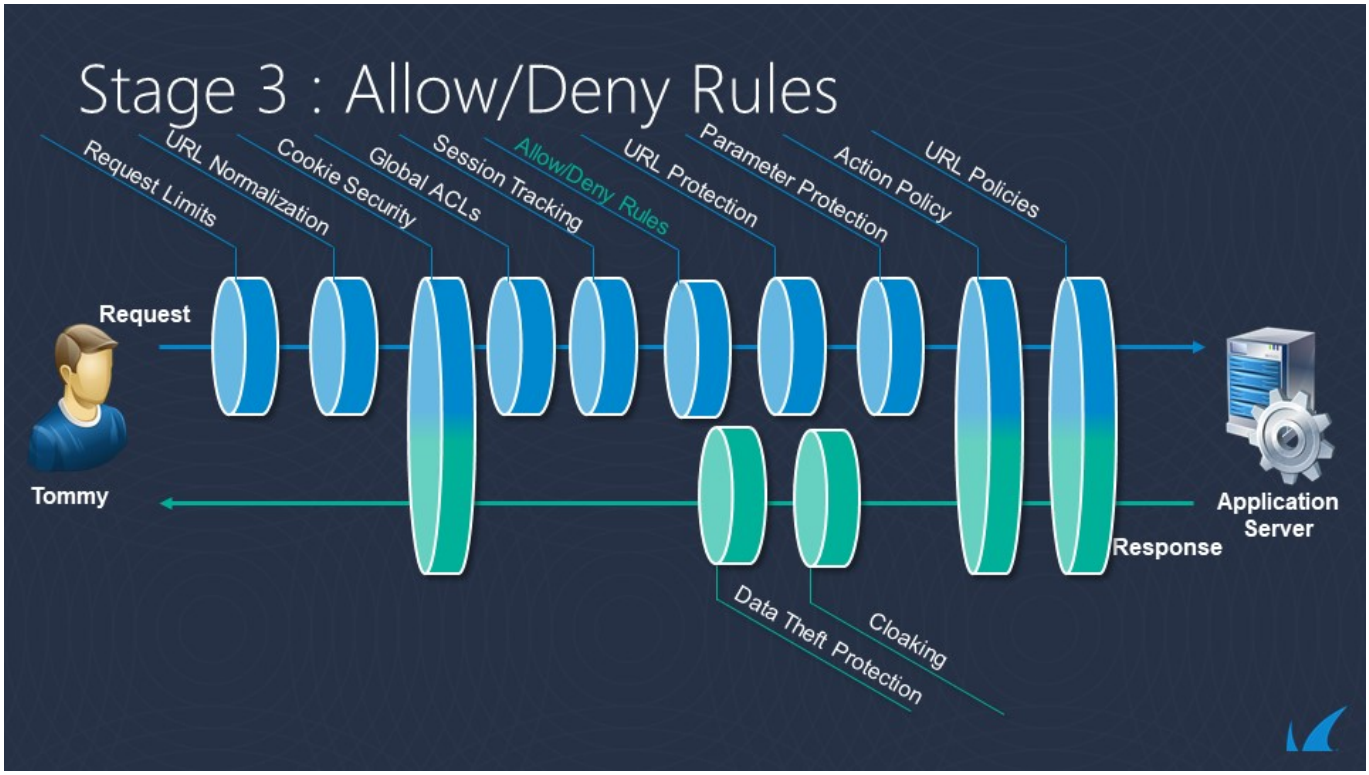
Allow/Deny Rules

https://campus.barracuda.com/doc/46204110/

Allow/Deny rules are used to define strict access control rules for the services. Requests to the service are allowed or denied based on the URL ACL and Header ACL configuration. For more information, see Allow/Deny Rules for Headers and URLs.

This image shows the enforcement points for Allow/Deny rules in the Request/Response flow:



For more information on the complete evaluation flow for requests and responses, see Evaluation Policy and Flow.

Allow/Deny Rules for URLs

To Add a URL ACL Rule

URL: /v1/virtual_services/{virtual_service_id}/url_adrs
Method: POST
Description: Creates an access control (ACL) rule for the specified URL.

