Aerohive Networks Inc.

Web Security Proxy Test Plan for “Congo” Project

Revision History

|  |  |  |  |
| --- | --- | --- | --- |
| Version | Date | Author | Description |
| 0.1 | 10/03/2011 | Kevin Lin | Initial version |
| 1.0 | 10/17/2011 | Kevin Lin | After review from Adam Cain (acain), Patrick Yip (pyip) and Linda Knudstrup (lknudstrup) |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

Table of Contents

[Table of Contents 2](#_Toc307840475)

[1. Introduction 4](#_Toc307840476)

[2. Test Objectives 4](#_Toc307840477)

[2.1. Expectations with using default usernames 8](#_Toc307840478)

[3. Test Acceptance Criterion from Development 9](#_Toc307840479)

[4. Product Pass Criterion 9](#_Toc307840480)

[5. Test Bed/Topo Design 9](#_Toc307840481)

[6. Test Case 9](#_Toc307840482)

[6.1. Key Scenarios 20](#_Toc307840483)

[6.2. Function Test Case 20](#_Toc307840484)

[6.3. Stress Test Case 20](#_Toc307840485)

[6.4. Duration Test Case 20](#_Toc307840486)

[6.5. Performance Test Case 20](#_Toc307840487)

[6.6. Capacity Test Case 20](#_Toc307840488)

[6.7. Compatibility Test Case 20](#_Toc307840489)

[6.8. CLI Management (Automation Status: No) 20](#_Toc307840490)

[6.9. GUI Management-HiveManager 20](#_Toc307840491)

[6.10. GUI Management-HiveUI 20](#_Toc307840492)

[7. Appendix 20](#_Toc307840493)

[7.1. Additional meeting notes 20](#_Toc307840494)

Glossary and Abbreviations

AP – Access Point

BR – Branch Router

WS – WebSense

# Introduction

This test plan addresses the test coverage for the Web Security Proxy feature during HiveOS Congo release. The goal of the testing is to cover provisioning and ability to forward HTTP and HTTPS traffic to Barracuda or WebSense servers and also receive web contents back from these web proxy services.

In the past, HiveOS devices were only deployed in private LAN environments as Layer-2 network devices functioning as bridges for wireless and wired LANs. For the upcoming branch router product lines, HiveOS devices will be deployed in branch offices as gateways to the internet functioning as Layer-3 network devices, forwarding IP traffic between the private network (LAN) and the internet (WAN). The HiveOS network stack needs to be enhanced to support the IP forwarding requirement and configurations of network interfaces to function properly in a network topology connected to both a WAN and LAN environment.

Congo is the initial release which constitutes a telecommuter-optimized low-end AP, Cloud VPN Gateway, 3G Support, Routing, and a couple new HiveOS and HiveManager features. This document addresses the Web Security Proxy feature to break off specific traffic and send it to an alternate destination rather than the tunnel or Internet. This feature is only applicable to HTTP/HTTPS traffic.

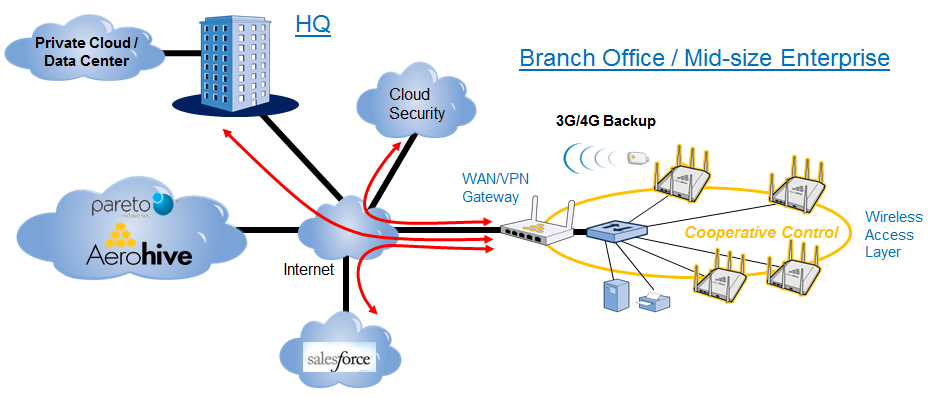


Figure – Overview of HiveOS L3 support

This feature is a required feature in Routing MRD, section 4.1.3.

