Ran:			
Tester:			
Configuration / Build:			
Machine Number:			
Pre-Condition: QZ100			
Bugs found:			
Step	**Description**	**Observation**	**Result**
	If you are on a Windows 2000 or XP machine, copy the "reg" folder (located in the 3rd-party-AV dir on the Acceptance share) to the root of your C: drive and run GSS-reg.bat. If you are on a Windows 98 or ME machine, copy the reg9x folder to the root of your C: drive and run GSS-reg.bat	Open regedit and verify the following 13 entries were successfully added to the registry at the following location: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall: 1) {9209615F-276E-4406-8607-DF2B3C9F0F34} 2) {C6F5B6CF-609C-428E-876F-CA83176C021B} 3) {D1FF75E7-DD42-4CFD-B052-20B3FFF4EDB8} 4) {E5EE9939-259F-4DE2-8023-5C49E16A4F43} 5) {DCB2928E-61F6-11D6-B259-00C04FF4B435} 6) {BB85F18B-43C6-48B5-ABA9-6A5DDA65AA1B} 7) {76542EE3-5849-11D2-9C18-00609707C0FF} 8) {3B29A786-5803-4e9e-9B58-3014A5B4E519}	

		9) {12E2B9E9-05B1-407d-B0FD-B5F350535125} 10) McAfee Personal Firewall Plus 11) McAfee SecurityCenter 12) ZoneAlarm Pro 13) AVG7	
	Launch SecNet installation		
	Verify that SecNet notifies the user that it has detected the presence of several third-party security application software packages, among them is: Norton Internet Security Family Edition		
	Keep the window open and execute the next test case		
Comments \ Issues:			

2.1.2 Detection of third party redundant security application: Norton Anti-Virus 2004

Description: During installation, SecNet shall notify the user if any known 3rd-party redundant security application software is detected (as listed in the Redundant Security Applications list)			
Test Case ID: QZ111			
GSS Requirements Met: ZIN004 / ZIDAV003			
Date Ran:			
Tester:			
Configuration / Build:			
Machine Number:			
Pre-Condition: QZ110			
Bugs found:			
Step	**Description**	**Observation**	**Result**
1.	Verify that SecNet notifies the user that it has detected the presence of several third-party security application software packages, among them is: Norton AntiVirus 2004 Norton AntiVirus SYMLT MSI Norton AntiVirus Parent MSI		
Comments \ Issues:			

2.1.3 Detection of third party redundant security application: McAfee Anti-Virus

Description: During installation, SecNet shall notify the user if any known 3rd-party redundant security application software is detected (as listed in the Redundant Security Applications list)			
Test Case ID: QZ112			
GSS Requirements Met: ZIN004 / ZIDAV005			
Date Ran:			
Tester:			
Configuration / Build:			
Machine Number:			
Pre-Condition: QZ110			
Bugs found:			
Step	**Description**	**Observation**	**Result**
	Verify that SecNet notifies the user that it has detected the presence of several third-party security application software packages, among them is: McAfee Internet Security		
Comments \ Issues:			

2.1.4 Detection of third party redundant security application: Panda Titanium 2004

Description: During installation, SecNet shall notify the user if any known 3rd-party redundant security application software is detected (as listed in the Redundant Security Applications list)			
Test Case ID: QZ113			
GSS Requirements Met: ZIN004 / ZIDAV007			
Date Ran:			
Tester:			
Configuration / Build:			
Machine Number:			
Pre-Condition: QZ110			
Bugs found:			
Step	**Description**	**Observation**	**Result**
1.	Verify that SecNet notifies the user that it has detected the presence of several third-party security application software packages, among them is: Panda Titanium AntiVirus 2004		
Comments \ Issues:			

2.1.5 Detection of third party redundant security application: AVG Anti-Virus Professional 7.0

Description: During installation, SecNet shall notify the user if any known 3rd-party redundant security application software is detected (as listed in the Redundant Security Applications list)			
Test Case ID: QZ114			
GSS Requirements Met: ZIN004 / ZIDAV009			
Date Ran:			
Tester:			
Configuration / Build:			
Machine Number:			
Pre-Condition: QZ110			
Bugs found:			
Step	**Description**	**Observation**	**Result**
	Verify that SecNet notifies the user that it has detected the presence of several third-party security application software packages, among them is: AVG Anti-Virus 7.0		
Comments \ Issues:			

2.1.6 Detection of third party redundant security application: BlackICE Firewall 3.6

Description: During installation, SecNet shall notify the user if any known 3rd-party redundant security application software is detected (as listed in the Redundant Security Applications list)			
Test Case ID: QZ119			
GSS Requirements Met: ZIN004 / ZIDFW001			
Date Ran:			
Tester:			
Configuration / Build:			
Machine Number:			
Pre-Condition: QZ110			
Bugs found:			
Step	**Description**	**Observation**	**Result**
	Verify that SecNet notifies the user that it has detected the presence of several third-party security application software packages, among them is: BlackICE		
Comments \ Issues:			

2.1.7 Detection of third party redundant security application: Norton Firewall 2004

Description: During installation, SecNet shall notify the user if any known 3rd-party redundant security application software is detected (as listed in the Redundant Security Applications list)			
Test Case ID: QZ116			
GSS Requirements Met: ZIN004 / ZIDFW003			
Date Ran:			
Tester:			
Configuration / Build:			
Machine Number:			
Pre-Condition: QZ110			
Bugs found:			
Step	**Description**	**Observation**	**Result**
1.	Verify that SecNet notifies the user that it has detected the presence of several third-party security application software packages, among them is: Norton AntiSpam		
Comments \ Issues:			

2.1.8 Detection of third party redundant security application: McAfee Personal Firewall Plus 5.0

Description: During installation, SecNet shall notify the user if any known 3rd-party redundant security application software is detected (as listed in the Redundant Security Applications list)			
Test Case ID: QZ117			
GSS Requirements Met: ZIN004 / ZIDFW004			
Date Ran:			
Tester:			
Configuration / Build:			
Machine Number:			
Pre-Condition: QZ110			
Bugs found:			
Step	**Description**	**Observation**	**Result**
1.	Verify that SecNet notifies the user that it has detected the presence of several third-party security application software packages, among them is: McAfee Personal Firewall Plus		
Comments \ Issues:			

2.1.9 Detection of third party redundant security application: Zone Alarm 4.x

Description: During installation, SecNet shall notify the user if any known 3rd-party redundant security application software is detected (as listed in the Redundant Security Applications list)			
Test Case ID: QZ118			
GSS Requirements Met: ZIN004 / ZIDFW006			
Date Ran:			
Tester:			
Configuration / Build:			
Machine Number:			
Pre-Condition: QZ110			
Bugs found:			
Step	**Description**	**Observation**	**Result**
1.	Verify that SecNet notifies the user that it has detected the presence of several third-party security application software packages, among them is: ZoneAlarm Pro		
Comments \ Issues:			

2.1.10 Detection of third party redundant security application: Norton Security Suite 2004

Description: During installation, SecNet shall notify the user if any known 3rd-party redundant security application software is detected (as listed in the Redundant Security Applications list)			
Test Case ID: QZ119-B			
GSS Requirements Met: ZIN004 / ZIDFW007			
Date Ran:			
Tester:			
Configuration / Build:			
Machine Number:			
Pre-Condition: QZ110			
Bugs found:			
Step	**Description**	**Observation**	**Result**
1.	Verify that SecNet notifies the user that it has detected the presence of several third-party security application software packages, among them is: Norton Internet Security		
Comments \ Issues:			

2.1.11 Detection of third party redundant security application: McAfee Security Suite 6.0

Description: During installation, SecNet shall notify the user if any known 3rd-party redundant security application software is detected (as listed in the Redundant Security Applications list)			
Test Case ID: QZ119-C			
GSS Requirements Met: ZIN004 / ZIDFW007			
Date Ran:			
Tester:			
Configuration / Build:			
Machine Number:			
Pre-Condition: QZ110			
Bugs found:			
Step	**Description**	**Observation**	**Result**
1.	Verify that SecNet notifies the user that it has detected the presence of a third party redundant security application software: McAfee Security Center		
Comments \ Issues:			

2.1.12 Desktop shortcut created

Description: After installation, verify a SecNet desktop shortcut is created			
Test Case ID: QZ100			
GSS Requirements Met: ZIN002			
Author: John Bee			
Date Ran:			
Tester:			
Configuration / Build:			
Machine Number:			
Pre-Condition: QZ100			
Bugs found:			
Step	**Description**	**Observation**	**Result**
1.	After SecNet setup, verify that on the desktop, a shortcut titled “SecNet Security & Privacy” now exists.		
Expected Results: A desktop shortcut titled “SecNet Security & Privacy” should be created			
Comments \ Issues:			

2.1.13 Program Group created

Description: Verify that a Program Group (with 4 shortcuts) is created after installation			
Test Case ID: QZ110			
GSS Requirements Met: ZIN003, ZUN001			
Author: John Bee			
Date Ran:			
Tester:			
Configuration / Build:			
Machine Number:			
Pre-Condition: **QZ100**			
Bugs found:			
Step	**Description**	**Observation**	**Result**
1.	After installation, go to Start menu \ Programs		
2.	Verify that SecNet created a program group called “SecNet Security & Privacy” with three shortcuts and one subfolder shortcut. The three shortcuts are “SecNet Diagnostics”, “SecNet”, and “Uninstall SecNet”). The subfolder shortcut is “SecNet Help” with two shortcuts: “SecNet Help” and “Getting Started”		
Expected Results: SecNet should create a program group called “SecNet Security & Privacy”			
Comments \ Issues:			

2.2 Main Application

2.2.1 System tray when started

Description: The product shall place an icon in the system tray when started.			
Test Case ID: QZ200			
GSS Requirements Met: ZFM001			
Author: John Bee			
Date Ran:			
Tester:			
Configuration / Build:			
Machine Number:			
Pre-Condition: Reload a fresh platform			
Bugs found:			
Step	**Description**	**Observation**	**Result**
	Install and activate SecNet		
	Restart the computer		
	Verify the SecNet icon is resident in the system tray after Windows has finished processing the user's desktop profile after OS login		
Expected Results: SecNet should place an icon in the system tray when started.			
Comments \ Issues:			

2.2.2 System tray while minimized

Description: The product shall minimize to the system tray when closed from the Desktop.			
Test Case ID: QZ210			
GSS Requirements Met: ZFM002			
Author: John Bee			
Date Ran:			
Tester:			
Configuration / Build:			
Machine Number:			
Pre-Condition: TC QZ200			
Bugs found:			
Step	**Description**	**Observation**	**Result**
	Install and activate SecNet		
	Restart the computer		
	After Windows has finished processing the user's desktop profile after OS login, open the SecNet UI		
	After the UI is open and connected to the internet, close it		
	Verify that the icon remains in the system tray	The first time SecNet UI is closed a message appears saying SecNet is still protecting your PC	
Expected Results: SecNet should minimize to the system tray when closed from the Desktop			
Comments \ Issues:			

2.3 Activation

2.3.1 Security services activated

Description: Security services shall be activated if user authentication and authorization are successful.			
Test Case ID: QZ130			
GSS Requirements Met: ZAC002			
Author: John Bee			
Date Ran:			
Tester:			
Configuration / Build:			
Machine Number:			
Pre-Condition: QZ100			
Bugs found:			
Step	**Description**	**Observation**	**Result**
	After installation and activation (test case QZ100), verify that SecNet's features are active (not grayed) in the UI		
Expected Results: SecNet should activate security services if user authentication and authorization are successful.			
Comments \ Issues:			

2.3.2 No internet connection: SecNet UI launch

Description: The activated product shall launch when an Internet connection is not available.			
Test Case ID: QZ150			
GSS Requirements Met: ZAC004			
Author: John Bee			
Date Ran:			
Tester:			
Configuration / Build:			
Machine Number:			
Pre-Condition: QZ200			
Bugs found:			
Step	**Description**	**Observation**	**Result**
1.	Disconnect from the internet (physically disconnect the network cable or on some OS go to the Windows control panel and disable the net tap)		
2.	Launch SecNet and verify the UI launches with a window that says “No Internet Connection Available”		
Expected Results: SecNet UI should launch even with no internet connection available			
Comments \ Issues:			

2.3.3 No internet connection: Virus scan

Description: The activated product shall be able to run a virus scan when an Internet connection is not available.			
Test Case ID: QZ160			
GSS Requirements Met: ZAC004			
Author: John Bee			
Date Ran:			
Tester:			
Configuration / Build:			
Machine Number:			
Pre-Condition: QZ205			
Bugs found:			
Step	**Description**	**Observation**	**Result**
1.	Launch the SecNet UI	Verify that a page is displayed that says “Internet Connection is temporarily unavailable”	
2.	Switch to the Anti-Virus and click “Scan Now”		
3.	Select a drive (or a folder) and click “Scan Now”		
4.	Verify the scan completes successfully		
Expected Results: SecNet should be able to run a virus scan successfully without an available internet connection.			
Comments \ Issues:			

2.3.4 No internet connection: Spyware scan

Description: The activated product shall be able to run a spyware scan when an Internet connection is not available.			
Test Case ID: QZ170			
GSS Requirements Met: ZAC004			
Author: John Bee			
Date Ran:			
Tester:			
Configuration / Build:			
Machine Number:			
Pre-Condition: QZ205			
Bugs found:			
Step	**Description**	**Observation**	**Result**
1.	Launch the SecNet UI	Verify that a page is displayed that says “Internet Connection is temporarily unavailable”	
2.	Click Anti-Spyware and click “Scan Now”		
3.	Select a drive or folder and click “Scan Now”		
4.	Verify the scan completes successfully		
Expected Results: SecNet should be able to run a spyware scan successfully without an available internet connection.			
Comments \ Issues:			

