Revision A

McAfee Web Gateway 7.8.2 Release Notes

Contents

About this release

This document contains important information about the current release. We recommend that you read the whole document.

McAfee® Web Gateway (Web Gateway) 7.8.2 is provided as a controlled release. It is a major version that includes new features and enhancements and resolves issues present in previous versions.

If you have implemented the bonding configuration that was available as an unsupported feature before the release of Web Gateway 7.5.2, remove any settings of this configuration before upgrading to this new product version. Otherwise you risk creating an unstable state on the appliance.

End of Helix proxy support

The Helix proxy is a third-party proxy for handling real-time streaming data. Support of this proxy on Web Gateway ended in December 2017.

Accordingly, the first product versions that did no longer support this proxy were 7.6.2.18, 7.7.2.7, and 7.8.0.2.

This information was, however, not included in the documentation at the time when these product versions were released.

What's new

The current release of the product includes these new features and enhancements.

TLS protocol handling made configurable

Use of different TLS protocol versions can be configured on Web Gateway.

The options for configuring these versions are part of the settings for internal communication with the file server and the user interface that the administrator works with.

Improved processing of Skype traffic

Processing of Skype traffic on Web Gateway has been improved by removing issues that impacted the processing when HTTPS scanning was also activated. This is achieved through letting Skype traffic bypass HTTPS scanning.

Bypassing can be enabled if skipping content scanning is considered an acceptable risk. Certificate verification will still happen in this case.

Better user experience with DNS handling

DNS handling has been improved for dual stack environments (IPv4/IPv6).

DNS queries for A and AAAA records can be made simultaneously and the preferred answer can be used to connect to the server if it does not come later than the fallback IP address type version.

Higher version of operating system

The version of the operating system used on a Web Gateway appliance has moved up to MLOS 3.

Further improvements

Further improvements have been added to Web Gateway to make its administration more comfortable.

- An option is provided for including a URL for a Certificate Revocation List (CRL) or for validating certificates under the Online Certificate Status Protocol (OSCP) in certificates issued by a certificate authority on Web Gateway.
- The **URL.Destination.IP** property, which has its value set to the IP address found by the first DNS lookup when a request is processed, is updated by the proxy on Web Gateway after connecting successfully to a web server.

  The update is intended to solve the problem that the IP address used after connecting successfully might differ, for example, due to retries after a failure, from the IP address that the property was first set to.
- Log files can pushed under the Secure Copy Protocol (SCP) as well as under the Secure File Transfer Protocol (SFTP) from Web Gateway to a web server that only accepts SHA-256 encryption.
- A list with URL categories that access to is illegal in the United Kingdom has been added to the lists of categories that are by default blocked when URL filtering is performed on Web Gateway.

- The name found in the DNS lookup for a domain controller is used when a handshake to set up a connection for use in authenticating users under the NTLM authentication method. Use DNS name of DC for NTLM handshake
- The output that is produced when the status of connections is queried using the -s connections command on Web Gateway has been enlarged.

  It now includes the IP address of the web server that the last request before a given request was sent to. More status information is also provided in a textual format, replacing information in numerical format.

Resolved issues

The current release of the product resolves these issues. For a list of issues fixed in earlier releases, see the Release Notes for the specific release.

Bugzilla reference numbers are in parentheses.

Network communication

- The syntax for configuring an transparent bridge interface included an alternative naming component, which led to a high number of errors when customers tried to configure the interface. (1229036)
- CPU load went up on Web Gateway until processing web traffic stopped. This was due to a particular setting of the IP version preference for DNS lookups, which resulted in a high number of unsuccessful queries. (1237287)
- A deadlock occurred on Web Gateway, which brought CPU usage down. (1238987)
- When information was retrieved from an FTP server, directory listings on Web Gateway failed to show directories that only access rights had been set for, but no user or user group information. (1239829)

Secure network protocols

- A failure in performing an OpenSSL socket operation impacted communication in a Central Management cluster of Web Gateway appliances, which caused several other issues. (1212115)
- An infinite loop occurred in processing traffic on Web Gateway when the certificate for a particular website was parsed in HTTPS communication. (1227099)
- A problem with handling the handshake in HTTPS scanning led to 100% work load for one of the core processes on Web Gateway, which blocked any further processing of traffic. (1227976)
- Web Gateway could not make use of the server name included in the SSL Client Hello message for some TLS protocol versions. As a result, the **URL.Host** property was not set as expected and the SNI to the server was not sent. (1229997)
- When Web Gateway was running in reverse proxy mode using transparent SSL connections with IPv6 configured, the default SSL certificate was not delivered as expected. (1231306)
- Retrieving an external list failed when using a list of known certificate authorities that did not provide entries in separate lines. (1233308)
- After a failure of the TLS handshake, for example, due to a timeout, Web Gateway did not close all client connections properly, which created some long-running connections. (1238295)
- After accessing Web Gateway over an HTML-based interface, the certificate for the interface, which had been created by referring to an internal certificate authority, was not trusted by JVM, which meant that the certificate had to be confirmed for each new browser session. (1237146)
- In a reverse proxy configuration, Web Gateway closed the connection to a web server due to problems with handling HTTP2 traffic. (1244440)