# Test Objectives

For Congo project, the testing for this feature will be done on BR-100 hardware, with configuration solely done on HiveManager. Testing will be focused on end-to-end functionality and the usability of the feature, and also covers the different use cases defined in MRD and FS.

Two deployment scenarios will be covered:

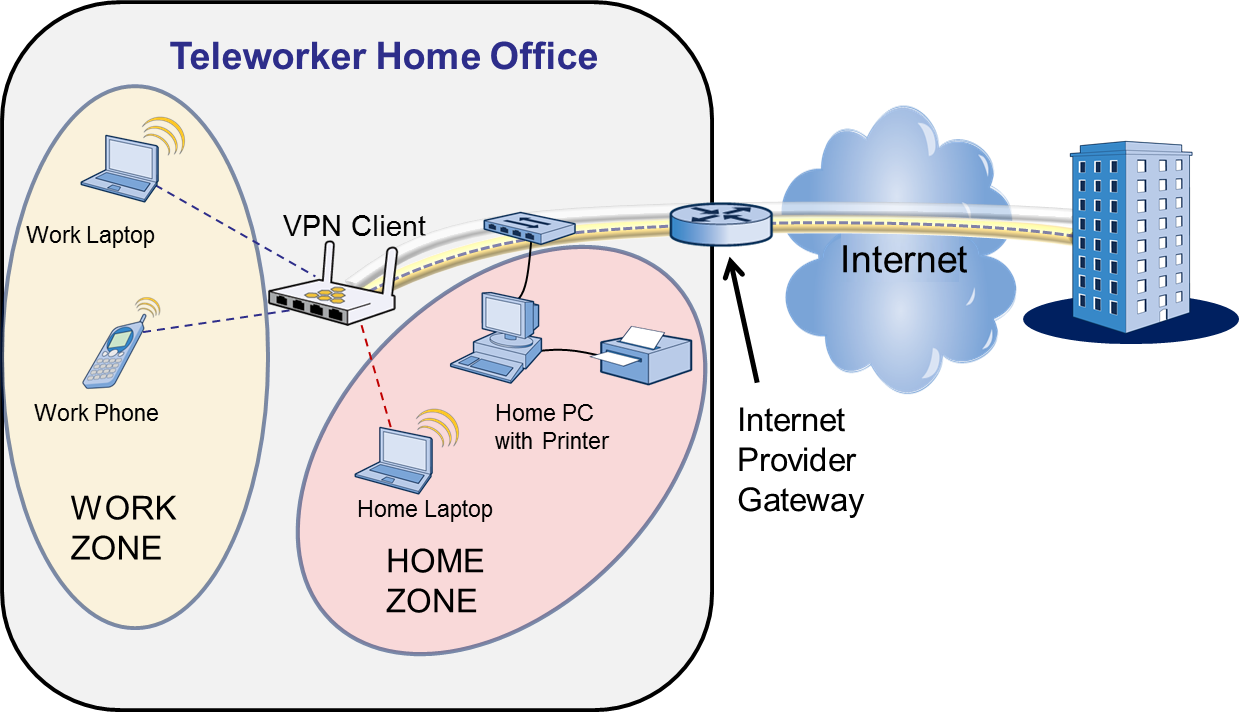


Figure – BR-100 in home office, behind another NAT device

In the first case, the BR-100 will be placed behind a NAT device (such as a common home Netgear or Linksys router).

