Trend Micro, Inc. February 14, 2008

Service Pack 1 for
InterScan™ Web Security Appliance 3.1

Note: This readme file was current as of the date above. However, all customers are advised to check Trend Micro's Web site for documentation updates at:
http://www.trendmicro.com/download/product.asp?productid=70

Contents

1. About InterScan Web Security Appliance

Trend Micro™ InterScan™ Web Security Appliance (IWSA) provides multi-layer, multi-threat protection at the Internet gateway to dynamically defend against Web-based attacks. IWSA leverages both local and in-the-cloud security information to protect HTTP and FTP traffic, and includes antivirus, anti-spyware, and new Web Reputation. These features collaborate to block access to malicious pages or links based on reputation scoring, prevent spyware downloads, and detect spyware activity on clients to trigger agent-less cleanup. The Advanced edition provides flexible policy-based control over Java applets and Active X controls, in addition to URL filtering.

This section describes the following:

- Overview of This Patch Release
- Who Should Install This Patch Release
- Files Included in This Release

1.1 Overview of This Release

Service Pack 1 for IWSA 3.1 is a standalone service pack and not a full product. The purpose of this service pack release is to add Web Cache Communication Protocol (WCCP) version 2 support to IWSA 3.1 and to update the appliance with several product fixes.

Refer to What's New for a description of WCCP support and the product fixes.

1.2 Who Should Install This Patch Release

If you are running IWSA 3.1 and want to take advantage of WCCP capabilities and general product fixes, then you should install this service pack release.

Note: Service Pack 1 is for IWSA 3.1 and cannot be installed on an older version. If you are currently running an older version of IWSA and want to install this service pack, then upgrade to IWSA 3.1 before attempting the install. For instructions, see the Trend Micro Web site, http://www.trendmicro.com/download for the appropriate readme.

1.3 Files Included in This Release

Module Filename	**Build No.**
iwss-process	1211
IWSSPIScanVsapi.so	1211
libhttpproxy.so	1211
libicap.so	1211
IWSSPIJavascan.so	1211
libIWSSCommonLDAP.so	1211
libIWSSCommonUSERID.so	1211
svcmonitor	1211
isdelvd	1211
libIWSSUIJNI.so	1211
http_config_httpproxy.jsp	1211
http_config_user.jsp	1211
ftp_config_proxy.jsp	1211
IWSSGui.jar	1211
i18n_warnmsg.js	1211
wccp_router_list.js	1211
S99ISWCCPd	1211
wccpd	1211
greconfig	1211
natconfig	1211
nat.sh	1211
gre.sh	1211
rclwss	1211
libnetsnmp.so.10.0.1	1211
libnetsnmpagent.so.10.0.1	1211
libnetsnmphelpers.so.10.0.1	1211
libnetsnmpmibs.so.10.0.1	1211
libnetsnmptrapd.so.10.0.1	1211

2. What's New?

The following are new for Service Pack 1:

- WCCP Support
- Resolved Known Issues (from IWSA 3.1)

2.1 WCCP Support

IWSA 3.1 + Service Pack 1 provides support for WCCP version 2, a protocol defined by Cisco Systems. See your Cisco product documentation for more information on the protocol.

The following are the benefits gained when IWSA supports WCCP:

- Transparency of deployment without endpoint configuration
- High availability and load balancing between multiple IWSA systems
- Automated load balancing reconfiguration when adding or removing IWSA appliances
- Support Cisco router, switch, and firewall implementations of the protocol

The WCCP implementation for IWSA is compatible with Cisco routers, switches, PIX firewalls, and ASA security devices.

Trend Micro recommends using the following Cisco IOS versions when configuring WCCP with IWSA:

- 12.2(0) to 12.2(22). Avoid using releases 23 and above within the 12.2 family.
- 12.3(10) and above. Avoid using releases 0-9 in the 12.3 family.

Trend Micro recommends using version 7.2(3) and above for the Cisco PIX firewall and avoiding version 7.2(2).

Note: Non-Cisco devices that support WCCP version 2 have not been explicitly tested by Trend Micro. Therefore, interoperability cannot be guaranteed.

