Technical Guide

URL Offload

Feature Overview and Configuration Guide

Introduction

This guide describes the URL offload feature, and how to configure it. You can use this feature to bypass a VPN or a proxy server for particular destinations, and then send this traffic direct to the Internet. Destinations to be bypassed (offloaded) are based on provided lists of endpoint URLs or IP addresses typically associated with a cloud based application service. You can either:

- manually configure particular endpoint URLs or IP entries that you want to offload

or

- configure a router to periodically fetch and filter URLs or IP entries from the Microsoft Office365 endpoint service.

The Microsoft Office endpoint service can then automatically update information about which URLs or IP addresses can be offloaded directly to the Internet.

This speeds up access to Microsoft Office365 cloud services when your network architecture routes all traffic to a VPN or Proxy server by default.

Contents

Products and software version that apply to this guide

This guide applies to AlliedWare Plus™ products that support URL offload, running version **5.5.0-0.1** or later.

From version **5.5.0-0.3** onwards URL offload is able to fully parse the URL data from the Microsoft endpoint data. Previously any URL retrieved from the Microsoft endpoint that was not a valid FQDN (for example *test.example.com) were marked as ‘unusable’.

To see whether your product supports URL offload, 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.

Related documents

The following documents give more information about other firewall features on AlliedWare Plus products:

- The Application Awareness Feature Overview and Configuration Guide
- The Firewall and Network Address Translation (NAT) Feature Overview and Configuration Guide
- The Software Defined WAN (SD-WAN) Feature Overview and Configuration Guide

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

Terms and concepts

The following terms and concepts are used in this feature overview guide.

Table 1: URL offload terms

TERM	DESCRIPTION
Endpoint	Describes the set of endpoint entries for a single service within the data returned by the Office365 endpoint service.
Endpoint entry	A single IP address or a URL address.
Endpoint entry filter	A filter used to exclude a single endpoint entry from the Office365 endpoint data. The CLI keyword is filter-entry.
Endpoint exclude entry	An endpoint entry that is added to the PAC file to be excluded from URL offload before the include list is processed. The CLI keyword is exclude-entry.
Endpoint filter	A filter used to include or exclude entire endpoints from the Office365 endpoint data. The CLI keyword filter is filter-endpoint.
Endpoint source	A configuration object that configures a source for endpoints. This can be the Office365 JSON service, or a list of manually configured endpoint entries.
JSON	JavaScript Object Notation. This is an open standard file format or data interchange format that uses human readable text to transmit data objects.
Microsoft Office 365 endpoints service	This is the service provided by Microsoft that provides current URLs and IP addresses in use by Office365 and related services in a machine readable JSON format. A previous iteration of this service was in XML format and has been discontinued.
PAC file	Proxy Auto-Configuration file. This is a JavaScript file used by client PCs and applications to make routing decisions based on a URL or IP address. The format was originally defined by Netscape in 1996. Since then, IPv6 has come about. Extensions to support IPv6 were proposed by Microsoft, but not accepted by Mozilla, which has resulted in inconsistent behaviour between browsers for IPv6 APIs. The URL offload feature generates a PAC file that handles this inconsistency between web browsers.
WPAD	Web Proxy Auto-Discovery Protocol. This is for client PCs to automatically find the PAC file for the network. For the first try to find the PAC file, URL uses DHCP option 252. If this doesn't work, it looks for a host with the DNS name WPAD in the local domain containing a file named 'wpad.dat' at the root directory on port 80.

Usage

- The URL offload feature can be used as an alternative to SD-WAN DPI Learning for client PCs accessing the Office365 endpoint service.

What is URL offload?

This feature is useful to speed up access to cloud services when your network architecture routes all traffic via a VPN, or to a proxy server by default. Use this feature to bypass a proxy or VPN link for certain URLs/IPs, by offloading them directly to an Internet link instead. This improves the performance of cloud services, reduces the bandwidth demands on VPN links, and reduces the session load on proxy servers.

This feature fetches endpoint data about which URLs and IP addresses need to be offloaded from an ‘endpoints service’. Currently, the only provider that is supported is the Microsoft Office365 endpoints service. It is also a reliable way of fetching all of the endpoints in use by Microsoft Office365 associated with a Content Delivery Network (CDN).

The endpoint data can then be used to automatically generate and serve a Proxy Auto-Configuration (PAC) file to client PCs. The PAC file is configured as part of the DHCP server configuration, and is downloaded by clients served directly from the router. You can use a default template, or you can configure a custom template for the PAC file. This feature automatically keeps the PAC file used by network clients up to date, removing this burden from a network administrator.

When configured, URL offloading also automatically generates dynamic firewall entities based on the endpoints data. This allows a network administrator to easily configure firewall filtering and policy based routing based on the endpoints data. This secures the network against client PCs trying to bypass a proxy or VPN link without authorization.

How does URL offload work?

Microsoft provides an endpoint service that returns URLs and IP addresses currently in use, and organizes this data into categories. This is provided in JavaScript Object Notation (JSON) format. You can configure URL offload to periodically fetch the data from this service. From this data, a list is built of URL and IP entries to be offloaded, rather than sent to a VPN or Proxy server. Filtering capabilities are provided to allow you to restrict which addresses from the service can, or cannot be offloaded.

This dynamic endpoint data is used to generate a PAC file that can be served to client PCs via a DHCP option. This allows the client PC to route traffic either to a proxy/VPN, or direct to the Internet. This avoids a network administrator having to manually copy PAC files to individual client PCs.

However, this doesn't allow the router to decide what traffic will be allowed direct to the Internet. This poses some security concerns for a network administrator if PAC files located on client PCs are removed, corrupted or bypassed. To protect the network from this improper client behavior, the data is also used to generate dynamic ‘entity’ configuration. This is then used by the router to filter or policy route traffic based on the fetched endpoints.

URL offload performs the following functions:

- Fetches and filters endpoints from an endpoint service and keeps them up to date.
- Generates a PAC file which can be downloaded by client PCs via DHCP (WPAD option 252). This prevents the client PCs from sending affected URLs to the proxy/VPN server.
- Only allows traffic that matches the configured endpoints to be sent directly to the Internet.
- Policy routes and filters traffic based on whether traffic matches configured endpoints.

Configuration

To configure URL offload follow the steps below:

1. Configure a route to the Internet and DNS server

A default route is needed so that the feature can perform DNS lookup to the endpoint service URL and fetch the Office365 endpoint information. For examples, see **11. Configuration examples**.

2. Configure endpoint sources and associated filters

This is where the feature will fetch and manage endpoints for a particular service.

Step 1: **Create endpoint source**

This is the configuration entity used to hold configuration for the Microsoft Office365 endpoint source. The type is user selectable. The command is **endpoint-source**.