2.3.5 No internet connection: Preferences

Description: The activated product shall allow the user to set preferences for each of its features when an Internet connection is not available.			
Test Case ID: QZ180			
GSS Requirements Met: ZAC004			
Author: John Bee			
Date Ran:			
Tester:			
Configuration / Build:			
Machine Number:			
Pre-Condition: QZ205			
Bugs found:			
Step	**Description**	**Observation**	**Result**
1.	Launch the SecNet UI	Verify that a page is displayed that says “Internet Connection is temporarily unavailable”	
2.	Switch to the feature pages for Firewall, Privacy Manager, and Form-Filler, and activate each using the “enable” checkbox, then click Preferences		
3.	Verify the Preference settings for each feature can be changed		
Expected Results: Users should be able to change the preferences in SecNet without an available internet connection.			
Comments \ Issues:			

2.4 Anti-Virus

2.4.1 Scan drives

Description: The Anti-Virus service shall provide support to scan sets of drives.			
Test Case ID: QZ300			
GSS Requirements Met: ZAV002			
Author: John Bee			
Date Ran:			
Tester:			
Configuration / Build:			
Machine Number:			
Pre-Condition: QZ100			
Bugs found:			
Step	**Description**	**Observation**	**Result**
1.	Go to the Anti-Virus pane of the SecNet UI and disable Real-Time virus protection		
2.	Copy the eicar.com virus test file into two drives (C: and another one)		
3.	Go to the Anti-Virus pane of the SecNet UI and select “Scan Now”		
4.	Set the “If a virus is found field” to Delete.		
5.	Select the two drives where the test virus file was copied and then click “Scan Now” *(ensure there is a checkmark next to both drives)*		
6.	When the scan is complete, click OK.		
7.	Click the “See last report” link of the Anti-Virus scan now pane.		
8.	Verify a report is generated that lists viruses being deleted from both of the drives scanned.		
Expected Results: SecNet’s Anti-Virus service should have successfully scanned the selected drives.			
Comments \ Issues:			

2.4.2 Scan folders

Description: The Anti-Virus service shall provide support to scan sets of folders.			
Test Case ID: QZ305			
GSS Requirements Met: ZAV002			
Author: John Bee			
Date Ran:			
Tester:			
Configuration / Build:			
Machine Number:			
Pre-Condition: QZ300			
Bugs found:			
Step	**Description**	**Observation**	**Result**
1.	Go to the Anti-Virus pane of the SecNet UI and disable Real-Time virus protection		
2.	Copy eicar.com virus test file into two different folders		
3.	Go to the Anti-Virus pane of the SecNet UI and select “Scan Now”		
4.	Set the “If a virus is found field” to Delete.		
5.	Select the two folders where the virus test file resides and click “Scan Now” *(ensure there is a checkmark next to both folder names)*	A little dialog will appear when the scan is finished	
6.	When the scan is complete, click OK.		
7.	Click the “See last report” link of the Anti-Virus scan now pane.		
8.	Verify a report is generated that lists viruses being deleted from both of the folders scanned.		
Expected Results: SecNet’s Anti-Virus service should have successfully scanned the selected folders.			
Comments \ Issues:			

2.4.3 Scan files for viruses

Description: The Anti-Virus service shall provide support to scan sets of files.			
Test Case ID: QZ310			
GSS Requirements Met: ZAV002			
Author: John Bee			
Date Ran:			
Tester:			
Configuration / Build: /			
Machine Number:			
Pre-Condition: TC QZ300			
Bugs found:			
Step	**Description**	**Observation**	**Result**
1.	Go to the Anti-Virus pane of the SecNet UI and disable Real-Time virus protection		
2.	Copy eicar.com virus test file into two different folders		
3.	Go to the Anti-Virus pane of the SecNet UI and select “Scan Now”		
4.	Set the “If a virus is found field” to Delete.		
5.	Select the two copies of eicar.com in the different folders from step 2 and click “Scan Now” *(ensure there is a checkmark next to filename in both folders)*	A little dialog will appear when the scan is finished	
6.	When the scan is complete, click OK.		
7.	Click the “See last report” link of the Anti-Virus scan now pane.		
8.	Verify a report is generated that lists viruses being deleted from both of the files scanned.		
Expected Results: SecNet’s Anti-Virus service should have successfully scanned the selected files			
Comments \ Issues:			

2.4.4 Scan hidden and unhidden folders for viruses in zipped and password-protected files

Description: The Anti-Virus service shall provide support to scan files			
Test Case ID: QZ312			
GSS Requirements Met: ZAV002, ZAV006			
Author: John Bee			
Date Ran:			
Tester: (new)			
Configuration / Build: /			
Machine Number:			
Pre-Condition: TC QZ300			
Bugs found:			
Step	**Description**	**Observation**	**Result**
1.	Copy the folder titled “zip-hid-pw” up on the Acceptance share to your local C: drive		
2.	Open windows explorer and right-click on the folder, selecting “Scan for Viruses”	Verify that in the right selectable menu there is an option Scan for Viruses	
3.	Verify the following: • A dialog appears, saying the file c:\zip-hid-pw\hiddenfolder_zipped\no_password_fake_virus_file.zip was infected • A dialog appears, saying the file c:\zip-hid-pw\hiddenfolder_zipped\password_protected_fake_virus_file.zip was infected • A dialog appears, saying the file c:\zip-hid-pw\hiddenfolder_zipped_hiddenfile\no_password_fake_virus_file.zip was infected • A dialog appears, saying the file c:\zip-hid-pw\hiddenfolder_zipped_hiddenfile\password_protected_fake_virus_file.zip was infected • A dialog appears, saying the file c:\zip-hid-pw\zipped\no_password_fake_virus_file.zip was infected • A dialog appears, saying the file c:\zip-hid-pw\zipped\password_protected	Click No Click No Click No Click No Click No Click No	

	_fake_virus_file.zip was infected • A dialog appears, saying the file c:\zip-hid-pw\zipped_hiddenfile\no_password_fake_virus_file.zip was infected • A dialog appears, saying the file c:\zip-hid-pw\zipped_hiddenfile\password protected__fake_virus_file.zip was infected IN ALL – verify 12 viruses were found (a dialog should appear saying as much)	Click No Click No	
Expected Results: Using right click SecNet should be able to scan files, folders and drives			
Comments \ Issues:			

2.4.5 Scan files for viruses using the mouse right click

Description: The Anti-Virus service shall provide support to scan files			
Test Case ID: QZ311			
GSS Requirements Met: ZAV002, ZAV013			
Author: Yves Boulanger			
Date Ran:			
Tester:			
Configuration / Build: /			
Machine Number:			
Pre-Condition: TC QZ300			
Bugs found:			
Step	**Description**	**Observation**	**Result**
4.	Create a directory called c:\testSecNet		
5.	Copy virus test file (eicar.com) into c:\testSecNet		
6.	Launch windows explorer and navigate to the root directory c:\		
7.	Position cursor over directory c:\testSecNet in right side window where files are listed		
8.	Right-click and select “Scan for viruses”	Verify that in the right selectable menu there is an option Scan for Viruses	
9.	Verify that SecNet detects the virus test file under c:\testSecNet		
Expected Results: Using right click SecNet should be able to scan files, folders and drives			
Comments \ Issues:			

2.4.6 Scheduled virus definition file update: Daily

Description: The Anti-Virus service shall provide a capability to establish scheduled daily checks for virus definition file updates.			
Test Case ID: QZ315			
GSS Requirements Met: ZAV003			
Author: John Bee			
Date Ran:			
Tester:			
Configuration / Build: /			
Machine Number:			
Pre-Condition: SecNet should be installed, activated, and running for at least 5 minutes. This is to allow enough time for all initial startup updates to occur and create the registry values that are used.			
Bugs found:			
Step	**Description**	**Observation**	**Result**
	Go to Anti-Virus and click "Preferences"		
	Select "Manual" in the Update "Frequency" dropdown list and click OK		
	Choose "View -> Console" from the SecNet menubar	The "Event Console" opens.	
	Size the "Event Console" so you can see the width of most lines.		
	Disable Firewall to reduce the activity reported in the console.		
	Choose "SecNet -> Shutdown" from the SecNet menubar	SecNet is completely shutdown and not even running in the system tray.	
	Run the steps below in the Comments section		
	Launch SecNet and wait about 1 minute for the initial console activity to complete.		
	Set the system date ahead 1 day in the "Date and Time" Control Panel		
	Go to Anti-Virus and click "Preferences"		
	Select "Daily" in the Update "Frequency" dropdown list and click OK		
	Watch the console		
	Verify that within 2 minutes the console reports "Updating the Anti-Virus definition file"		
Expected Results: SecNet's Anti-Virus services should run a scheduled daily check for virus definition file updates.			

Comments \ Issues:

Steps:
- Click "Start" to open the "Start" menu
- Click "Run.." to open the Run dialog
- Type "Regedit" to run the registry editor application
- Goto " HKEY_LOCAL_MACHINE\SOFTWARE\Zero Knowledge\SecNet"
- Double click the registry key “VirusDBUpdateId”
- Edit the current value to be one less than the current value
- Click the “OK” button

2.4.7 Scheduled virus definition file update: Weekly

Description: The Anti-Virus service shall provide a capability to establish scheduled weekly checks for virus definition file updates.			
Test Case ID: QZ320			
GSS Requirements Met: ZAV003, ZFW002			
Author: John Bee			
Date Ran:			
Tester:			
Configuration / Build: /			
Machine Number:			
Pre-Condition: SecNet should be installed, activated, and running for at least 5 minutes. This is to allow enough time for all initial startup updates to occur and create the registry values that are used.			
Bugs found:			
Step	**Description**	**Observation**	**Result**
	Go to Anti-Virus and click "Preferences"		
	Select "Manual" in the Update "Frequency" dropdown list and click OK		
	Choose "View->Console" from the SecNet menubar	The "Event Console" opens.	
	Size the "Event Console" so you can see the width of most lines.		
	Disable Firewall to reduce the activity reported in the console.		
	Choose "SecNet->Shutdown" from the SecNet menubar	SecNet is completely shutdown and not even running in the system tray.	
	Run the steps below in the Comments section		
	Launch SecNet and wait about 1 minute for the initial console activity to complete.		
	Set the system date ahead 1 week in the "Date and Time" Control Panel		
	Go to Anti-Virus and click "Preferences"		
	Select "Weekly" in the Update "Frequency" dropdown list and click OK		
	Watch the console		
	Verify that within 2 minutes the console reports "Updating the Anti-Virus definition file"		
Expected Results: SecNet's Anti-Virus services should run a scheduled weekly check for virus definition file updates.			
Comments \ Issues: Steps:			

- Click "Start" to open the "Start" menu
- Click "Run.." to open the Run dialog
- Type "Regedit" to run the registry editor application
- Goto " HKEY_LOCAL_MACHINE\SOFTWARE\Zero Knowledge\SecNet"
- Double click the registry key “VirusDBUpdateId”
- Edit the current value to be one less than the current value
- Click the “OK” button

2.4.8 Scheduled virus definition file update: Manual

Description: The Anti-Virus service shall provide a capability to establish scheduled manual checks for virus definition file updates.			
Test Case ID: QZ325			
GSS Requirements Met: ZAV003, ZFW002			
Author: John Bee			
Date Ran:			
Tester:			
Configuration / Build: /			
Machine Number:			
Pre-Condition: SecNet should be installed, activated, and running for at least 5 minutes. This is to allow enough time for all initial startup updates to occur and create the registry values that are used.			
Bugs found:			
Step	**Description**	**Observation**	**Result**
	Go to Anti-Virus and click "Preferences"		
	Select "Manual" in the Update "Frequency" dropdown list and click OK		
	Choose "View->Console" from the SecNet menubar	The "Event Console" opens.	
	Size the "Event Console" so you can see the width of most lines.		
	Disable Firewall to reduce the activity reported in the console.		
	Choose "SecNet->Shutdown" from the SecNet menubar	SecNet is completely shutdown and not even running in the system tray.	
	Run the steps below in the Comments section		
	Launch SecNet and wait 1 minute for the initial console activity to complete.		
	Go to Anti-Virus and click "Preferences"		
	Click the "Update" button in the update area		
	Watch the console		
	Verify that the console reports "Updating the Anti-Virus definition file"		
Expected Results: SecNet's Anti-Virus services should run manual virus definition file updates when requested by the user.			
Comments \ Issues: Steps: - Click "Start" to open the "Start" menu - Click "Run.." to open the Run dialog - Type "Regedit" to run the registry editor application - Goto " HKEY_LOCAL_MACHINE\SOFTWARE\Zero Knowledge\SecNet" - Double click the registry key "VirusDBUpdateId"			

- Edit the current value to be one less than the current value
- Click the “OK” button