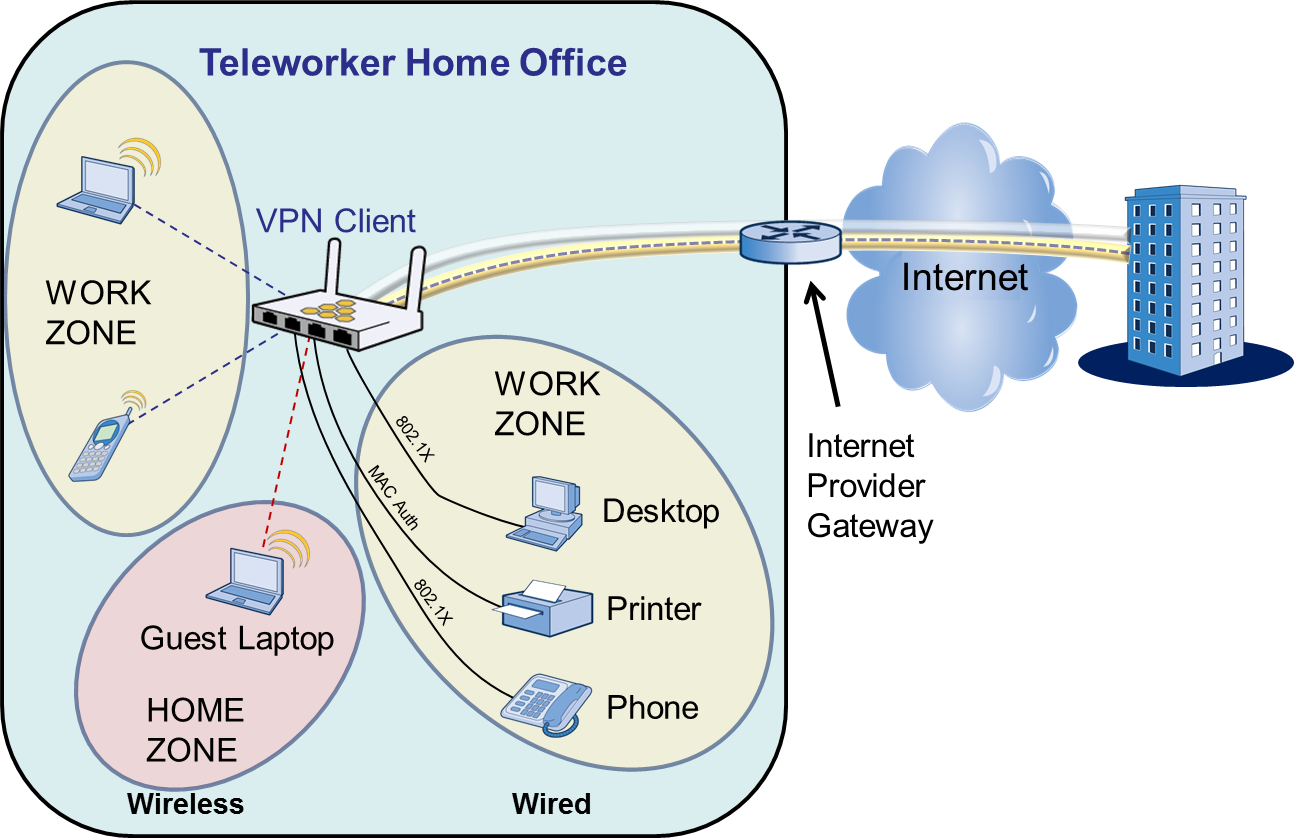


Figure – BR-100 in home office, connected directly to the MODEM/ISP as the only NAT device

In the second case, the BR-100 will be used as the sole NAT device in the home office with all clients connected directly or indirectly (via a network switch) to the internet.

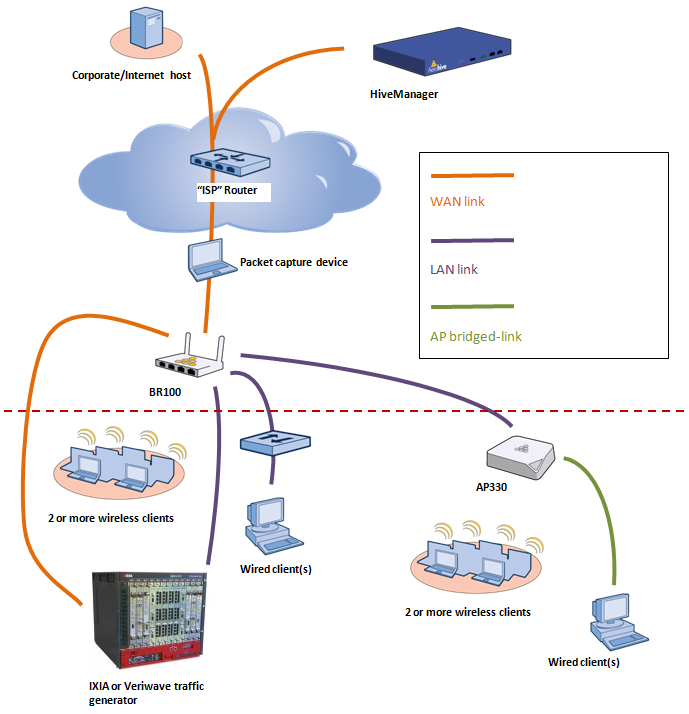


Figure – Diagram from WAN testing topology. For this feature, we focus on having 1 or 2 AP330 in the branch office, and have clients attached to the AP330.