Syntax

```
endpoint-source <name> type {office365|manual}
no endpoint-source <name> type {office365|manual}
```

Use the **no** variant of this command to remove an endpoint source name and type.

Example In this example, the name of the endpoint source identifier is ‘worldwide’, and the type selected is ‘office365’:

```
awplus#configure terminal
awplus(config)#url-offload
awplus(config-url-offload)#endpoint-source worldwide type office365
awplus(config-endpoint-office365)#
```

Step 2: **Set the URL for the endpoint source**

This is the URL used as the source of the endpoint information. The command is **url (endpoint office365)**.

Syntax

```
url <url>
no url
```

Use the **no** variant of this command to remove a configured URL as the source for the Office365 endpoints service.

Example To set the URL 'https://endpoints.office.com/endpoints/worldwide':

```
awplus(config-endpoint-office365)#url https://endpoints.office.com/
endpoints/worldwide
```

At this point, if the router has Internet connectivity, you can check that the data can be fetched successfully, by exiting configuration mode and using the commands **url-offload update-now** to trigger a manual update attempt, and then **show url-offload endpoint-source office365 raw-data**. For example:

```
awplus(config-endpoint-office365)#exit
awplus#url-offload update-now
awplus#show url-offload endpoint-source office365 worldwide raw-data
```

If a large amount of output is displayed on the console, this means that the data has been fetched successfully.

Step 3: **Configure filtering for the endpoint source**

Re-enter configuration mode for the endpoint source to configure filtering. By default, no entries are included:

```
awplus#configure terminal
awplus(config)#url-offload
awplus(config-url-offload)#endpoint-source worldwide type office365
awplus(config-endpoint-office365)#
```

The Office365 endpoint information contains data for a large number of different services. For some endpoints, this includes URL entries for 3rd party services, for example, Facebook, Dropbox or Google. For this reason, it may not be desirable for a network administrator to include all of the entries of this information in the list of URLs to be sent directly to the Internet.

There are two commands to filter the endpoint information, **filter-endpoint include-all** and **filter-endpoint**.

The following **filter-endpoint include-all** command includes all endpoints in the data retrieved from the Office365 endpoint service. This will create quite a large PAC file and is unlikely to be the desired end result. But, this can be used to just exclude specific entries, rather than to build a list of things to include.

Syntax

```
filter-endpoint include all
no filter-endpoint include all
```

Use the **no** variant of this command to disable this filter.

The following **filter-endpoint** commands include/exclude specific endpoints in the data retrieved from the Office365 endpoint service. Exclude filters take precedence over include filters. Using exclude here, removes an endpoint from the list of included endpoints. Include adds an endpoint to the list of included endpoints. The filter commands are designed to be generic enough to be flexible.

Syntax

```
filter-endpoint {include|exclude} key <key> boolean {true|false}
filter-endpoint {include|exclude} key <key> string <value>
filter-endpoint {include|exclude} key <key> integer <value>
no filter-endpoint
```

Use the **no** variant of this command to remove all filtering.

Endpoint example

The following example shows an endpoint for the endpoint source name ‘test’:

```
awplus#show url-offload endpoint-source office365 test raw-data
[
  {
    "id": 1,
    "serviceArea": "Exchange",
    "serviceAreaDisplayName": "Exchange Online",
    "urls": [
      "outlook.office.com",
      "outlook.office365.com"
    ],
    "ips": [
      "13.107.6.152/31",
      ...
      "204.79.197.215/32",
      "2603:1006::/40",
      ...
      "2620:1ec:a92::153/128",
      "2a01:111:f400::/48"
    ],
    "tcpPorts": "80,443",
    "expressRoute": true,
    "category": "Optimize",
    "required": true
  },
```

The data fetched from the endpoint service includes approximately 150 endpoints like this with varying numbers of entries in each. The filtering commands can be used to add or remove endpoints that match certain criteria.

Examples

To include all endpoints with the key ‘required’ set to ‘true’, use the command:

```
awplus(config-endpoint-office365)#filter-endpoint include key required
boolean true
```

To exclude the endpoint entry with ‘id’ 123, use the command:

```
awplus(config-endpoint-office365)#filter-endpoint exclude key id integer 123
```

To include endpoint entries with ‘category’ ‘Optimize’, use the command:

```
awplus(config-endpoint-office365)#filter-endpoint include key category
string Optimize
```

Once the endpoints have been included or excluded, the included endpoints are processed into a list of endpoint entries, each containing a URL or an IP address. Further filtering can then be done on this list with the commands **filter-entry exclude** and **filter-entry exclude type**. Use these commands to remove specific entries from the list.

Syntax

```
filter-entry exclude {ip|ipv6|url} <value>
no filter-entry exclude {ip|ipv6|url} <value>
filter-entry exclude type {ip|ipv6|url}
no filter-entry exclude type {ip|ipv6|url}
```

Use the **no** variants of these commands to remove configured filters.

Examples To remove the URL ‘www.example.com’ from the list. This is sent straight to the proxy before processing include entries. Use the command:

```
awplus(config-endpoint-office365)#filter-entry exclude url www.example.com
```

To remove the URL ‘example.com’ from the list, use the command:

```
awplus(config-endpoint-office365)#no filter-entry exclude url
www.example.com
```

To remove all IP entries from being stored and included in the PAC file list. This is sent straight to the proxy before processing include entries. Use the command:

```
awplus(config-endpoint-office365)#filter-entry exclude ip
```

To stop excluding IP entries, use the command:

```
awplus(config-endpoint-office365)#no filter-entry exclude type ip
```

The filtering commands above only add or remove entries to the list of included entries. Once the list is complete, a network administrator may still want to add entries to specifically exclude from URL offload. For example, if an endpoint includes a wildcard for an entire domain, but an administrator wants a particular host in that domain to still communicate via the tunnel/proxy.

You could configure an exclude entry for that particular host. This could also be done as part of configuring a separate manual endpoint, but in some cases it is clearer to link the exclude entry to the Office365 source in the configuration. You can configure this with the **exclude-entry** command.

Syntax

```
exclude-entry exclude {ip|ipv6|url} <value>
no exclude-entry exclude {ip|ipv6|url} <value>
```

Use the **no** variant of this command to remove the exclusion.

Example To explicitly exclude URL ‘www.example.com’ results in entries going straight to the proxy before processing include entries:

```
awplus(config-endpoint-office365)#exclude-entry url www.example.com
```

Step 4: **Configure update interval for the endpoint source**

Changes to the Office365 IP addresses and URLs are typically published by Microsoft near the last day of each month. This may differ due to operational, support or security requirements. Version checking is used to advise any changes to endpoint data that may need to be obtained via JSON.

