Technical Guide

Web Redirect

Feature Overview and Configuration Guide

Introduction

This guide describes the Web Redirect feature and how to configure it. Web Redirect has 2 modes:

- HTTP mode, where it lets you redirect HTTP client requests to a specified URL, either periodically or on an ongoing basis. You can exclude specified client requests from being redirected.
- Proxy chaining mode, where it forwards all HTTP/HTTPS traffic to an upstream explicit proxy server, except for specified exclusions. Excluded traffic is sent directly to the Internet.

Products and software version that apply to this guide

This guide applies to AlliedWare Plus™ firewalls and routers, running version **5.4.8-1.1** or later.

For more information, see the following documents:

- The product’s Datasheet
- The product’s Command Reference

These documents are available from the above links on our website at alliedtelesis.com.

The following features have been introduced in later releases:

- proxy chaining mode: 5.5.0-2.3 onwards
- exclusion by destination IP address or subnet: 5.5.2-1.1 onwards.

Contents

Web Redirect in HTTP mode

Web Redirect tracks HTTP clients based on their IP address (IPv4 or IPv6). When the first HTTP request is sent by a given client the device intercepts the request and sends an HTTP "Redirect" message back to the client with the 302 Response code and includes the configured server URL.

Time interval settings determine when the client is next eligible to be redirected.

Limitations

- 1000 client devices can be monitored at once. If more than that are active (waiting for a redirect repeat time to expire), the surplus will always be redirected.
- Clients are monitored by IP address. If DHCP is used and lease times are shorter than the redirect repeat time, and an IP is reallocated, there is a chance the new client may not be redirected straight away.
- Redirection of HTTPS is not supported.
- Client exclusion by MAC address or vendor OUI can only be supported when clients are connected to the device at Layer 2. If clients are routed (Layer 3 forwarded) to the device, the MAC address of the client will not be available. That is because the source MAC in the packet will be that of the nearest Layer 3 device.

Where could you use Web Redirect?

This feature could be used in apartment buildings as part of the Internet gateway service for tenants. You could for example, redirect users' web-browsers to a site that presents them with advertising information once in a given period. Or you could possibly redirect users to a sign-in or payment page.

Configuring Web Redirect in HTTP mode

The following items can be configured:

- The URL to redirect to
- How often each client should be redirected
- How long a client should be idle before they get redirected (to avoid redirecting a request for a web-page element, rather than the page itself)
- Exclusion lists for IP addresses and subnets
- Exclusion lists for MAC addresses and MAC OUID (Organization Unique Identifier)/vendor codes
- The redirection of requests that come from hardware devices or system processes rather than web browsers.

Here are the basic steps required to configure Web Redirect:

Step 1. **Configure the URL that clients are redirected to**

This is specified with the **server-url** command. The URL can be either HTTP or HTTPS and the protocol must be specified.

For example:

```
awplus# configure terminal
awplus(config)# web-redirect
awplus(config-web-redirect)# server-url http://redirectexample.com
```

Step 2. **Configure the two timer values: repeat-time and idle-time**

There are two timer commands: **repeat-time** and **idle-time**:

- **repeat-time**: sets the interval (in seconds) between redirects for a client. After the specified interval the client will be ***eligible*** to be redirected again. If no ‘repeat-time’ is specified, every client request will be eligible for a redirect immediately. Whether or not an eligible client is immediately redirected at the expiry of the repeat time depends on the **idle-time**.

  For example, if the user is busy browsing a website and loading new content, then it would be undesirable to be immediately redirected after the expiry of the repeat time interval. To ensure an ideal user experience, it is better to wait for an additional period of time to ensure current web site content is fully downloaded, and for the browser to have been idle before redirection occurs.

  For example:

  ```
  awplus(config)# web-redirect
  awplus(config-web-redirect)# repeat-time 3600
  ```

- **idle-time**: sets the interval, following the repeat time, for which a client must be idle before it will be redirected again. This interval makes it likely that it will be a web page request that is redirected, rather than some sub-component of the page. This ensures the full page that the user is being redirected to is displayed, rather than a sub-component of the current page being browsed to.