2.4.9 Scheduled virus definition file update: Automatic

Description: The Anti-Virus service shall provide a capability to establish scheduled automatic checks for virus definition file updates.			
Test Case ID: QZ330			
GSS Requirements Met: ZAV003, ZFW002			
Author: John Bee			
Date Ran:			
Tester:			
Configuration / Build: /			
Machine Number:			
Pre-Condition: SecNet should be installed, activated, and running for at least 5 minutes. This is to allow enough time for all initial startup updates to occur and create the registry values that are used.			
Bugs found:			
Step	**Description**	**Observation**	**Result**
	Go to Anti-Virus and click “Preferences”		
	Select “Manual” in the Update “Frequency” dropdown list and click OK		
	Choose “View->Console” from the SecNet menubar	The “Event Console” opens.	
	Size the “Event Console” so you can see the width of most lines.		
	Disable Firewall to reduce the activity reported in the console.		
	Choose “SecNet->Shutdown” from the SecNet menubar	SecNet is completely shutdown and not even running in the system tray.	
	Run the steps below in the Comments section		
	Launch SecNet and wait about 1 minute for the initial console activity to complete.		
	Set the system clock ahead 3 hours in the “Date and Time” Control Panel		
	Go to Anti-Virus and click “Preferences”		
	Select “Automatic” in the Update “Frequency” dropdown list and click OK		
	Watch the console		
	Verify that within 2 minutes the console reports “Updating the Anti-Virus definition file”		
Expected Results: SecNet’s Anti-Virus services should run automatic virus definition file updates.			
Comments \ Issues: Steps: - Click "Start" to open the "Start" menu			

- Click "Run.." to open the Run dialog
- Type "Regedit" to run the registry editor application
- Goto " HKEY_LOCAL_MACHINE\SOFTWARE\Zero Knowledge\SecNet"
- Double click the registry key “VirusDBUpdateId”
- Edit the current value to be one less than the current value
- Click the “OK” button

2.4.10 Detailed anti-virus scan report: Successful Completion

Description: The Anti-Virus product shall provide a detailed report once the virus scan is successfully completed.			
Test Case ID: QZ335			
GSS Requirements Met: ZAV004			
Author: John Bee			
Date Ran:			
Tester:			
Configuration / Build:			
Machine Number:			
Pre-Condition:			
Bugs found:			
Step	**Description**	**Observation**	**Result**
	Copy virus test file (eicar.com) into a folder		
	Go to the Anti-Virus pane of the SecNet UI and select “Scan Now”		
	Select a few folders to be scanned including the folder where you placed the virus test file, and then click “Scan Now”		
	Let the scan finish to completion	A SecNet Anti-Virus dialog will appear	
	On the dialog, click the “See the detailed report” link	Default browser will launch	
	Verify the default browser launches an HTML report with the details of the scan		
Expected Results: SecNet should provide a detailed report once the virus scan is successfully completed.			
Comments \ Issues: If the default browser is Netscape Navigator 4.74, a Navigator profile will have to be created before the report can be shown. The dialog to create this profile is a Netscape dialog and it’s usually hidden behind SecNet, so make sure you look for it.			

2.4.11 Scanning of POP3 email attachments

Description: The Anti-Virus service provides scanning capability for POP3 email attachments			
Test Case ID: QZ345			
GSS Requirements Met: ZAV005			
Author: John Bee			
Date Ran:			
Tester:			
Configuration / Build: /			
Machine Number:			
Pre-Condition:			
Bugs found:			
Step	**Description**	**Observation**	**Result**
	On the test computer ensure Real Time Anti-Virus is enabled in the SecNet Anti-Virus pane.		
	On the test computer ensure the POP3 email client is not running.		
	From another computer (without SecNet or any other Anti-Virus software active) send an email to the POP3 account of the test computer with the attachment “EICAR.COM”. The message should have the subject “test email subject text” and a message body with the text “test email body text”.		
	On the test computer go to the Anti-Virus pane of the SecNet UI and select “Preferences”		
	On the test computer enable the checkbox titled “Scan incoming email messages and attachments (POP3)”		
	In the dropdown above it, select “Delete the file” and click OK		
	On the test computer launch the POP3 email client. (Receive messages)		
	Confirm that the test message received has no attachment.		
	Confirm that the test message body has text inserted indicating that the attachment has been deleted by SecNet.		
Expected Results: The email attachment should be deleted. The email body should have text inserted which indicates that SecNet has deleted the attachment.			
Comments \ Issues: Note: The email server used for this test is MDaemon (a free mail server available at www.altn.com).			

MDaemon must be installed on a Win2000 or XP machine (it can even be a test machine) on the same Windows domain as the other machines being tested. After it is installed, create a domain (i.e. zeroquar.com) and email accounts for each tester and note the IP address of the machine on which MDaemon is installed. When it comes time to run this test case, the POP3 and SMTP server address for them to use on their test machine email programs (Outlook 2000, Outlook Express, Eudora, etc.) will be the IP address of the machine on which Mdaemon is running.

2.4.12 Date/time of definition update

Description: The Anti-Virus product displays the date and time of the last virus definition update.			
Test Case ID: QZ365			
GSS Requirements Met: ZAV007			
Author: John Bee			
Date Ran:			
Tester:			
Configuration / Build:			
Machine Number:			
Pre-Condition:			
Bugs found:			
Step	**Description**	**Observation**	**Result**
1.	Go to the Anti-Virus pane of the SecNet UI and select “Preferences”		
2.	Click the “Update” button	Notice that next to the update button, it will indicate a quick connection to the server and will return a result like: “The Anti-Virus definition file is up-to-date.”	
3.	Click OK	Look in the Details pane to the right	
4.	Verify that the “Last Update” item indicates the current time		
Expected Results: SecNet’s Anti-Virus service should display the date and time of the last virus definition update.			
Comments \ Issues:			

2.4.13 Date/time of user-initiated scan

Description: The Anti-Virus product displays the date and time of the last virus scan (user-initiated)			
Test Case ID: QZ370			
GSS Requirements Met: ZAV008			
Author: John Bee			
Date Ran:			
Tester:			
Configuration / Build: /			
Machine Number:			
Pre-Condition:			
Bugs found:			
Step	**Description**	**Observation**	**Result**
1.	Go to the Anti-Virus pane of the SecNet UI and select “Scan Now”		
2.	Select a folder to scan and click “Scan Now” button	A dialog will pop-up	
3.	Click OK		
4.	Click “Done”	Look in the Details pane to the right	
5.	Verify the “Last Scan” item indicates the current time		
Expected Results: SecNet’s Anti-Virus service should display, under “Last Scan”, the date and time of the last virus scan.			
Comments \ Issues:			

2.4.14 Date/time of scheduled scan

Description: The Anti-Virus product displays the date and time of the last virus scan (scheduled)			
Test Case ID: QZ375			
GSS Requirements Met: ZAV008			
Author: John Bee			
Date Ran:			
Tester:			
Configuration / Build:			
Machine Number:			
Pre-Condition:			
Bugs found:			
Step	**Description**	**Observation**	**Result**
1.	Go to the Anti-Virus pane of the SecNet UI and select “Scheduled Scan”		
2.	Ensure that the “Enable Scheduled Scan” is checked		
3.	Select only one folder to scan, check the checkbox for the current day of the week and set a time 2 minutes from the current system time		
4.	Click OK	Look in the Details pane to the right	
5.	Verify the “Last Scan” item indicates the current time		
Expected Results: SecNet’s Anti-Virus service should display, under “Last Scan”, the date and time of the last virus scan.			
Comments \ Issues:			

2.4.15 Prompt to disinfect when virus found: manual scan

Description: The Anti-Virus product provides the user with the capability to specify the action (attempt to disinfect the file) to be triggered upon virus detection during a manual scan.			
Test Case ID: QZ380			
GSS Requirements Met: ZAV009			
Author: John Bee			
Date Ran:			
Tester:			
Configuration / Build:			
Machine Number:			
Pre-Condition:			
Bugs found:			
Step	**Description**	**Observation**	**Result**
	Ensure Real Time Anti-Virus is disabled in the SecNet Anti-Virus pane.		
	Create the folder “C:\testSecNet”		
	Copy the sample virus file (eicar.com) to the folder “C:\testSecNet”		
	Go to the Anti-Virus pane of the SecNet UI and select “Scan Now”		
	In the “If a virus is found” dropdown, select the option titled “Disinfect”		
	Expand the tree above and click on the folder “C:\testSecNet”		
	Click “Scan Now”		
	Click OK when scan is finished.		
	Select See Last Report		
	Confirm that the Last Report indicates that: ‘File was infected with “EICAR_Test_File” virus and was unable to be disinfected. The file was deleted instead.’		
Expected Results: Last Report indicates: ‘File was infected with “EICAR_Test_File” virus and was unable to be disinfected. The file was deleted instead.’			
Comments \ Issues:			

2.4.16 Delete file when virus found: manual scan

Description: The Anti-Virus product provides the user with the capability to specify the action (delete the file) to be triggered upon virus detection during a manual scan.			
Test Case ID: QZ392			
GSS Requirements Met: ZAV009			
Author: John Bee			
Date Ran:			
Tester:			
Configuration / Build:			
Machine Number:			
Pre-Condition:			
Bugs found:			
Step	**Description**	**Observation**	**Result**
1.	Copy the sample virus file (eicar.com) to a folder		
2.	Go to the Anti-Virus pane of the SecNet UI and select “Scan Now”		
3.	In the “If a virus is found” dropdown, select the option titled “Delete”		
4.	Expand the tree above and click the folder that contains the sample virus file		
5.	Click “Scan Now”		
6.	Click “See the detailed report” on the pop-up dialog saying that the scan is finished.		
7.	Scroll down to the “Files” section and verify the following text:	“File infected with “EICAR_Test_File” virus and was successfully deleted.”	
8.	Scroll down to the “Report Summary” section and verify the following text:	“Total infected files: 1” “Total deleted files: 1”	
9.	Go to the folder and verify that the file has been deleted		
Expected Results: SecNet’s Anti-Virus services should provide the user with the capability to specify the action (delete infected file) to be triggered upon virus detection during a manual scan			
Comments \ Issues:			

2.4.17 Delete file when virus found: incoming mail

Description: The Anti-Virus product provides the user with the capability to specify the action (delete infected file) to be triggered upon virus detection in an incoming mail.			
Test Case ID: QZ394			
GSS Requirements Met: ZAV009			
Author: John Bee			
Date Ran:			
Tester:			
Configuration / Build:			
Machine Number:			
Pre-Condition:			
Bugs found:			
Step	**Description**	**Observation**	**Result**
1.	Copy the sample virus file (eicar.com) to a folder		
2.	Go to the Anti-Virus pane of the SecNet UI and select “Preferences”		
3.	Select the option titled “Delete the file” in “Real-Time and Email Protection” section		
4.	Shutdown SecNet, toggle to your email program, and create an e-mail with the sample virus file as an attachment to the test machine email account (don’t send it yet)		
5.	Launch SecNet, toggle back to your email and send the mail		
6.	Verify that SecNet detects the virus in the incoming mail and deletes it		
Expected Results: SecNet’s Anti-Virus services should provide the user with the capability to specify the action (delete infected file) to be triggered upon virus detection in an incoming mail.			
Comments \ Issues: Make sure to use the email account set up for testers on the machine running MDaemon.			

2.4.18 "Report only" when virus found: manual scan

Description: The Anti-Virus product provides the user with the capability to specify the action (report only) to be triggered upon virus detection during a manual scan.			
Test Case ID: QZ395			
GSS Requirements Met: ZAV009			
Author: John Bee			
Date Ran:			
Tester:			
Configuration / Build:			
Machine Number:			
Pre-Condition:			
Bugs found:			
Step	**Description**	**Observation**	**Result**
1.	Ensure Real-Time Anti-Virus is disabled in the SecNet Anti-Virus pane.		
2.	Create the folder "C:\testSecNet"		
3.	Copy the sample virus file (eicar.com) to the folder "C:\testSecNet"		
4.	Go to the Anti-Virus pane of the SecNet UI and select "Scan Now"		
5.	In the "If a virus is found" dropdown, select the option titled "Report Only"		
6.	Expand the tree above and click on the folder "C:\testSecNet"		
7.	Click "Scan Now"		
8.	Click OK when the scan is finished.		
9.	Click "See Last report."		
10.	Confirm that the Last Report indicates: 'File is infected with "EICAR_Test_File" virus.'		
Expected Results: Last Report indicates that a File infected with "EICAR_Test_File" virus was found			
Comments \ Issues:			

2.4.19 Define recurrent scan on selected items and different settings

Description: The Anti-virus service shall provide a capability to define recurrent virus scan schedule item(s) by setting the file(s), folder(s) and drive(s) to scan; the day(s) of the week to run the scan, and the time-of-day to run the scan			
Test Case ID: QZ398			
GSS Requirements Met: ZAV010			
Author: Yves Boulanger			
Date Ran:			
Tester:			
Configuration / Build:			
Machine Number:			
Pre-Condition:			
Bugs found:			
Step	**Description**	**Observation**	**Result**
	Copy the sample virus file (eicar.com) to a folder		
	Go to the Anti-Virus pane of the SecNet UI and select “Scheduled Scan”		
	Click “Enable scheduled scan”		
	Under “Items to scan”, select a few folders including the folder that contained the sample virus file		
	Under “Scan Schedule” set the time to 2 minutes ahead of the current time, set every 1 week, and set the day of the week to today’s date		
	Under “Action” set it to Report Only		
	Close SecNet and wait for the scheduled scan time to pass		
	Open SecNet UI and go to the Anti-Virus pane. Verify that the date of the last scan has been changed to the set scheduled scan time		
	Under “Scan Now” click “see last report”. Verify that the selected files were scanned at the specified time.		
Expected Results: SecNet’s Anti-virus service should have scanned the selected items at the scheduled time			
Comments \ Issues:			