WebSense will be responsible for testing the Aerohive extensions on their server, and also cover scalability testing.

End-to-end automation is not possible because a Barracuda and WebSense account is required for the functionality to work. We currently do not have such an agreement in place with our partners for such automation effort.

There is no performance or scaling requirements for this feature. However, multiple clients behind the same BR-100; wired and wireless, will be tested simultaneously to ensure the feature will work for at least two devices.

Unit test plan is provided in the document. From timing and configuration point of view, these test cases will not be repeated, but will instead the feature will be re-verified after configuration is pushed down from the HiveManager.

The following browsers will be tested:

* IE9 on Windows 7
* Firefox 6 on Windows 7
* Safari on MacOSX
* IE8 on Windows XP

## Expectations with using default usernames

This is what we expect with default username:

|  |  |  |  |
| --- | --- | --- | --- |
| **Scenario** | **Barracuda** | **WebSense** | **Comment** |
| No default username/domain entered in HM | Default username must be entered | No default username, default domain is optional. |  |
| No default username, and no username for client (eg. open mode/PSK) | Default username must be entered, and will be enforced | Default user policy will be used on WebSense account |  |
| Any authentication method that returns an username already in web security database | User policy will be enforced.  Barracuda does not look at domain information | User policy will be enforced.  WebSense will take username, or domain.com\username |  |
| Any authentication method that returns an username that is not already defined in the web security database | -- apply all configured rules that are set to apply to "Everyone"  -- i.e., treat user as anonymous and don't apply any policies that are user (group) specific | Default policy will be used.  WebSense auto provisioning will be used  (on by default, depends on customer config on WS) |  |
| Invalid account ID or key used | User gets 403 forbidden message | HTTP: 200 message, auth required page  HTTPS: User gets 403 forbidden message |  |

# Test Acceptance Criterion from Development

* Approved – MRD

<add Jive link for the MRD>

* Approved – Functional Specifications

<add KT link to the FS>



* Approved – Unit Test Plans

<add KT link to the unit test plan>



# Product Pass Criterion

Feature testing is considered pass when test result meets or exceeds the requirement defined in the expected result field. The expected result field is defined by the requirements stated in the functional specification and/or MRD; whichever is stricter; plus additional quality and usability expectations set by the test engineer.

This feature will also adhere to the general pass criterion described for the overall Congo release.

# Test Bed/Topo Design

Testbed topology will be the same as described in figure 2 and figure 3. Barracuda and WebSense servers reside in the cloud, and BR-100 will establish tunnel back to the corporate office. Overall network configuration is not important for this feature. Detailed network settings will be described within the test case if needed.

# Test Case

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | CloudProxy\_Feature\_Configuration\_1 | | |
| Priority | Accept | Automation Flag | NA |
| Topology to use | n/a | | |
| Description | Configure Web Proxy service in HiveManager | | |
| Pre-condition | Default configuration | | |
| Test procedure | Log into HiveManager, navigate to: Home 🡪 Administration 🡪 HiveManager Services  1. Check the box next to “Barracuda Server Settings”  2. Enter the required field, represented by a \*  3. Click on “Update” after all the required fields have been entered correctly  4. Repeat the process for WebSense configuration | | |
| Expect result | HiveManager should save the results. Check by navigating to a different page and come back to it.  Configuration should also be saved across HiveManager reboots and upgrades. | | |

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | CloudProxy\_Feature\_Configuration\_2 | | |
| Priority | High | Automation Flag | NA |
| Topology to use | n/a | | |
| Description | Change configuration for Web Proxy service in HiveManager | | |
| Pre-condition | Having an existing web security configuration | | |
| Test procedure | Log into HiveManager, navigate to: Home 🡪 Administration 🡪 HiveManager Services  1. Check the box next to “Barracuda Server Settings”  2. Change values within the required field, represented by a \*  3. Click on “Update” after all the required fields have been entered correctly  4. Repeat the process for WebSense configuration | | |
| Expect result | HiveManager should save the results. Check by navigating to a different page and come back to it.  Also check that the configuration is saved across HiveManager reboots and upgrades. | | |

