Advanced Security and Clickjacking Protection

Advanced Security

Advanced Security allows you to set the policies like data theft protection, brute force prevention and virus scan on a key which is defined by the URL, domain and HTTP headers.

To Add an URL Policy

URL: /v1/virtual_services/{virtual_service_id}/advanced_security
Method: POST
Description: Creates an URL policy with the given values.

Parameter Name	Data Type	Mandatory	Description
Input Parameters:			
name	Alphanumeric	Yes	The name of the new URL policy.
status	String	Optional	Apply the URL policy to the Service. The values include: • on • off
host_match	Alphanumeric	Yes	A host name 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, refer 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.
mode	String	Optional	The mode of action for request violations matching the URL Policy. The values include: • active - This mode blocks the intrusions and logs the events. • passive - This mode allows the intrusions to be passed to the server, but logs the events.
parse_urls_in_scripts	String	Optional	Controls whether to parse URLs in the scripts so that they can be used for URL translation or instant SSL. The values include: • yes • no By default, this is set to *Yes*.
enable_virus_scan	String	Optional	Scans all files uploaded through multipart/form-data messages for the presence of viruses. Requests containing virus signatures are denied. The values include: • yes • no By default, this is set to *No*.

enable_data_theft_protection	String	Optional	Enable data theft protection for the service. When this is enabled and the parameter "Enabled" is set to "Yes" on the **SECURITY POLICIES > Data Theft Protection** page, all URL policies will look for the data type element (configured on the **SECURITY POLICIES > Data Theft Protection** page) in server response pages. The values include: • yes • no By default, this is set to *No*.
enable_bruteforce_prevention	String	Optional	Enable bruteforce attack prevention for the URL policy. The values include: • yes • no By default, this is set to *No*.
rate_control_pool	Enumeration	Optional	The rate control pool(s) defined on the **ADVANCED > Libraries** page (if any).
web_scraping_policy	Enumeration	Optional	The web scraping policy that needs to be associated with the URL policy of the service. A web scraping policy can be created on the **WEBSITES > Web Scraping** page.

Example

Request:

curl http://10.11.28.58:8000/restapi/v1/virtual_services/service1/advanced_security -u'eyJldCI6IjE0NzMzMTUxMTYiLCJwYXNzd29yZCI6ImU3MGZlNzFjMTNkZGNhMDAyZTgzNTk3YzZl\nYTg2MmQ1IiwidXNlciI6ImFkbWluIn0=\n:' -X POST -H Content-Type:application/json -d'{"name":"policy","host_match":"www.xyz.com","url_match":"/frames/deeptree/start_11.php/indexing/","extended_match":"*","extended_match_sequence":"1","status":"on","mode":"active","parse_urls_in_scripts":"yes","enable_virus_scan":"yes","enable_bruteforce_prevention":"yes","enable_data_theft_protection":"yes","rate_control_pool":"default-pool"}'

Response:

{"id":"policy","token":"eyJldCI6IjE0NzMzMTUyMTAiLCJwYXNzd29yZCI6IjRmNWJlZjY5MjcwOTllNmNjYTYzNzFjMjk1\nZTdhZTZhIiwidXNlciI6ImFkbWluIn0=\n"}

To Update an URL Policy

URL: /v1/virtual_services/{virtual_service_id}/advanced_security/{URL_policy_id}

Method: PUT

Description: Updates the values of given parameters in the given URL policy

Parameter Name	Data Type	Mandatory	Description
Input Parameters:			
status	String	Optional	Apply the URL policy to the Service. The values include: • on • off
host_match	Alphanumeric	Optional	A host name to be matched against the host in the request.
url_match	URL	Optional	A URL to be matched to the URL 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, refer 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.
mode	String	Optional	The mode of action for request violations matching the URL Policy. The values include: • active - This mode blocks the intrusions and logs the events. • passive - This mode allows the intrusions to be passed to the server, but logs the events.
parse_urls_in_scripts	String	Optional	Controls whether to parse URLs in the scripts so that they can be used for URL translation or instant SSL. The values include: • yes • no By default, this is set to *Yes*.
enable_virus_scan	String	Optional	Scans all files uploaded through multipart/form-data messages for the presence of viruses. Requests containing virus signatures are denied. The values include: • yes • no By default, this is set to *No*.
response_charset	Enumeration	Optional	The character set to be used in the response page. The enumerated values include: • ascii • iso-8859-1 • utf-8 • gbk • gb2312 • iso-2022-cn • hz • big5 • euc-tw • shift-jis • euc-jp • iso-2022-jp • euc-kr • johab • iso-2022-kr • none
web_scraping_policy	Enumeration	Optional	The web scraping policy that needs to be associated with the URL policy of the service. A web scraping policy can be created on the **WEBSITES > Web Scraping** page.