2.2 Resolved Known Issues (from IWSA 3.1)

- In case of a hard disk crash, the RAID array needs to be rebuilt, but the `raid_fix_remove.sh` script that re-creates the RAID disk fails to do this. This problem does not occur at runtime. This service pack resolves this issue.
- The active update interval for virus pattern default was once a week. If you have not customized this setting yet, this service pack will change it to once per hour for better protection.
- Under certain conditions, `localhost` may be deleted from `/etc/hosts`. This could cause problems, such as logging to a local database may not work. This service pack resolves this issue.
- SNMP was not configured correctly, making the `svcmonitor.sh` script unable to restart any failed processes. This service pack resolves this issue.
- The ability to change your administrative UI password from the IWSA Preconfiguration Utility (Console Manager) has been removed since the product now supports multiple administrator accounts. Administrator account passwords can be changed using the IWSA Web console.
- If IWSA 3.1 is running in transparent mode, and one of the clients is using HTTP 1.0, and the request URL is "/" and no host header is specified, then it is possible that the HTTP proxy plug-in can crash when trying to write the HTTP access log. This service pack resolves this issue.
- This service pack corrects the issue where an IWSA proxy process goes into an infinite loop, causing IWSA to use a high amount of CPU in ICAP mode. This condition occurs when the following conditions are met during file download:
  - AAXS or IntelliTunnel is licensed and enabled.
  - Large file download method is using deferred scan.
  - Some MIME types are configured to skip virus scanning.
- IWSA has sluggish performance due to corrupted LDAP user IP cache and LDAP group cache. Also, when using the advanced authentication method with referral chasing enabled to authenticate LDAP users, the `krb5.conf` configuration file becomes corrupt. With this service pack, the synchronization methods used between threads have been enhanced to use semaphores to address the issues.
- When using IWSA in ICAP mode to support the Web Reputation Service (WRS) anti-pharming feature, there were noticeable performance issues when no DNS was configured. This service pack addresses the latency issue by not performing DNS or NBNS queries when IWSA is configured in ICAP mode.
- FTP-over-HTTP connection was lost when changing directories using a symbolic or soft link. FTP-over-HTTP now stays connected when changing directories using soft links.
- The Active Directory lookup for groups does not work properly when an LDAP user's common name contains a comma and the Global Catalog is enabled. With this service pack, a new string check is added to handle the comma character in the common name of LDAP users. This addresses the issue for Active Directory group lookups when Global Catalog is enabled.
- IWSA generates core dump files because of a synchronization issue with configuration file access. This service pack addresses the core dump issue by synchronizing the configuration file access.
- When IWSA is configured to block executable file types, a URL that contains a non-standard format (http:/...) instead of the standard format (http://...) is blocked. The non-standard format

causes IWSA to identify the URL as an executable file. With this service pack, a file name checking method is modified to properly handle the non-standard URL format.

3. What's Changed?

This section describes what has changed for Service Pack 1.

3.1 RAID status checking

If you suspect a hard drive problem or a corrupt daemon on your IWSA unit, then Technical Support may direct you to use the new `iwsaSmokeTest.sh` script to diagnose the problem. To understand and correct the problem, it is best that you only use this script under the direction of Technical Support.

4. Documentation Set

In addition to this `readme.pdf` file, the standard IWSA 3.1 documentation set for this release includes the following:

- Quick Start Guide—Covers setting up the IWSA hardware to work in your network, activating the software, and opening the product console.
- Online Help—Context-sensitive help screens that provide guidance for performing a task.
- Administrator's Guide—Detailed configuration instructions and in-depth information about IWSA.
- Upgrade Guide—Describes how to upgrade from IWSA 2.5 Service Pack 1 to IWSA 3.1 (non SP1 release).
- Knowledge Base—A searchable database of known product issues, including specific problem-solving and troubleshooting topics.

  `http://esupport.trendmicro.com/`

You can download electronic versions of the printed manuals from the Trend Micro Web site: `http://www.trendmicro.com/download/product.asp?productid=70`

Note: This readme is currently the only source of static documentation for WCCP configuration. The online Knowledge Base may contain additional documentation over time as new information becomes available.