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | CloudProxy\_Feature\_Configuration\_3 | | |
| Priority | Middle | Automation Flag | NA |
| Topology to use | n/a | | |
| Description | Configuration error check for Web Proxy service in HiveManager | | |
| Pre-condition | Default configuration | | |
| Test procedure | Log into HiveManager, navigate to: Home 🡪 Administration 🡪 HiveManager Services  1. Check the box next to “Barracuda Server Settings”  2. Change values within the required field, represented by a \*  3. Enter too little/too many characters, enter special characters, and enter strings where numbers are expected.  4. Click on “Update” after all the required fields have been entered  5. Repeat the process for WebSense configuration | | |
| Expect result | HiveManager should throw errors, and not save the results. Check by navigating to a different page and come back to it. | | |

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | CloudProxy\_Feature\_Configuration\_4 | | |
| Priority | Middle | Automation Flag | NA |
| Topology to use | n/a | | |
| Description | Test button for Web Proxy service in HiveManager | | |
| Pre-condition | Default configuration | | |
| Test procedure | Log into HiveManager, navigate to: Home 🡪 Administration 🡪 HiveManager Services  1. Check the box next to “Barracuda Server Settings”  2. Enter valid values within the required field, represented by a \*  3. Click on “Test” after all the required fields have been entered  4. Repeat the process with invalid values (invalid accounts etc)  5. Repeat the process for WebSense configuration | | |
| Expect result | HiveManager should give some sort of success message when valid account is entered.  HiveManager should give some sort of failure message when non-valid account information is entered.  HiveManager should do some error checking for the fields to make sure the information entered is not out-of-bound or if user entered invalid characters. | | |

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | CloudProxy\_Feature\_Configuration\_5 | | |
| Priority | High | Automation Flag | NA |
| Topology to use | n/a | | |
| Description | Push CloudProxy config from HiveManager down to a BR | | |
| Pre-condition | BR already connected to HM, CloudProxy already configured in HM | | |
| Test procedure | Log into HiveManager  1. Modify the config for the BR.  2. In network config, select Barracuda as web proxy service  3. Push down the config to BR using delta config  4. Repeat step 3 with complete upload  5. Repeat the process for WebSense configuration | | |
| Expect result | HiveManager should give error message if Barracuda/WebSense was not already configured in the HiveManager Service page.  Only either Barracuda OR WebSense configuration should be pushed down to a BR  The pushed down configuration should be correct.  Barracuda:  web-security-proxy barracuda-v1 account-id <id>  web-security-proxy barracuda-v1 http-proxy-host <host>  web-security-proxy barracuda-v1 https-proxy-host <host>  web-security-proxy barracuda-v1 default-username <username>  web-security-proxy barracuda-v1 subnet <subnet>  web-security-proxy barracuda-v1 enable  web-security-proxy barracuda-v1 whitelist <list of whitelist here>  WebSense:  web-security-proxy websense-v1 account-id <id>  web-security-proxy websense-v1 http-proxy-host <host>  web-security-proxy websense-v1 http-proxy-port 8081  web-security-proxy websense-v1 https-proxy-host <host>  web-security-proxy websense-v1 https-proxy-port 8081  web-security-proxy websense-v1 account-key \*\*\*  web-security-proxy websense-v1 enable  web-security-proxy websense-v1 whitelist <list of whitelist here> | | |

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | CloudProxy\_Feature\_Configuration\_6 | | |
| Priority | High | Automation Flag | NA |
| Topology to use | n/a | | |
| Description | Whitelist should be correct and configurable in the HiveManager | | |
| Pre-condition | Basic web security configuration | | |
| Test procedure | Log into HiveManager  1. In Hivemanager Services page, edit Barracuda or WebSense  2. Click on the edit button for the respective whitelists  3. Modify the white lists and apply the change | | |
| Expect result | HiveManager should have a pre-defined list of websites defined in the whitelist. It should be as follows:  Barracuda:  .purewire.com  download.microsoft.com  ntservicepack.microsoft.com  cdm.microsoft.com  wustat.windows.com  windowsupdate.microsoft.com  .windowsupdate.microsoft.com  update.microsoft.com  .update.microsoft.com  WebSense:  .mailcontrol.com  .blackspider.com  download.microsoft.com  ntservicepack.microsoft.com  cdm.microsoft.com  wustat.windows.com  windowsupdate.microsoft.com  .windowsupdate.microsoft.com  update.microsoft.com  .update.microsoft.com  After applying the changes, go back to edit menu and make sure the changes have been saved. | | |