2.4.20 The Anti-Virus service shall keep a detailed log of last scan results

Description: The Anti-Virus service shall maintain a detailed log of last scan results detailing boot sector, drives, folders and files scans			
Test Case ID: QZ399			
GSS Requirements Met: ZAV014			
Author: Yves Boulanger			
Date Ran:			
Tester:			
Configuration / Build:			
Machine Number:			
Pre-Condition:			
Bugs found:			
Step	**Description**	**Observation**	**Result**
	Copy the sample virus file (eicar.com) to a folder		
	Go to the Anti-Virus pane of the SecNet UI and select “Scan Now”		
	Under “Items to scan”, select a drive, a few files and folders including the folder that contains the sample virus file		
	Click on “Scan Now”		
	Click “See the detailed report” on the pop-up dialog saying that the scan is finished.		
	Verify that the log report details the boot sector, drives, folders and files scanned		
Expected Results: SecNet’s Anti-Virus scan provides a detailed report of the scanned items.			
Comments \ Issues:			

2.4.21 Disabling real-time protection against viruses

Description: The Anti-Virus service provides the capability to enable or disable a real-time protection against viruses			
Test Case ID: QZ401			
GSS Requirements Met: ZAV011			
Author: Yves Boulanger			
Date Ran:			
Tester:			
Configuration / Build: /			
Machine Number:			
Pre-Condition:			
Bugs found:			
Step	**Description**	**Observation**	**Result**
	Disable Real-time Anti-Virus protection in SecNet		
	Create a directory c:\testSecNet		
	Copy the test virus (eicar.com) to the c:\testSecNet directory		
	Launch eicar.com from c:\testSecNet using Windows Explorer	The DOS application should launch.	
	Go to the Anti-Virus pane of the SecNet UI and select “Preferences”		
	Under “Real-time and e-mail protection”, select “Delete the file”		
	Enable Real-time Anti-Virus protection in SecNet		
	Launch eicar.com from c:\testSecNet using the Windows Explorer	SecNet indicates a virus has been found and deleted.	
Expected Results: SecNet’s Anti-Virus service provides real time virus protection			
Comments \ Issues:			

2.4.22 Real-time anti-virus services should detect infected files in use

Description: The Anti-Virus service warns the user about infected files that are in use, recommends running a full scan and ensures such files are tagged to be deleted after next reboot			
Test Case ID: QZ402			
GSS Requirements Met: ZAV012			
Author: Yves Boulanger			
Date Ran:			
Tester:			
Configuration / Build: /			
Machine Number:			
Pre-Condition:			
Bugs found:			
Step	**Description**	**Observation**	**Result**
	Disable SecNet Real-time Anti-Virus		
	Shutdown SecNet and create a directory c:\testSecNet and copy the virus test file (eicar.com from www.eicar.org) into it		
	Copy the test application (testApp.exe) into c:\testSecNet		
	Launch a command prompt window		
	In command prompt navigate to c:\testSecNet		
	In command prompt execute the command: testApp eicar.com		
	Launch SecNet and enable SecNet Real-time Anti-Virus		
	With Windows Explorer, single-click on the file eicar.com in c:\testSecNet (put focus on eicar.com but do not launch it)	(Note: On W9x machines, you will have to double-click the eicar.com file)	
	Verify that SecNet warns the user of an in-use infected file.	Message indicates SecNet is unable to disinfect the file and was deleted instead. Advises user to run a system scan.	
Expected Results: Real-time anti-virus services should detect the presence of an in use infected file			
Comments \ Issues:			

2.5 Firewall

2.5.1 Warning dialog about unauthorized programs

Description: The firewall service warns users when unauthorized programs attempt to send information to remote machines over the internet.			
Test Case ID: QZ400			
GSS Requirements Met: ZFW001			
Author: John Bee			
Date Ran:			
Tester:			
Configuration / Build: /			
Machine Number:			
Pre-Condition:			
Bugs found:			
Step	**Description**	**Observation**	**Result**
	If Firewall is not enabled in the SecNet UI, enable it.		
	Launch whatever web chat application is installed on your PC		
	Verify a pop-up dialog appears asking you to allow or deny access to that application		
Expected Results: SecNet should warn the user about unauthorized programs trying to send information to remote machines over the internet			
Comments \ Issues:			

2.5.2 Ability to disable firewall

Description: The firewall service provides a capability which allows users to disable the firewall functionality.			
Test Case ID: QZ405			
GSS Requirements Met: ZFW002, ZFW003			
Author: John Bee			
Date Ran:			
Tester:			
Configuration / Build: /			
Machine Number:			
Pre-Condition:			
Bugs found:			
Step	**Description**	**Observation**	**Result**
	Open the SecNet UI, and go to Firewall		
	Click “Internet Access Rules” and click the gray “?” (question mark icon) next to your web chat application, then click OK		
	Launch whatever web chat application is installed on your PC		
	Verify a pop-up dialog appears asking you to allow or deny access to that application. CLICK ON BLOCK		
	Go to Firewall pane and disable the firewall by unselecting the check box next to “Enable Firewall”		
	Exit, then launch the web chat application installed on your PC		
	Verify that no pop-up dialog appears and that communication between chat program and its server are established		
Expected Results: The firewall services can be disabled			
Comments \ Issues:			

2.5.3 Allow a program to access internet

Description: The firewall service provides a capability which allows users to allow a program to access the internet			
Test Case ID: QZ410			
GSS Requirements Met: ZFW004			
Author: John Bee			
Date Ran:			
Tester:			
Configuration / Build: /			
Machine Number:			
Pre-Condition:			
Bugs found:			
Step	**Description**	**Observation**	**Result**
1.	Install and activate SecNet		
2.	After activation, restart the PC. The firewall services should be enabled by default.		
3.	Launch IE	If a SecNet pop-up dialog appears asking you to allow or deny access to that application click “Allow” and make sure the check box to remember this action is checked	
4.	Exit IE		
5.	Open the SecNet UI and click Firewall		
6.	Click “Internet Access Rules”. Under actions select a red x mark for IE		
7.	Click OK to activate your action		
8.	Launch IE and verify that IE can not access the internet		
9.	Exit IE		
10.	Open the SecNet UI and click Firewall		
11.	Click “Internet Access Rules”. Under actions select a green check mark for IE		
12.	Click OK to activate your action		
13.	Launch IE and verify that now you can access the Web		
Expected Results: SecNet should allow user selected programs to access the internet			
Comments \ Issues:			

2.5.4 Block a program from accessing internet

Description: The firewall service provides a capability which allows users to block a program from accessing the internet.			
Test Case ID: QZ415			
GSS Requirements Met: ZFW004			
Author: John Bee			
Date Ran:			
Tester:			
Configuration / Build: /			
Machine Number:			
Pre-Condition:			
Bugs found:			
Step	**Description**	**Observation**	**Result**
	Launch whatever web chat application is installed on your PC		
	When the SecNet pop-up dialog appears asking you to allow or deny access to that application, click "Allow" and make sure the check box to remember this action is checked	(Note: SecNet dialog will not appear unless your chat application has a SecNet firewall setting of "?" on the Internet Access Rules page.)	
	Exit the web chat application	*Ensure web chat application is exited from the taskbar. (note some chat applications – such as Yahoo Messenger – must be shut down from task bar)*	
	Open the SecNet UI and click Firewall		
	Click "Internet Access Rules" and verify that a green checkmark is displayed under actions for the chat application		
	Under actions select a red x mark for the chat application		
	Click OK to activate your action		
	Launch the chat application		
	Verify that SecNet will not allow the chat application to communicate with the web		
Expected Results: SecNet should block user selected programs from accessing the internet			
Comments \ Issues:			

2.5.5 Add programs to the access list

Description: The firewall service provides a capability which allows users to add programs for which internet access rules can be defined.			
Test Case ID: QZ420			
GSS Requirements Met: ZFW005, ZFW007			
Author: John Bee			
Date Ran:			
Tester:			
Configuration / Build: /			
Machine Number:			
Pre-Condition:			
Bugs found:			
Step	**Description**	**Observation**	**Result**
1.	Open the SecNet UI and click Firewall	The “Enable Firewall” checkbox must be enabled	
2.	Click “Internet Access Rules” and click “Add Program”		
3.	Select an executable file and verify it appears in the program list		
4.	Verify its options can be set to “allow”, “block”, or “prompt”		
Expected Results: Verify its options can be set to allow, block, or prompt			
Comments \ Issues:			

2.5.6 Remove a program with defined access rules: Block

Description: The firewall service provides a capability which allows users to remove programs for which internet access rules are defined as “Block”.			
Test Case ID: QZ425			
GSS Requirements Met: ZFW006			
Author: John Bee			
Date Ran:			
Tester:			
Configuration / Build: /			
Machine Number:			
Pre-Condition:			
Bugs found:			
Step	**Description**	**Observation**	**Result**
	Open the SecNet UI and click Firewall	The “Enable Firewall” checkbox must be enabled	
	Click “Internet Access Rules”, select one of the registered programs that has a “Block” status, and then click “Remove Program”		
	Verify that the program no longer appears in the list		
	Launch the app and verify it can connect to the internet and a SecNet pop-up displays, asking if it is ok that it connect.		
Expected Results: Launch the app and verify it can connect to the internet and a SecNet pop-up displays, asking if it is ok that it connect.			
Comments \ Issues:			

2.5.7 Remove a program with defined access rules: Allow

Description: The firewall service provides a capability which allows users to remove programs for which internet access rules are defined as “Allow”.			
Test Case ID: QZ430			
GSS Requirements Met: ZFW006, ZFW007			
Author: John Bee			
Date Ran:			
Tester:			
Configuration / Build: /			
Machine Number:			
Pre-Condition: “Internet Explorer” has a SecNet Firewall Internet Access Rule of ALLOW.			
Bugs found:			
Step	**Description**	**Observation**	**Result**
1.	Ensure “Internet Explorer” is closed.		
2.	Open the SecNet UI and click Firewall.	The “Enable Firewall” checkbox must be enabled	
3.	Click “Internet Access Rules”, select “Internet Explorer” which has an “Allow” status, and then click “Remove Program” then click “OK”		
4.	Verify that “Internet Explorer” no longer appears in the list		
5.	Launch “Internet Explorer” and verify that a SecNet pop-up displays, asking if it is ok to connect.		
6.	Select Allow in SecNet pop-up and confirm that “Internet Explorer” can access the Internet.		
Expected Results: Launch “Internet Explorer” and verify it can connect to the internet and that a SecNet pop-up displays, asking if it is ok for “Internet Explorer” to connect.			
Comments \ Issues:			

2.5.8 Manage program's firewall rules: Customize

Description: The firewall service provides a capability which allows users to customize program rules to either Allow, Block, or Prompt for Inbound/Outbound connectivity.			
Test Case ID: QZ435			
GSS Requirements Met: ZFW008			
Author: John Bee			
Date Ran:			
Tester:			
Configuration / Build: /			
Machine Number:			
Pre-Condition:			
Bugs found:			
Step	**Description**	**Observation**	**Result**
1.	Open the SecNet UI and click Firewall	The "Enable Firewall" checkbox must be enabled	
2.	Click "Internet Access Rules", select one of the registered programs and then click the "Customize Rules" button		
3.	Select a program with an Inbound tag and click the radio button titled "Disable this rule" and then click OK		
4.	Select the program's Outbound tag and click the radio button titled "Block" and then click OK		
5.	Verify that the program now has a check-plus icon beside it		
Expected Results: Verify that the program now has a check-plus icon beside it			
Comments \ Issues:			

2.5.9 Manage program's firewall rules: Disable

Description: The firewall service provides a capability which allows users to disable the rules for a registered program.			
Test Case ID: QZ440			
GSS Requirements Met: ZFW008			
Author: John Bee			
Date Ran:			
Tester:			
Configuration / Build: /			
Machine Number:			
Pre-Condition:			
Bugs found:			
Step	**Description**	**Observation**	**Result**
1.	Open the SecNet UI and click Firewall	The "Enable Firewall" checkbox must be enabled	
2.	Click "Internet Access Rules", select one of the registered programs that has an "Allow" status, and then click the "Customize Rules" button		
3.	Select a program with an (Inbound) tag and click the radio button titled "Disable this rule" and then click OK		
4.	Select the program's (Outbound) tag and click the radio button titled "Disable this rule" and then click OK		
5.	Verify that the program now has a blue question mark beside it		
Expected Results: Verify that the program now has a blue question mark beside it			
Comments \ Issues:			

2.5.10 View active connections

Description: The firewall service provides a capability which allows users to view a list of programs with active connections.			
Test Case ID: QZ445			
GSS Requirements Met: ZFW009			
Author: John Bee			
Date Ran:			
Tester:			
Configuration / Build: /			
Machine Number:			
Pre-Condition:			
Bugs found:			
Step	**Description**	**Observation**	**Result**
1.	Open the SecNet UI and click Firewall	The “Enable Firewall” checkbox must be enabled	
2.	Click “Active Connections”		
3.	Verify a list of programs with “Activity” and “Since” columns”		
4.	Click “Details” and verify a more detailed list of programs		
Expected Results: Click “Details” and verify a more detailed list of programs			
Comments \ Issues:			

2.5.11 View log of blocked connections

Description: The firewall service provides a capability which allows users to view a log of blocked connections.			
Test Case ID: QZ450			
GSS Requirements Met: ZFW010			
Author: John Bee			
Date Ran:			
Tester:			
Configuration / Build: /			
Machine Number:			
Pre-Condition:			
Bugs found:			
Step	**Description**	**Observation**	**Result**
1.	Open the SecNet UI and click Firewall	The “Enable Firewall” checkbox must be enabled	
2.	Click “View Log”		
3.	Verify a list of blocked packets is shown. If none are shown, make sure Internet Explorer is cleared from the Internet Access Rules list and then launch it. When a SecNet dialog appears asking for access, block it, wait approximately 5 minutes, then go back to the log and see that packets have been blocked.		
Expected Results: Verify a list of blocked packets is shown			
Comments \ Issues:			