5. Installation

This section describes the following:

- Installing the Service Pack
- Rolling Back the Service Pack to the Previous Version 3.1 Configuration

5.1 Installing the Service Pack

If you are new to IWSA, consult the Quick Start Guide for instructions on how to set up, configure, and update IWSA.

Note: In order to upgrade to Service Pack 1, you must first install OS patch 1024 or above before you apply the SP1 application patch. The SP1 application patch script aborts if the OS was not updated first.

To update IWSA 3.1 to SP1, complete the following steps:

1) If you have not done so already, download IWSA 3.1 Service Pack 1 file, `IWSA2500_31_en_sp1.tgz`, from `http://www.trendmicro.com/download/product.asp?productid=70`.
2) Uncompress the `IWSA2500_31_en_sp1.tgz` file.

This file contains the OS upgrade file, `iwsa31_en_US.tar.gz` and the application patch file, `iwsa_31_ar32_en_sp1.tgz`.

3) Apply the OS update by copying the OS upgrade file, `iwsa31_en_US.tar.gz`, to a location where it can be accessed by your local system's browser.
4) From the IWSA 3.1 Web console, click **Browse** on the **Administration > IWSA Configuration > Update OS** page, select the upgrade file `iwsa31_en_US.tar.gz`, and then click **Update**. The appliance reboots.
5) Click **Return** to refresh the IWSA Web console.
6) Copy the IWSA 3.1 application upgrade file (`iwsa_31_ar32_en_sp1.tgz`) to a location where it can be accessed by your local system's browser.
7) From the IWSA 3.1 Web console, click **Browse** on the **Administration > IWSA Configuration > System Patch** page, select the upgrade file `iwsa_31_ar32_en_sp1.tgz`, and then click **Upload**.
8) Click the **Install** link in the IWSA 3.1 Web console.

The upgrade process should take about two minutes. The upgrade process displays `IWSA 3.1 EN SP1 2500` to indicate that the upgrade was successful.

5.2 Rolling Back the Service Pack to the Previous Version 3.1 Configuration

To rollback:

1) Open the IWSA Web console (**Administration > IWSA Configuration > System Patch**).
2) Cick the **Uninstall** link under the **Installed Patches** section of the service pack.
   The system returns to the last known good configuration prior to Service Pack 1.

6. System Requirements

Open the IWSA console with Microsoft™ Internet Explorer (version 6.0 or 7.0) or Mozilla Firefox (version 1.5 or 2.0).

Appliance Hardware and Installed Programs

- Operating System: Linux™ Kernel 2.6.14
- Database: PostgreSQL 7.4.16 (for logs and reports)
- CPU: Intel™ Xeon™ 2.8GHz x 2 with Hyper-threading (4 virtual CPU equivalency)
- Memory: 2GB or 4GB; (2/4 x 1024MB DDR)
- Existing customers with 2GB can successfully upgrade to 3.1.
- Flash IDE Drive: 256MB (boot device)
- Hard Drives: Two 40GB RAID set in mirror configuration

Compatible Directory Servers

- Microsoft Active Directory™ 2000 and 2003
- Linux OpenLDAP Directory 2.2.16
- Sun™ Java System Directory Server 5.2 (formerly Sun ONE Directory Server)

Compatible ICAP Cache Servers

- ICAP servers that support ICAP 1.0

7 Post-Installation Configuration

In order to use WCCP functionality, this section describes the following:

- Specifying static routes to access subnets
- Configuring the Cisco device and IWSA for WCCP
- Configuring IWSA for a WCCP service group
- Configuration 1: Firewall only between WCCP Router and Internet
- Configuration 2: Firewall on client machine
- Configuration 3: Stateful firewall between client and IWSA
- Controlling WCCP Logging
- Sample PIX firewall configuration

7.1 Specifying static routes to access subnets

If WCCP is enabled for IWSA and a default gateway configured on IWSA is not aware of the client's network, then you will need to use the IWSA Preconfiguration Utility (from the console manager) to specify an additional gateway (static route) that is able to communicate with the client's network. Specifying this static route in IWSA provides the designated router with the client's network address. With this information, IWSA knows which route to use in order to communicate with the HTTP or FTP client.