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | CloudProxy\_Feature\_HTTP\_1 | | |
| Priority | High | Automation Flag | NA |
| Topology to use | Figure 2 or figure 3 | | |
| Description | Request simple HTTP web pages with URLs allowed by policy and OK content | | |
| Pre-condition | Basic web security configured, BR up with VPN tunnel | | |
| Test procedure | 1. From a client, visit allowed websites using HTTP ([www.google.com](http://www.google.com), [www.ietf.org](http://www.ietf.org) 🡨 change this to something simpler)  2. Repeat with different browsers  3. Repeat for both Barracuda and WebSense  4. Turn on debugs for tinyproxy to check if everything is okay 🡨 unit test tp | | |
| Expect result | User should see expected web page content | | |

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | CloudProxy\_Feature\_HTTP\_2 | | |
| Priority | High | Automation Flag | NA |
| Topology to use | Figure 2 or figure 3 | | |
| Description | Request content-rich HTTP web pages with URLs allowed by policy and OK content | | |
| Pre-condition | Basic web security configured, BR up with VPN tunnel | | |
| Test procedure | 1. From a client, visit allowed websites using HTTP ([www.yahoo.com](http://www.yahoo.com), www.cnn.com)  2. Repeat with different browsers  3. Repeat for both Barracuda and WebSense | | |
| Expect result | User should see expected web page content. No browser errors or warnings. | | |

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | CloudProxy\_Feature\_HTTP\_3 | | |
| Priority | High | Automation Flag | NA |
| Topology to use | Figure 2 or figure 3 | | |
| Description | Request simple HTTP web pages with URLs disallowed by policy, BR up with VPN tunnel | | |
| Pre-condition | Basic web security configured, disallowed contents configured on web security website | | |
| Test procedure | 1. From a client, visit allowed websites using HTTP ([www.facebook.com](http://www.facebook.com), www.porn.com)  2. Repeat with different browsers  3. Repeat for both Barracuda and WebSense | | |
| Expect result | User should see access denied page | | |

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | CloudProxy\_Feature\_HTTP\_4 | | |
| Priority | High | Automation Flag | NA |
| Topology to use | Figure 2 or figure 3 | | |
| Description | Request simple HTTP web pages with URLs disallowed by content | | |
| Pre-condition | Basic web security configured, disallowed contents configured on web security website, BR up with VPN tunnel | | |
| Test procedure | 1. From a client    1. visit: “Links under “Real-time Alalysis Test Pages” in  <http://testdatabase.websense.com>“. This page has good examples of what ought to work, and what should not work.    2. Barracuda, TBD – we can leverage the same URL from WebSense.   2. Repeat with different browsers  3. Repeat for both Barracuda and WebSense | | |
| Expect result | User should error page | | |

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | CloudProxy\_Feature\_HTTPS\_1 | | |
| Priority | High | Automation Flag | NA |
| Topology to use | Figure 2 or figure 3 | | |
| Description | Request simple HTTPS web pages with URLs allowed by policy and OK content, BR up with VPN tunnel | | |
| Pre-condition | Basic web security configured | | |
| Test procedure | 1. From a client, visit allowed websites using HTTPS ([www.google.com](http://www.google.com), www.ietf.org)  2. Repeat with different browsers  3. Repeat for both Barracuda and WebSense | | |
| Expect result | User should see expected web page content | | |

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | CloudProxy\_Feature\_HTTPS\_2 | | |
| Priority | High | Automation Flag | NA |
| Topology to use | Figure 2 or figure 3 | | |
| Description | Request content-rich HTTPS web pages with URLs allowed by policy and OK content, BR up with VPN tunnel | | |
| Pre-condition | Basic web security configured | | |
| Test procedure | 1. From a client, visit allowed websites using HTTPS (outlook.aerohive.com)  2. Repeat with different browsers  3. Repeat for both Barracuda and WebSense | | |
| Expect result | User should see expected web page content. No browser errors or warnings. | | |

