TREND MICRO™

6.0 InterScan™ Web Security Virtual Appliance

Hardware Certification Guide

Antivirus and Content Security at the Web Gateway

Contents

Chapter 1

Suggested Test Flow

This chapter presents the suggested test flow for InterScan Web Security Virtual Appliance (IWSVA) 6.0 and details each step in the flow.

Figure 1-1 shows the suggested test flow for IWSVA 6.0.

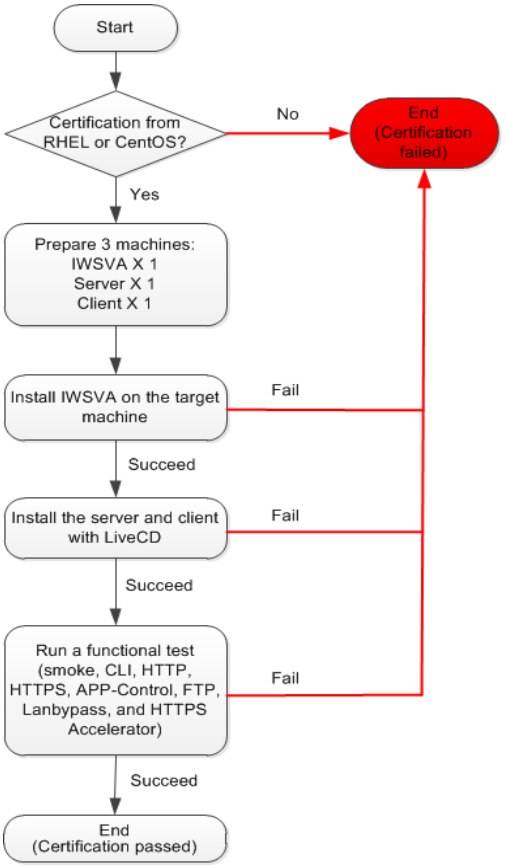

FIGURE 1-1. Test flow for IWSVA 6.0

Table 1-1 describes the specific steps in the test flow.

TABLE 1-1. Specific steps in the test flow

NO.	STEP
1	Check the certification from RHEL or CentOS. **Note:** IWSVA 6.0 was compiled based on CentOS v6.0, so Trend Micro assumes that the target machine has been certified by CentOS.
2	Prepare three machines for installing IWSVA, the client, and the server.
3	Install IWSVA 6.0 on the target machine.
4	Install the server and client with LiveCD. **Note:** Certain configurations are required for LiveCD setup. Please check chapter 4 for detailed configurations.
5	Run a functional test. **Note:** The functional test consists of the following: Smoke test/CLI test HTTP/HTTPS/FTP/App-Control test LAN bypass/HTTPS Accelerator cards test

If IWSVA 6.0 passes all the tests, then the certification process is completed.

Chapter 2

System and Network Architecture

Basic Deployment

Network address settings are hard-coded and specified as required:

- Server machine
  - IP address: 192.168.0.1
  - Network mask: 255.255.255.0
  - Gateway: 192.168.0.254
- Client machine
  - IP address: 192.168.0.2
  - Network mask: 255.255.255.0
  - Gateway: 192.168.0.254
- IWSVA (test/certification target)
  - IP address: 192.168.0.3
  - Network mask: 255.255.255.0
  - Gateway: 192.168.0.254
  - DNS: 127.0.0.1

It is strongly recommended that the Data Collection Client be on the same network segment with the preceding IP addresses. *Figure 2-1* is a sample network.

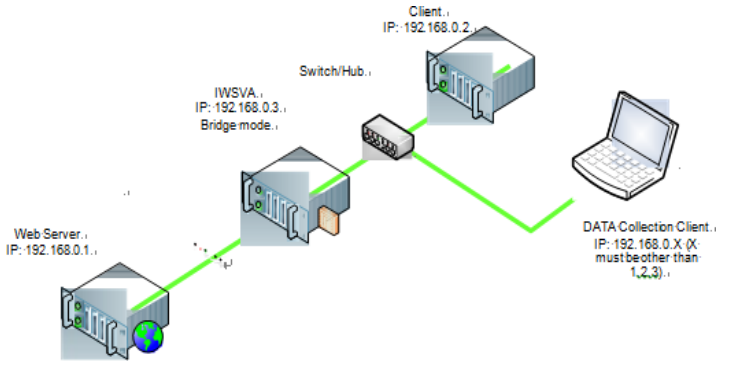

FIGURE 2-1. Sample network

Note: The tests must be performed in an isolated network segment.