Note: To avoid deployment related issues, Trend Micro recommends placing IWSA in the network where the WCCP traffic redirection is defined. For example, if WCCP traffic redirection is defined on interface 0 of a router (ip wccp 80 redirect in), and interface 0 is in the network 192.168.100.0/24, then IWSA should be placed in this network to avoid deployment related issues. Certain firewall types such as Cisco PIX515 only allows redirect in to be configured on an interface, and this particular network is where IWSA should be placed to avoid deployment related issues.

To specify a static route:

1) Logon to the Console Manager using ssh or a serial connection.
   For a serial connection, logon as `root`.
   For ssh, logon as `remote admin` with the `remoteadmin` password, then provide the root password.
2) From the **Main Menu**, select **option 1, System Configuration**.
3) From the **System Configuration Menu**, select **option 2, Configure Device Settings**.
4) From the **Device Settings Menu**, select **option 3, Change Route Settings**.
5) From the **Change Route Settings Menu**, select the option for the route setting you want to add or change.
   Repeat this step for each route setting you want to add or change.
6) Complete the prompts with appropriate information as they appear on the screen.

7.2 Configuring the Cisco device and IWSA for WCCP

In order to prevent communication related issues, WCCP needs to be configured on the Cisco router or switch before being configured on IWSA.

To configure a Cisco device and IWSA for WCCP:

1) Configure WCCP on either the router or switch being used with IWSA.
   Refer to your Cisco device manual for configuration details.
2) Log into the IWSA Web console.
3) Click **HTTP**.
4) Click the **Proxy Scan Settings** item in the "Configuration" section.
5) Select **Forward Proxy**.
6) Select **Enable Transparency**.
7) Select **Use Web Cache Coordination Protocol (WCCP)**.
8) Enter the router IP address(es).
   A maximum of eight routers can be entered. Enter only valid IP address(es).
9) Optionally, enter a password.
   If you specify no password for IWSA, then you should specify no password for the router. If you specify a password for IWSA, then ensure that the same password is also used for the Cisco device(s).

   While certain routers support Message-Digest algorithm 5 (MD5) encryption types 0-7, IWSA only supports WCCP encryption types 0-6. Therefore, if you set the optional router password type for WCCP communication, choose a value from 0-6. Encryption type 7 is a Cisco proprietary type and is not supported.
10) Choose the WCCP forwarding method: **GRE** or **Layer 2**.

Typically, Cisco routers only support GRE. Cisco switches only support the Layer 2 redirect assignment method. If in doubt, refer to the router or switch manual.

11) Click **Save** to save the WCCP settings.

After the WCCP configuration is saved, you can use the `show ip wccp` command on the router or switch to verify that IWSA has been added as one of the WCCP cache engines. If this addition is successful, various information displays, including the IWSA IP address (`Web Cache ID`) and the state of the IWSA unit, which will be `Usable`. The following is a typical display indicating that IWSA was added successfully:

```
WCCP Cache-Engine information:

    Web Cache ID:          192.168.62.100
    Protocol Version:      2.0
    State:                 Usable
    Initial Hash Info:     00000000000000000000000000000000
                           00000000000000000000000000000000
    Assigned Hash Info:    FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF
                           FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF
    Hash Allotment:        256 (100.00%)
    Packets Redirected:    0
    Connect Time:          00:05:07
    Bypassed Packets
       Process:            0
       Fast:               0
       CEF:                0
```

If IWSA was not added successfully as one of the WCCP cache engines, then no information will be displayed. In this case, you can use the `debug ip wccp packet` command to determine the problem.

On IWSA, certain WCCP communication-related information is also available from the `http.log` file in the `/etc/iscan/log/` directory. To locate this information, search for log entries that begin with `WCCP`.

7.3 Configuring IWSA for a WCCP service group

After installed, IWSA uses service ID `80` (a WCCP component) to represent the WCCP service group. The associated router redirects HTTP and FTP traffic to this service group. In order to work with IWSA, configure your routers using the same service ID. If a router does not have ID `80` available, then choose another service ID and then customize IWSA as described in this section.

