Release Notes for Websense IQ-Series Appliances

Topic 70128 | Release Notes | IQ-Series Appliance | Updated: 16-Apr-2015

Applies to:	Websense IQ-Series appliance v1.4, 1.4.1

Contents

The Websense IQ-Series appliance is a component of Websense blueSKY Security Gateway. This web protection solution provides on-premises URL analysis and application/protocol detection for web traffic, along with centralized policy management and reporting capabilities in the cloud. The appliance Quick Start Guide illustrates the ease with which this web security solution can be implemented.

The IQ-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 blueSKY Security Gateway analytics are applied and policy is enforced. Management of on-premises appliances is also performed in the cloud.

View detailed product user information in the following Help systems:

- Websense IQ-Series Appliance Help
- Websense blueSKY Security Gateway Help

Use these Release Notes to learn about important version 1.4.1 updates, version 1.4 product features, installation and upgrade tips, and resolved and known issues.

Version 1.4.1 release updates

Topic 70129 | Release Notes | IQ-Series Appliance | Updated: 16-Apr-2015

Applies to:	Websense IQ-Series appliance v1.4, 1.4.1

Version 1.4.1 of the Websense IQ-Series appliance includes resolutions for the following security issues:

- **Google intermediate certificate update**

  Google recently updated its intermediate certificate with the Common Name (CN) of "Google Internet Authority G2." Without the new certificate provided in this release, user requests to access Google sites generate a block page when session-based authentication is in effect.

- **OpenSSL vulnerabilities**

  The following vulnerabilities in OpenSSL libraries have been updated:

CVE ID	Description
CVE-2014-3570	Bignum squaring (BN_sqr) may produce incorrect results on some platforms. This bug may allow remote attackers to bypass some cryptographic protections.
CVE-2014-3571	A carefully crafted DTLS message can cause a segmentation fault in OpenSSL due to a NULL pointer dereference. This bug could lead to a denial of service attack.
CVE-2014-3572	An OpenSSL client may accept a handshake using an ephemeral ECDH cipher suite using an ECDSA certificate if the server key exchange message is omitted. This effectively removes forward secrecy from the cipher suite.
CVE-2014-8275	OpenSSL accepts several non-DER-variations of certificate signature algorithm and signature encodings. OpenSSL also does not enforce a match of the signature algorithm between the signed and unsigned portions of the certificate. If the contents of the signature algorithm or the encoding of the signature are modified, the certificate's fingerprint could be changed. Custom applications that rely on the uniqueness of the fingerprint (e.g., certificate blacklists) may be affected.
CVE-2015-0204	An OpenSSL client may accept the use of an RSA temporary key in a non-export RSA key exchange cipher suite. A server could present a weak temporary key and downgrade the security of the session. (This is the vulnerability known as FREAK.)

CVE ID	Description
CVE-2015-0205	An OpenSSL server will accept a DH key for client authentication without the certificate verify message. This bug effectively allows a client to authenticate without the use of a private key. Servers that trust a client certificate authority that issues certificates containing DH keys may be affected.
CVE-2015-0206	A memory leak can occur in the dtls1_buffer_record function if an attacker sent repeated DTLS records with the same sequence number but for the next epoch. The memory leak could be exploited by an attacker in a denial of service attack through memory exhaustion.
CVE-2015-0209	A malformed EC private key file consumed by the d2i_ECPrivateKey function could cause a use-after-free condition. This, in turn, could cause a double-free in several private key parsing functions, leading to a denial of service attack or memory corruption for applications that receive EC private keys from untrusted sources.
CVE-2015-0286	Boolean comparisons may not be properly performed, disrupting certificate verification operations. This bug affects any application that performs certificate verification and could result in a denial of service attack.
CVE-2015-0287	Reusing a structure in ASN.1 parsing may cause memory corruption via an invalid write, resulting in a denial of service attack. This bug may affect applications that parse structures containing CHOICE or ANY DEFINED BY components.
CVE-2015-0288	A carefully crafted X.509 certificate authentication request can cause a NULL pointer dereference, resulting in a denial of service attack.
CVE-2015-0289	Carefully crafted ASN.1-encoded PKCS#7 input with missing content could trigger a NULL pointer dereference on parsing, resulting in a denial of service attack.
CVE-2015-0292	Maliciously crafted base64 data could trigger a segmentation fault or memory corruption, resulting in a denial of service attack.
CVE-2015-0293	A specially crafted SSLv2 CLIENT-MASTER-KEY message can trigger an OPENSSL_assert (i.e., an abort) in servers that both support SSLv2 and enable export cipher suites.