For example:

```
awplus(config)# web-redirect
awplus(config-web-redirect)# idle-time 300
```

Step 3. Configure the exclusions

There are several exclusion commands available to limit the clients that are redirected, if necessary.

The commands are:

- **exclude ip**: specify a source host address or subnet that should not be redirected. This can be either IPv4 or IPv6. This enables the exclusion of individual hosts or portions of a network that should not be redirected.
- **exclude dst-ip**: specify a destination host address or subnet that should not be redirected. This can be either IPv4 or IPv6.
- **exclude mac**: specify the MAC address of a device that should not be redirected, or a Vendor OUI (Organizationally Unique Identifier, first half of a MAC address xx:xx:xx, specific to a particular vendor) relating to devices that should not be redirected. The Vendor OUI may be useful for excluding a particular group of devices, where the devices are not grouped in a subnet, for example, an IoT device spread throughout a network. Note that the MAC and OUI matching adds load to the device, due to the need to retrieve the MAC address information.
- **browser-only**: limit redirection to only HTTP requests sent by a web browser, rather than another application. For example, hosts may be using HTTP to request automatic software updates but it may be inappropriate for theses requests to be redirected. The browser-only option identifies browser requests by the "Mozilla" string in the User-Agent field of the HTTP request. If the string is not present the request is not redirected. All common browsers include "Mozilla" in their User-Agent field.

Monitoring Web Redirect in HTTP mode

The **show web-redirect** command displays information about the status of the feature, the total number of redirected hosts being tracked and information about when each host (by IP) was last redirected and when it will next be eligible for redirection.

Output 1: Example output from **show web-redirect**

```
awplus#show web-redirect
Mode:       HTTP redirection
Status:     Enabled
Total number of redirected clients: 5
Clients:Address            Last Redirection           Next redirection after
-------------------------------------------------------------------------------
192.0.2.0.2                Tue 23 Aug 2022 11:03:50   Wed 24 Aug 2022 11:03:50
192.0.2.0.17               Tue 23 Aug 2022 10:51:11   Wed 24 Aug 2022 10:51:11
192.0.2.0.31               Tue 23 Aug 2022 05:33:42   Wed 24 Aug 2022 05:33:42
2001:db8::2:121            Tue 23 Aug 2022 17:48:06   Wed 24 Aug 2022 17:48:06
2001:db8::1:ab6d           Tue 23 Aug 2022 01:18:39   Wed 24 Aug 2022 01:18:39
```

The **show web-redirect** output contains the following fields:

PARAMETER	DESCRIPTION
Status	Enabled or Disabled, to indicate if the feature is active or not.
Total number of redirected clients	The number of clients that have been redirected and are now being actively monitored for future redirection. Note that this does not include devices that have been excluded.
Clients	A table containing the details of clients that have been redirected and are now being actively monitored for future redirection, by IP address. ■ **Address:** The IPv4 or IPv6 address of the client. ■ **Last Redirection**: The actual time of the last redirection. ■ **Next redirection after**: The date and time after which the client will next be eligible for redirection. This time depends on the ‘repeat-time configuration and as this time approaches, the idle-time if configured.

Configuration examples for HTTP mode

This section provides a basic Web Redirect configuration followed by examples of the:

- idle-time parameter
- IP subnet exclusion
- vendor MAC OUI exclusion
- browser-only mode

Basic Web Redirect configuration

For a simple configuration where clients are to be redirected to ***www.example.com*** once a day (every 86400 seconds), use the following configuration:

```
web-redirect
 server-url http://www.example.com
 repeat-time 86400
 enable
```

Idle-time

You can use the idle-time parameter to ensure the page the browser is redirected to displays as a full page, rather than as a sub-component of a page. Additionally, redirecting once the host has been idle for some time maintains the browsing flow and reduces annoying interruptions.

