Release Notes for Websense i-Series Appliances

Topic 70074 | Release Notes | i-Series Appliance | Updated: 17-Apr-2014

Applies to:	Websense i-Series appliance v1.2, 1.2.1

Contents

The Websense i-Series appliance is a component of Websense Cloud Web Security Gateway, a Web security solution that provides on-premises URL analysis and application/protocol detection for Web traffic, along with centralized policy management and reporting capabilities in the cloud.

The i-Series appliance hosts the Websense URL category master database, allowing the efficient analysis of web site request URLs. The appliance also provides protocol detection capabilities and policy enforcement.

When analysis indicates that a web request requires further examination, the appliance transparently routes that traffic to the cloud, where Websense Cloud Web Security Gateway analytics are applied and policy is enforced. Management of on-premises appliances is also performed in the cloud.

You can deploy the Websense i-Series appliance as a virtual appliance. For virtual appliance information, see the Websense Cloud Web Security Getting Started Guide.

View detailed product user information in the following Help systems:

- Websense i-Series Appliance Help
- Websense Cloud Security Help

Use these Release Notes to learn about a critical update to the version 1.2 i-Series appliances. These notes also contain a list of version 1.2 product features, installation and upgrade tips, and resolved and known issues lists.

See the Websense Cloud Security Release Notes for updates on cloud portal changes. You must log on to the Cloud Security portal to view the Release Notes.

Version 1.2.1 release update

Topic 70075 | Release Notes | i-Series Appliance | Updated: 17-Apr-2014

Applies to:	Websense i-Series appliance v1.2, v1.2.1

This release of the Websense i-Series appliance addresses the following 2 important fixes:

- **OpenSSL Vulnerability CVS-2014-0160 (Heartbleed)**

  The critical OpenSSL Vulnerability (Heartbleed) identified in CVE-2014-0160 affects the Websense i-Series appliances for version 1.2.

  This vulnerability does not affect customers who are running the following appliance versions: i-Series version 1.1.

  If you are running version 1.2, you must upgrade to version 1.2.1 to protect your network from the OpenSSL vulnerability.

  Note

  The i-Series appliance terminates SSL only for serving block pages, quota pages, confirm pages, and auth pages, which do not require outbound SSL interaction with origin servers. As a result, the appliance vulnerability is somewhat limited, but can still be exploited within your local area network (LAN).

  SSL scanning is handled by Websense cloud services, which are not affected by the bug.

- **Traffic server operations terminated unexpectedly**

  Some non-HTTP traffic could cause this unexpected proxy behavior.

New version 1.2 product features

Topic 70076 | Release Notes | i-Series Appliance | Updated: 17-Apr-2014

Applies to:	Websense i-Series appliance v1.2, v1.2.1

This version of Websense Cloud Web Security Gateway contains new features and fixes. Among the new features is the capability to access appliance management functions via the serial port, in case other access is unavailable for some reason.

This section of the Release Notes describes the new features available for this release of the Websense i-Series appliance:

VLAN tag support

This version of the appliance can be configured to analyze virtual LAN (VLAN) tagged and untagged traffic. If your Cloud Security deployment is on a virtual appliance, you must have installed a Silicom bypass card in order to use VLAN tags. See *Virtual appliance*, page 5, for more information about the bypass card.

All VLAN traffic is analyzed unless you define some of that traffic as trusted. You can bypass analysis for untagged traffic and for specific VLAN tags in the Websense Cloud Security portal. See the Websense Cloud Web Security Getting Started Guide for configuration details.

The i-Series appliance supports the use of a single VLAN tag for management communication traffic from the appliance to the cloud and database download services. This tag is also used by any client that communicates with the appliance bridge interface (B1 and B2) either explicitly for management purposes or transparently for authentication, quota, or confirm actions. Configure the appliance VLAN setting in the First-Time Configuration Wizard Routing page or on the **Configuration > Interfaces and Routing** screen.

> **Note**
> You must configure valid routing between the bridge interface and any client generating traffic that is intercepted by the appliance, taking into account the VLAN tag defined on the Routing page.

Diagnostic test utility

A new diagnostics utility lets you run a series of system tests to determine network connectivity status and health. Click the Diagnostics tab on the **Status > Alerts and Diagnostics** page to display a table that shows the list of tests to run.

When you click **Run Diagnostics** to begin the tests, the Results column displays test status (In progress) and results (Passed, Failed, or Could not complete). For tests that do not complete or fail, the Details column displays more information, including suggestions for resolving an issue that caused a failure.

Websense recommends that you run the diagnostics utility at initial appliance deployment and any time after that when the appliance appears not to be functioning properly.

YouTube education support

The YouTube for Schools service provides access for educational institutions to YouTube EDU and school-specific content from inside the school network, and blocks all other YouTube content. This feature is active for end users only if the YouTube Web category is not blocked.

See Websense Cloud Security Help for configuration information.

Websense cloud portal change

You can also configure VLAN support in the Network Devices **Networking** tab in the cloud portal. Mark the **Support VLAN tags** check box if you want the appliance to analyze VLAN tagged and untagged traffic. All VLAN traffic will be analyzed unless you define some of that traffic as trusted. See the Websense Cloud Web Security Getting Started Guide for information about VLAN support in the cloud portal.