Minimum Server/Client Hardware Requirements

- CPU: Intel™ Core™ 2 Duo Processor E6750 2.66 GHz
- Memory: 2 GB or higher
- CD-ROM: bootable
- NIC: CentOS 6.0 compatible

Note: If no physical machine is available for the client and server, you must construct them on virtual machines.

Minimum Data Collection Client Requirement

Internet Explorer (IE) is used for the Data Collection Client, and it requires at least IE 7.

Chapter 3

Configuration of IWSVA

Hardware Requirements

- Single 2.0 GHz Intel™ Core™ 2 Duo 64-bit processor (Intel™ VT™ or equivalent)
- 4-GB RAM
- 20-GB disk space that IWSVA will automatically partition as required
- A monitor that supports 1024 x 768 resolution with 256 colors or higher
- Two network cards for IWSVA to support Transparent Bridge configuration

Further Requirements

The IWSVA machine, the server, and the client must be able to communicate with each other over the network.

LAN Bypass Card List

Trend Micro recommends that the following LAN bypass cards be used in bridge mode to ensure maximum compatibility:

- SD: PXG2BPFIL-SD, PXG2BPI-SD, and PEG2BPI6-SD
- Non-SD: PEG2BPFID and PEG2BPI

HTTPS Accelerator Card List

IWSVA supports the following Silicom cards:

- PCI-E 61
- PCI-X 51
- PESC62

Installing IWSVA

Perform the following steps to install IWSVA:

1. Start IWSVA installation.

   Insert the IWSVA installation CD into the CD-ROM drive of the target machine.

   A page appears, displaying the IWSVA installation menu.
2. Select **Install IWSVA**.

   The license acceptance page appears.
3. Click **Accept**.

   A page appears where you can choose a keyboard language.
4. Select the keyboard language for the system.

The IWSVA installer scans your hardware to ensure that the minimum specifications have been met and displays the results illustrated in *Figure 3-1*.

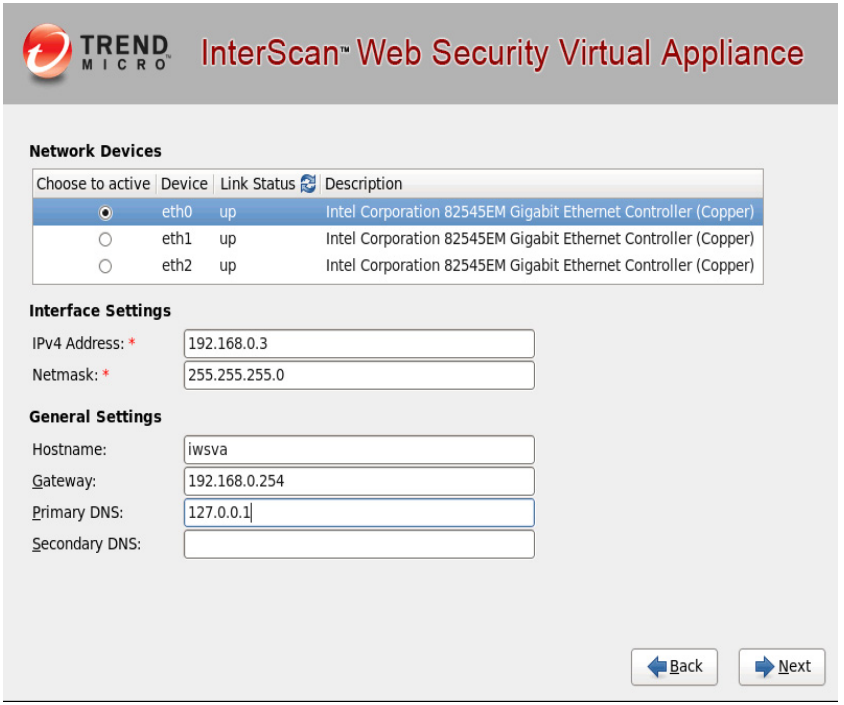

FIGURE 3-1. Hardware scan results

Note: If the host hardware contains any components that do not meet the minimum specifications, the installer will highlight the non-conforming components, and the installation will stop. See chapter 7 for more details.