2.6 Anti-Spyware

2.6.1 Delete all detected spyware

Description: The Anti-Spyware product provides the user with the capability to delete all detected spyware from the users machine			
Test Case ID: QZ500			
GSS Requirements Met: ZAS001			
Author: John Bee			
Date Ran:			
Tester:			
Configuration / Build: /			
Machine Number:			
Pre-Condition:			
Bugs found:			
Step	**Description**	**Observation**	**Result**
1.	Open the SecNet UI, and click Anti-Spyware	The “Enable real-time spyware protection” checkbox must be enabled	
2.	In the “Statistics” frame, under “Spyware Detected”, click “Current List”		
3.	Check the checkboxes of any detected spyware and then click the Delete button	A pop-up dialog will appear, asking if you are sure you want to go through with the deletion	
4.	Click Yes, and verify that the selected spyware is removed from the list		
Expected Results: Click Yes, and verify that the selected spyware is removed from the list			
Comments \ Issues:			

2.6.2 Scheduled scan of spyware

Description: The Anti-Spyware product provides a capability to establish a scan schedule.			
Test Case ID: QZ505			
GSS Requirements Met: ZAS003			
Author: John Bee			
Date Ran:			
Tester:			
Configuration / Build: /			
Machine Number:			
Pre-Condition:			
Bugs found:			
Step	**Description**	**Observation**	**Result**
	Open the SecNet UI, and click Anti-Spyware	The "Enable real-time spyware protection" checkbox must be enabled	
	Click "Scheduled Scan"		
	Click "Enable Scheduled Scan"		
	Expand the directory tree and select a folder to scan		
	In the "Start time" box, type a time that is two minutes from the current time		
	Select the current day of the week, and then click OK	A pop-up dialog will appear to say to make sure SecNet is running. Click OK on this dialog	
	When the scheduled time arrives, verify SecNet shows a little icon in the system tray when the scan runs	Mouse over the icon and it will say "Anti-Spyware is scanning for Spyware"	
	Verify that the "Last Scan" time indicated in the "Statistics" frame of the Anti-Spyware UI indicates the correct time of the last scan		
Expected Results: Verify that the "Last Scan" time indicated in the "Statistics" frame of the Anti-Spyware UI indicates the correct time of the last scan			
Comments \ Issues:			

2.6.3 Real-time scan of spyware

Description: The Anti-Spyware product detects Spyware.			
Test Case ID: QZ510			
GSS Requirements Met: ZAS002			
Author: John Bee			
Date Ran:			
Tester:			
Configuration / Build: /			
Machine Number:			
Pre-Condition:			
Bugs found:			
Step	**Description**	**Observation**	**Result**
1.	Open the SecNet UI, and click Anti-Spyware	The "Enable real-time spyware protection" checkbox must be enabled	
2.	Set Anti-Spyware preferences as follows: Disable delete tracking cookies Enable display new spyware found every 0 hour(s) and 10 minutes		
3.	Click "Current List" and verify that Alexa is not on the list. If so delete it.		
4.	Go to a known spyware website (www.alexa.com to install the alexa toolbar)		
5.	Ensure Alexa toolbar is installed in IE		
6.	Open the SecNet UI, and select Anit-Spyware – Current List.		
7.	Wait for 10 minutes		
8.	Confirm that Alexa registry entries appear in the Anti-Spyware – Current List.		
Expected Results: Anti-Spyware – Current List will indicate details about Alexa spyware and have identified Alexa registry entries.			
Comments \ Issues:			

2.6.4 Anti-Spyware service maintains a log of current and deleted spyware

Description: The Anti-Spyware service shall maintain a log of deleted spyware and a list of non-deleted spyware.			
Test Case ID: QZ511			
GSS Requirements Met: ZAS006			
Author: John Bee			
Date Ran:			
Tester:			
Configuration / Build: /			
Machine Number:			
Pre-Condition:			
Bugs found:			
Step	**Description**	**Observation**	**Result**
	Open the SecNet UI, and click Anti-Spyware	The "Enable real-time spyware protection" checkbox must be enabled	
	Click "Current List" and verify that Alexa is on the list.		
	Open the SecNet UI, and select Anit-Spyware – View Log.		
	Confirm that an Alexa entry appears in the list with today's date.		
Expected Results: Anti-Spyware – Log should have an Alexa entry under the "Spyware deleted" column with the date it was deleted (today's date).			
Comments \ Issues:			

2.6.5 Schedule spyware definition file update: Automatic

Description: The Anti-Spyware service shall provide a capability to establish scheduled automatic checks for Spyware definition file updates.			
Test Case ID: QZ515			
GSS Requirements Met: ZAS004			
Author: John Bee			
Date Ran:			
Tester:			
Configuration / Build: /			
Machine Number:			
Pre-Condition: SecNet should be installed, activated, and running for at least 5 minutes. This is to allow enough time for all initial startup updates to occur and create the registry values that are used.			
Bugs found:			
Step	**Description**	**Observation**	**Result**
	Go to Anti-Spyware and click "Preferences"		
	Select "Manual" in the Update "Frequency" dropdown list and click OK		
	Choose "View->Console" from the SecNet menubar	The "Event Console" opens.	
	Size the "Event Console" so you can see the width of most lines.		
	Disable Firewall to reduce the activity reported in the console.		
	Choose "SecNet->Shutdown" from the SecNet menubar	SecNet is completely shutdown and not even running in the system tray.	
	Run the steps below in the Comments section		
	Launch SecNet and wait about 1 minute for the initial console activity to complete.		
	Set the system clock ahead 3 hours in the "Date and Time" Control Panel		
	Go to Anti-Spyware and click "Preferences"		
	Select "Automatic" in the Update "Frequency" dropdown list and click OK		
	Watch the console		
	Verify that within 2 minutes the console reports "Updating the Anti-Spyware definition file"		
Expected Results: SecNet's Anti-Spyware services should run automatic spyware definition file updates.			
Comments \ Issues: Steps:			

- Click "Start" to open the "Start" menu
- Click "Run.." to open the Run dialog
- Type "Regedit" to run the registry editor application
- Goto " HKEY_LOCAL_MACHINE\SOFTWARE\Zero Knowledge\SecNet"
- Double click the registry key “SpywareDBUpdateId”
- Edit the current value to be one less than the current value
- Click the “OK” button

2.6.6 Scheduled spyware definition file update: Manual

Description: The Anti-Spyware service shall provide a capability to establish scheduled manual checks for spyware definition file updates.			
Test Case ID: QZ520			
GSS Requirements Met: ZAS004			
Author: John Bee			
Date Ran:			
Tester:			
Configuration / Build: /			
Machine Number:			
Pre-Condition: SecNet should be installed, activated, and running for at least 5 minutes. This is to allow enough time for all initial startup updates to occur and create the registry values that are used.			
Bugs found:			
Step	**Description**	**Observation**	**Result**
1.	Go to Anti-Spyware and click “Preferences”		
2.	Select “Manual” in the Update “Frequency” dropdown list and click OK		
3.	Choose “View->Console” from the SecNet menubar	The “Event Console” opens.	
4.	Size the “Event Console” so you can see the width of most lines.		
5.	Disable Firewall to reduce the activity reported in the console.		
6.	Choose “SecNet->Shutdown” from the SecNet menubar	SecNet is completely shutdown and not even running in the system tray.	
7.	Run the steps below in the Comments section		
8.	Launch SecNet and wait 1 minute for the initial console activity to complete.		
9.	Go to Anti-Spyware and click “Preferences”		
10.	Click the “Update” button in the update area		
11.	Watch the console		
12.	Verify that the console reports “Updating the Anti-Spyware definition file”		
Expected Results: SecNet’s Anti-spyware services should run manual spyware definition file updates when requested by the user.			
Comments \ Issues: Steps: - Click "Start" to open the "Start" menu - Click "Run.." to open the Run dialog - Type "Regedit" to run the registry editor application - Goto " HKEY_LOCAL_MACHINE\SOFTWARE\Zero Knowledge\SecNet"			

- Double click the registry key “SpywareDBUpdateId”
- Edit the current value to be one less than the current value
- Click the “OK” button

2.6.7 Scheduled spyware definition file update: Daily

Description: The Anti-Spyware service shall provide a capability to establish scheduled daily checks for spyware definition file updates.			
Test Case ID: QZ525			
GSS Requirements Met: ZAS004			
Author: John Bee			
Date Ran:			
Tester:			
Configuration / Build: /			
Machine Number:			
Pre-Condition: SecNet should be installed, activated, and running for at least 5 minutes. This is to allow enough time for all initial startup updates to occur and create the registry values that are used.			
Bugs found:			
Step	**Description**	**Observation**	**Result**
	Go to Anti-Spyware and click "Preferences"		
	Select "Manual" in the Update "Frequency" dropdown list and click OK		
	Choose "View->Console" from the SecNet menubar	The "Event Console" opens.	
	Size the "Event Console" so you can see the width of most lines.		
	Disable Firewall to reduce the activity reported in the console.		
	Choose "SecNet->Shutdown" from the SecNet menubar	SecNet is completely shutdown and not even running in the system tray.	
	Run the steps below in the Comments section		
	Launch SecNet and wait about 1 minute for the initial console activity to complete.		
	Set the system date ahead 1 day in the "Date and Time" Control Panel		
	Go to Anti-Spyware and click "Preferences"		
	Select "Daily" in the Update "Frequency" dropdown list and click OK		
	Watch the console		
	Verify that within 2 minutes the console reports "Updating the Anti-Spyware definition file"		
Expected Results: SecNet's Anti-spyware services should run a scheduled daily check for spyware definition file updates.			
Comments \ Issues: Steps:			

- Click "Start" to open the "Start" menu
- Click "Run.." to open the Run dialog
- Type "Regedit" to run the registry editor application
- Goto " HKEY_LOCAL_MACHINE\SOFTWARE\Zero Knowledge\SecNet"
- Double click the registry key “SpywareDBUpdateId”
- Edit the current value to be one less than the current value
- Click the “OK” button

2.6.8 Scheduled spyware definition file update: Weekly

Description: The Anti-Spyware service shall provide a capability to establish scheduled weekly checks for spyware definition file updates.			
Test Case ID: QZ530			
GSS Requirements Met: ZAS004			
Author: John Bee			
Date Ran:			
Tester:			
Configuration / Build: /			
Machine Number:			
Pre-Condition: SecNet should be installed, activated, and running for at least 5 minutes. This is to allow enough time for all initial startup updates to occur and create the registry values that are used.			
Bugs found:			
Step	**Description**	**Observation**	**Result**
	Go to Anti-Spyware and click "Preferences"		
	Select "Manual" in the Update "Frequency" dropdown list and click OK		
	Choose "View->Console" from the SecNet menubar	The "Event Console" opens.	
	Size the "Event Console" so you can see the width of most lines.		
	Disable Firewall to reduce the activity reported in the console.		
	Choose "SecNet->Shutdown" from the SecNet menubar	SecNet is completely shutdown and not even running in the system tray.	
	Run the steps below in the Comments section		
	Launch SecNet and wait about 1 minute for the initial console activity to complete.		
	Set the system date ahead 1 week in the "Date and Time" Control Panel		
	Go to Anti-Spyware and click "Preferences"		
	Select "Weekly" in the Update "Frequency" dropdown list and click OK		
	Watch the console		
	Verify that within 2 minutes the console reports "Updating the Anti-Spyware definition file"		
Expected Results: SecNet's Anti-spyware services should run a scheduled weekly check for spyware definition file updates.			
Comments \ Issues: Steps:			

- Click "Start" to open the "Start" menu
- Click "Run.." to open the Run dialog
- Type "Regedit" to run the registry editor application
- Goto " HKEY_LOCAL_MACHINE\SOFTWARE\Zero Knowledge\SecNet"
- Double click the registry key “SpywareDBUpdateId”
- Edit the current value to be one less than the current value
- Click the “OK” button

2.6.9 Date/time of last Spyware definition update

Description: The Anti-Spyware product displays the date and time of the last Spyware definition update.			
Test Case ID: QZ535			
GSS Requirements Met: ZAS005			
Author: John Bee			
Date Ran:			
Tester:			
Configuration / Build: /			
Machine Number:			
Pre-Condition:			
Bugs found:			
Step	**Description**	**Observation**	**Result**
	Open the SecNet UI, and click Anti-Spyware	The "Enable real-time spyware protection" checkbox must be enabled	
	Click Preferences, click the Update button, and then click OK		
	Verify that the "Last Update" section of the Statistics frame displays the date and time of the last definition file update		
Expected Results: Verify that the "Last Update" section of the Statistics frame displays the date and time of the last definition file update			
Comments \ Issues:			

2.7 Pop-up / Ad Blocker

2.7.1 Blocks IE generated pop-ups

Description: The Pop-up Blocker provides the capability to block Internet Explorer-generated pop-up windows			
Test Case ID: QZ600			
GSS Requirements Met: ZPB001			
Author: John Bee			
Date Ran:			
Tester:			
Configuration / Build: /			
Machine Number:			
Pre-Condition:			
Bugs found:			
Step	**Description**	**Observation**	**Result**
	Go to SecNet UI and select Pop-Up Blocker pane		
	Check the Pop-up Blocker checkbox to enable Pop-Up Blocker		
	Open Internet Explorer		
	In IE, open http://www.beta.SecNet.net/test/tcpopup/TC_Popups_JS.html		
	Verify that onLoad.html, fromHead.html and fromBody.html pop ups are not opened		
	Close IE		
	Verify that onUnload.html popup is not opened		
Expected Results: Ensure Pop-ups are blocked.			
Comments \ Issues:			