Load Balancing for WCCP Communication

Using the Well-Known Service Group for WCCP communication with more than one IWSA device as part of the service group does not load balance as well as using the Dynamic Service Group (default service ID `80` for IWSA). The load balancing offered by the Well-Known Service Group deviates more from the round robin concept than does the Dynamic Service Group. This may be due to the load balancing algorithm WCCP uses, and the way the WCCP router or firewall operates.

For best performance and resource usage distribution among IWSA devices, Trend Micro recommends using the Dynamic Service Group (default service ID `80` for IWSA) where applicable.

Note: In order to prevent communication related issues, WCCP needs to be configured on the Cisco router or switch before being configured on IWSA (see "7.2 Configuring the Cisco device and IWSA for WCCP").

Configuring IWSA to use the Dynamic Service Group

The WCCP's Dynamic Service ID is configurable by editing the `/etc/iscan/IWSSPIProtocolHttpProxy.pni` file.

You can modify the following default entries from `80` to the desired service ID.

```
wccp_dynamic_service=dynamic 80
wccp_service_info=80 protocol=tcp
flags=src_ip_hash,dst_ip_hash,source_port_hash priority=120 ports=80,21
```

Note: The second and third lines of the above code should be typed as a single line. Because of space limitations in this readme, this code occupies two lines.

To configure the Dynamic Service ID:

1) Access the IWSA Preconfiguration Console Manager through ssh or serial connection.
2) From the **Main Menu**, select **option 2, Utilities**.
3) From the **Utilities Menu**, select **option 1, Start Shell Interface**.
4) From the shell, stop the WCCP daemon by issuing the following command:
   ```
   /usr/iwss/S99ISWCCPd stop
   ```
5) Modify the following parameters in the `/etc/iscan/IWSSPIProtocolHttpProxy.pni` file by modifying the default service ID from `80` to the desired value.

   Example:

```
wccp_dynamic_service=dynamic 99
wccp_service_info=99 protocol=tcp
flags=src_ip_hash,dst_ip_hash,source_port_hash priority=120 ports=80,21
```

6) Change the WCCP service ID on the WCCP-supported Cisco device to the configured service ID.
   In the above example, the configured service ID is `99`.
7) From the console manager, restart the WCCP daemon by issuing the following command:
   ```
   /usr/iwss/S99ISWCCPd restart
   ```

Note: In order to implement the new service ID on IWSA, restart the wccpd daemon after the service ID is modified. This results in both IWSA and the supported WCCP Cisco device being configured to use the same service ID, which allows them to belong to the same service group. As members of the same service group, IWSA and the WCCP Cisco device can communicate with each other.

The valid customizable WCCP Dynamic Service ID range is from 51-255, while 0-50 is reserved for Well-Known services. Certain WCCP routers only accept service ID range from 0-99.

Configuring IWSA to use the Well-Know Service Group

For some older routers that do not support WCCP Dynamic Service group, IWSA can be configured to use the Well-Known Service group.

Note: If IWSA is configured to use the Well-Known Service ID to join a Well-Known Service group, then Trend Micro recommends configuring only one router on each IWSA device.

To configure the Well-Known Service ID:

1) Access the IWSA Preconfiguration Console Manager through ssh or serial connection.
2) From the **Main Menu**, select **option 2, Utilities**.
3) From the **Utilities Menu**, select **option 1, Start Shell Interface**.
4) Modify the following parameters in the `/etc/iscan/IWSSPIProtocolHttpProxy.pni` file by commenting out the first two lines and then by adding the third one below:

```
   #    wccp_dynamic_service=dynamic 80
   #    wccp_service_info=80 protocol=tcp
flags=src_ip_hash,dst_ip_hash,source_port_hash priority=120 ports=80,21
   wccp_std_service=standard 0
```