Installation, deployment, and upgrade

Topic 70077 | Release Notes | i-Series Appliance | Updated: 17-Apr-2014

Applies to:	Websense i-Series appliance v1.2, v1.2.1

Installation

Installation and set up for the Websense i-Series appliance are summarized on the Quick Start poster that was shipped with your appliance. Click here to view a copy of the quick start guide.

See the Websense Cloud Web Security Getting Started Guide for information about system configuration.

If your network includes a firewall, ensure that the following destination TCP ports are open:

Port	Purpose
8002	Configuration and policy update information retrieval from Websense Cloud Security. This port must be open for an i-Series appliance to retrieve periodic configuration setting and policy updates from the cloud service.
8081	Proxy service. This is where the Websense Cloud Security cloud-based content analysis is provided.

Port	Purpose
80	Notification page components. The default notification pages refer to style sheets and images served from the Websense Cloud Security platform. For these pages to appear correctly, this web site is accessed directly (i.e., not through Websense Cloud Security).
443	Service administration. The Websense administration portal is similarly unproxied. Otherwise, it would be possible for you to accidentally block access and then be unable to rectify the situation.

It is also recommended that the outbound Network Time Protocol (NTP) port (UDP 123) be open as well to allow time/clock synchronization in the system.

Note

The transfer of new password and appliance registration information between the cloud portal and the appliance takes several minutes. You may experience a delay when logging in after a change is made to these settings.

Deployment

Additional considerations should be examined for some i-Series appliance deployments, including those that use:

- an i-Series virtual appliance
- endpoint devices or PAC-enabled clients that communicate directly with the cloud

Virtual appliance

The i-Series virtual appliance may be deployed with or without the network bypass capability. Download the appliance image (OVF format) from the MyWebsense downloads page, and see the Websense Cloud Web Security Getting Started Guide for virtual appliance deployment instructions.

Note

If you want to deploy a virtual appliance with the network bypass capability, your hardware must support the ESXi DirectPath I/O function.

If you plan to deploy a virtual appliance, you should verify the following system requirements:

- VMware vSphere ESXi platform versions 5.1 or 5.5

- 6 CPU cores, 12 GB RAM (minimum)
- 128 GB hard disk drive
- Optional: Silicom network bypass card (Silicom PE2G2BPI80-SD-R) with 2 dedicated network interfaces (must be installed on ESXi in VMDirectPath mode)

  Some models of HP hardware do not support VMDirectPath mode.

Mixed-mode deployment issues

If your network includes an i-Series appliance along with endpoint devices or PAC-enabled clients that communicate with the cloud directly (for example, roaming users), you may encounter additional deployment issues. You should consider the following port information before you deploy:

- Use of the site's egress as a policy connection is not supported. As a result, endpoint or PAC-enabled clients are treated as roaming users regardless of whether they are connected within the network LAN.
- Endpoint device and PAC-enabled client traffic directly to the cloud service in a network that includes an i-Series appliance is supported on ports 8081 and 8082.
- Endpoint device traffic directly to the cloud service in a network that includes an i-Series appliance is supported on port 80, but traffic from a PAC-enabled client on port 80 is not supported.
- Applications that use HTTP (e.g., IM clients) may still try to use port 80 or 443 for outbound traffic. This traffic is intercepted and processed by the i-Series appliance, which may lead to inconsistencies. This potential problem should be checked on a per-site, per-application basis, and a resolution determined based on a customer's actual needs, for example:
  - Block the applications at the firewall level
  - Use explicit proxy mode for the applications
  - Use other ports for the applications

Upgrade

Use the following steps to upgrade from a previous version of Websense Cloud Security:

1. Click **Network Devices** in the cloud portal.
2. Select the appropriate appliance for the upgrade and click **Properties & Statistics**.
3. Click **Version History**.
4. Find the desired upgrade and click the **Download** icon in the Action column. This operation downloads the upgrade to the selected appliance.

   Clicking the **View** icon in the Description column opens the Release Notes for that upgrade.

5. In the i-Series appliance **Configuration > Upgrade Management** page, find the upgrade in the table at the top of the screen. Click the **Download** icon in the Action column. This operation downloads the upgrade to the appliance.
6. When the upgrade status is changed to Downloaded (you may need to refresh the screen to see the change), click the **Install** icon to install the upgrade.

Important

Upgrade status may display as "Failed" after a successful upgrade from version 1.1 to version 1.2. This incorrect error message may appear if you refresh the appliance user interface immediately after the upgrade operation.

Please wait approximately 5 minutes to refresh the user interface after the upgrade.

If the problem persists after this time period, please contact Websense Technical Support.

Resolved and known issues

Topic 70078 | Release Notes | Websense i-Series Appliance | Updated: 17-Apr-2014

Applies to:	Websense i-Series appliance v1.2, v1.2.1

A list of resolved and known issues for the Websense i-Series appliance is available in the Websense Technical Library. If you are not already logged on to MyWebsense, this link takes you to the log in screen.