5. Click **Next**.
6. Use the following IWSVA settings:
   - IPv4 address: 192.168.0.3/255.255.255.0
   - Host name: iwsva

- Gateway: 192.168.0.254
- Primary DNS: 127.0.0.1

7. Click **Next**.
8. On the time zone page, specify the time zone for **IWSVA**.

   Use the drop-down list to display all the supported time zones or point to your location using the time zone map.
9. Click **Next**.
10. Specify passwords for the **root**, **enable**, and **admin** accounts.

    Type **123456** as the password for all accounts, as show in *Figure 3-2*.

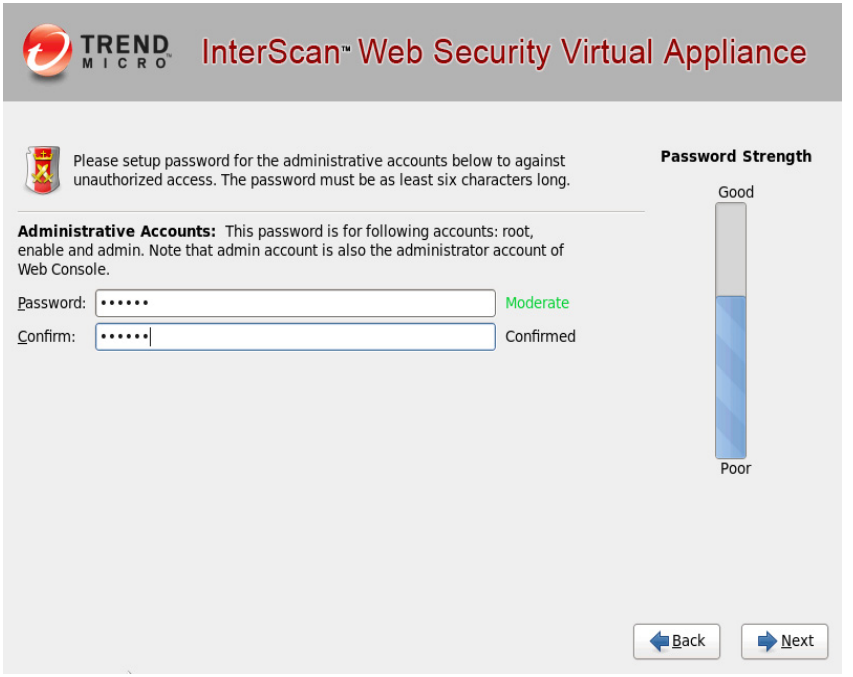

FIGURE 3-2. Setting the administrative account password

11. Click **Next**.

    A page appears for you to confirm all the configuration settings.

12. Confirm that the selected values are correct and then click **Next**.

    The installer prompts you to begin the installation. Selecting **Continue** will erase any data on the hard disk partition and format the hard disk. If you have data on the hard disks that you would like to keep, cancel the installation and back up the information before proceeding.

13. Click **Continue**.

    A page appears that provides the formatting status of the local drive for the IWSVA installation. When formatting completes, the IWSVA installation begins. Once the installation is completed, a summary screen appears.

    The installation log is saved in the **/root/install.log** file for reference.

14. Click **Reboot** to restart the system.

    The CD automatically ejects. Remove the CD from the drive to prevent reinstallation.

Deploying IWSVA

After installation, IWSVA works in forward proxy mode. Run the deployment wizard to activate and deploy IWSVA as Bridge mode.

Perform the following steps to activate IWSVA:

1. From the Data Collection Client, open the IE browser and connect to the URL http://192.168.0.3:1812. Log in with the username **admin** and password **123456**, as shown in *Figure 3-3*.

FIGURE 3-3. Login page

2. In the deployment wizard dialog box that pops up, click **Start** to start the deployment wizard. Select **Transparent bridge mode**, as shown in *Figure 3-4*.