Parameter Name	Data Type	Mandatory	Description
Input Parameters:			
name	Alphanumeric	Yes	A name for the URL ACL.
enable	String	Yes	Apply the URL ACL rule to the service. The values include: • on • off
host_match	Alphanumeric	Yes	A hostname to be matched against the host in the request.
url_match	URL	Yes	A URL to be matched to the URL in the request.
extended_match	String	Yes	An expression that consists of a combination of HTTP headers and/or query string parameters. For information on how to write extended match expressions, see Extended Match Syntax Help .
extended_match_sequence	Numeric	Optional	A number to indicate the order in which the extended match rule must be evaluated in the requests.
action	Enumeration	Optional	The action to be taken on the request matching the URL. The enumerated values include: • redirect • deny_and_log • allow • deny_with_no_log • process
deny_response	Enumeration	Conditional	The response to be sent to the client if the request is denied. A deny response is used when the action is set to "**deny_and_log**" or "**deny_with_no_log**". The enumerated values include: • response_page • reset • permanent_redirect • temporary_redirect

response_page	Enumeration	Conditional	The response page to be sent to the client, if “**deny_response**” is set to "**response_page**". The enumerated values include: • default • default-virus • default-error-resp • default-captcha-response-page • default-suspected-activity-error-page • default-captcha-tries-error-page • default-captcha-sessions-error-page
redirect_url	Alphanumeric	Conditional	The URL to redirect the request if **action** or **deny_response** is set to **temporary_redirect** or **permanent_redirect** . It can be a fully qualified URL (like http://www.example.com/index.html) or a full path (like /index.html).
Follow Up Action	Enumeration	Optional	The follow-up action to be taken whenever the request is denied. The enumerated values include: • None • Block Client-IP • Challenge with CAPTCHA
Follow Up Action Time	Numeric	Optional	Sets the time (sec) to block the client IP if **Follow Up Action** is set to **Block Client-IP**. The time can range between 1 to 600000 seconds.

Example:

Request:

curl http://10.11.25.233:8000/restapi/v1/virtual_services/HTTP1/url_adrs -u 'eyJldCIFkbWluIn0=\n:' -X POST -H Content-Type:application/json -d '{"name": "url_test1","host_match":"*","url_match":"/index.html","extended_match":"*","response_page":" default"}'

Response:

{"id":"url_test1","token":"eyJldCI6kbWluIn0=\n"}

To Retrieve URL ACL Rules

URL: /v1/virtual_services/{virtual_service_id}/{url_adr_id}

Method: GET			
Description: Lists all URL ACLs if “url_adr_id” is not specified.			
Parameter Name	**Data Type**	**Mandatory**	**Description**
Input Parameters:			
parameters	Alphanumeric	Optional	Any specific parameter name that needs to be retrieved.

Example 1:

Request:

curl http://10.11.25.233:8000/restapi/v1/virtual_services/HTTP1/url_adrs -u 'eyJldCI6WluIn0=\n:' -X GET

Response:

{"parameters":null,"object":"URL: Allow/Deny Rules","data":[{"enable":"on","extended_match_sequence":"1","name":"url_test1","deny_response":"response_page","comments":"","host_match":"*","extended_match":"*","response_page":"default","url_match":"/index.html","redirect_url":"","action":"process","id":"url_test1"}],"limit":null,"service_id":"HTTP1","token":"eyJldCImFkbWluIn0=\n","offset":null}

Example 2:

Request:

curl http://10.11.25.234:8000/restapi/v1/virtual_services/HTTP1/url_adrs/url_test1 -u 'eyJldCI6FkbWluIn0=\n:' -X GET

Response:

{"enable":"on","extended_match_sequence":"1","name":"url_test1","deny_response":"response_page","comments":"","host_match":"*","extended_match":"*","response_page":"default","url_match":"/index.html","redirect_url":"","action":"process","id":"url_test1","token":"eyJldCI6FkbWluIn0=\n"}

To Update a URL ACL Rule

URL: /v1/virtual_services/{{virtual_service_id}/url_adrs/{url_adr_id}
Method: PUT
Description: Updates a URL ACL rule with the given values.