Use the command **update-interval** to periodically update the endpoint information and generated PAC file. An update interval must be configured for the endpoint source. The minimum update interval is hourly as recommended by Microsoft. The time of the update is not fixed. After each update, the device will wait for this long before doing the next update. If an update interval is configured, changing configuration will also trigger an update.

Syntax

```
update-interval {days <1-30>|hours <1-720>|minutes <1-43200>}
no update-interval
```

Use the **no** variant of this command to disable automatic updates.

Example To configure the update interval to one hour, use the commands:

```
awplus#configure terminal
awplus(config)#url-offload
awplus(config-url-offload)#endpoint-source worldwide type office365
awplus(config-endpoint-office365)#update-interval hours 1
```

3. Configure policy based routing and filtering

The URL offload feature generates some dynamic firewall entities. These can be used to policy route or filter traffic that matches the endpoint information irrespective of whether a client PC has a PAC file applied or not. In this example, the client PCs are located in a pre-existing entity labeled ‘private.lan’.

To configure all matching entries to be forwarded to an Internet gateway address ‘192.168.1.1’ and all specifically excluded traffic or any other traffic to gateway address ‘192.168.2.1’ (for example, proxy or tunnel), use the following commands:

```
awplus#configure terminal
awplus(config)#policy-based-routing
awplus(config-pbr)#ip policy-route 1 from private.lan to URL_Offload.exclude_entries nexthop
192.168.2.1
awplus(config-pbr)#ip policy-route 2 from private.lan to URL_Offload.include_entries nexthop
192.168.1.1
awplus(config-pbr)#ip policy-route 3 from private.lan to any nexthop 192.168.2.1
awplus(config-pbr)#policy-based-routing enable
```

4. Configure a firewall

In some cases a network administrator may want to allow all Office365 traffic and block all other traffic using a firewall. For example, on a router acting as a boundary device with a single internal/external interface. In this situation Policy Based Routing (PBR) and/or PAC file distribution is performed on a separate device:

```
awplus#configure terminal
awplus(config)#firewall
awplus(config-firewall)#rule 10 deny any from private.lan to URL_Offload.exclude_entries
awplus(config-firewall)#rule 20 permit any from private.lan to URL_Offload.include_entries
awplus(config-firewall)#rule 30 deny any from private.lan to public.wan
```

Also, if you are using a firewall, it may be necessary to configure rules to permit the traffic originating from the router WAN source address to access external HTTPS and DNS to fetch the endpoint data from the external service.

For more information about configuring entities and rules, see Firewall and Network Address Translation (NAT) Feature Overview and Configuration Guide.

5. Configure PAC file parameters

The URL offload feature can generate a proxy auto-configuration (PAC) file for use by client PCs in the network. A PAC file is used by client devices to direct traffic to the correct proxy. It is written in JavaScript with particular functions that need to be supported by the process that is directing the traffic. For example, a web browser would use the PAC file to decide whether to send requests to a proxy, or direct to the default gateway. There is documentation about PAC file formats and contents available on the Internet.

Because it is up to the client process to interpret and obey the PAC file, there are opportunities for interoperability issues or for the process to ignore the PAC file. The behavior for IPv4 addresses is reasonably well-defined, but IPv6 is handled differently between common browsers. For this reason, PAC files with IPv6 configuration often have issues with forcing traffic to go direct from some browsers. However, the PAC file generated by the URL offload feature has been tested to correctly function with IPv6 entries on the three most common browsers (Chrome, Firefox and Edge).

The URL offload feature creates the PAC file by building some condition statements and replacing values in a template with them. There is a default template, with a user-configurable proxy address, or the user can specify a custom template. Custom templates must include the strings ‘%%INCLUDE_MATCHES%%’ and ‘%%EXCLUDE_MATCHES%%’ to be a valid template.

The contents of the current template can be shown using the command **show url-offload pac-file template**. This shows the default template if a custom template is not configured. The default template can be used as an example when constructing a custom template. If a custom template includes the string ‘%%PROXY_ADDRESS%%’, it will be replaced by the proxy address configured in the URL offload configuration, but it is not mandatory to include this field for custom templates. Some helper functions used in the condition statements will also be added at the start of the template.

Default template Here is an example of the default template:

```
awplus#show url-offload pac-file template
function FindProxyForURLEx(url, host)
{
    var direct = "DIRECT";
    var proxyServer = "PROXY %%PROXY_ADDRESS%%";
    var host_ips;

    /* Host is on local network (no dots in name) */
    if (isPlainHostName (host))
    {
        return direct;
    }

    /* Exclude matches */
    if(%%EXCLUDE_MATCHES%%)
    {
        return proxyServer;
    }

    /* Include matches */
    if(%%INCLUDE_MATCHES%%)
    {
        return direct;
    }

    return proxyServer;
}

function FindProxyForURL(url, host)
{
    return FindProxyForURLEx (url, host);
}
```

Step 1: Setting the proxy address

The minimum configuration for generating the PAC file is to set the proxy address. The string used is not checked and replaces the '%%PROXY_ADDRESS%%' string in the template. Use the command **pac-file proxy-address**.

Syntax

```
awplus(config-url-offload)#pac-file proxy-address <address>
awplus(config-url-offload)#no pac-file proxy-address
```

Use the **no** variant of this command to remove the configured proxy address.

Example For example, to configure the proxy address '10.10.10.10' listening on port '8080':

```
awplus#configure terminal
awplus(config)#url-offload
awplus(config-url-offload)#pac-file proxy-address 10.10.10.10:8080
```

Step 2: Using a custom template

A custom template can be created and stored in the device flash, or served via HTTP from a remote server. The template file is fetched each time the PAC file is updated (with a 1 minute cache). Use the command **pac-file template**.

Syntax

```
awplus(config-url-offload)#pac-file template {local|remote} <url>
awplus(config-url-offload)#no pac-file template
```

Use the **no** variant of this command to remove the configured proxy address.

Examples To configure the device to use a template called ‘wpad.template’ stored in the local flash, use the commands:

```
awplus#configure terminal
awplus(config)#url-offload
awplus(config-url-offload)#pac-file template local flash:/wpad.template
```

To revert back to the default template, use the commands:

```
awplus#configure terminal
awplus(config)#url-offload
awplus(config-url-offload)#no pac-file template
```

6. Configure PAC file hosting

To make the PAC file available for client PCs to download, it needs to be hosted by the router. By default, it is not hosted. The PAC file may be hosted on the same port as the main management HTTP server or a different port. The reason that it may be desirable to host it on a separate port is because all clients need access to download the PAC file, and a network administrator may wish to limit access to the main HTTP management service. Use the command **pac-file http-server port**.