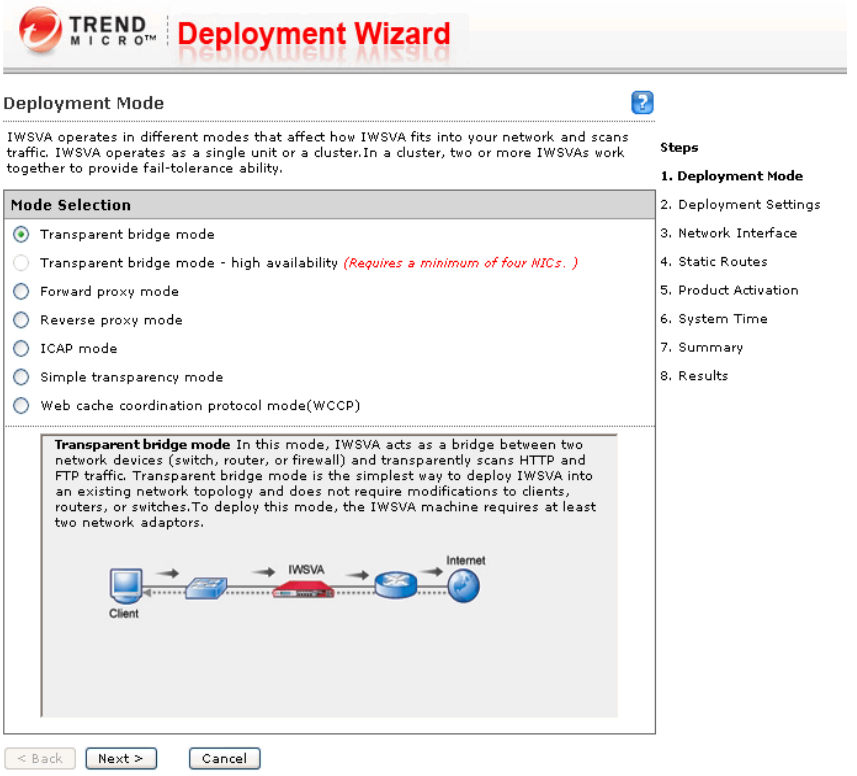

FIGURE 3-4. Deployment Mode

3. Click **Next**. Configure network interface information for IWSVA, as shown in *Figure 3-5*.

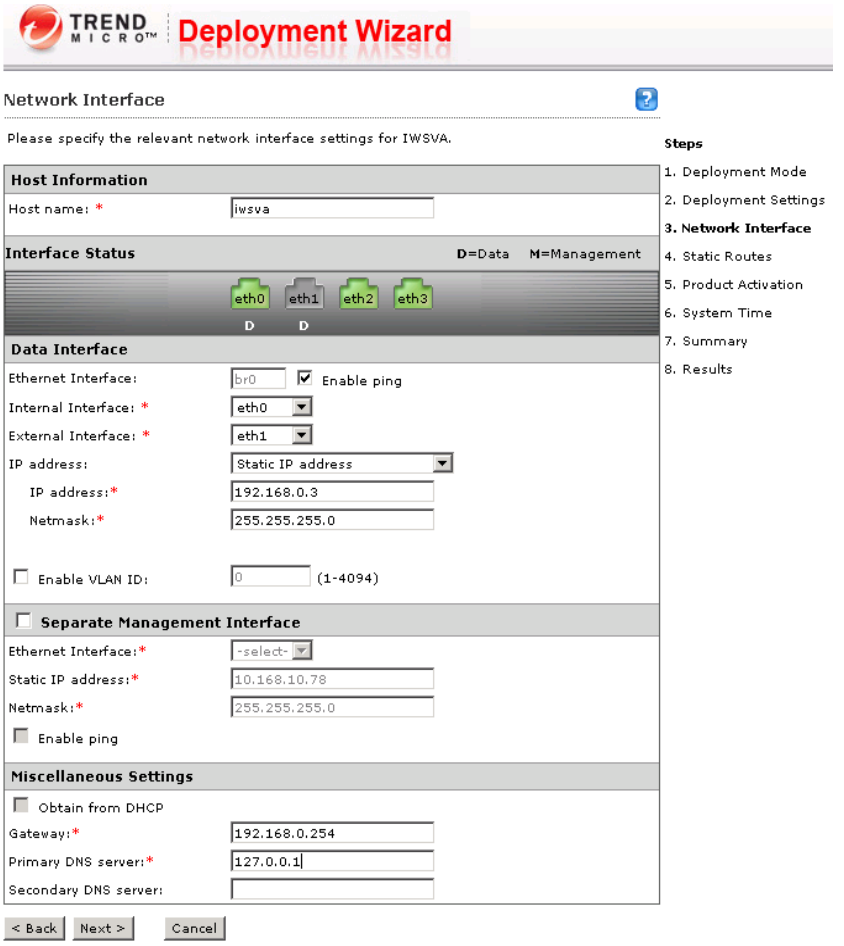

FIGURE 3-5. Network Interface

4. Click **Next** to go to the **Static Routes** page. Ignore this page and click **Next**. On the **Product Activation** page shown in *Figure 3-6*, enter the activation code.