To set an idle time of 10 minutes use the following configuration:

```
web-redirect
 server-url http://www.example.com
 repeat-time 86400
 idle-time 600
 enable
```

IP subnet exclusion

To exclude packets with a source IP subnet 192.0.2.128/28 from being redirected, use the following configuration:

```
awplus(config-web-redirect)#exclude ip 192.0.2.128/28
```

To exclude packets with a destination IP subnet 192.0.2.128/28 from being redirected, use the following configuration. This is available from version 5.5.2-1.1 onwards:

```
awplus(config-web-redirect)#exclude dst-ip 192.0.2.128/28
```

You can also exclude IPv6 addresses or prefixes.

Vendor MAC OUI exclusion

If the network contains a number of IP devices that occasionally check for software updates, or could be managed via HTTP (e.g. IP cameras) and being redirected would interfere with those updates, then they need to be excluded. If they are not in an isolated IP subnet but are all from the same vendor, they can be excluded using the vendor's MAC OUI. Assuming this is aa:bb:cc, the command in web-redirect mode would be:

```
awplus(config-web-redirect)#exclude mac aa:bb:cc
```

Note that MAC/OUI exclusions will not work for IPv6-based requests.

Browser-only mode

PCs use HTTP for all sorts of purposes aside from web browsing, such as getting software updates or applications interacting with remote servers. It may not be suitable for these sorts of HTTP requests to be redirected, for example, when the redirect is to present advertising to the user.

In this situation the **browser-only** mode can be used. All modern browsers specify "Mozilla" in some form in the "User-Agent" field of their HTTP requests, while this is not present in other applications.

To use **browser-only** mode, use the following command in **web-redirect** mode:

```
awplus(config-web-redirect)#browser-only
```

Web Redirect in proxy chaining mode

From software version 5.5.0-2.3 onwards, you can configure Web Redirect in proxy chaining mode.

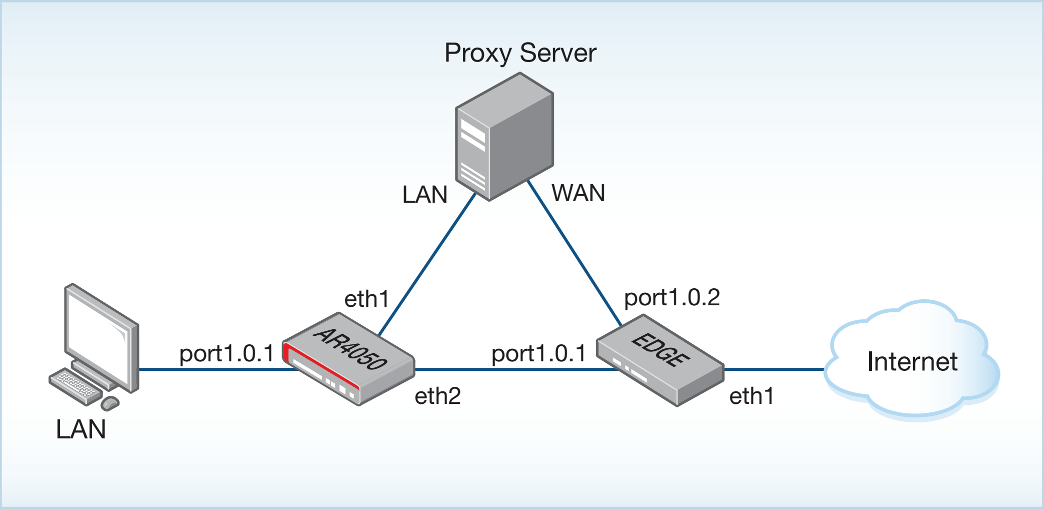
In proxy chaining mode, web redirect forwards all HTTP/HTTPS traffic to an upstream explicit proxy server. You can add exclusions to the web-redirect rules. As well as the exclusions available for HTTP mode (see "Basic Web Redirect configuration" on page 7), you can exclude traffic from specified applications and URLs. Excluded traffic is sent directly to the Internet.

This features lets you use a proxy server to handle additional security processing of your network traffic. The exclusions let you exempt low security risk traffic from additional security processing and send it directly to the Internet, reducing the load on the proxy server.

Clients using Web Redirect do not need to know about the proxy server, so there is no configuration change on their side. The Allied Telesis firewall or router is responsible for deciding where to forward the traffic: to the proxy server or directly to the Internet.