Caution: Configuring a port that is in use by another service may cause the device to restart.

Syntax

```
awplus(config-url-offload)#pac-file http-server port <port>
awplus(config-url-offload)#no pac-file http-server
```

Use the **no** variant of this command to disable serving URL offload PAC files.

Examples To configure and enable PAC file hosting on port 80, use the following commands:

```
awplus#configure terminal
awplus(config)#url-offload
awplus(config-url-offload)#pac-file http-server port 80
```

Note: Configuring the hosting on port 80 may result in a redirect to port 443. When hosting the PAC file is enabled, the PAC file is hosted at ‘<router_address>:<port>/wpad.dat’.

For example, to disable the hosting of the PAC file, use the commands:

```
awplus#configure terminal
awplus(config)#url-offload
awplus(config-url-offload)#no pac-file http-server
```

7. Configure DHCP server WPAD option

Informing the client PCs where to download the PAC file is done via DHCP option 252. The router DHCP server is configured to serve PAC files to clients. Alternatively the router DHCP server can act purely as a forwarding agent to inform clients to obtain PAC files from an external DHCP server dedicated for this purpose.

To configure an AlliedWare Plus DHCP server to provide option 252, the following steps need to be taken:

Step 1:

Configure option 252 as an ASCII text option with the name ‘wpad’. The name is user-selectable:

```
awplus#configure terminal
awplus(config)#ip dhcp option 252 name wpad ascii
```

Step 2:

Create a DHCP pool for the address range to be served and set the ‘wpad’ option to point to ‘wpad.dat’ on the router. Note that the network and mask for the pool need to be configured before configuring other options:

```
awplus#configure terminal
awplus(config)#ip dhcp pool test
awplus(dhcp-config)#network 192.168.2.0 255.255.255.0
awplus(dhcp-config)#option wpad http://192.168.2.1/wpad.dat
```

If there are multiple prefixes (subnets) being served from the router, this will need to be done for each prefix, configuring the ‘wpad’ option with the correct router address for each one. If you are using an external DHCP server, please review the documentation for the server to see how to configure option 252.

8. Configure clients to use PAC file

The details of configuring clients to use a PAC file are beyond the scope of this guide. Generally if the clients are using DHCP, it should be enough to set the proxy configuration to ‘automatic’ or equivalent. Alternatively, a URL for the PAC file can usually be entered. Proxy settings can usually be applied at a system-wide level or configured in the browser.

PAC files are stored in the browser cache within each client PC. Over time they will age and become stale. When the cache entry expires, the client PC browser should automatically check for and download the latest version of the PAC file. This assumes the most recent cumulative security update is installed into your client PC.

The following table shows where to find proxy settings:

Table 2: Where to find proxy settings

APPLICATION	WHERE TO FIND PROXY SETTINGS
Ubantu	Settings -> Network -> Network proxy
Windows 10	Settings -> Network and Internet -> Proxy
Firefox	Preferences -> Options -> General -> Network Settings
Chrome	Settings -> Advanced -> System -> Open your computer's proxy settings
Internet Explorer	Settings -> Internet Options

9. Force an update

To manually trigger an update of the PAC file, use the command **url-offload update now**:

```
awplus#url-offload update-now
```

It is not normally necessary to use this command, as updates will occur when configuration is changed, and at the configured update interval.

10. Automatic updates for the parsing functionality

The format used by Office365 may change. A resource is available for you to download from the Allied Telesis update server. This resource updates the URL offload parsing functionality to understand the new data format. To enable this functionality, use the command **parser-updates enable**:

```
awplus#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
awplus(config)#url-offload
awplus(config-url-offload)#parser-updates enable
```

The default polling interval for checking updates is 60 minutes. To change the polling interval, use the command **parser-updates interval**.

Syntax

```
parser-updates interval {minutes <10-525600>|hours <1-8760>|days <1-365>|
weeks <1-52>}
no parser-updates interval
```

Use the **no** variant of this command to set the polling interval back to the default of 60 minutes.

Example To configure the interval to update every 180 minutes, use the command:

```
awplus#configure terminal
awplus(config)#url-offload
awplus(config-url-offload)#parser-updates interval minutes 180
```

11. Configuration examples

Each of the following examples shows how to configure each component of URL offload. Each component can be used in isolation, or combined.

Example 1 The following example creates, hosts and distributes a PAC file using all endpoints listed by the Office365 endpoint service. This is updated hourly:

```
url-offload
 endpoint-source test type office365
  url https://endpoints.office.com/endpoints/worldwide
  update-interval hours 1
 filter-endpoint include all
 pac-file proxy-address 192.168.3.254:8080
 pac-file http-server port 80
!
!
ip domain-lookup
!
ip dhcp option 252 name wpad ascii
!

ip dhcp pool test
 network 192.168.2.0 255.255.255.0
 option wpad http://192.168.2.1/wpad.dat
!
!
!
service dhcp-server
!
interface eth1
 description Internet
 ip address 192.168.1.2/24
!
interface vlan1
 ip address 192.168.2.1/24
!
interface vlan2
 description proxy vlan
 ip address 192.168.3.1/24
!
#route to Internet json service.
ip route 0.0.0.0/0 192.168.1.1
```

Example 2 The following filtering example only includes URLs from the Office365 endpoint service marked with category ‘Optimize’:

```
url-offload
 endpoint-source test type office365
  url https://endpoints.office.com/endpoints/worldwide
  update-interval hours 1
 filter-endpoint include key category string Optimize
 pac-file proxy-address 192.168.3.1:8080
 pac-file http-server port 80
!
!
ip domain-lookup
!
ip dhcp option 252 name wpad ascii
!

ip dhcp pool test
 network 192.168.2.0 255.255.255.0
 option wpad http://192.168.2.1/wpad.dat
!
!
!
service dhcp-server
!
interface eth1
 description Internet
 ip address 192.168.1.2/24
!
interface vlan1
 description Internal LAN
 ip address 192.168.2.1/24
!
interface vlan2
 description proxy vlan
 ip address 192.168.3.1/24
!
#route to internet for json service
ip route 0.0.0.0/0 192.168.1.1
```