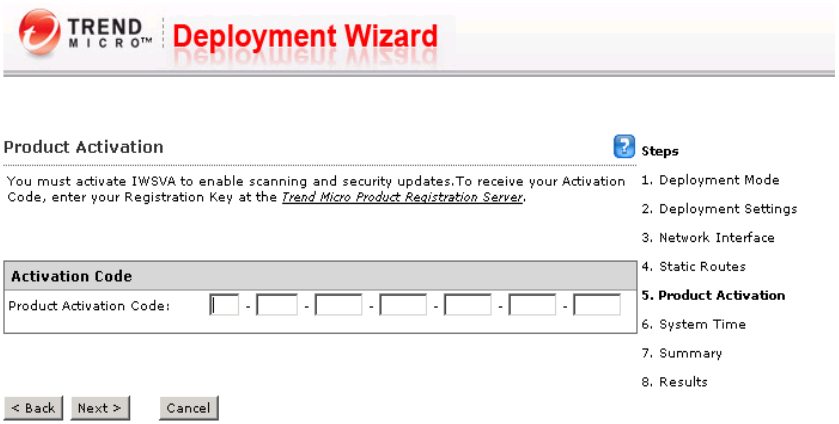

FIGURE 3-6. Product Activation

5. Click **Next** and follow the wizard to finish the deployment.

Chapter 4

Configuration of the Server and Client Machines

Configuring the Server Machine

1. Boot up from distributed LiveCD.

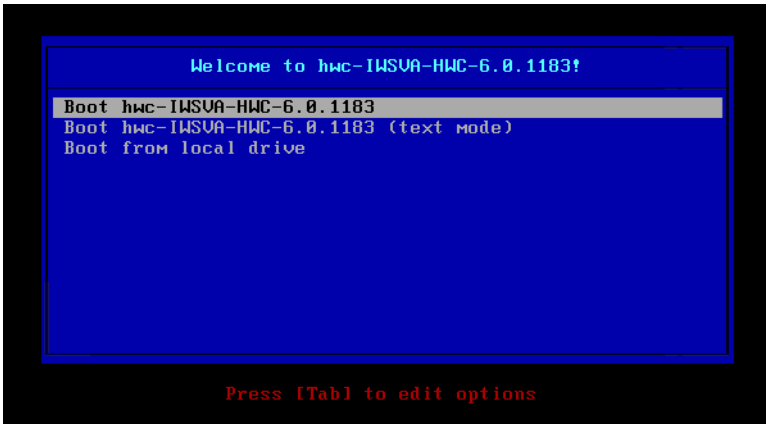

FIGURE 4-1. Boot options

2. Choose the first option shown in *Figure 4-1* and press **Enter**.

After the Server machine reboots, the LiveCD stays in the login screen and presents the login prompt, as shown in *Figure 4-2*.

FIGURE 4-2. Login prompt

3. Log in as the **root** user.

   The **root** user does not have a password by default.