Important version 1.4 updates

The version 1.4 release of the Websense IQ-Series appliance includes resolutions of the following 2 security vulnerabilities:

- **Bash vulnerabilities (Shellshock)**

The critical Bash vulnerabilities were first identified in CVE-2014-6271. Subsequent investigation of the Bash code revealed other, related vulnerabilities.

The vulnerabilities present in Bash (Bourne Again Shell) up to version 4.3 could be exploited by malicious persons, including over HTTP.

Many programs like SSH, telnet, and CGI scripts allow Bash to run in the background, allowing the vulnerability to be exploited remotely over the network.

- **SSL vulnerability (POODLE)**

  The critical SSLv3 vulnerability was identified in CVE-2014-3566.

  SSL (Secure Sockets Layer) is the standard security technology for establishing an encrypted link between a web server and a browser. TLS (Transport Layer Security) has since superseded SSL. However, support for the older SSL version 3.0 still exists in the majority of applications and can therefore lead to software (such as browsers) being forced into using a vulnerable SSLv3 connection.

  The vulnerability could be exploited by inducing a client's browser into making multiple browser requests over HTTPS with SSLv3, and inferring details about the encrypted contents that allow an attacker to compromise the security of SSLv3.

Version 1.4 product features

Topic 70129 | Release Notes | IQ-Series Appliance | Updated: 16-Apr-2015

Applies to:	Websense IQ-Series appliance v1.4, 1.4.1

This release of the Websense IQ-Series appliance includes the following appliance infrastructure enhancements.

- The appliance alert system implementation is enhanced in this release to reduce the display of redundant or inappropriate alerts.
- Appliance user interface services are upgraded for improved security and compliance.
- Cryptographic hash functions are upgraded for improved security.
- Apache Traffic Server (ATS) is upgraded for improved network efficiency and performance.

Installation and upgrade

Topic 70130 | Release Notes | IQ-Series Appliance | Updated: 16-Apr-2015

Applies to:	Websense IQ-Series appliance v1.4, 1.4.1

Installation

Installation and set up for the Websense IQ-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 Getting Started Guide for information about system configuration.

> **Important**
> Use of Microsoft Internet Explorer 8 (or below) on a Windows XP machine is not supported.

If your network includes a firewall, you need to ensure that destination TCP ports are open for connection to the cloud service. By default, the appliance is configured to use standard destination ports 80 and 443 for these connections.

> **Note**
> Upgrade from a previous appliance version does not change port configuration settings. If you want to use destination ports 80 and 443, you should modify appliance settings manually after the upgrade process.

Alternatively, and depending on your corporate firewall policy, you can configure your appliance to use the following ports, which are used for non-appliance connections to the cloud service:

Port	Purpose
8002	Configuration and policy update information retrieval from Websense blueSKY. This port must be open for an IQ-Series appliance to retrieve periodic configuration setting and policy updates from the cloud service.
8081	Proxy service. This is where Websense cloud-based content analysis is provided.
80	Notification page components. The default notification pages refer to style sheets and images served from the Websense blueSKY platform. For these pages to appear correctly, this web site is accessed directly (i.e., not through Websense blueSKY).
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.

You can switch between the standard and alternative ports at any time using the appliance command-line interface (CLI). See the Getting Started Guide for detailed instructions about switching port settings.

You should also open the outbound Network Time Protocol (NTP) port (UDP 123) 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.

Upgrade

Use the following steps to upgrade from a previous version of the Websense IQ-Series appliance:

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 IQ-Series appliance **Configuration > Upgrade Management** page, find the upgrade in the table at the top of the screen. The upgrade status should be **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. 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 70131 | Release Notes | Websense IQ-Series Appliance | Updated: 16-Apr-2015

Applies to:	Websense IQ-Series appliance v1.4, 1.4.1

Please contact Websense Technical Support for a list of known issues for this version of Websense blueSKY Security Gateway.