

NAME

httpscreen.cf - screening policy for httpscreen and httpsscreen

SYNOPSIS

```
(permit | deny) get size <url-size> <url-regex> [ args <sep-char> (
(permit | deny) arg size <arg-size> <arg-regex> )+ ]
(permit | deny) post size <url-size> <url-regex> [ args <sep-char> (
(permit | deny) arg size <arg-size> <arg-regex> )+ ] [ ( (permit | deny) data
size <data-size> <data-regex> )+ ]
map <url-regex> <substitute-exp> <dst-ip>:<dst-port>;(<dst-ip>:<dst-port>)\
"<option>"("<option>")\
```

DESCRIPTION

The httpscreen policy file httpscreen.cf specifies:

Permitted or denied URLs

Permitted or denied arguments and data for a specific

URL substitutions

URL based configuration options

URL based backend mapping.

The policy files are usually maintained on the firewall in the /usr/local/etc/local/httpscreen directory and are linked to a specific connection policy in config.oper(5) through the screen option described in httpscreen(6).

The httpscreen.cf file is block oriented. Lines that start with a hash (#) are commentary and are therefore ignored. All other lines must start either with a directive (permit, deny, map) or a space in case of a multi line statement block.

The permit directive defines which method for a specific URL is allowed. If the URL matches the regular expression (regex(3)) <url-regex> and its size in its URL encoded form is less or equal to <url-size> the rest of the request of the request will be checked. If the requested URL contains arguments separated by <sep-arg> characters all these arguments are checked against the permit arg and/or deny arg rules in the rest of statement. In case any part of the argument does not match any of the rules, the request is denied by default.

The map directive defines URL based substitution, distribution and options. If a request does not match any map rule it will not be serviced. If a request was permitted by a permit statement and its URL matches the <url-regex> of a map rule it will be substituted by the <substitute-

`exp`>. The `<substitute-exp>` can contain the well known `\<n>` place holders to the n-th matched sub-part of the match expression.

In case a map rule matches the request it will be forwarded to one of the backend servers represented by `<dst-ip>` (destination IP address) and `<dst-port>` (destination port). If multiple servers are specified separated by a `;` (semi colon), one will be chosen at random. If a chosen server does not respond a new one will be chosen until no server is left to choose from. If no server is available, an overload error is send to the client indicating that the service is currently unavailable.

Currently there are only two URL based options are available and that apply on the matching URLs.

`auth` requires authentication

`ssl` enables SSL on the backend connections in case of httpscreen

EXAMPLES

Allow GET requests without arguments with a maximum URL encoded size of 250 characters.

```
permit get size 250 /*.
```

Deny GET request with `..` in the URL.

```
deny get size 250 /*.\.\..*
```

Allow GET requests with any arguments with a maximum URL encoded size of 250 characters for the URL and the arguments.

```
permit get size 250 /* args &
permit arg size 250 /*.
```

Allow POST requests with data and a maximum URL encoded size of 250 characters for the URL and the data arguments.

```
permit post size 250 /*.
permit data size 250 /*.
```

Allow POST requests with arguments, data and with a maximum URL encoded size of 250 characters.

```
permit post size 250 /* args &
permit arg size 250 /*.
permit data size 250 /*.
```

Match any URL and forward it unchanged to the server 192.168.1.80 at port 80.

```
map      (.*)      \1      192.168.1.80:80
```

FILES

`/usr/local/etc/local/httpscreen/http.cf`

Location of an example 'httpscreen.cf(5) configuration file n the firewall.

SEE ALSO

`screenmk(1)`.

BUGS

Please report bugs to fwsupport@tunix.nl.

AUTHOR

Copyright 1999-2003 TUNIX Internet Security & Opleidingen

VERSION

Version \$Revision: 1.7 \$ \$Date: 2003/05/16 08:53:43 \$ (\$Name: HTTPSCREEN_02 \$)