4. Open the Command Line Interface (CLI) by entering the **clish** command, as shown in *Figure 4-3*.

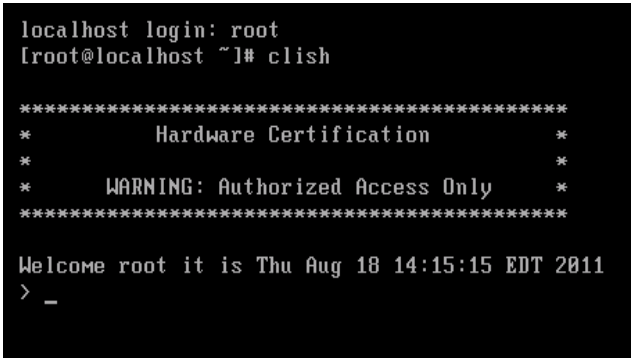

FIGURE 4-3. Opening the CLI

5. Configure this LiveCD as a Web server by entering the **configure server** command, as shown in *Figure 4-4*.

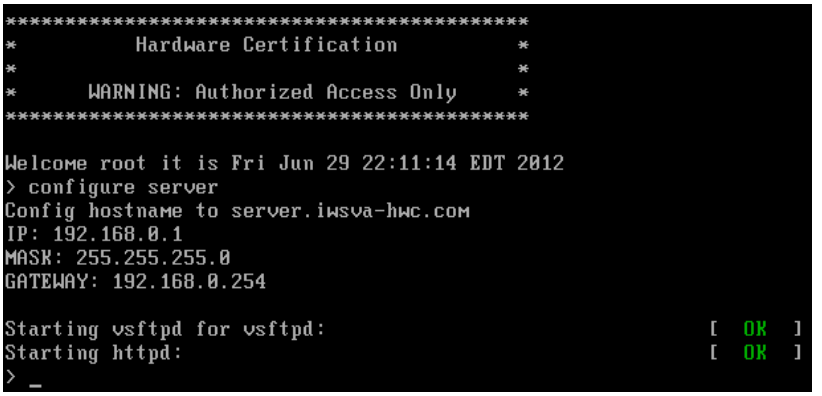

FIGURE 4-4. Entering the configure server command

In this step, the following configurations have been made:

- The IP address has been changed to 192.168.0.1.
- The vsftpd service for the FTP server has been started.

- The apache httpd service for the HTTP server has been started.
- The SSH service has been restarted.

Configuring the Client Machine

1. Repeat Step 1 to Step 4 in *Configuring the Server Machine* on page 4-1.
2. Configure this LiveCD as a client by entering the **configure client** command, as shown in *Figure 4-5*.

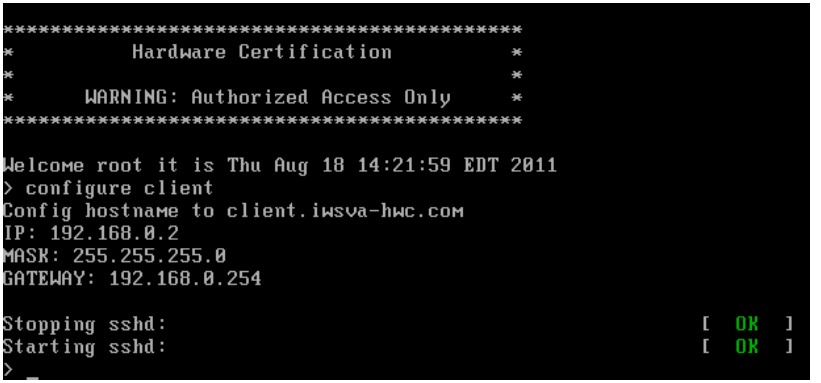

FIGURE 4-5. Entering the configure client command

In this step, the following configurations have been made:

- The IP address has been changed to 192.168.0.2.
- The SSH service has been restarted.

Chapter 5

Starting a Functional Test

In CLI, enter the **functional_test** command from the Client machine to start a functional test.

See *Figure 5-1* and *Figure 5-2* for details.

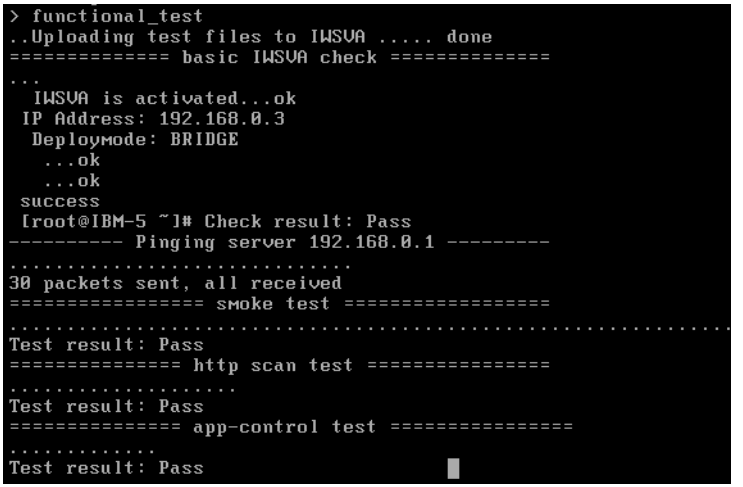

FIGURE 5-1. Functional test (1)