Logical network diagram

The diagram below shows the logical network setup. Here, traffic meeting the exclusion rules by-passes the upstream proxy server and is forwarded directly on to the Internet.



Limitations

- Exclusions are only applied to new connections. For exclusions by application, you need to enable Deep Packet Inspection (DPI) learning, so applications can be identified by the first packet in the connection. See the Application Awareness Feature Overview and Configuration Guide for more information.
- Exclusions by URL regular expressions do not work if TLS 1.3 with Encrypted SNI (ESNI) is used.

Configuring Web Redirect in proxy chaining mode

Follow the steps below to configure Web Redirect in proxy chaining mode:

Step 1. Configure the mode to proxy

This is set using the **mode** command.

```
awplus# configure terminal
awplus(config)# web-redirect
awplus(config-web-redirect)# mode proxy
```

Step 2. Configure the proxy server address and port

This is set using the **proxy-host** command. The proxy-host can be an IPv4 address, IPv6 address, or a hostname.

```
awplus# configure terminal
awplus(config)# web-redirect
awplus(config-web-redirect)# proxy-host 172.16.1.150 port 3128
```

Step 3. Configure the exclusions

There are two additional exclusion commands available:

- **exclude app**: This command allows traffic identified by Application Awareness' DPI to bypass the upstream proxy server and be sent directly to the Internet. For this exclusion to work, DPI and DPI learning needs to be enabled. As soon as DPI identifies the traffic, the exclusion will start working.
- **exclude url**: This command allows traffic with HTTP request or hostname in the HTTPS SNI field matching the URL regular expression to bypass the upstream proxy server and be sent directly to the Internet.

Note that application-based exclusions are much faster than URL-based exclusions, which require the session to be proxied.

You can configure multiple exclusion commands at the same time, including the exclusions listed in "Basic Web Redirect configuration" on page 7.

Exclusions by application

1. Enable DPI and DPI learning. You can use the built-in application list, or use Procera as the provider if you have bought an Advanced Firewall license:

```
awplus# configure terminal
awplus(config)# dpi
awplus(config-dpi)# provider {procera|built-in}
awplus(config-dpi)# learning
awplus(config-dpi)# enable
```

2. Add the DPI application names to the exclusion list:

```
awplus# configure terminal
awplus(config)# web-redirect
awplus(config-web-redirect)# exclude app office
awplus(config-web-redirect)# exclude app skype
```

With the configuration above, traffic identified by DPI as **office** and **skype** is sent directly to the Internet.

Exclusions by URL regular expression

1. Add the URL regular expressions to the exclusion list:

```
awplus# configure terminal
awplus(config)# web-redirect
awplus(config-web-redirect)# exclude url .microsoft.com
awplus(config-web-redirect)# exclude url .live.com
```

With the configuration above, traffic that matches the URL regular expressions **.microsoft.com** or **.live.com** is sent directly to the Internet.

Other examples of exclusions by URL regular expression include:

```
exclude url .chime.aws
exclude url .lb.slack-msgs.com
exclude url .microsoft.com
exclude url .officehome.msocdn.com
exclude url .zoom.us
exclude url a.slack-edge.com
exclude url a.slack-imgs.com
exclude url admin.slack.com
```

Monitoring Web Redirect in proxy chaining mode

To see the connections redirected by the proxy, use the **show firewall connections** command.

In proxy chaining mode, the **show web-redirect** command only shows that redirection is enabled:

```
awplus#show web-redirect
Mode:        Proxy chaining redirection
Status:      Enabled
```

Allied Telesis™ NETWORK SMARTER

North America Headquarters | 19800 North Creek Parkway | Suite 100 | Bothell | WA 98011 | USA | T: +1 800 424 4284 | F: +1 425 481 3895
Asia-Pacific Headquarters | 11 Tai Seng Link | Singapore | 534182 | T: +65 6383 3832 | F: +65 6383 3830
EMEA & CSA Operations | Incheonweg 7 | 1437 EK Rozenburg | The Netherlands | T: +31 20 7950020 | F: +31 20 7950021

alliedtelesis.com