2.7.2 SecNet maintains a log of blocked pop-ups

Description: The Popup Blocker service shall maintain a log of blocked pop-ups			
Test Case ID: QZ601			
GSS Requirements Met: ZPB008			
Author: Yves Boulanger			
Date Ran:			
Tester:			
Configuration / Build: /			
Machine Number:			
Pre-Condition: TC QZ600			
Bugs found:			
Step	**Description**	**Observation**	**Result**
1.	Go to SecNet UI and select Pop Up Blocker pane		
2.	NOTE: If Yahoo Toolbar or Alexa are running, make sure they are shut down or removed because their toolbars will catch pop-ups first.		
3.	Enable the Pop-Up Blocker		
4.	Click on View Log		
5.	Select Clear Log		
6.	Close SecNet		
7.	Open Internet Explorer		
8.	go to the web page: http://www.beta.SecNet.net/test/tcpopup/TC_Popups_JS.html		
9.	Open SecNet		
10.	Go to the Pop-Up Blocker pane		
11.	Click on View Log		
12.	Verify that a log indicates Pop-Ups have been blocked from the web page: www.beta.SecNet.net/test/tcpopup/TC_Popups_JS.html		
Expected Results: Log file indicates Pop ups were blocked from the web page: www.beta.SecNet.net/test/tcpopup/TC_Popups_JS.html have been blocked.			
Comments \ Issues:			

2.7.3 Blocks HTTP web ads

Description: The Pop-up Blocker provides the capability to block web browser HTTP ads.			
Test Case ID: QZ605			
GSS Requirements Met: ZPB002			
Author: John Bee			
Date Ran:			
Tester:			
Configuration / Build: /			
Machine Number:			
Pre-Condition:			
Bugs found:			
Step	**Description**	**Observation**	**Result**
1.	Go to SecNet UI and select Pop Up Blocker pane		
2.	Check the box Enable Ad Blocker		
3.	load web page http://www.beta.SecNet.net/test/qd/TCAd.html		
4.	Verify that the sample ads, a red apple and a green apple in the SAMPLE ADs column of the table, are not visible		
Expected Results: SecNet should block pop up ads			
Comments \ Issues:			

2.7.4 Disabling Pop-Up Blocker

Description: The user must be able to disable the Pop-up Blocker feature.			
Test Case ID: QZ610			
GSS Requirements Met: ZPB004			
Author: John Bee			
Date Ran:			
Tester:			
Configuration / Build: /			
Machine Number:			
Pre-Condition: Ensure Internet Explorer 6.0 is installed on test workstation			
Bugs found:			
Step	**Description**	**Observation**	**Result**
1.	Go to SecNet UI and select Pop Up Blocker pane		
2.	Uncheck the box Pop-up Blocker to disable Pop-Up Blocker		
3.	Open Internet Explorer		
4.	In IE open http://www.beta.SecNet.net/test/tcpopup/TC_Popups_JS.html		
5.	Verify that onLoad.html, fromHead.html and fromBody.html pop ups are opened		
6.	Close IE		
7.	Verify that onUnload.html popup is opened		
8.	Close onLoad.html, fromHead.html fromBody.html, and onUnload.html pop ups		
Expected Results: Ensure pop-ups are allowed.			
Comments \ Issues:			

2.7.5 Disabling Ad-Blocker

Description: The user must be able to disable the Ad Blocker feature			
Test Case ID: QZ615			
GSS Requirements Met: ZPB005			
Author: John Bee			
Date Ran:			
Tester:			
Configuration / Build: /			
Machine Number:			
Pre-Condition:			
Bugs found:			
Step	**Description**	**Observation**	**Result**
1.	Go to SecNet UI and select Pop Up Blocker pane		
2.	Uncheck the box Enable Ad Blocker to disable the Ad Blocker		
3.	Load web page http://www.beta.SecNet.net/test/qd/TCAd.html		
4.	Verify that the sample ads, a red apple and a green apple in the SAMPLE ADs column of the table, are visible		
Expected Results: SecNet should allow pop up ads			
Comments \ Issues:			

2.7.6 Manually update blocked ads list

Description: The Ad Blocker service provides the capability to manually update the Blocked Ads List			
Test Case ID: QZ620			
GSS Requirements Met: ZPB006			
Author: John Bee			
Date Ran:			
Tester:			
Configuration / Build: /			
Machine Number:			
Pre-Condition:			
Bugs found:			
Step	**Description**	**Observation**	**Result**
1.	Go to SecNet UI and select Pop Up Blocker pane		
2.	Click the Blocked ads list link		
3.	Confirm Blocked ads list is empty	Blocked ads should be empty after a fresh installation of SecNet	
4.	Click on Update Now	The Blocked ads list should be populated as a result of the Update	
5.	Verify that the Blocked Ad list is populated		
Expected Results: SecNet's blocked ads list is populated as a result of the Update Now.			
Comments \ Issues:			

2.7.7 Add address to blocked ads list

Description: The Ad Blocker service provides the capability for adding an address to the Blocked Ads List			
Test Case ID: QZ625			
GSS Requirements Met: ZPB007			
Author: John Bee			
Date Ran:			
Tester:			
Configuration / Build: /			
Machine Number:			
Pre-Condition:			
Bugs found:			
Step	**Description**	**Observation**	**Result**
1.	Go to SecNet UI, select Pop Up Blocker pane and click on Blocked Ads List		
2.	Check that "www.beta.SecNet.net/test/qd/XYZ/" is not in listed in the BLOCKED ADS list		
3.	Shutdown SecNet UI (and from the system tray)		
4.	Launch SecNet		
5.	Go to SecNet UI, select Pop Up Blocker pane and check that the Ad Blocker is enabled		
6.	Using IE, load the page http://www.beta.SecNet.net/test/qd/TCXYZ.html	NOTE: Ensure this URL is entered exactly as specified in steps including capital letters. Refresh if required.	
7.	Confirm that two apples are visible in sample ads table entry		
8.	Close IE		
9.	Go to SecNet UI, select Pop Up Blocker pane, click on Blocked Ads List, and click on NEW		
10.	Add www.beta.SecNet.net/test/qd/XYZ/ to list of blocked ads then click OK	NOTE: Ensure this URL is entered exactly as specified in steps including capital letters and trailing slash.	
11.	Using IE, load the page http://www.beta.SecNet.net/test/qd/TCXYZ.html	NOTE: Ensure this URL is entered exactly as specified, capital letters and all.	
12.	Confirm two apples are NOT visible in sample ads table entry		
13.	Close IE		
14.	Delete		

	www.beta.SecNet.net/test/qd/XYZ/ from SecNet Blocked Ads List the click OK		
15.	Using IE, load page http://www.beta.SecNet.net/test/qd/TCXYZ.html	NOTE: Ensure this URL is entered exactly as specified in steps including capital letters and trailing slash.	
16.	Verify that two apples are visible in sample ads table entry		
Expected Results: The Ad Blocker service should provide the capability for adding an address to the Blocked Ads List			
Comments \ Issues:			

2.8 Privacy Manager

2.8.1 Detect user-listed keywords via HTTP

Description: The Privacy Manager shall provide the capability to detect user-listed keywords communicated through applications using HTTP protocols			
Test Case ID: QZ700			
GSS Requirements Met: ZPM001			
Author: John Bee			
Date Ran:			
Tester:			
Configuration / Build: /			
Machine Number:			
Pre-Condition: "Privacy Manager -> Protect Personal Information -> Keyword list area" is empty			
Bugs found:			
Step	**Description**	**Observation**	**Result**
1.	Click the Privacy Manager link.		
2.	Ensure that the "Enable Privacy Manager" checkbox is checked, and click "Protect Personal Information"		
3.	In the keyword list area, in the add text field, enter a "keyword" (text or alphanumeric).		
4.	Click Add and then click OK.		
5.	Launch a site with a search engine.		
6.	Enter the "keyword" into the search field and then click search.		
7.	Verify that Privacy Manager detects the use of the "keyword" for outgoing HTTP protocol.		
Expected Results: Verify that Privacy Manager detects the use of the "keyword" for outgoing HTTP protocol.			
Comments \ Issues:			

2.8.2 Allow HTTP detected communication of user-listed info

Description: The Privacy Manager product provides the capability for the user to allow HTTP detected communication of the user-listed information.			
Test Case ID: QZ701			
GSS Requirements Met: ZPM003			
Author: John Bee			
Date Ran:			
Tester:			
Configuration / Build: /			
Machine Number:			
Pre-Condition: Test Case QZ700			
Bugs found:			
Step	**Description**	**Observation**	**Result**
	In the "SecNet – Privacy Manager" dialog box, click Allow.		
	Verify that the Privacy Manager will allow the use of the "keyword" successfully for HTTP protocol.		
Expected Results: Verify that the Privacy Manager will allow the use of the "keyword" successfully for HTTP protocol.			
Comments \ Issues:			

2.8.3 Detect user-listed keywords via SMTP

Description: The Privacy Manager shall provide the capability to detect user-listed keywords communicated through applications using SMTP protocol.			
Test Case ID: QZ705			
GSS Requirements Met: ZPM001			
Author: John Bee			
Date Ran:			
Tester:			
Configuration / Build: /			
Machine Number:			
Pre-Condition: "Privacy Manager -> Protect Personal Information -> Keyword list area" is empty			
Bugs found:			
Step	**Description**	**Observation**	**Result**
1.	Click the Privacy Manager link.		
2.	Click the Protect Personal Information link.		
3.	In the keyword list area, in the add text field, enter a "keyword" (text or alphanumeric).		
4.	Click Add and then click OK.		
5.	Launch the email application loaded on the platform		
6.	Attempt to send an email with the keyword in the body of the email.		
7.	Verify that Privacy Manager detects the "keyword" for outgoing SMTP protocol.		
Expected Results: Verify that Privacy Manager detects the "keyword" for outgoing SMTP protocol.			
Comments \ Issues:			

2.8.4 Allow SMTP detected communication of user-listed info

Description: The Privacy Manager product provides the capability for the user to allow SMTP detected communication of the user-listed information.			
Test Case ID: QZ706			
GSS Requirements Met: ZPM003			
Author: John Bee			
Date Ran:			
Tester:			
Configuration / Build: /			
Machine Number:			
Pre-Condition: Test Case QZ705			
Bugs found:			
Step	**Description**	**Observation**	**Result**
1.	In the "SecNet – Privacy Manager" dialog box, click Allow.		
2.	Verify that the Privacy Manager will allow the use of the keyword successfully for SMTP protocol.		
Expected Results: Verify that the Privacy Manager will allow the use of the keyword successfully for SMTP protocol.			
Comments \ Issues:			

2.8.5 Detect user-listed keywords via IRC

Description: The Privacy Manager shall provide the capability to detect user-listed keywords communicated through IRC chat applications.			
Test Case ID: QZ710			
GSS Requirements Met: ZPM002			
Author: John Bee			
Date Ran:			
Tester:			
Configuration / Build: /			
Machine Number:			
Pre-Condition: "Privacy Manager -> Protect Personal Information -> Keyword list area" is empty			
Bugs found:			
Step	**Description**	**Observation**	**Result**
	Click the Privacy Manager link.		
	Ensure Privacy Manager is enabled.		
	Click the Protect Personal Information link.		
	In the keyword list area, in the add text field, enter a "keyword" (text or alphanumeric).		
	Click Add and then click OK.		
	Minimize SecNet		
	Launch MIRC 6.14 chat application		
	Open a chat sessions		
	Enter the "keyword"		
	Minimize MIRC 6.14.		
	Confirm SecNet Detects the "keyword". SecNet will warn the user that it has found outgoing Internet Traffic containing potentially sensitive information.		
Expected Results: Confirm SecNet Detects the "keyword". SecNet will warn the user that it has found outgoing Internet Traffic containing potentially sensitive information..			
Comments \ Issues:			

2.8.6 Allow IRC Chat detected communication of user-listed info

Description: The Privacy Manager product provides the capability for the user to allow detected communication of the user-listed information.			
Test Case ID: QZ711			
GSS Requirements Met: ZPM003			
Author: John Bee			
Date Ran:			
Tester:			
Configuration / Build: /			
Machine Number:			
Pre-Condition: Test Case QZ710			
Bugs found:			
Step	**Description**	**Observation**	**Result**
1.	Click the Privacy Manager link.		
2.	Ensure Privacy Manager is enabled.		
3.	Click the Protect Personal Information link.		
4.	In the keyword list area, in the add text field, enter a “keyword” (text or alphanumeric).		
5.	Click Add and then click OK.		
6.	Launch MIRC 6.14 chat application loaded on the platform (SYSTEM A)		
7.	Launch MIRC 6.14 chat application on another computer (without SecNet) (SYSTEM B)		
8.	Open a chat sessions with (SYSTEM A) and (SYSTEM B) connected to the same server and chat room		
9.	From (SYSTEM A) attempt to enter the “keyword”		
10.	Confirm SecNet Detects the “keyword” prompting the operator for an action.	*Note that the SecNet dialogue may be obscured by a MIRC 6.14 window.*	
11.	Allow the “keyword” to be send		
12.	Confirm (SYSTEM B) receives the “keyword”	(SYSTEM B) should receive the “keyword”	
13.	From (SYSTEM A) attempt to enter the “keyword”		
14.	Confirm SecNet Detects the “keyword” prompting the operator for an action.	*Note that the SecNet dialogue may be obscured by a MIRC 6.14 window.*	
15.	Block the “keyword” from being sent		
16.	Confirm (SYSTEM B) does not	(SYSTEM B) should not receive	

	receive the “keyword”	the “keyword”	
17.	From (SYSTEM A) attempt to enter the text “Hello”		
18.	Confirm (SYSTEM B) receives the test “Hello”	(SYSTEM B) should receive “Hello”	
Expected Results: Verify that the Privacy Manager will allow or block the use of the “keyword” successfully for an IRC chat application.			