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | CloudProxy\_Feature\_HTTPS\_3 | | |
| Priority | High | Automation Flag | NA |
| Topology to use | Figure 2 or figure 3 | | |
| Description | Request simple HTTPS web pages with URLs disallowed by policy, BR up with VPN tunnel | | |
| Pre-condition | Basic web security configured, disallowed contents configured on web security website | | |
| Test procedure | 1. From a client, visit allowed websites using HTTPS ([www.facebook.com](http://www.facebook.com), www.porn.com)  2. Repeat with different browsers  3. Repeat for both Barracuda and WebSense | | |
| Expect result | User should see HTTPS 403 error | | |

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | CloudProxy\_Feature\_HTTPS\_4 | | |
| Priority | High | Automation Flag | NA |
| Topology to use | Figure 2 or figure 3 | | |
| Description | Request simple HTTPS web pages with URLs mixed with allowed and disallowed by content, BR up with VPN tunnel | | |
| Pre-condition | Basic web security configured, disallowed contents configured on web security website | | |
| Test procedure | 1. From a client, visit www.gmail.com   2. Repeat with different browsers  3. Repeat for both Barracuda and WebSense | | |
| Expect result | User should see some parts of contents allowed, and 403 error for pages which is configured to be blocked | | |

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | CloudProxy\_Feature\_Username\_1 | | |
| Priority | Accept | Automation Flag | NA |
| Topology to use | Figure 2 or figure 3 | | |
| Description | Test various combination of usernames, described in table 2.1 to ensure expected results are met | | |
| Pre-condition | After HTTP and HTTPS testing | | |
| Test procedure | 1. Configure web security feature on HM based on the conditions defined in table 2.1 2. Associate users with various usernames based in the table, and try out HTTP and HTTPS traffic accordingly. | | |
| Expect result | Expected results are defined in table 2.1. | | |

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | CloudProxy\_Feature\_Account\_1 | | |
| Priority | Accept | Automation Flag | NA |
| Topology to use | Figure 2 or figure 3 | | |
| Description | Use invalid account ID in configuration | | |
| Pre-condition | Basic web security configured | | |
| Test procedure | 1. Configure web security with invalid account ID 🡨change service host, or use iptables   (what if heavy delay from WS to BR, what should we do? Also, think about how often we need to do “keepalive” to the web security servers)   1. Configure deny for “If connectivity to the URL filtering server is lost” 2. Use client to visit any web page 3. Configure permit for “If connectivity to the URL filtering server is lost” | | |
| Expect result | When default = deny, user should not be able to see web page  When default = permit, user should be able to see web page just fine | | |

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | CloudProxy\_Feature\_MultipleUser\_1 | | |
| Priority | High | Automation Flag | NA |
| Topology to use | Figure 2 or figure 3 | | |
| Description | Validate feature with users on both wired and wireless interfaces, all with different user-profiles | | |
| Pre-condition | Basic web security configured, BR up with VPN tunnel | | |
| Test procedure | 1. Use at least 4 clients    1. 2 on wired interface. Different ports and different usernames (CWP)    2. 2 on wireless interface. 2 different SSIDs and different usernames (802.1x) 2. From all users, browse using HTTP to: [www.cnn.com](http://www.cnn.com) and [www.facebook.com](http://www.facebook.com) 3. From all users, browse using HTTPS to: outlook.aerohive.com and www.porn.com   4. Repeat for both Barracuda and WebSense | | |
| Expect result | For all users, only [www.cnn.com](http://www.cnn.com) and outlook.aerohive.com should be accessible. | | |

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | CloudProxy\_Feature\_MultipleUser\_2 | | |
| Priority | High | Automation Flag | NA |
| Topology to use | Figure 4 | | |
| Description | Validate feature with users associated to AP330 within the LAN of the BR | | |
| Pre-condition | Basic web security configured, BR up with VPN tunnel | | |
| Test procedure | 1. Place AP330 on the LAN side, with hive==hive of BR 2. Use same SSID and security+user profile on both AP330 and BR to ensure roaming cache will be passed between the devices 3. Associate client to AP330, using 802.1x 4. Pass HTTP and HTTPS traffic | | |
| Expect result | Traffic should be passed to the web security servers using the correct username used during the 802.1x authentication. AP330 should pass the authenticated username to BR as part of roaming cache.  User HTTP and HTTPS traffic should be screened accordingly by the web security servers. | | |