Example 3 The following example configures the policy based routing component based on the entities dynamically created by the URL offload JSON download. Entries included for URL offload are sent direct to the local Internet gateway, whereas all other traffic is sent to a VPN link. Full tunnel configuration is not included.

```
zone private
 network lan
  ip subnet 192.168.2.0/24 interface vlan1
!
url-offload
 endpoint-source test type office365
  url https://endpoints.office.com/endpoints/worldwide
  update-interval hours 1
  filter-endpoint include key category string Optimize
!
policy-based-routing
 ip policy-route 10 from private.lan to URL_Offload.exclude_entries nexthop
tunnel0
 ip policy-route 20 from private.lan to URL_Offload.include_entries nexthop
192.168.1.1
 ip policy-route 30 from private.lan nexthop tunnel0
!
ip name-server 192.168.2.15
ip domain-lookup
!
!
interface eth1
 description Internet
 ip address 192.168.1.2/24
!
interface vlan1
 description Internal LAN
 ip address 192.168.2.1/24
!
interface tunnel0
 description VPN
 ip address 192.168.3.1/24
!
ip route 0.0.0.0/0 192.168.1.1
#Default route to Internet to access json service. Any traffic not matching
policy routing rules or originating from the router will used this route.
!
```

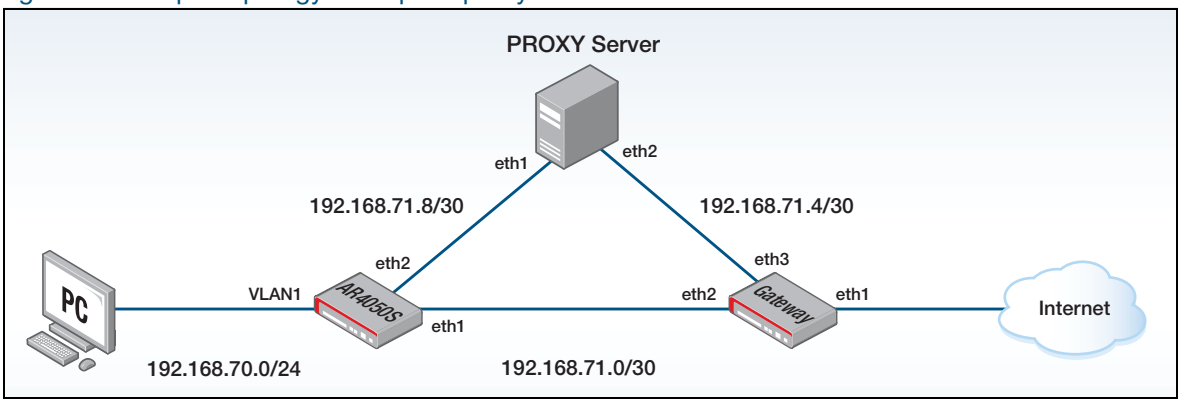
Example 4 The following example shows firewall rules to only allow URL offload traffic to go out to the Internet. The first firewall rule permits traffic originating from the router to access the Internet. This allows URL offload to fetch endpoint information, and allows access to the update manager and DNS services.

```
zone private
 network lan
  ip subnet 192.168.2.0/24 interface vlan1
!
zone public
 network INTERNET
  ip subnet 0.0.0.0/0 interface eth1
!
zone ROUTER
 network EXTERNAL
  ip subnet 192.168.1.0/24
  host EXTERNAL_INT
   ip address 192.168.1.2
!
firewall
 rule 10 permit any from ROUTER.EXTERNAL.EXTERNAL_INT to public
 rule 20 deny any from private.lan to URL_Offload.exclude_entries
 rule 30 permit any from private.lan to URL_Offload.include_entries
 rule 40 deny any from private.lan to public
 protect
!
url-offload
 endpoint-source test type office365
  url https://endpoints.office.com/endpoints/worldwide
  update-interval hours 1
  filter-endpoint include key category string Optimize
!
ip name-server 192.168.2.15
ip domain-lookup
!
!
ip dhcp pool test
 network 192.168.2.0 255.255.255.0
!
interface eth1
 description Internet
 ip address 192.168.1.2/24
!
interface vlan1
 description Internal LAN
 ip address 192.168.2.16/24
!
ip route 0.0.0.0/0 192.168.1.1
!
```

Example 5 The following example shows a configuration where an explicit proxy server is used. Configuration is required on the endpoint devices using it. The device ‘AR4050S’ develops the dynamic URL offload entity and PAC file from the endpoint source ‘worldwide’. ‘AR4050S’ functions as the DHCP server for endpoint devices connected to vlan1. WPAD distributes the built PAC files with the DHCP clients learning the existence and location of the PAC file via DHCP option 252, before using HTTP to download the PAC file from ‘AR4050S’, served from listen port 8080.

After applying the proxy settings specified PAC file, all HTTP and HTTPS traffic which is not associated with Office365 is sent to the specified proxy address ‘192.168.71.9:3128’. Office365 related traffic is sent unchanged. If a user either maliciously or unintentionally configures their system to ignore the proxy settings described in the PAC file, then all web traffic is sent unedited, potentially bypassing the proxy server. To stop this from happening, ‘AR4050S’ is configured with firewall rules that block all HTTP and HTTPS traffic that doesn’t have a destination address described by the dynamic URL offload entity.

Figure 1: Example topology for explicit proxy server with IPv4



.

```
hostname AR4050S
!
zone LAN
 network INTERNAL_LINKS
  ip subnet 192.168.71.0/30
  ip subnet 192.168.71.4/30
 network PROXY
  ip subnet 192.168.71.8/30
 network VLAN1
  ip subnet 192.168.70.0/24 interface vlan1
  host GATEWAY
   ip address 192.168.70.1
!
zone WAN
 network ANY
  ip subnet 0.0.0.0/0 interface eth1
!
application proxy
 protocol tcp
 dport 3128
!
firewall
 rule 10 permit any from LAN.INTERNAL_LINKS to LAN.INTERNAL_LINKS
 rule 20 permit proxy from LAN.VLAN1 to LAN.PROXY
 rule 30 permit http from LAN.VLAN1 to URL_Offload.include_entries
 rule 40 permit https from LAN.VLAN1 to URL_Offload.include_entries
 rule 50 permit any from LAN.VLAN1 to LAN.VLAN1.GATEWAY
 rule 60 deny http from LAN.VLAN1 to WAN.ANY log
 rule 70 deny https from LAN.VLAN1 to WAN.ANY log
 rule 80 permit any from LAN to WAN.ANY
 protect
!
```

```
!
!
service url-offload
url-offload
 endpoint-source WORLDWIDE type office365
  url https://endpoints.office.com/endpoints/worldwide
  update-interval hours 12
  filter-endpoint include key required boolean true
  filter-entry exclude type ipv6
  filter-entry exclude type url
 pac-file proxy-address 192.168.71.9:3128
 pac-file http-server port 8080
!
!
!
ip name-server 8.8.8.8
ip domain-lookup
!
ip dhcp option 252 name wpad ascii
!
ip dhcp pool VLAN1
 network 192.168.70.0 255.255.255.0
 range 192.168.70.10 192.168.70.200
 dns-server 192.168.70.1
 default-router 192.168.70.1
 option wpad http://192.168.70.1:8080/wpad.dat
!
!
!
service dhcp-server
!
interface port1.0.1-1.0.8
 switchport
 switchport mode access
!
interface eth1
 ip address 192.168.71.2/30
!
interface eth2
 ip address 192.168.71.8/30
!
interface vlan1
 ip address 192.168.70.1/24
!
!
ip dns forwarding
!
ip route 0.0.0.0/0 192.168.71.1
```