Web filtering

- Under particular circumstances in HTTPS communication, blocked requests for web access were displayed as allowed by a reporting tool. (1214902)
- A problem with setting names of users and user groups for authentication occurred when two processing threads tried to modify the same objects. This led to a failure of the core process with term signal 6, 9, or 11. (1220000)
- In a reverse-proxy configuration, the domain was incorrectly specified within a certificate that Web Gateway had provided because no value had been set for the **URL.Domain** property in the criteria of the relevant rule. (1225333)
- When the **URL.Host.BelongsToDomains** property had *true* as its value, the **List.LastMatches** property was not set as expected. (1229424)
- When Web Gateway submitted to Cloud Threat Detection (CTD), an incorrect submission occurred due to misreading a folder name as a file name, which caused an internal sandboxing error. (1232472)
- In a reverse proxy configuration, requests for two URLs with *plugin* or *progress* as parts of their paths were not forwarded to the web server. (1233526)
- When performing uploads of multi-part files, the Content-Disposition header was not evaluated, so no file name was set and the opener module could not handle the file, which was therefore blocked. (1238031)
- Anti-malware filtering could not be performed for an archive file because a file name property had not been set by the opener module. (1239051)
- The application/bat media type was not included in a list of media type list used for filtering purposes. (1239455)
- In a reverse proxy configuration, Web Gateway closed the connection to a web server due to problems with handling HTTP2 traffic. (1244440)
- When an update of DAT files had been performed, the dashboard incorrectly displayed older file versions. (1245036)

Vulnerabilities

- Web Gateway was affected by several Meltdown as well as Spectre V1 and V2 vulnerabilities. Of these, CVE-2017-5715 and CVE-2017-5754 had already been addressed by implementing fixes in previous versions of Web Gateway. After a fix for CVE-2017-5753 has also been implemented, Web Gateway is not affected anymore. (1223903)
- A glibc package, which is used on Web Gateway, was affected by the CVE-2018-1000001 vulnerability. Even if this had no impact on any Web Gateway services, a fix was implemented in the package, which removed the vulnerability. (1226665)
- Web Gateway was affected by the CVE-2018-0489 vulnerability, which allowed bypassing when the SAML authentication method was used. After an appropriate fix has been implemented, Web Gateway is not affected anymore. (1232037)
- Web Gateway was affected by the CVE-2016-1549, CVE-2018-7170, CVE-2018-7182, CVE-2018-7183, CVE-2018-7184, and CVE-2018-7185 vulnerabilities, which were related to time setting under NTP. After an appropriate fix has been implemented, Web Gateway is not affected anymore. (1233205)
- Web Gateway was affected by the CVE-2017-12940, CVE-2017-12941, and CVE-2017-12942 vulnerabilities, which were related to use of the unrar file extraction utility. After a fix has been implemented, Web Gateway is not affected anymore. (1237431)
- Web Gateway was affected by the CVE-2018-1124 and CVE-2018-1126 vulnerabilities, which exposed it to security risks that were caused by integer overflow and truncation issues. After suitable fixes have been implemented, Web Gateway is not affected anymore. (1242481)

- Web Gateway was affected by the CVE-2018-0732 vulnerability, which occurred when using OpenSSL, allowing a Denial of Service attack that exploited the time required to generate a key for a very large prime value sent by a malicious server during the SSL handshake. After a suitable fix has been implemented, Web Gateway is not affected anymore. (1243835)
- Web Gateway was affected by the CVE-2018-6677 vulnerability, which allowed unauthorized access to files by typing a path and file name in particular text fields. After a suitable fix has been implemented, Web Gateway is not affected anymore. (1243953)
- Web Gateway was affected by the CVE-2018-6678 vulnerability, which occurred when system preferences enabled running arbitrary appliance executables without arguments. After a suitable fix has been implemented, Web Gateway is not affected anymore. (1243971)

