Extended Match Syntax

https://campus.barracuda.com/doc/17629567/

Extended Match and Condition Expression

Extended Match and Condition Expressions can be configured for various rule types, allowing you to specifically define which requests/responses need the rule applied. You can configure conditions based on parameters or elements of a request/response, combining them in a flexible manner, and applying the rule security settings only to those that match the defined expression.

A few examples:

- Header Host co example.com - match a request whose Host header contains example.com
- Parameter userid ex - match any request in which the parameter **userid** is present
- (Header Host eq `www.example.com`) && (Client-IP eq `10.0.0.0/24`) - match a request whose host header is `www.example.com` and whose client IP address is in the 10.0.0.* subnet.

Quick reference

- Extended Match Expression:
  - Element Match
  - (Expression) [Join (Expression) ...]
- Join:
  - &&, ||
- Element Match:
  - Element [Element Name] Operator [Value]
- Element:
  - Request Elements: Method, HTTP-Version, Client-IP, URI, URI-Path, Header
  - Request Parameters: Parameter, Pathinfo
  - Response Elements: Status-code, Response-Header
- Operator:
  - Matching: eq, neq, req, nreq
  - Containing: co, nco, rco, nrco
  - Existence: ex, nex

Structure of an Extended Match Expression

An Extended Match expression consists of one or more **Element Matches**, combined using **Join**

operators AND and OR. Parentheses delimit individual Element Matches when using join operators. Parentheses can be nested.

An Element Match consists of an **Element**, an optional **Element Name**, an **Operator** followed by an optional **Value**. Some elements (like **Header)** require an Element Name (like **User-Agent)** whereas some elements (like **HTTP-Version**) require no further qualification. Also, some operators (like **eq**) require a value, whereas some don't (like **ex**).

Tokens are delimited by space and the parenthesis characters. Double quotes (") can be used to enclose single tokens which contain parenthesis characters or spaces. The back-slash character can also be used to escape, that is, remove the special meaning of the special characters (space and parenthesis).

Operators

The following are the possible operators in an Element Match. The operators are case insensitive so, for example, **eq**, **Eq** and **EQ** all behave the same.

- **eq** - true if the operand is equal to the given value. A case insensitive string comparison is performed, so a value of "01" does not equal the value "1", whereas the values "one" and "ONE" are equal.
- **neq** - true if the operand is not equal to the given value. A case insensitive string comparison is performed.
- **co** - true if the operand contains the given value.
- **nco** - true if the operand does not contain the given value.
- **rco** - true if the operand contains the given value, specified as a regular expression.
- **nrco** - true if the operand does not contain the given value, specified as a regular expression.
- **req** - true if the operand matches the given value, specified as a regular expression.
- **nreq** - true if the operand does not match the given value, specified as a regular expression.
- **ex** - true if the operand exists. A value is not required.
- **nex** - true if the operand does not exist. A value is not required.

Elements

The following Elements are allowed in an expression. Elements and Element Names are case insensitive, so **Method** and **METHOD** behave the same.

- **Client-IP** - The IP address of the client sending the request. The IP address can be either host IP address or subnet IP address specified by a mask. Only **eq** and **neq** operations can be used with this element. Examples: (Client-IP eq 192.168.1.0/24), (Client-IP eq 192.168.1.10)

- **Method** - The HTTP Method specified in the request. Example: (Method eq GET)
- **HTTP-Version** - The version of the HTTP protocol of the request. Example: (HTTP-Version eq HTTP/1.1)
- **URI** - The Uniform Resource Identifier in the request. This includes any query parameters in the request. Example: (URI rco /abc.*html?userid=b)
- **URI-path** - The path portion of the URI, excluding any query parameters. Example: (URI-path req \/.*copy%20[^/]*)
- **Parameter** - A parameter in the query string part of the URL and serves as a name-value pair. The special parameter "$NONAME_PARAM" allows reference to a parameter when the parameter name is absent. Examples: (Parameter sid eq 1234), (Parameter $NONAME_PARAM co abcd)
- **Pathinfo** - The portion of the URL considered the PATH_INFO on the server. The Barracuda Web Application Firewall uses a set of known extensions to determine whether a portion of the URL is the Pathinfo or not. For example, if the request URL is `/twiki/view.cgi/Engineering`, then, `/Engineering` is considered to be the pathinfo rather than part of the URL. Example: (PathInfo rco abc*)
- **Header** - An HTTP header in the request. Requires an Element Name to identify which header, following the word **Header**. Example: (Header Accept co gzip). This will check if the "Accept:" header contains the string "gzip".
- **X509_OU** - The Organizational Unit (OU) stated in the X.509 certificate. Example: (X509_OU eq Engineering Division). When **Client Authentication** is enabled for a HTTPS service, the certificate presented by the client is matched with the element value. If the request matches the rule, the Barracuda Web Application Firewall executes the specified action.

To **Enable Client Authentication**, click **Edit** in the **Options** column next to the service on the **BASIC > Services** page in the **Configured Virtual Services** section.

Not all elements are allowed in every expression. The following restrictions apply:

- Request rules (ACLs, URL Policy, URL Profiles) allow only the elements **Method**, **HTTP-Version**, **Header**, **Client-IP**, **URI**, **URI-Path**, **PathInfo**, and **Parameter**.
- Request Rewrite Condition allows only the elements **Method**, **HTTP-Version**, **Header**, **Client-IP**, and **URI**.
- Response Rewrite Condition allows only the elements Method, **HTTP-Version**, **Header**, **Client-IP**, **URI**, **Status-code** and **Response-Header**.

Joins

Expressions can be joined using:

- || - Or, checks if either expression is true.
- **&&** - And, checks if both expressions are true.

Element Matches can be combined as long as the Element Matches are enclosed in parentheses. You cannot combine Element Matches without parentheses. **Example**: (Header cookie ex) && (URI rco .*\.html) && (Method eq GET)

Nested sub-expressions can be created by enclosing expressions in parentheses, making the expression more readable as well as unambiguous. **Example**: (HTTP-Version eq HTTP/1.1) && ((Header Host eq `www.example.com`) || (Header Host eq `website.example.com`))

Escaping

The space character and the parentheses characters are special characters which cause the parser to split the string into tokens at these separators. In some cases, you must specify these characters as part of the value itself. For example, the User-Agent header typically contains both spaces and parentheses, as in:

User-Agent: Mozilla/5.0 (Linux i686; en-US; rv:1.8.1.3) Firefox/2.0.0.3

When a value contains space or parenthesis characters, they must be escaped by prefixing them with a back-slash (\), or by enclosing the entire value in double-quotes ("). **Examples**:

- Header User-Agent eq "Mozilla/5.0 (Linux i686; en-US; rv:1.8.1.3) Firefox/2.0.0.3"
- Header User-Agent eq Mozilla/5.0\ \(Linux\ i686;\ en-US;\ rv:1.8.1.3\)\ Firefox/2.0.0.3

The double-quote character itself must be escaped with a back-slash. This is true whether or not it is inside a quoted string. Note that the single quote character has no special meaning, and is treated as any other character.

To specify the back-slash character itself, it must be escaped as "\\". This is true whether or not it is within a quoted string.

The back-slash character escapes all characters, not just special characters. Thus, "\c" stands for the character "c" etc. In other words, back-slash followed by any character stands for the character, whether or not that character has a special meaning in the extended match syntax.