Example 6 The following configuration example is designed for you to use with a transparent web proxy. This means no configuration is necessary on the endpoint devices. In the previous example the device ‘AR4050S’ develops the dynamic URL offload entity from the endpoint source ‘worldwide’. Unlike in the explicit proxy example, all web traffic including Office365 traffic, is sent by the endpoint device unchanged. This endpoint device traffic is received by the device ‘AR4050S’ and policy routed. So, Office365 traffic hits the first rule and is sent directly to the gateway device. All other web traffic then hits the bottom two rules and is redirected to the proxy server.

```
hostname AR4050S
!
zone LAN
 network VLAN1
  ip subnet 192.168.70.0/24
!
zone WAN
 network DIRECT
  ip subnet 0.0.0.0/0 interface eth2
!
!
service url-offload
url-offload
 endpoint-source WORLDWIDE type office365
  url https://endpoints.office.com/endpoints/worldwide
  update-interval hours 12
  filter-endpoint include key required boolean true
  filter-entry exclude type ipv6
  filter-entry exclude type url
!
!
policy-based-routing
 ip policy-route 10 from LAN to URL_Offload.include_entries nexthop
102.168.71.1
 ip policy-route 20 match http from LAN to WAN.DIRECT nexthop 192.168.71.9
 ip policy-route 30 match https from LAN to WAN.DIRECT nexthop 192.168.71.9
 policy-based-routing enable
!
ip name-server 8.8.8.8
ip domain-lookup
!
!
ip dhcp pool VLAN1
 network 192.168.70.0 255.255.255.0
 range 192.168.70.10 192.168.70.200
 dns-server 192.168.70.1
 default-router 192.168.70.1
!
!
!
service dhcp-server
!
interface port1.0.1-1.0.8
 switchport
 switchport mode access
!
interface eth1
 ip address 192.168.71.2/30
!
interface eth2
 ip address 192.168.71.8/30
!
interface vlan1
 ip address 192.168.70.1/24
!
!
ip dns forwarding
!
ip route 0.0.0.0/0 192.168.71.1
```

Example 7 The following configuration is designed to use IPv6 hosts with an explicit proxy server. This means a proxy server in which configuration is necessary on end devices using the proxy server. The device ‘AR4050S’ develops the dynamic URL offload entity and PAC file from the endpoint source ‘WORLDWIDE’. ‘AR4050S’ is configured as a stateless DHCPv6 server, with ‘AR4050S’ distributing only DNS server address of FD00:1::1 as well as the domain ‘test.lc’. The end hosts auto-configure addressing using SLAAC.

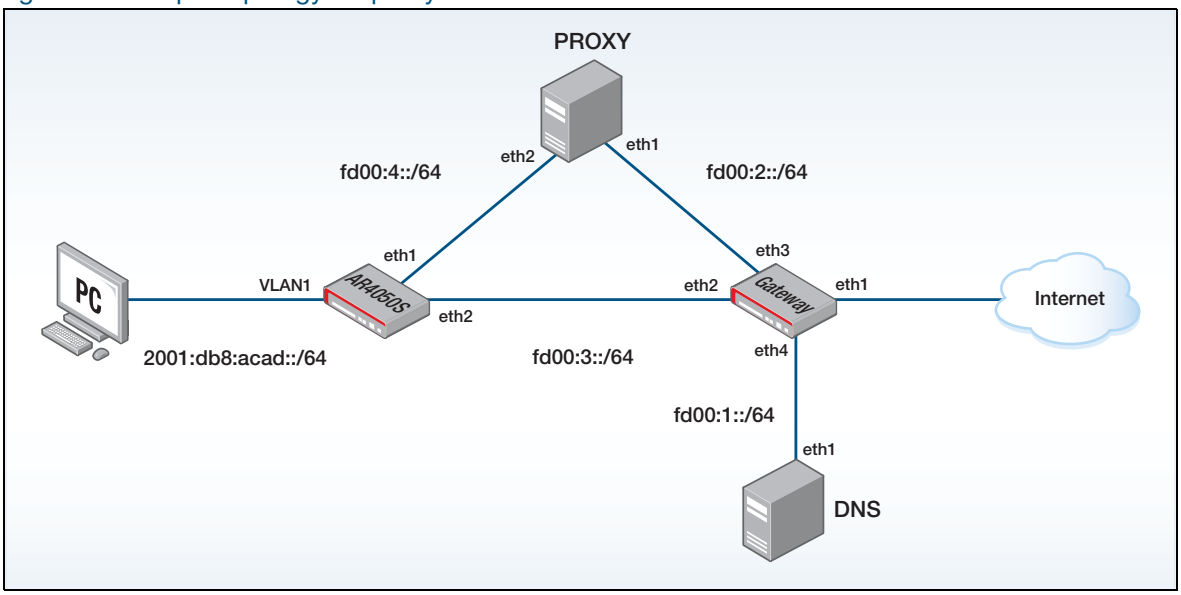
Unlike previous examples, this network is configured to discover proxy settings using DNS. When a user opens a web browser, assuming proxy auto-discovery is enabled, then the end host will send a DNS request for a FQDN with a prefix of ‘wpad’ and a suffix of the defined domain. In this case the request will be sent to attempt to resolve the FQDN of ‘wpad.test.lc’.

On resolution, the end host knows the existence and location of the PAC file. The end host then uses HTTP to download the PAC file from the resolved IP, in this case ‘2001:db8:acad::1’. As there is no mechanism for defining a specific port, port 80 must be used. Because of this, it is necessary to rebind the port used for HTTP management of the device, regardless of if the device has HTTP management enabled or not.

After applying the proxy settings specified PAC file, all HTTP/HTTPS traffic which is not associated with office365 will be sent to the specified proxy server at ‘proxy.test.lc:3128’. Office365 related traffic will be sent unchanged.

If the end user, either maliciously or unintentionally, configures their system to ignore the proxy settings described in the PAC file, then all web traffic will be sent unedited, potentially bypassing the proxy server. To stop this from occurring ‘AR4050S’ has been configured with firewall rules which block all HTTP/HTTPS traffic which doesn’t have a destination address described by the dynamic URL offload entity.