Parameter Name	Data Type	Mandatory	Description
Input Parameters:			
enable	String	Yes	Apply the URL ACL rule to the Service. The values include: • on • off
host_match	Alphanumeric	Optional	A hostname to be matched against the host in the request.
extended_match	String	Optional	An expression that consists of a combination of HTTP headers and/or query string parameters. For information on how to write extended match expressions, see Extended Match Syntax Help .
extended_match_sequence	Numeric	Optional	A number to indicate the order in which the extended match rule must be evaluated in the requests.
action	Enumeration	Optional	The action to be taken on the request matching the URL. The enumerated values include: • redirect • deny_and_log • allow • deny_with_no_log • process
deny_response	Enumeration	Optional	The response to be sent to the client if the request is denied. A deny response is used when the action is set to "**deny_and_log**" or "**deny_with_no_log**". The enumerated values include: • response_page • reset • permanent_redirect • temporary_redirect
response_page	Enumeration	Optional	The response page to be sent to the client, if "**deny_response**" is set to "**response_page**". The enumerated values include: • default • default-virus • default-error-resp • default-captcha-response-page • default-suspected-activity-error-page • default-captcha-tries-error-page • default-captcha-sessions-error-page

redirect_url	Alphanumeric	Optional	The URL to redirect the request if **action** or **deny_response** is set to **temporary_redirect** or **permanent_redirect** . It can be a fully qualified URL (like http://www.example.com/index.html) or a full path (like /index.html).

Example:

Request:

curl http://10.11.25.108:8000/restapi/v1/virtual_services/HTTP1/url_adrs/url_test1 -u 'eyJldCI6IjEFkbWluIn0=\n:' -X PUT -H Content-Type:application/json -d '{"url_match":"/index1.html","host_match":"a.com"}'

Response:

{"id":"url_test1","token":"eyJldCI6FkbWluIn0=\n"}

To Delete a URL ACL Rule

URL: /v1/virtual_services/{virtual_service_id}/url_adrs/{url_adr_id}
Method: DELETE
Description: Deletes the given URL ACL rule.

Example:

Request:

curl http://10.11.25.233:8000/restapi/v1/virtual_services/HTTP1/url_adrs/url_test2 -u 'eyJldCI6FkbWluIn0=\n:' -X DELETE

Response:

{"msg":"Successfully deleted","token":"eyJldCmFkbWluIn0=\n"}

Allow/Deny Rules for Headers

To Add a Header ACL

URL: /v1/virtual_services/{virtual_service_id}/header_adrs			
Method: POST			
Description: Creates a header ACL rule with the given values.			
Parameter Name	**Data Type**	**Mandatory**	**Description**
Input Parameters:			
name	Alphanumeric	Yes	A name for the header ACL.
header_name	Alphanumeric	Yes	Name of the header to be matched in the request.
status	String	Yes	Apply the Header ACL rule to the service. The values include: • on • off
mode	String	Optional	The mode to determine how the service responds to the offending traffic. The enumerated values include: • passive - This mode allows the intrusions to be passed to the server, but logs the events. • active - This mode blocks the intrusions and logs the events.
max_header_value_length	Numeric	Optional	Maximum allowable length for the header.
denied_metachars	String	Optional	Metacharacters to be denied in the request header value.

Example:

Request:

curl http://10.11.25.233:8000/restapi/v1/virtual_services/HTTP1/header_adrs -u 'eyJldCI6IjkbWluIn0=\n:' -X POST -H Content-Type:application/json -d '{"name": "test2","header_name":"test2"}'

Response:

{"id":"test2","token":"eyJldCFkbWluIn0=\n"}

To Retrieve Header ACL

URL: /v1/virtual_services/{virtual_service_id}/{header_adr_id}

Method: GET			
Description: Lists all header ACLs if “header_adr_id” is not specified.			
Parameter Name	**Data Type**	**Mandatory**	**Description**
parameters	Alphanumeric	Optional	Any specific parameter name that needs to be retrieved.