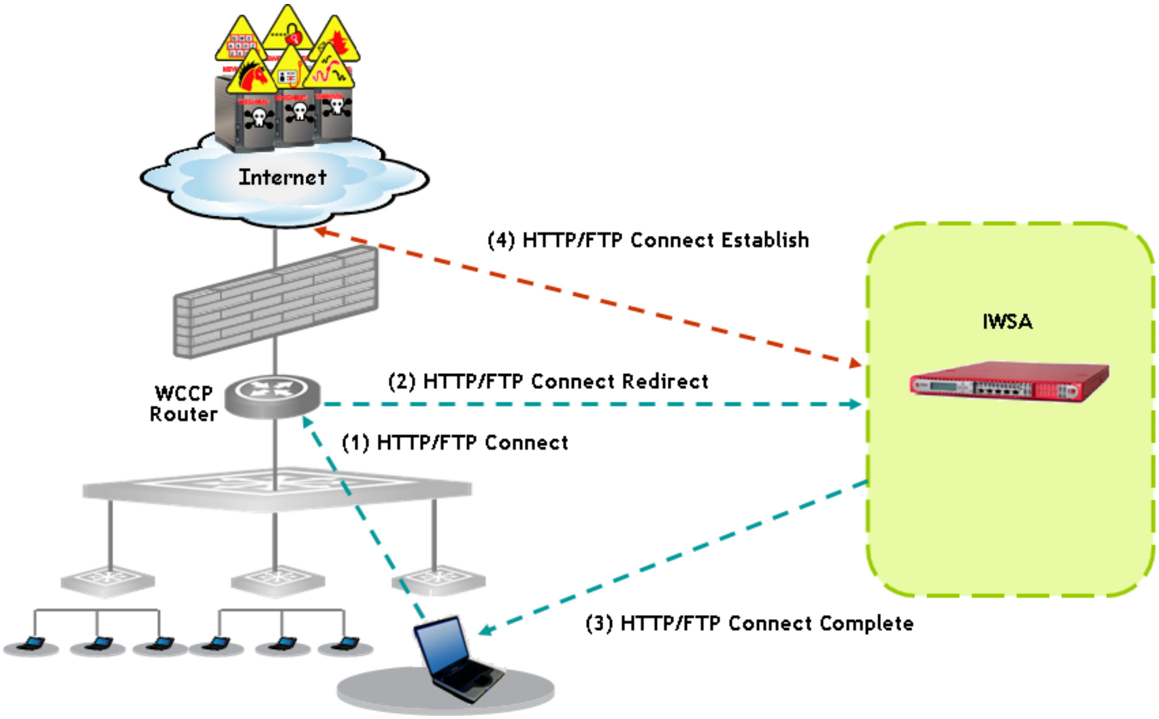
5) Change the WCCP service ID on the WCCP-supported Cisco device to the configured service ID.
   In the above step, the configured ID is 0. Typically, Cisco devices with WCCP support use the string, `web-cache`, as part of the WCCP command for using service ID 0.

6) From the shell, restart the WCCP daemon by issuing the following command:
`/usr/iwss/S99ISWCCPd restart`

Note: Based on WCCP specification, the Well-Known service group configuration does not support FTP traffic redirection to IWSA for scanning. Configure the WCCP Cisco device to use the Well-Known service type prior to configuring IWSA to avoid WCCP communication issues.

7.4 Configuration 1: Firewall only between WCCP Router and Internet

The following graphic illustrates HTTP and FTP traffic.


Internet
(4) HTTP/FTP Connect Establish
IWSA
WCCP Router
(2) HTTP/FTP Connect Redirect
(1) HTTP/FTP Connect
(3) HTTP/FTP Connect Complete

7.5 Configuration 2: Firewall on client machine

If the client machine (laptop in the previous graphic) uses a personal firewall in addition to the firewall between the WCCP router and the Internet, then IWSA cannot support FTP scanning (see “8.2 FTP scanning is not supported under multiple firewalls”).

7.6 Configuration 3: Stateful firewall between client and IWSA

If a stateful firewall exists between the client machine (laptop in graphic above) and IWSA, then IWSA cannot support FTP scanning (see “8.2 FTP scanning is not supported under multiple firewalls”).

7.7 Controlling WCCP Logging

HTTP and WCCP both write to the HTTP log. While HTTP uses the verbose attribute to enable or disable detailed logging, WCCP uses a different attribute to enable or disable logging.

By default, WCCP logging is enabled. You can disable WCCP logging by adding the line `wccp_logging=0` to the `/etc/iscan/IWSSPIProtocolHttpProxy.pni` file. Changing the line to `wccp_logging=1` turns WCCP logging back on again.