enable_data_theft_protection	String	Optional	Enable data theft protection for the service. When this is enabled and the parameter "Enabled" is set to "Yes" on the **SECURITY POLICIES > Data Theft Protection** page, all URL policies will look for the data type element (configured on the **SECURITY POLICIES > Data Theft Protection** page) in server response pages. The values include: • yes • no By default, this is set to *No*.
rate_control_pool	Enumeration	Optional	The rate control pool(s) defined on the **ADVANCED > Libraries** page (if any).
enable_bruteforce_prevention	String	Optional	Enable bruteforce attack prevention for the URL policy. The values include: • yes • no By default, this is set to *No*.
enable_invalid_status_code_only	String	Optional	Monitors and counts only invalid requests from a single client or all sources. If set to ***no***, it counts both valid and invalid requests from a single client or all sources. It blocks the requests when it exceeds the specified value in **max_allowed_accesses_per_ip** and **max_allowed_accesses_from_all_sources**. The values include: • yes • no
count_window	Numeric	Optional	The time in seconds for allowing the maximum number of requests as per the settings in the parameter **max_allowed_accesses_per_ip** or **max_allowed_accesses_from_all_sources**. • **Range** – 1 to 3600.
max_allowed_accesses_per_ip	Numeric	Optional	The maximum number of requests allowed per IP address to access the service, if the parameter **counting_criterion** is set to *per_ip*.
counting_criterion	String	Optional	The criteria for allowing the requests. The values include: • per_ip • all_sources
exception_clients	Alphanumeric	Optional	The IP addresses that should be exempted (not locked out). You can enter a single, or a range of IP addresses, or a combination of both with comma (,) as a delimiter without any space. **Example**: 10.10.10.10,11.11.11.11,10.10.11.11. The range of IP addresses must be separated with a hyphen (-). **Example**: 10.10.10.1-10.10.10.10. This makes an exception list of client IPs (permitted users). Ensure that there are no overlapping IP ranges.

Example

Request:

curl http://10.11.28.58:8000/restapi/v1/virtual_services/service1/advanced_security/policy -u'eyJldCI6IjE0NzMzMTUxMTYiLCJwYXNzd29yZCI6ImU3MGZlNzFjMTNkZGNhMDAyZTgzNTk3YzZl\nYTg2MmQ1Iiwid

XNlciI6ImFkbWluIn0=\n:' -X PUT -H Content-Type:application/json -d'{"enable_invalid_status_code_only":"yes","count_window":"20","max_allowed_accesses_per_ip":"11","counting_criterion":"all_sources","exception_clients":"10.11.23.63"}'

Response:

{"id":"policy","token":"eyJldCI6IjE0NzMzMTYzNzAiLCJwYXNzd29yZCI6Ijc4YjczYjI2ZDJhOGI0OWQ2NzRhMzExNmJj\nYWQxYWZkIiwidXNlciI6ImFkbWluIn0=\n"}

To Delete a URL Policy

URL: /v1/virtual_services/{virtual_service_id}/advanced_security/{url_policy-id}
Method: DELETE
Description: Deletes the given URL policy.

Example

Request:

curl http://10.11.28.58:8000/restapi/v1/virtual_services/service1/advanced_security/policy -u'eyJldCI6IjE0NjQyNTQwOTUiLCJwYXNzd29yZCI6IjljZmQwMDM4NWE2NzZlYmZkMjQxNTczYTkx\nODRlM2FmIiwidXNlciI6ImFkbWluIn0=\n:' -X DELETE

Response:-

{"msg":"Successfully deleted","token":"eyJldCI6IjE0NzMzMTcwNjkiLCJwYXNzd29yZCI6IjA2MTdhODQ5OTA5YzllOTlkNmYzOTMyMjg4\nODcxNmQxIiwidXNlciI6ImFkbWluIn0=\n"}

Clickjacking Protection

Clickjacking (also known as UI redressing and iframe overlay) is a malicious technique where an attacker tricks a user to click on a button or link on a website by hiding clickable elements inside an invisible iframe. By this, the attacker hijacks the clicks meant for the actual page and routes the user to another page which is owned by another application, domain or both. The X-Frame-Options HTTP response header can be used to detect and prevent such iframe based UI redressing. The Barracuda Web Application Firewall inserts the X-Frame-Options header to determine whether a browser should be allowed to render a page in a "iframe", and if allowed, the iframe origin that needs to be matched. For more information, refer to Enabling Clickjacking Protection for a Service.

To Update a Clickjacking Protection Policy for a Service

URL: /v1/virtual_services/{virtual_service_id}/clickjacking_protection
Method: PUT
Description: Updates the values of given parameters in the given clickjacking protection policy

Parameter Name	Data Type	Mandatory	Description
Input Parameters:			
status	String	Optional	Insert the “X-Frame-Options” header in the responses. The values include: • on • off

render_page_inside_iframe	String	Optional	The option to render the page. The values include: • never - The browser will not display the page if the page is within the iframe. • same_origin - The browser allows the page to be displayed if the page within the iframe is from the same origin. • allowed_origin - The browser allows the page specified in the ***allowed_origin*** to be displayed when embedded in the iframe.
allowed_origin_uri	Alphanumeric	Optional	The origin URI that needs to be rendered even if it is in an iframe when **render_page_inside_iframe** is set to **allowed_origin**.

Example

Request

curl http://10.11.28.58:8000/restapi/v1/virtual_services/service1/clickjacking_protection -u'eyJldCI6IjE0NzMzMTcwNjkiLCJwYXNzd29yZCI6IjA2MTdhODQ5OTA5YzllOTlkNmYzOTMyMjg4\nODcxNmQxIiwidXNlciI6ImFkbWluIn0=\n:' -X PUT -H Content-Type:application/json -d '{"status":"on","render_page_inside_iframe":"allowed_origin","allowed_origin_uri":"/data/index/cgi"}'

Response:

{"msg":"Configuration Updated","token":"eyJldCI6IjE0NzMzMTgxNjciLCJwYXNzd29yZCI6IjViNDA5YzAwM2RmMjI3NWZmMzZjMWM5YzE1\nNDNmYmI5IiwidXNlciI6ImFkbWluIn0=\n"}