Comments \ Issues:

Ensure that MIRC 6.14 from www.mirc.com is installed before starting this test.

Note do not use “Hello” as the “keyword”

2.8.7 Block HTTP detected communication of user-listed info

Description: The Privacy Manager product provides the capability for the user to block detected communication of the user-listed information for HTTP protocols.			
Test Case ID: QZ721			
GSS Requirements Met: ZPM003			
Author: John Bee			
Date Ran:			
Tester:			
Configuration / Build: /			
Machine Number:			
Pre-Condition: "Privacy Manager -> Protect Personal Information -> Keyword list area" is empty			
Bugs found:			
Step	**Description**	**Observation**	**Result**
	Launch Internet Explorer		
	Go to www.google.com		
	Enter a "keyword" (text or alphanumeric) into the search field and then click google search.	NOTE: make sure the keyword is not already in the list area.	
	Close Internet Explorer.		
	Click the SecNet - Privacy Manager link.		
	Ensure Privacy Manager is enabled.		
	Click the Protect Personal Information link.		
	In the keyword list area, in the add text field, enter the same "keyword" entered before.		
	Click Add and then click OK.		
	Launch Internet Explorer		
	Go to www.google.com		
	Enter the same "keyword" (text or alphanumeric) into the search field and then click google search.	The SecNet – Privacy Manager should prompt the user to allow or block the communication.	
	In the "SecNet – Privacy Manager" dialog box, click Block	*This step may occur more than once.*	
	Verify that the Privacy Manager successfully blocks the use of the "keyword" for HTTP protocol. A page cannot be displayed message is displayed.		
Expected Results: The Privacy Manager successfully blocks the use of the "keyword" for HTTP protocol. A page cannot be displayed message is displayed.			

Comments \ Issues:

2.8.8 Block SMTP detected communication of user-listed info for SMTP protocols

Description: The Privacy Manager product provides the capability for the user to block detected communication of the user-listed information **for SMTP protocols.**			
Test Case ID: QZ722			
GSS Requirements Met: ZPM003			
Author: John Bee			
Date Ran:			
Tester:			
Configuration / Build: /			
Machine Number:			
Pre-Condition: "Privacy Manager -> Protect Personal Information -> Keyword list area" is empty			
Bugs found:			
Step	**Description**	**Observation**	**Result**
1.	Ensure Privacy Manager is enabled.		
2.	Launch the POP3 email application installed on the loaded platform		
3.	Send an e-mail with a "keyword" (text or alphanumeric) in the body of the mail message.	The SecNet – Privacy Manager should not interfere with the mail message sent	
4.	Click the SecNet - Privacy Manager link.		
5.	Click the Protect Personal Information link.		
6.	In the keyword list area, in the add text field, enter the same "keyword" entered before.		
7.	Click Add and then click OK.		
8.	Send an e-mail with the "keyword" in the body of the mail message.		
9.	When prompted to BLOCK or ALLOW the message to be sent select BLOCK		
10.	Verify that the Privacy Manager successfully blocks the email containing the "keyword" in the body of the mail message..		
Expected Results: The Privacy Manager blocks the email from being sent.			
Comments \ Issues:			

2.8.9 Block detected communication of user-listed info for IRC applications

Description: The Privacy Manager product provides the capability for the user to block detected communication of the user-listed information for an IRC Chat Application.			
Test Case ID: QZ723			
GSS Requirements Met: ZPM003			
Author: John Bee			
Date Ran:			
Tester:			
Configuration / Build: /			
Machine Number:			
Pre-Condition: "Privacy Manager -> Protect Personal Information -> Keyword list area" is empty			
Bugs found:			
Step	**Description**	**Observation**	**Result**
	Enable Privacy Manager		
	Add a "keyword" in the Protect Personal Information Dialogue		
	Disable Privacy Manager		
	Launch the MIRC chat application		
	Establish a chat session		
	Attempt to use a "keyword" (text or alphanumeric) within the content of the chat text	The SecNet – Privacy Manager should not interfere with the MIRC chat application	
	Exit MIRC chat application		
	Enable Privacy Manager		
	Launch the MIRC chat application		
	Establish a chat session		
	Attempt to use a "keyword" (text or alphanumeric) within the content of the chat text		
	Verify that the Privacy Manager will successfully block the use of the "keyword" for an MIRC chat application.	The SecNet – Privacy Manager should detect the "keyword" used with the MIRC application	
Expected Results: Verify that the Privacy Manager will successfully block the use of the "keyword" for an IRC chat application.			
Comments \ Issues: Install MIRC 6.14 from www.mirc.com before starting this test.			

2.8.10 Add cookies to Trusted Web Site List

Description: The Privacy Manager shall provide the capability to add IE browser cookies to a Trusted Web Sites List			
Test Case ID: QZ725			
GSS Requirements Met: ZPM004			
Author: John Bee			
Date Ran:			
Tester:			
Configuration / Build: /			
Machine Number:			
Pre-Condition: IE must be installed on the platform			
Bugs found:			
Step	**Description**	**Observation**	**Result**
1.	Launch Internet Explorer		
2.	Select Internet options -> delete cookies		
3.	Verify that the directory c:\documents and settings\USER_NAME\cookies contains no cookies (note that on Millenium, there is no "Documents and Settings" folder. Cookies are kept in "C:\windows\temporary internet files")	USER_NAME is the name of the user currently logged on the machine	
4.	Do not close Internet Explorer		
5.	Launch SecNet		
6.	Ensure Privacy Manager is enabled		
7.	With internet explorer go to the web sites: www.google.com www.amazon.com	Note: you may have to do a search to get Google or Amazon to leave a cookie on your machine	
8.	In SecNet click the Privacy Manger link		
9.	Click the Manage Cookies link		
10.	Verify that the cookies listed in SecNet's "Website's that left cookies on your computer" are also listed under the directory c:\documents and settings\USER_NAME\cookies (note that on Millenium, there is no "Documents and Settings" folder. Cookies are kept in "C:\windows\temporary internet files")		
11.	In the "Website's that left cookies on your computer" "Domain" area, select the cookie google.com		

12.	Click “Add to Trusted Sites” and then click OK		
13.	Ensure the cookie google.com is added to the “Trusted Websites” domain area		
14.	Select Clean Now in the Privacy Manager – Manage Cookies pane		
15.	Ensure Cookies from google.com are not deleted from the “Web sites that left cookies on your computer” list		
16.	Verify that the cookies from google.com listed in SecNet’s “Website’s that left cookies on your computer” are also listed under the directory c:\documents and settings\USER_NAME\cookies (note that on Millenium, there is no “Documents and Settings” folder. Cookies are kept in “C:\windows\temporary internet files”)		
Expected Results: Ensure the cookie selected is added to the “Trusted Websites” domain area and is not deleted when Privacy Manager Clean Now function is used.			
Comments \ Issues:			

2.8.11 Remove browser history

Description: The Privacy Manager product must provide the capability to remove IE browser history			
Test Case ID: QZ730			
GSS Requirements Met: ZPM005			
Author: John Bee			
Date Ran:			
Tester:			
Configuration / Build: /			
Machine Number:			
Pre-Condition: Ensure no third party tool bars are installed in Internet Explorer			
Bugs found:			
Step	**Description**	**Observation**	**Result**
1.	Launch Internet Explorer		
2.	Select - Tools / Internet Options / Home Page / Use Blank		
3.	Exit Internet Explorer		
4.	Launch Internet Explorer	Home page should be “blank”	
5.	Select - Tools / Internet Options / Clear History		
6.	Select - View / Explorer Bar / History		
7.	Confirm that no web sites visited are listed in the History pane		
8.	Go to the following web sites: www.google.com www.amazon.com		
9.	In history pane ensure “TODAY” (if present) is expanded.	*Take no action if “TODAY” is not present.*	
10.	Confirm that web sites visited appear in the history pane		
11.	Go to blank home page		
12.	Leave Internet Explorer OPEN		
13.	Ensure Privacy Manager is enabled		
14.	In SecNet / Privacy Manager / Preferences - Uncheck all options		
15.	In SecNet / Privacy Manager / Preferences - Under Browser Cleanup - check “History, Address bar and Temporary internet files”		
16.	Select OK		
17.	In Privacy Manager Pane select Clean Now		
18.	Click Start		
19.	Ensure Internet Explorer history pane		

	is open		
20.	Confirm that the History pane no longer contains entries for web sites visited.		
Expected Results: Ensure web sites visited have been removed from IE history			
Comments \ Issues: Note: “TODAY” in history pane of IE is not always present. When present it should be expanded to view the IE history list,			

2.8.12 Clean browser cache

Description: The Privacy Manager product must provide the capability to clean IE browser cache.			
Test Case ID: QZ735			
GSS Requirements Met: ZPM006			
Author: John Bee			
Date Ran:			
Tester:			
Configuration / Build: /			
Machine Number:			
Pre-Condition:			
Bugs found:			
Step	**Description**	**Observation**	**Result**
1.	Launch Internet Explorer		
2.	In tools / internet options: Delete Cookies, Delete Files, Clear History		
3.	Select tools / internet options / settings / view files		
4.	Ensure list of files is empty		
5.	close tools menu		
6.	Go to URL www.google.com		
7.	Go to URL www.amazon.com		
8.	Select tools / internet options / settings / view files		
9.	The list of files should not be empty		
10.	Leave Internet Explorer open		
11.	Open SecNet		
12.	Click the Privacy Manager Link		
13.	Under Privacy Manager Preferences select all options.		
14.	Click the Clean Now link.		
15.	Click Start then click Done		
16.	In Internet Explorer Select tools / internet options / settings / view files		
17.	Ensure file list is empty		
Expected Results: Ensure file list has been cleared.			
Comments \ Issues:			

2.8.13 Remove cookies

Description: The Privacy Manager product must provide the capability to remove IE browser cookies			
Test Case ID: QZ740			
GSS Requirements Met: ZPM007			
Author: John Bee			
Date Ran:			
Tester:			
Configuration / Build: /			
Machine Number:			
Pre-Condition:			
Bugs found:			
Step	**Description**	**Observation**	**Result**
1.	Launch Internet Explorer		
2.	Select Internet options -> delete cookies		
3.	Verify that the directory c:\documents and settings\USER_NAME\cookies contains no cookies (note that on Millenium, there is no "Documents and Settings" folder. Cookies are kept in "C:\windows\temporary internet files")	USER_NAME is the name of the user currently logged on the machine	
4.	Do not close Internet Explorer		
5.	Launch SecNet		
6.	Ensure Privacy Manager is enabled		
7.	With internet explorer go to the web sites: www.google.com www.amazon.com		
8.	In SecNet click the Privacy Manger link		
9.	Click the Manage Cookies link		
10.	Verify that the cookies listed in SecNet's "Web site's that left cookies on your computer" are also listed under the directory c:\documents and settings\USER_NAME\cookies (note that on Millenium, there is no "Documents and Settings" folder. Cookies are kept in "C:\windows\temporary internet files")		
11.	Select Clean Now in the Privacy Manager – Manage Cookies pane		
12.	Ensure Cookies are deleted from the "Web sites that left cookies on your computer" list		

13.	Verify that the cookies from google.com and amazon.com previously listed in SecNet's "Website's that left cookies on your computer" are no longer found under the directory c:\documents and settings\USER_NAME\cookies (note that on Millenium, there is no "Documents and Settings" folder. Cookies are kept in "C:\windows\temporary internet files")		
Expected Results: Ensure cookies are deleted.			
Comments \ Issues:			

2.8.14 Add keywords to list

Description: The Privacy Manager should provide the capability to add keywords to the keyword list.			
Test Case ID: QZ745			
GSS Requirements Met: ZPM008			
Author: John Bee			
Date Ran:			
Tester:			
Configuration / Build: /			
Machine Number:			
Pre-Condition:			
Bugs found:			
Step	**Description**	**Observation**	**Result**
	Click the Privacy Manager link.		
	Click the Protect Personal Information link.		
	Enter a keyword in the Add text field.		
	Click Add and then click OK.		
	On the Privacy Manager page, click the Protect Personal Information link.		
	Ensure the keyword was added.		
Expected Results: Ensure the keyword was added.			
Comments \ Issues:			

2.8.15 Delete keywords from list

Description: The Privacy Manager should provide the capability to delete keywords from the keyword list.			
Test Case ID: QZ750			
GSS Requirements Met: ZPM009			
Author: John Bee			
Date Ran:			
Tester:			
Configuration / Build: /			
Machine Number:			
Pre-Condition:			
Bugs found:			
Step	**Description**	**Observation**	**Result**
	Click the Privacy Manager link.		
	Click the Protect Personal Information link.		
	Select a keyword.		
	Click Delete and then click OK.		
	On the Privacy Manager page, click the Protect Personal Information link.		
	Ensure the keyword has been deleted.		
Expected Results: Ensure the keyword has been deleted.			
Comments \ Issues:			

2.9 Parental Control

2.9.1 Deny new internet connections via restricted list

Description: The Parental Control service must provide the ability to deny new Internet connections to a list of restricted programs			
Test Case ID: QZ800			
GSS Requirements Met: ZPC002			
Author: John Bee			
Date Ran:			
Tester:			
Configuration / Build: /			
Machine Number:			
Pre-Condition:			
Bugs found:			
Step	**Description**	**Observation**	**Result**
1.	Click the Parental Control link.		
2.	Check the Enable Parental Control check box.		
3.	Click the Restricted Programs link.		
4.	Click Add Program.		
5.	In the “Open” dialog box, browse to a program that you want to restrict and then click it.		
6.	Click Open and then click OK.		
7.	Launch the program selected to be restricted in step 5.		
8.	Ensure Parental Control do not allow new internet connections through the restricted program.		
Expected Results: Ensure Parental Control do not allow new internet connections through the restricted program.			
Comments \ Issues:			