Example 1:

Request:

curl http://10.11.25.233:8000/restapi/v1/virtual_services/HTTP1/header_adrs -u 'eyJldCmFkbWluIn0=\n:' -X GET

Response:

{"parameters":null,"object":"URL: Allow/Deny Rules","data":[{"denied_metachars":"%00%04%1b%08%7f","mode":"ACTIVE","status":"on","name":"test1","header_name":"prashu1","id":"test1","comments":null,"max_header_value_length":"512"},{"denied_metachars":"%00%04","mode":"PASSIVE","status":"on","name":"test2","header_name":"test2","id":"test2","comments":"test","max_header_value_length":"4"}],"limit":null,"service_id":"HTTP1","token":"eyJldluIn0=\n",

Example 2:

Request:

curl http://10.11.25.234:8000/restapi/v1/virtual_services/HTTP1/header_adrs/test1 -u 'eyJldCI6IjbWluIn0=\n:' -X GET

Response:

{"mode":"ACTIVE","status":"on","name":"test1","header_name":"test1","comments":null,"max_header_value_length":"512","blocked_attack_types":[],"denied_metachars":"%00%04%1b%08%7f","custom_blocked_attack_types":[],"id":"test1","token":"eyJFkbWluIn0=\n"}

To Update a Header ACL

URL: /v1/virtual_services/{virtual_service_id}/header_adrs/{header_adr_id}
Method: PUT
Description: Updates a header ACL with the given values.

Parameter Name	Data Type	Mandatory	Description
Input Parameters:			
status	String	Yes	Apply the Header ACL rule to the service. The values include: • on • off
mode	String	Optional	The mode to determine how the service responds to the offending traffic. The enumerated values include: • passive - This mode allows the intrusions to be passed to the server, but logs the events. • active - This mode blocks the intrusions and logs the events.
max_header_value_length	Numeric	Optional	Maximum allowable length for the header.
denied_metachars	String	Optional	Metacharacters to be denied in the request header value.
blocked_attack_types	String	Optional	Attack types that needs to be matched with the values of the specified header. The values include: • ldap_injection • directory_traversal • directory_traversal_strict • apache_struts_attacks • cross_site_scripting • remote_file_inclusion • sql_injection_strict • sql_injection • os_command_injection • remote_file_inclusion_strict • os_command_injection_strict • python_php_attacks • http_specific_attacks • cross_site_scripting_strict
custom_blocked_attack_types	String	Optional	Custom attack types to be matched with the values of the specified header.

Example 1:

Request:

curl http://10.11.25.233:8000/restapi/v1/virtual_services/HTTP1/header_adrs/test2 -u 'eyJldCIFkbWluIn0=\n:' -X PUT -H Content-Type:application/json -d '{"max_header_value_length":"4","comments":"test","mode":"PASSIVE","denied_metachars":"%00%04"}'

Response:

{"id":"test2","token":"eyJldCI6IuIn0=\n"}

Example 2:

Request:

curl http://10.11.25.234:8000/restapi/v1/virtual_services/HTTP1/header_adrs/test1 -u 'eyJldCI6IjE0NDI1NDg4MjAiLCJwYXNzd29yZCI6Ijc0MmVlN2UxNmJlNTY5MDQ1N2ZhY2M0ZTE3\nYjM1Y2E4IiwidXNlciI6ImFkbWluIn0=\n:' -X PUT -H Content-Type:application/json -d '{"max_header_value_length":"4","comments":"test","mode":"PASSIVE","denied_metachars":"%00%04","custom_blocked_attack_types":["barr"],"blocked_attack_types":["remote_file_inclusion","cross_site_scripting"]}'

Response:

{"id":"test1","token":"eyJldCI6IjE0NDI1NjE4NzkiLCJwYXNzd29yZCI6IjUyZWQxYWMzNzdjNzU2NGE2YzM1MDY4YTUw\nODQxZjdkIiwidXNlciI6ImFkbWluIn0=\n"}

To Delete a Header ACL

URL: /v1/virtual_services/{virtual_service_id}/header_adrs/{header_adr_id}
Method: DELETE
Description: Deletes the given header ACL.

Example:

Request:

curl http://10.11.25.233:8000/restapi/v1/virtual_services/HTTP1/header_adrs/test2 -u 'eyJldCI6IjE0NDY1MzgyOTEiLCJwYXNzd29yZCI6IjI4MmZjMDZiZWM5MTkxNDEzYWIzM2U1YTUw\nZGRjNzU3IiwidXNlciI6ImFkbWluIn0=\n:' -X DELETE

Response:

{"msg":"Successfully deleted","token":"eyJldCI6IjE0NDY1NDA4MjQiLCJwYXNzd29yZCI6ImVmZmQwNDA5M2IyNWMxYjQzOGJlZDdhMDhk\nMGRlOWRiIiwidXNlciI6ImFkbWluIn0=\n"}

Figures