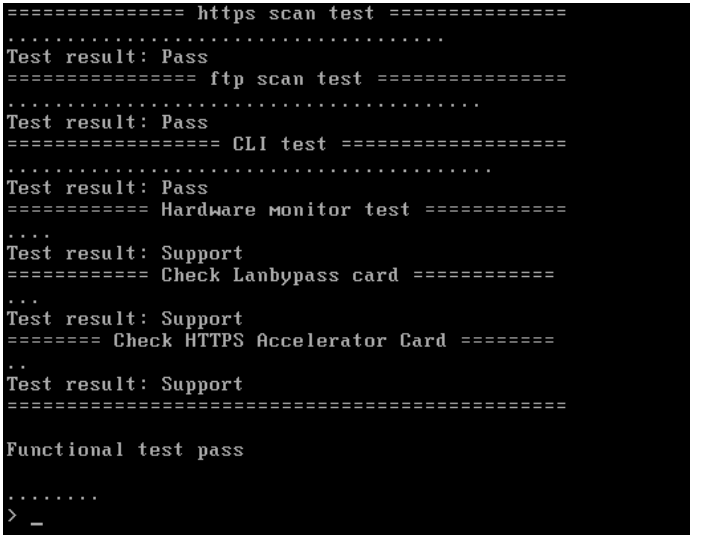

FIGURE 5-2. Functional test (2)

A functional test consists of the following:

- Smoking test: stops/starts all IWSVA-related services to verify the health of IWSVA installation.
- HTTP test: initiates some requests for virus infected and uninfected Web pages to verify the HTTP scan functionality of IWSVA.
- HTTPS test: initiates some requests for virus infected and uninfected Web pages to verify the HTTPS scan functionality of IWSVA.
- APP-control test: initiates socket connections between the client and the server and transfers packets with specific context to verify the APP-control functionality of IWSVA.
- FTP test: initiates FTP connections to some virus infected and uninfected files to verify the FTP scan functionality of IWSVA.
- CLI test: tests the CLI's hardware compatibility
- LAN bypass card check: checks whether the bypass function works with this machine.

- HTTPS Accelerator card check: check whether the accelerator function works with this machine.

Chapter 6

Collecting the Test Results from IWSVA

1. On the Data Collection Client, open the IE browser and connect to the URL http://192.168.0.3:1812. Log in with the username **admin** and password **123456**, as shown in *Figure 6-1*.

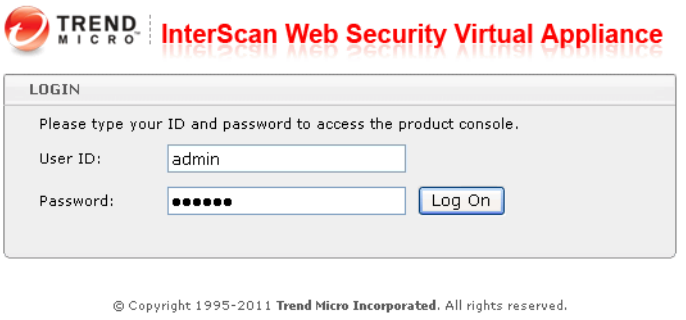

FIGURE 6-1. Login page

2. In the navigation area, choose **Administration** > **Support**, as shown in *Figure 6-2*.

FIGURE 6-2. Generating a system information file

3. Click **Generate System Information File**.

On the page shown in *Figure 6-3*, you can check the information packaging progress.

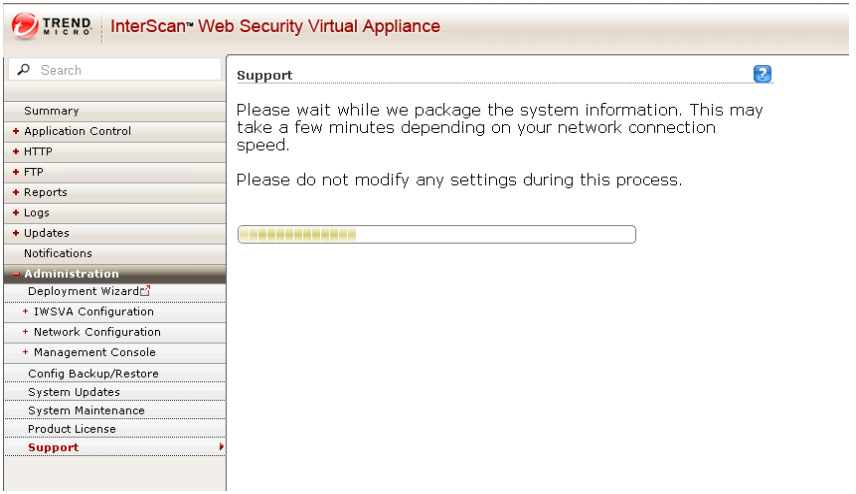

FIGURE 6-3. Information packaging progress

A file named **functional_test_result.tgz** will be listed in the **Select Core or System File(s)** text box, as shown in *Figure 6-4*.