Miscellaneous

- The dashboard showed an alert about the maximum number of entries being reached in the list of downloaded URLs ranked according to bandwidth, with no option for the administrator to disable this alert. (1219799)
- After parsing netlink messages, data was buffered incorrectly and passed on to the kernel, creating potential problems with bandwidth throttling. (1227038)
- After accessing Web Gateway over an HTML-based interface, Japanese characters were displayed as empty boxes in the templates for messages to the user. (1227543)
- When an unsupported size was submitted for resizing the cache partition, the process failed when the partition was unmounted, but not re-mounted again. (1235391)
- When processing FTP-over-HTTP traffic, Japanese characters were not displayed correctly. (1240337)
- The core process on Web Gateway failed after a shut down for a restart had been performed, which was due to a problem with the DXL thread during the cleanup. The following restart failed again. (1241620)
- The core process on Web Gateway failed with term signal 6 due to problems with handling empty chunks encountered in image streams. (1244748)

Installation information

The procedure for installing a new product version on a Web Gateway appliance depends on the product version that you are currently running.

Create a configuration backup before the installation and be sure to save it in an external location, so it is still available in case you cannot access Web Gateway after the installation failed.

- **7.3.x or later** — Upgrade to the new version from the interface of Web Gateway or from a system console.
- **7.2.x or earlier 7.x, 6.9x, or 6.8.x** — Re-image the appliance using an image of the new version.

  Download an image of the new version from the download page of the McAfee Content & Cloud Security Portal at https://contentsecurity.mcafee.com/software_mwg7_download.

A tool is provided for upgrading to a new version offline. This tool can, however, not be used to install the current new version, which is **7.8.2**.

Upgrading from 7.3.x or later

Upgrading from a 7.3.x or later version requires that you activate a repository for the new version.

The upgrade procedure includes these high-level steps:

1 Activate the repository.

2 Perform the upgrade.

There are two methods for performing the upgrade:

- Upgrading from the interface of Web Gateway
- Upgrading from a system console

Activate the repository

Activate the repository for the new version from a system console. You can use a local system console or work remotely with SSH.

When upgrading with SSH, consider using a terminal multiplexer to ensure that the upgrade will not fail due to an unstable or broken SSH connection.

You can use either of the two multiplexers that Web Gateway has installed: *tmux* or *screen*.

Task

1 Log on to the appliance where you want to perform the upgrade.

2 Run this command:

```
mwg-switch-repo 7.8.2
```

You can now upgrade to the new version from the interface of Web Gateway or from a system console.

Upgrade from the interface

To upgrade from the interface of Web Gateway, proceed as follows.

Task

1 Select **Configuration** | **Appliances**.

2 On the appliances tree, select the appliance where you want to perform the upgrade.

The appliance toolbar appears on the upper right of the tab.

3 Click **Update Appliance Software**.

The upgrade starts, and you are logged off from the interface.

When the upgrade is complete, a message is displayed to inform you about the completion.

If you are running Web Gateway as an appliance on a virtual machine, a warning is also displayed on the host system where you created the virtual machine. This warning tells you that an operating system is being used that is not recommended.

To optimize the operation of the virtual machine, adapt its settings by configuring the recommended operating system, which is CentOS, 64 bit, version 7.

4 To perform the restart of the appliance that is required:

   a Log on to the interface again.

   b Select **Configuration** | **Appliances**, then select your appliance.

   c On the appliance toolbar, click **Reboot**.

Upgrade from a system console

Upgrade to the new version from a local system console or remotely using SSH.
When upgrading with SSH, consider using a terminal multiplexer to ensure that the update will not fail due to an unstable or broken SSH connection.

You can use either of the two multiplexers that Web Gateway has installed: *tmux* or *screen*.

Task

1 Log on to the appliance where you want to perform the upgrade.

2 Run the following commands:

```
yum upgrade yum
```

```
yum upgrade
```

When the upgrade is complete, a message is displayed to inform you about the completion.

If you are running Web Gateway as an appliance on a virtual machine, a warning is also displayed on the host system where you created the virtual machine. This warning tells you that an operating system is being used that is not recommended.

To optimize the operation of the virtual machine, adapt its settings by configuring the recommended operating system, which is CentOS, 64 bit, version 7.

3 Run the following command to restart the appliance:

```
reboot
```

When the restart is complete, a logon prompt appears. You can now log on to the interface of Web Gateway and start working with the new version.

Known issues

For a list of known issues in this product release, see KB89719.

Getting product information by email

The Support Notification Service (SNS) delivers valuable product news, alerts, and best practices to help you increase the functionality and protection capabilities of your McAfee products.
To receive SNS email notices, go to the SNS Subscription Center at https://sns.secure.intelsecurity.com/signup_login to register and select your product information options.

Where to find product documentation

Go to docs.mcafee.com to find the product documentation for this product.

Go to support.mcafee.com to find supporting content on released products, including technical articles.

0A00

McAfee
Together is power.