V-Series Appliance v7.5.2 Resolved and Known Issues

Resolved Issues: Topic 55142 / Updated: 14-September-2010

Applies To:	Websense V-Series Appliances v7.5.2 Models V5000 G2, V10000, and V10000 G2 This patch can be applied directly to both v7.5.0 and v7.5.1 appliances

Resolved issues

Websense V-Series corrections

- Websense Directory Agent collects user and group information from Directory Server and collates it for hybrid filtering. It is installed on each appliance, but typically is enabled on only one appliance. The Directory Agent service can now be enabled and disabled in the Command Line Utility in Appliance Manager. Here are situations where you may want to change the setting for this service:
  - If you have a single Active Directory tree but multiple Domain Controllers, you may choose to have multiple User Services. But in this situation, you should use only a single Directory Agent service in the network. Make sure Directory Agent is disabled on secondary appliances.
  - If you have multiple (replicated) Active Directory trees, you should use only a single Directory Agent. Make sure Directory Agent is disabled on secondary appliances.
  - If you want each Directory Agent to manage a different context in the directory tree (with no overlaps), then running multiple Directory Agents is appropriate.
  - If you have multiple Directory Services, each with its own unique data, then running multiple Directory Agents would be appropriate.
- The total disk space displayed in Appliance Manager is now consistent with the disk space on the appliance.
- The results of the **show disk** command in the command-line interface are now consistent with the disk usage statistics displayed in Appliance Manager.

- A correct warning message is now displayed if you set the Policy Source IP address to 169.254.x.x.
- The Command Line Utility in Appliance Manager now enables you to start and stop two individual Web Security services (TRITON console and Directory Agent).
- The NIC driver has been upgraded to improve appliance stability.
- When network traffic was slow and an appliance patch file size exceeded 800MB, the patch file did not upload to the appliance. This has been corrected.
- When the IP address of the P1 interface is entered in the Redirect Hostname parameter for Transparent Proxy Authentication, this address is now preserved during an appliance upgrade. For example: LOCAL proxy.config.http.transparent_auth_hostname STRING <IP-address-of-P1>

Websense Web Security corrections

- The Websense Network Agent component could experience a stalled thread that could cause CPU overload. When this occurred, the software could fail to block a significant number of protocols that should have been blocked. The issue causing the stalled thread has been resolved, and blocking occurs as expected
- Filtering Service sometimes did not correctly determine which policy took precedence if both groups and domains were assigned to a Delegated Administrator (DA) role. Filtering Service could obtain the role ID for a domain only if the case of the domain name matched the case of the domain name as it was assigned to the DA role. Case no longer matters for domain name assignments to DA roles. Policy precedence is now correctly determined by this sequence:
    a. Use DA role based on assignment to user name.
    b. Else, use DA role based on assignment to IP address.
    c. Else, use DA role based on assignment to network IP address range.
    d. Else, use DA role with the highest priority for both group objects and OU objects.
- Users in the Domain Users group are now filtered by the policy assigned to that group if the default Domain Users group path is changed.
- Filtering Service now receives the ID for a specific role when a delegated administrator’s Managed Clients list contains only group clients.
- If an administrator modifies a user’s group attribute in a global catalog server, or moves group clients between roles (thus changing which delegated administrator is responsible for users in the group), the use’s role assignment is changed appropriately, and the role cache used by Filtering Service is automatically refreshed.

Websense Content Gateway corrections

- You are now able to save configuration changes made via Content Gateway Manager after viewing any log files in the management console. You no longer see these error messages at Restart: “Unable to read or write config file” or “Permission denied.”
- You now receive the expected email message alert whenever a proxy reset occurs for an out-of-memory condition, malformed response, and other interruptions, if you have enabled reset alarms in the file **records.config**.
- The SSL Incident List now shows the correct URL in the default tunnel rule for gotomeeting.com.
- You can now use the Content Gateway Manager to remove all tunneled ports. Browse to **Configure > Protocols > HTTP > General**. Remove the Tunnel Ports that are listed and click **Apply**. This console option was not working correctly in the previous version.
- FTP sites accessed using Internet Explorer (IE) version 6 now render completely and no longer display the underlying HTML code.
- If you enable and configure NTLM with credential caching, and then later disable NTLM credential caching, credentials are no longer pulled from the cache.
- Websense Content Gateway was incorrectly treating proxy authentication headers as case-sensitive. This caused some clients, such as Windows Media Player, to occasionally fail to authenticate. Content Gateway is now case-insensitive when examining authentication headers, in compliance with the HTTP RFC.
- It is now possible to route traffic from the Google AdWords client successfully through Websense Content Gateway with SSL turned on.
- Users in terminal server groups are now identified correctly, and the correct filtering policy is applied to them, when the users access HTTPS sites with SSL Manager enabled.
- File transfers with the iDisk application at idisk.mac.com now upload successfully when proxied by Content Gateway.
- Large files such as ISO images can now be downloaded successfully from slow servers. A slow server is defined here as one that serves less than 11 MB in the first 30 seconds of the download.
- The correct URL is now sent from Websense Content Gateway to the Policy Engine when an HTTPS POST transaction is performed and ICAP Server is in use.

Known Content Gateway issues still existing in v7.5.2

Manual authentication overrides SSL category bypass

Sites using transparent proxy mode with WCCP may see SSL Web sites decrypted, even when those sites belong to categories for which SSL Bypass has been configured.