Configuration steps:

1) If the WCCP is already enabled, stop the WCCP daemon from the command line after accessing the IWSA shell interface by `/usr/iwss/S99ISWCCPd stop`.
   See “7.3 Configuring IWSA for a WCCP service group” for details about accessing the IWSA shell.
2) Add the line `wccp_logging=0` under the [http] section in the `/etc/iscan/IWSSPIProtocolHttpProxy.pni` file.
3) Start the WCCP daemon from command line `/usr/iwss/S99ISWCCPd start`.

Note: WCCP logging only records WCCP control messages and not user traffic activities. The WCCP daemon needs to be restarted to pick up the WCCP logging settings in the `IWSSPIProtocolHttpProxy.pni` file.

7.8 Sample PIX firewall configuration

Below, is an example of how WCCP could be configured on a PIX firewall using a Well-Known and Dynamic Service ID, along with an enabled password. The `inside` statement represents the name associated with an inside (most trusted) network interface on a PIX firewall.

The command lines containing `web-cache` are used for a Well-Known Service ID. The command lines containing `80` are used for a Dynamic Service ID, with the default value for IWSA specified. For more detailed PIX firewall configurations, refer to relevant Cisco documentations.

```
wccp web-cache password <password>
wccp interface inside web-cache redirect in
wccp 80 password <password>
wccp interface inside 80 redirect in
```

The password is alpha-numeric and can be up to eight characters in length. The password is MD5-based and the same password specified for the firewall must be specified for IWSA

8. Known Issues

This section describes the following known issues:

- Rollback does not remove WCCP router parameter
- FTP scanning is not supported under multiple firewalls

8.1 Rollback does not remove WCCP router parameter

After rollback from SP1 to IWSA 3.1, the following parameter is left in the `IWSSPIProtocolHttpproxy.pni` file:

```
wccp_router=
```

This empty parameter does not cause any harm.

8.2 FTP scanning is not supported under multiple firewalls

If the client machine (laptop in graphic above) uses a personal firewall in addition to the firewall between WCCP and the Internet, then IWSA cannot support FTP scanning. Likewise, if a stateful firewall exists between the client machine and IWSA, then IWSA cannot support FTP scanning. This is because the client firewall or stateful firewall will disconnect an FTP session when it detects that the FTP control channel is going to one IP address (the FTP server) and the data channel is going to a different address (IWSA).

The only workaround to enable IWSA to perform FTP scanning is to disable the firewalls discussed in this section.

9. Release History

Service Pack 1 for IWSA 3.1	February 2008
IWSA 3.1	July 2007
IWSA 2.5 Service Pack 1	December 2006
IWSA 2.5 Patch 1, Build 1142	May 2006
IWSA 2.5	February 2006

10. Contact Information

A license to the Trend Micro software usually includes the right to product updates, pattern file updates, and basic technical support for one (1) year from the date of purchase only. After the first year, Maintenance must be renewed on an annual basis at Trend Micro's then-current Maintenance fees.

You can contact Trend Micro via fax, phone, and email, or visit us at:

`http://www.trendmicro.com`

Evaluation copies of Trend Micro products can be downloaded from our Web site.

Global Mailing Address/Telephone Numbers
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

For global contact information in the Asia/Pacific region, Australia and New Zealand, Europe, Latin America, and Canada, refer to:

`http://www.trendmicro.com/en/about/overview.htm`

The Trend Micro "About Us" screen displays. Click the appropriate link in the "Contact Us" section of the screen.

Note: This information is subject to change without notice.

11. About Trend Micro

Trend Micro, Inc. provides virus protection, anti-spam, and content-filtering security products and services. Trend Micro allows companies worldwide to stop viruses and other malicious code from a central point before they can reach the desktop.

12. License Agreement

Information about your license agreement with Trend Micro can be viewed at:

`http://www.trendmicro.com/en/purchase/license/`

Third-party licensing agreements can be viewed:

- By referring to the `IWSA_License_File.pdf` file in the Solutions CD
- The license agreement on the Trend Micro Web site
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~