Figure 2: Example topology for proxy server with IPv6



.

```
hostname AR4050S
!
no banner motd
!
service http
http port 8080
!
!
zone LAN
 network INTERNAL_LINKS
  ip subnet 192.168.71.4/30
  ipv6 subnet fd00:3::/64
  ipv6 subnet fe80::/16
 network MULTICAST
  ipv6 subnet ff02::/16
 network PROXY
  ipv6 subnet fd00:4::/64
 network VLAN1
  ipv6 subnet 2001:db8:acad::/64 interface vlan1
  host GATEWAY
   ipv6 address 2001:db8:acad::1
!
zone WAN
 network ANY
  ip subnet 0.0.0.0/0 interface eth1
  ipv6 subnet ::/0 interface eth1
!
application proxy
 protocol tcp
 dport 3128
!
firewall
 rule 10 permit any from LAN.INTERNAL_LINKS to LAN.INTERNAL_LINKS
 rule 20 permit any from LAN.INTERNAL_LINKS to LAN.MULTICAST
 rule 30 permit http from LAN.VLAN1 to LAN.PROXY
 rule 40 permit https from LAN.VLAN1 to LAN.PROXY
 rule 50 permit proxy from LAN.VLAN1 to LAN.PROXY
 rule 60 permit http from LAN.VLAN1 to URL_Offload.include_entries
 rule 61 permit http from LAN.VLAN1 to
URL_Offload.include_entries.fqdn_entries
 rule 70 permit https from LAN.VLAN1 to URL_Offload.include_entries
 rule 72 permit https from LAN.VLAN1 to
URL_Offload.include_entries.fqdn_entries
 rule 80 permit any from LAN.VLAN1 to LAN.VLAN1.GATEWAY
 rule 90 deny http from LAN.VLAN1 to WAN.ANY log
 rule 100 deny https from LAN.VLAN1 to WAN.ANY log
 rule 110 permit any from LAN to WAN.ANY
 protect
!
!
!
url-offload
 endpoint-source WORLDWIDE type office365
  url https://endpoints.office.com/endpoints/worldwide
  update-interval hours 12
  filter-endpoint include all
  filter-entry exclude type url
 pac-file proxy-address proxy.test.lc:3128
 pac-file http-server port 80
service url-offload
!
!
!
ip name-server fd00:1::1
ip domain-lookup
!
!
!
!
ipv6 dhcp pool VLAN1
 dns-server 2001:db8:acad::1
 domain-name test.lc
!
service dhcp-server
```

.

```
!
!
!
!
interface eth1
 description PROXY
 ipv6 address fd00:4::2/64
!
interface eth2
 description INTRANET
 ip address 192.168.71.6/30
 ipv6 address fd00:3::2/64
!
interface lo
 ip address 172.20.1.4/32
!
interface vlan1
 ipv6 address 2001:db8:acad::1/64
 no ipv6 nd suppress-ra
 ipv6 nd other-config-flag
 ipv6 dhcp server VLAN1
!
ipv6 forwarding
!
!
ip dns forwarding
ip dns forwarding cache size 10000 timeout 1800
!
ip route 0.0.0.0/0 192.168.71.5
ipv6 route ::/0 fd00:3::1
!
```

Show commands

Use the following show commands to monitor what is going on with your configured URL offload feature.

show running-config url-offload

Use this command to show the contents of the running-config for the URL offload feature. This is what is saved to the configuration file after configuration.

show url-offload endpoint-source

Use this command to show the list of endpoint sources and any configured parameters global to the source. This does not include filters or entries. For Office365 sources, the 'Update time' is the time when the source was last updated:

```
awplus#show url-offload endpoint-source

Microsoft Office365 endpoint sources:

Name: test
 URL: https://endpoints.office.com/endpoints/worldwide
 Update interval: 1 hours
 Update time: 2019-10-16T11:14:55Z

Manual endpoint sources:

Name: manual
```

show url-offload endpoint-source office365 raw-data

Use this command to show the JSON data fetched from the Microsoft Office365 endpoints service. Use this to work out what filtering is required. The output is quite long. URL and IPv4/IPv6 prefixes are converted to 'endpoint entries':

```
awplus#show url-offload endpoint-source office365 raw-data

[
  {
    "id": 1,
    "serviceArea": "Exchange",
    "serviceAreaDisplayName": "Exchange Online",
    "urls": [
      "outlook.office.com",
      "outlook.office365.com"
    ],
    "ips": [
      "13.107.6.152/31",
      "13.107.18.10/31",
      "13.107.128.0/22",
      "23.103.160.0/20",
      "40.96.0.0/13",
      "40.104.0.0/15",
      "52.96.0.0/14",
      "131.253.33.215/32",
      "132.245.0.0/16",
      "150.171.32.0/22",
      "191.234.140.0/22",
      "204.79.197.215/32",
      "2603:1006::/40",
      "2603:1016::/40",
      "2603:1026::/40",
```

```
      "2603:1026:200::/39",
      "2603:1026:400::/39",
      "2603:1026:600::/44",
      "2603:1026:620::/44",
      "2603:1026:800::/44",
      "2603:1026:820::/45",
      "2603:1036::/39",
      "2603:1036:200::/40",
      "2603:1036:400::/40",
      "2603:1036:600::/40",
      "2603:1036:800::/38",
      "2603:1036:c00::/40",
      "2603:1046::/37",
      "2603:1046:900::/40",
      "2603:1056::/40",
      "2603:1056:400::/40",
      "2603:1056:600::/40",
      "2603:1096::/38",
      "2603:1096:400::/40",
      "2603:1096:600::/40",
      "2603:1096:a00::/39",
      "2603:1096:c00::/40",
      "2603:10a6:200::/40",
      "2603:10a6:400::/40",
      "2603:10a6:600::/40",
      "2603:10a6:800::/40",
      "2603:10d6:200::/40",
      "2620:1ec:4::152/128",
      "2620:1ec:4::153/128",
      "2620:1ec:c::10/128",
      "2620:1ec:c::11/128",
      "2620:1ec:d::10/128",
      "2620:1ec:d::11/128",
      "2620:1ec:8f0::/46",
      "2620:1ec:900::/46",
      "2620:1ec:a92::152/128",
      "2620:1ec:a92::153/128",
      "2a01:111:f400::/48"
    ],
    "tcpPorts": "80,443",
    "expressRoute": true,
    "category": "Optimize",
    "required": true
  },
  ... > 100 more endpoints
]
```