When Manual Authentication is required for SSL sites, Websense software decrypts SSL sites (instead of bypassing them), because authentication is overriding the SSL Bypass.

A workaround is to remove the requirement for Manual Authentication.

Transparent Authentication with WCCP can fail in cookie mode

If your site has two or more Content Gateway instances pointing to the same WCCP router, do not use Cookie mode for credential caching. Instead, use IP mode.

If Cookie mode is in use, for most of the time the authentication works correctly. However, a user may receive 'Page cannot be displayed' instead of being forwarded to a block page.

To check this setting, navigate to **Configuration > Security > Access Control > Transparent Proxy Authentication**. Ensure that **Authentication Mode** is set to **IP mode** (the default). Click **Apply** if you made a change, and then restart the proxy to put the change into effect.

In IP mode, the client IP address is associated with a user name when the session is authenticated. Requests made from that IP address are not authenticated again until the Session TTL expires (default = 15 minutes). Requests made from that IP address within the time-to-live are considered to be made by the user associated with that IP address.

WCCP proxy cluster with IP spoofing requires source-based distribution

When a site deploys multiple Content Gateway servers in a WCCP cluster, with IP spoofing enabled, the default configuration for WCCP does not distribute the cache appropriately.

The workaround is to modify the default hash assignment to select source-based distribution. Your Websense support professional can assist you with this step.

Advertise packets not matching value in records.config

For routers and switches that support both GRE and L2, after Websense Content Gateway has registered for WCCP with the router (or switch), the device caches the negotiated mode, until Websense Content Gateway is de-registered.

De-registration occurs only if 3 heartbeat messages fail, and there is no response from Websense Content Gateway.

If your site changes the negotiation mode on Websense Content Gateway after it has registered once, and then restarts Websense Content Gateway, note that Content Gateway does not get de-registered. This is because the restart completes before 3 heartbeat failures. Thus, the router (or switch) mode still has the last value negotiated prior to the restart.

Websense Content Gateway also advertises this same value, and thus the file records.config does not match the advertised capability.

The workaround in this case is to disable WCCP in Websense Gateway Manager and wait until it de-registers, and then enable WCCP again. At that point, the router will advertise both GRE and L2, and Websense Content Gateway will choose the one configured in records.config.

Preferred method for changing the mode:

1. Disable WCCP on the router (all service groups to proxies).
2. Wait for all service groups to expire on proxies (1 minute).
3. Make desired changes on all proxies.
4. Enable WCCP on the router.

Alternate method for changing mode: (no access to switch or router):

1. Disable WCCP on the proxies.
2. Wait for all service groups to expire on the router (1 minute after last proxy is disabled).
3. Make changes on all proxies.
4. Enable WCCP on all proxies.

Keep in mind:

The router can choose the mode it wants, regardless of what the proxy asks or advertises.

Changing forwarding/redirect methods is best done in a maintenance window. A change of this sort requires all proxies to be de-registered (otherwise the router attempts to preserve the existing methods, regardless of the proxies' capabilities).

Websense Content Gateway auto-negotiates successfully even when it has been misconfigured in Content Gateway Manager. This means that it will never advertise a mode that the router doesn't support.

Cache distribution incorrect with WCCP cluster and IP spoofing

When a site deploys multiple Content Gateway servers in a WCCP cluster with IP spoofing enabled, the default configuration for WCCP does not correctly distribute the cache to the cluster.

The workaround is to modify the default hash assignment to select source-based distribution.

(link to related KB article here)

Known V-Series issues still existing in v7.5.2

Manager Web server automatically starts after all Web Security services stopped

If you log on to Appliance Manager and navigate to the **Configuration > General** page to stop Web Security services manually, the TRITON console Web server will automatically start after about 30 minutes. To work around this issue, please stop Web Security services again.

Directory Agent service cannot be started on Modules page if disabled from Command Line Utility.

If you disable Directory Agent service in the Command Line Utility in Appliance Manager, a red icon displays (but no gray icon) on the Modules page. The service cannot be started by the start/restart button on the Modules page. To re-enable Directory Agent, please use the Command Line Utility.

Snapshots archived during upgrade from v7.5.0

Snapshots generated by previous versions are archived during an upgrade or patch.

This is because snapshots are designed to be used for backup and restore to the same version only.

To upgrade based on a particular snapshot, restore the snapshot first, and then upgrade or apply the patch. After the upgrade, take a new snapshot, to preserve the initial state of the upgraded system.

During an upgrade or patch, snapshots from the previous version are saved into a tarball located under home/Websense/OldVersions/, packed in the Saved_Snapshots subfolder.

Do not enable/disable Directory Agent during Web Security module restart

While the Web Security module is being restarted, do not enable or disable Directory Agent. Wait for the restart process to be completed, and then proceed with the Directory Agent status change. An internal error occurs if you attempt to enable or disable during a restart.

Please do not press the **Stop** button during the enable or disable process for Directory Agent. The process would fail in this event.

Directory Agent status not saved in full backup

When you perform a full backup for the appliance, the status of Directory Agent (enabled or disabled) is not saved. After you restore from a full backup, please check the status of Directory Agent and set it as desired with the Command Line Utility.

Restart issue for Content Gateway after full backup is restored

On rare occasions, on systems that use SSL Manager, after you restore from a full backup, Content Gateway will not start. This can happen when the backup copy of the SSL Manager settings file has become corrupt. In that event, when the restore is complete, a corrupt copy of the file is active.

Please contact Technical Support for assistance with this issue.