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | CloudProxy\_Feature\_TunnelBehavior\_1 | | |
| Priority | High | Automation Flag | NA |
| Topology to use | Figure 2 or figure 3 | | |
| Description | Validate feature when tunnel is down or during 3G failover | | |
| Pre-condition | Basic web security configured, BR up with VPN tunnel | | |
| Test procedure | 1. Enable tinyproxy log (\_debug tinyproxy websense-v1/ barracuda-v1 info) 2. Setup web security to work properly with a client for both HTTP and HTTPS 3. Bring down VPN tunnel by making the CVG unreachable 4. Place client on different user-profiles – “tunnel all” or “split tunnel” 5. Repeat test case when client fails over to 3G and back | | |
| Expect result | Tunnel all clients should be denied access to all pages when tunnel is down  Split tunneled client should still be able to browse external websites just fine  Tinyproxy log would not have entries for tunneled traffic, only non-tunneled traffic would be shown  3G failover and failback scenarios is expected to work without user intervention | | |

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | CloudProxy\_Feature\_TunnelBehavior\_2 | | |
| Priority | High | Automation Flag | NA |
| Topology to use | Figure 2 or figure 3 | | |
| Description | Validate feature when tunnel is up | | |
| Pre-condition | Basic web security configured, BR up with VPN tunnel | | |
| Test procedure | 1. Enable tinyproxy log (\_debug tinyproxy websense-v1/ barracuda-v1 info) 2. Setup web security to work properly with a client for both HTTP and HTTPS 3. Bring down VPN tunnel by making the CVG unreachable 4. Place client on different user-profiles – “tunnel all” or “split tunnel” 5. Repeat test case when client fails over to 3G and back | | |
| Expect result | Tunnel all clients should be have all web traffic going back to corporate first  Split tunneled client web traffic should be split normally  Tinyproxy log would not have entries for tunneled traffic, only non-tunneled traffic would be shown  Same expectation under 3G backhaul mode | | |

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | CloudProxy\_Feature\_Whitelist\_1 | | |
| Priority | High | Automation Flag | NA |
| Topology to use | Figure 2 or figure 3 | | |
| Description | Validate whitelist works for both HTTP and HTTPS traffic | | |
| Pre-condition | Basic web security configured, BR up with VPN tunnel | | |
| Test procedure | 1. Enable tinyproxy log (\_debug tinyproxy websense-v1/ barracuda-v1 info) 2. Setup web security to work properly with a client for both HTTP and HTTPS 3. Add whitelist entry (eg. .facebook.com) 4. Browse [www.facebook.com](http://www.facebook.com) from client 5. Repeat test case for HTTPS website | | |
| Expect result | [www.facebook.com](http://www.facebook.com) should be blocked by default (social networking)  after adding .facebook.com to whitelist, users should now be able to browse to [www.facebook.com](http://www.facebook.com)  HTTPS website should also work  log should have an entry showing users are able to browse to [www.facebook.com](http://www.facebook.com) | | |

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | CloudProxy\_Feature\_Whitelist\_2 | | |
| Priority | High | Automation Flag | NA |
| Topology to use | Figure 2 or figure 3 | | |
| Description | Validate whitelist works for big files/download or heavy traffic | | |
| Pre-condition | Basic web security configured, BR up with VPN tunnel | | |
| Test procedure | 1. Enable tinyproxy log (\_debug tinyproxy websense-v1/ barracuda-v1 info) 2. Setup web security to work properly with a client for both HTTP and HTTPS 3. Find an outdated client (not current with all Microsoft updates) 4. Use windows update and download large number of files (windows service pack and security updates) | | |
| Expect result | Ensure client is able to download the files from windows update, and able to apply the updates just fine. | | |

## Key Scenarios

## Function Test Case

## Stress Test Case

## Duration Test Case

## Performance Test Case

Performance requirement is not defined for this feature

## Capacity Test Case

Capacity requirement is not defined for this feature

## Compatibility Test Case

Web browser capability defined in section 2

## CLI Management (Automation Status: No)

Not testing CLI for this feature

## GUI Management-HiveManager

<List HM test case or test log>

## GUI Management-HiveUI

<List HiveUI test case or test log>

# Appendix

## Additional meeting notes

~~Only web security on non-tunneled traffic~~

~~No logging on tunneled traffic~~

~~White list, tiny proxy will have a log~~

~~Add test case, if VPN tunnel is down, permit all or deny all defined at config~~

~~3G failover, and fail back, expected to work the same~~

~~User profile, when we use tunnel all, does it still go through web proxy~~

~~Whitelist test, make sure windows update also works. (go to webpage, download big update file)~~