2.9.2 Add new programs to the restricted list

Description: The Parental Control service must provide the ability to add new programs to the list of restricted programs			
Test Case ID: QZ805			
GSS Requirements Met: ZPC003			
Author: John Bee			
Date Ran:			
Tester:			
Configuration / Build: /			
Machine Number:			
Pre-Condition:			
Bugs found:			
Step	**Description**	**Observation**	**Result**
1.	Launch Internet Explorer		
2.	Select - Tools / Internet Options / Home Page / Use Blank		
3.	Exit Internet Explorer		
4.	Click the SecNet Parental Control link.		
5.	Check the Enable Parental Control check box.		
6.	Click the Restricted Programs link.		
7.	Click Add Program.		
8.	In the “Open” dialog box, browse to “Internet Explorer” and add it to the restricted programs list.		
9.	Click OK.		
10.	On the Parental Control page, click Restrict Programs.		
11.	Ensure “Internet Explorer” is present in the restricted programs list.		
12.	Launch “Internet Explorer” and attempt to navigate to www.google.com.		
13.	Ensure that SecNet indicates that “Internet Explorer was blocked by Parental Control”		
Expected Results: SecNet indicates that “Internet Explorer was blocked by Parental Control”			
Comments \ Issues:			

2.9.3 Remove a program from the restricted list

Description: The Parental Control service must provide the capability to remove a program from the list of restricted programs			
Test Case ID: QZ810			
GSS Requirements Met: ZPC004			
Author: John Bee			
Date Ran:			
Tester:			
Configuration / Build: /			
Machine Number:			
Pre-Condition:			
Bugs found:			
Step	**Description**	**Observation**	**Result**
1.	Click the Parental Control link.		
2.	Check the Enable Parental Control check box.		
3.	Click the Restricted Programs link.		
4.	In the Program Name area, select a program to remove.		
5.	Click Delete and then click OK.		
6.	From the Parental Control page, click Restricted Programs.		
7.	Ensure the restricted program has been removed.		
8.	Launch the program to ensure that it is now accessible.		
Expected Results: Launch the program to ensure that it is now accessible.			
Comments \ Issues:			

2.9.4 Disable Parental Control

Description: The user must be able to disable the parental control product.			
Test Case ID: QZ815			
GSS Requirements Met: ZPC005			
Author: John Bee			
Date Ran:			
Tester:			
Configuration / Build: /			
Machine Number:			
Pre-Condition:			
Bugs found:			
Step	**Description**	**Observation**	**Result**
1.	Click Parental Control.		
2.	Uncheck Enable Parental Control.		
3.	Access a restricted program to ensure Parental Controls are indeed disabled.		
Expected Results: Access a restricted program to ensure Parental Controls are indeed disabled.			
Comments \ Issues:			

2.9.5 Set password for parental control

Description: The user must be able to set a password for the parental control product.			
Test Case ID: QZ820			
GSS Requirements Met: ZPC006			
Author: John Bee			
Date Ran:			
Tester:			
Configuration / Build: /			
Machine Number:			
Pre-Condition:			
Bugs found:			
Step	**Description**	**Observation**	**Result**
1.	Click General in the left menu and then click Password.		
2.	Click the “Use a Password to protect my information” option button.		
3.	Type the new password in the New Password and Confirm Password text box and then click OK.		
4.	Click yes in the SecNet dialog box.		
5.	Ensure the password has been set/changed.		
Expected Results: Ensure the password has been set/changed.			
Comments \ Issues:			

2.9.6 Block access to website

Description: The user must be able to add sites to the list of sites to block from browsing.			
Test Case ID: QZ825			
GSS Requirements Met: ZPC007			
Author: John Bee			
Date Ran:			
Tester:			
Configuration / Build: /			
Machine Number:			
Pre-Condition:			
Bugs found:			
Step	**Description**	**Observation**	**Result**
1.	Click Parental Control.		
2.	Check Enable Parental Control.		
3.	Click Preferences.		
4.	Click New.		
5.	Enter the web site address to be blocked and then click OK.		
6.	Ensure the web site is restricted. For example, launch a browser and attempt to visit the blocked web address.		
Expected Results: Ensure the web site is restricted. For example, launch a browser and attempt to visit the blocked web address.			
Comments \ Issues:			

2.9.7 Remove websites from blocked list

Description: The user must be able to remove sites from the list of sites to block from browsing			
Test Case ID: QZ830			
GSS Requirements Met: ZPC008			
Author: John Bee			
Date Ran:			
Tester:			
Configuration / Build: /			
Machine Number:			
Pre-Condition:			
Bugs found:			
Step	**Description**	**Observation**	**Result**
1.	Click Parental Control.		
2.	Check Enable Parental Control.		
3.	Click Preferences.		
4.	Select a web site to remove from the restricted list.		
5.	Click Delete and then click OK.		
6.	Ensure the web site is not restricted. For example, launch a browser and attempt to visit the web site removed from the restricted list in step 4.		
Expected Results: Ensure the web site is not restricted. For example, launch a browser and attempt to visit the web site removed from the restricted list in step 4.			
Comments \ Issues:			

2.9.8 Add sites to Allow list

Description: The user must be able to add sites to the list of sites to allow for browsing.			
Test Case ID: QZ835			
GSS Requirements Met: ZPC009			
Author: John Bee			
Date Ran:			
Tester:			
Configuration / Build: /			
Machine Number:			
Pre-Condition:			
Bugs found:			
Step	**Description**	**Observation**	**Result**
1.	Disable parental controls		
2.	Launch Internet Explorer		
3.	Go to www.google.com		
4.	Search for "sex therapy"		
5.	Wait for search results	search results should be displayed	
6.	Close Internet Explorer		
7.	Enable parental controls		
8.	Launch Internet Explorer		
9.	Go to www.google.com		
10.	Search for "sex therapy"		
11.	A page indicating SecNet Parental Controls warns that the site is blocked due to content restricted by parental controls.	Parental Control message in place of search results should be displayed	
12.	Close Internet Explorer		
13.	In Parental Control Preferences to Web Sites I want to allow add: www.google.com and www.google.ca		
14.	Launch Internet Explorer		
15.	Go to www.google.com		
16.	search for "sex therapy"		
17.	Wait for search results and verify that search results are displayed.	search results should be displayed	
Expected Results: Ensure the web site is accessible even though Parental control would normally block the search results.			
Comments \ Issues:			

2.9.9 Parental Control -- log of blocked sites

Description: The Parental Control service shall maintain a log of blocked sites			
Test Case ID: QZ836			
GSS Requirements Met: ZPC011			
Author: John Bee			
Date Ran:			
Tester:			
Configuration / Build: /			
Machine Number:			
Pre-Condition:			
Bugs found:			
Step	**Description**	**Observation**	**Result**
	With Parental Control enabled, use your browser to go to www.playboy.com		
	Open the SecNet UI and click Parental Control		
	Click "View Log"		
	Verify that www.playboy.com is in the list of blocked sites.		
Expected Results: Ensure the blocked site is in "The following sites were blocked" list.			
Comments \ Issues:			

2.9.10 Remove sites from Allow list

Description: The user must be able to remove sites from the list of sites to allow for browsing.			
Test Case ID: QZ840			
GSS Requirements Met: ZPC010			
Author: John Bee			
Date Ran:			
Tester:			
Configuration / Build: /			
Machine Number:			
Pre-Condition:			
Bugs found:			
Step	**Description**	**Observation**	**Result**
	Click Parental Control.		
	Check Enable Parental Control.		
	Click Preferences.		
	In the "Web sites I want to allow" area, add www.playboy.com		
	Launch www.playboy.com in your browser and verify it can be seen		
	Toggle back to SecNet's Parental Control Preferences, select www.playboy.com, click Delete and then click OK to remove it from the list of sites to allow.		
	Toggle back to Internet Explorer (which should still be showing www.playboy.com), press F5 to refresh the page		
	Verify www.playboy.com is no longer accessible.		
Expected Results: Ensure the web site removed is no longer accessible.			
Comments \ Issues:			

2.10 Uninstall

2.10.1 Uninstall works from program group

Description: Verify that uninstall will remove SecNet via its Start menu program group.			
Test Case ID: QZ900			
GSS Requirements Met: ZUN001, ZUN002			
Author: John Bee			
Date Ran:			
Tester:			
Configuration / Build: /			
Machine Number:			
Pre-Condition:			
Bugs found:			
Step	**Description**	**Observation**	**Result**
1.	Install and activate SecNet		
2.	Open the UI, change and save some settings		
3.	Take note of the user profile-specific data files in: "C:\Documents and Settings\All Users\Application Data\Zero Knowledge\SecNet" and "C:\Documents and Settings***anyUserName***\Application Data\Zero Knowledge\SecNet" (note: on Millenium, the path is "c:\windows\application data\zero knowledge\SecNet")		
4.	Go to Start menu / Programs / SecNet Security and Privacy and click "Uninstall SecNet"		
5.	After uninstall is finished (after reboot), verify that: - Under the Start menu / Programs, there is no folder titled "SecNet Security and Privacy" - SecNet icon has been removed from the system tray - SecNet shortcut has been removed from the desktop - All SecNet registry keys have been removed - All files under the SecNet directory have been removed except user profile-specific data files which were noted in step 3 of this TC		

Expected Results: SecNet's uninstall utility should remove all installed artifacts except user profile-specific data files
Comments \ Issues:

2.11 Performance

2.11.1 Firewall Services Performance ratio

Description: The Windows benchmark tool (Performance Test) measure on Windows XP Home edition with a freshly installed operating environment varies by less than 30% between the case of SecNet not installed and SecNet installed with only Firewall services enabled.			
Test Case ID: QZ1000			
GSS Requirements Met: ZPR001			
Author: John Bee			
Date Ran:			
Tester:			
Configuration / Build: /			
Machine Number:			
Pre-Condition: 1. Load virgin platform of Windows XP home edition 2. Load Performance Test tool v5.0			
Bugs found:			
Step	**Description**	**Observation**	**Result**
1.	Launch Performance Test tool		
2.	From tool menu run Tests/CPU/All		
3.	From tool menu run Tests/2D Graphics/All		
4.	From tool menu run Tests/Memory/All		
5.	From tool menu run Tests/Disk/All		
6.	From tool menu run View/Show PassMark Rating		
7.	Take note of rating		
8.	Repeat steps 2 through 7 two more times		
9.	Calculate the rating average of all 3 steps [AVG_1]		
10.	Exit Performance Test tool		
11.	Install SecNet application		
12.	Activate the SecNet application and disable all options in SecNet except for the Firewall		
13.	Repeat steps 1 through 7 three times		
14.	Calculate the rating average of all 3 steps [AVG_2]		
15.	Verify that the ratio [AVG_2]/[AVG_1] > 0.7		
Expected Results: Verify that the ratio [AVG_2]/[AVG_1] > 0.7			

Comments \ Issues:

2.11.2 AntiVirus Services Performance ratio

Description: The Windows benchmark tool (Performance Test) measure on Windows XP Home edition with a freshly installed operating environment varies by less than 30% between the case of SecNet not installed and SecNet installed with only AntiVirus services enabled.

Test Case ID: QZ1010

GSS Requirements Met: ZPR002

Author: John Bee

Date Ran:

Tester:

Configuration / Build: /

Machine Number:

Pre-Condition:

1. Load virgin platform of Windows XP Home edition
2. Load Performance Test tool v5.0

Bugs found:

Step	Description	Observation	Result
	Launch Performance Test tool		
	From tool menu run Tests/CPU/All		
	From tool menu run Tests/2D Graphics/All		
	From tool menu run Tests/Memory/All		
	From tool menu run Tests/Disk/All		
	From tool menu run View/Show PassMark Rating		
	Take note of rating		
	Repeat steps 2 through 7 two more times		
	Calculate the rating average of all 3 steps [AVG_1]		
	Exit Performance Test tool		
	Install SecNet application		
	Activate the SecNet application and disable all options in SecNet except for the Antivirus		
	Repeat steps 1 through 7 three times		
	Calculate the rating average of all 3 steps [AVG_2]		
	Verify that the ratio [AVG_2]/[AVG_1] > 0.7		

Expected Results: Verify that the ratio [AVG_2]/[AVG_1] > 0.7

Comments \ Issues:

2.12 Platform Requirements

2.12.1 Operation with co-existent applications

Description:			
Test Case ID: QZ1100			
GSS Requirements Met: ZPL006			
Author: John Bee			
Date Ran:			
Tester:			
Configuration / Build: /			
Machine Number:			
Pre-Condition: Start with a clean OS			
Bugs found:			
Step	**Description**	**Observation**	**Result**
1.	Install SecNet on a clean OS image (with as little desktop applications as possible:, i.e. no Word, no RealPlayer, no chat, no email, no games, etc.)		
2.	Launch SecNet and verify that it is operational		
3.	Exit SecNet		
4.	Install an E-mail application		
5.	Install a Web E-mail application		
6.	Install a chat application		
7.	Install a desktop application		
8.	Install a Web Browser		
9.	Launch SecNet and verify that it is still operational		
Expected Results: SecNet should operate properly even if co-existent applications were installed after SecNet's installation			
Comments \ Issues:			