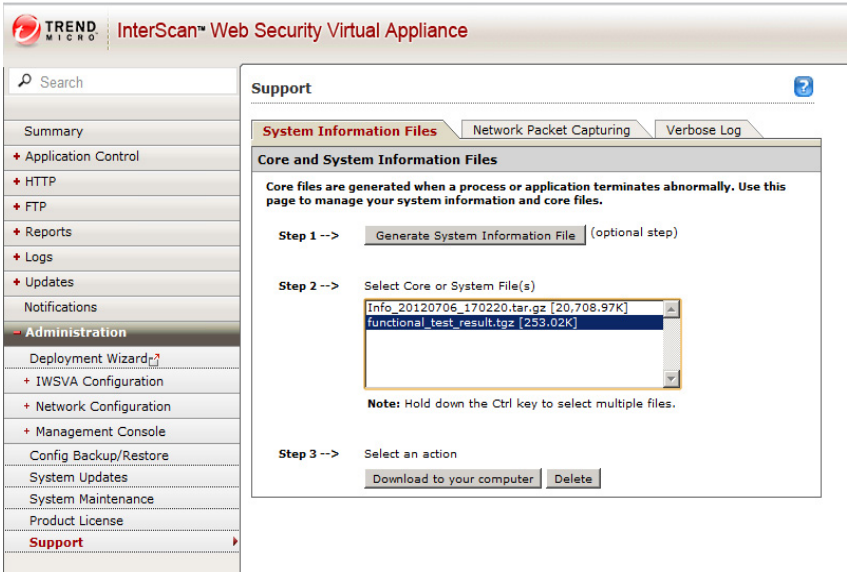

FIGURE 6-4. File generated

4. On the **Support** page, select the file **functional_test_result.tgz** from the **Select Core or System File(s)** text box, as shown in *Figure 6-4*.
5. Click **Download to your computer** and choose a local storage path to save the target file.
6. Repeat and download the **Info**_*yyyymmdd*_*xxxxxx*.**tar.gz** file.

Note: In the preceding file name, *yyyymmdd* is the date when the file was generated, and *xxxxxx* is a random number. The file name used in *Figure 6-4* is only an example.

Chapter 7

Troubleshooting

1. If you encounter a "failed hardware check" problem during the IWSVA installation, perform the following operation:

   Check whether the target machine passes CentOS 6.0 hardware check.

   Note: A copy of CentOS can be downloaded from http://isoredirect.centos.org/centos/6/isos/x86_64/.

   - If the target machine fails the CentOS 6.0 hardware check, it will fail the hardware certification.
   - If the machine fails the IWSVA hardware check but passes CentOS 6.0 hardware check, contact Trend Micro.

2. If the Ping test fails between the client and server, perform the following steps:

   a. Check the NIC card compatibility.

      If the machine has multiple NIC cards, LiveCD activates only the eth0 interface. Activate the desired interface by running the following command:

      ```
      ifconfig eth(*n) 192.168.0.(*ip) netmask 255.255.255.0 up
      ```

Note: **(*n)** is the desired interface ID.
(*ip) is the octet in the client or server IP address. The value is **1** for the server IP address and **2** for the client IP address.

b. Check whether IWSVA is powered on or installed properly.

3. If you encounter the error message "Buffer I/O error on device hde" or "Logical block 86326" when LiveCD is booting the test machine, ignore these messages and continue the test. These error messages will appear if you burn LiveCD in **track-at-once** mode. To avoid them, you can re-burn LiveCD in **disk-at-once** mode.

TREND MICRO INCORPORATED

10101 North De Anza Blvd. Cupertino, CA., 95014, USA

Tel:+1(408)257-1500/1-800 228-5651 Fax:+1(408)257-2003 info@trendmicro.com

www.trendmicro.com

Item Code: IBEM65994/130716