show url-offload endpoint-source office365 entries

Use this command to show all entries parsed from the Office365 JSON data before filtering is applied. For example, to show entries for the single endpoint source named ‘test’:

```
awplus#show url-offload endpoint-source office365 test entries
Endpoint source: test

Entries:
Type  Value
------------------------------------------------------------------------------
ip    104.146.128.0/17
...
ip    52.96.0.0/14
ip    65.54.170.128/25
ipv6  2001:df0:d9:200::/64
ipv6  2603:1006:1400::/40
ipv6  2603:1006:2000::/48
...
ipv6  2a01:111:f406:8000::/64
ipv6  2a01:111:f406:8801::/64
ipv6  2a01:111:f406:a003::/64
ipv6  2a01:111:f406:c00::/64
...
url   ocsp.int-x3.letsencrypt.org
url   cert.int-x3.letsencrypt.org
url   *.office365.com
url   *.symcb.com
url   *.lync.com
url   *.symcd.com
url   www.youtube.com
url   *.office.com
```

show url-offload endpoint-source office365 entries filtered

Use this command to show the include and exclude entries for all Office365 endpoint sources after filtering takes place, and exclude entries are added. For example, to show filtered entries for the endpoint source ‘test’:

```
awplus#show url-offload endpoint-source office365 test entries filtered
Endpoint source: test

Include entries:
Type  Value
------------------------------------------------------------------------------
ip    104.146.128.0/17
...
ip    65.54.170.128/25
ipv6  2001:df0:d9:200::/64
...
ipv6  2603:1016:2400::/40
ipv6  2603:1016::/36
...
url   ocsp.int-x3.letsencrypt.org
...

Exclude entries:
Type  Value
------------------------------------------------------------------------------
url   mobile.facebook.com
```

show url-offload endpoint-source office365 entries unusable

Use this command to show entries parsed from the endpoints data that are part of an endpoint that matches an endpoint filter, but are not in a format expected by URL offload. For example, to show unusable entries for the endpoint source ‘test’:

```
awplus#show url-offload endpoint-source office365 test entries unusable
Endpoint source: test
Unusable entries
-------------------------------------------------------------------------------
*-files.sharepoint.com
*-myfiles.sharepoint.com
*broadcast.officeapps.live.com
*cdn.onenote.net
*excel.officeapps.live.com
*onenote.officeapps.live.com
*powerpoint.officeapps.live.com
*rtc.officeapps.live.com
*shared.officeapps.live.com
*view.officeapps.live.com
*visio.officeapps.live.com
*word-edit.officeapps.live.com
*word-view.officeapps.live.com
```

show url-offload endpoint-source manual entries

Use this command to show the entries configured for a manual endpoint source. For example, to show manually configured entries for the endpoint source ‘test’:

```
awplus#show url-offload endpoint-source manual test entries
Endpoint source: test
Include Entries:
ID    Type  Value
-------------------------------------------------------------------------------
1     url   example.com
2     url   example2.com
3     ip    10.10.10.10/32

Exclude Entries:
ID    Type  Value
-------------------------------------------------------------------------------
1     url   exclude.example.com
```

show url-offload pac-file template

Shows the contents of the default or currently configured PAC file template. The output is shown and explained in section **5. Configure PAC file parameters**.

show url-offload pac-file

Use this command to show the current contents of the PAC file. This shows the PAC file that will be served to users:

```
awplus#show url-offload pac-file
function UO_isResolvable(host)
{
    return (typeof isResolvableEx === "function" ? isResolvableEx(host):
                                                   isResolvable(host));
}

function UO_dnsResolve(host)
{
    return (typeof dnsResolveEx === "function" ? dnsResolveEx(host):
                                                 dnsResolve(host));
}

function UO_isInNet(host_ips, network, mask, full_addr)
{
    const addrList = host_ips.split(";");
    for(var i = 0; i < addrList.length; i++)
    {
        const match = (typeof isInNetEx === "function" ?
                            isInNetEx(addrList[i], full_addr):
                            isInNet(addrList[i], network, mask));
        if (match)
        {
            return true;
        }
    }
    return false;
}

function FindProxyForURLEx(url, host)
{
    var direct = "DIRECT";
    var proxyServer = "PROXY 10.10.10.10:80";
    var host_ips;

    /* Host is on local network (no dots in name) */
    if (isPlainHostName (host))
    {
        return direct;
    }

    /* Exclude matches */
    if(shExpMatch (host, "exclude.example.com")
       || (UO_isResolvable(host) && (host_ips = UO_dnsResolve(host))
           && (UO_isInNet(host_ips, "10.10.10.10", "255.255.255.255",
"10.10.10.10/32"))))
    {
        return proxyServer;
    }

    /* Include matches */
    if(shExpMatch (host, "*.example.com")
       || shExpMatch (host, "*.sharepoint.com")
       || shExpMatch (host, "outlook.office.com")
       || shExpMatch (host, "outlook.office365.com")
       || (UO_isResolvable(host) && (host_ips = UO_dnsResolve(host))
           && (UO_isInNet(host_ips, "104.146.128.0", "255.255.128.0",
"104.146.128.0/17")
               || UO_isInNet(host_ips, "2001:df0:d9:200::", "64",
"2001:df0:d9:200::/64"))))
    {
        return direct;
    }

    return proxyServer;
}

function FindProxyForURL(url, host)
{
    return FindProxyForURLEx (url, host);
}
```

show entity

Use this command to see the dynamic entities that are created for URL offload:

```
awplus#show entity
Zone:          URL_Offload
 Network:      URL_Offload.exclude_entries
  Subnet:      10.10.10.11/32
  Host:        URL_Offload.exclude_entries.fqdn_entries
   FQDN IPv4: exclude.example.com
   FQDN IPv6: exclude.example.com
 Network:      URL_Offload.include_entries
  Subnet:      13.107.6.152/31
  Subnet:      13.107.18.10/31
  Subnet:      13.107.64.0/18
  Subnet:      13.107.128.0/22
  Subnet:      13.107.136.0/22
  Subnet:      23.103.160.0/20
  Subnet:      40.96.0.0/13
  Subnet:      40.104.0.0/15
  Subnet:      40.108.128.0/17
  Subnet:      52.96.0.0/14
  Subnet:      52.104.0.0/14
  Subnet:      52.112.0.0/14
  Subnet:      104.146.128.0/17
  Subnet:      131.253.33.215/32
  Subnet:      132.245.0.0/16
  Subnet:      150.171.32.0/22
  Subnet:      150.171.40.0/22
  Subnet:      191.234.140.0/22
  Subnet:      204.79.197.215/32
  Subnet:      2603:1006::/40
  Subnet:      2603:1016::/36
  Subnet:      2603:1026::/36
  Subnet:      2603:1036::/36
  Subnet:      2603:1046::/36
  Subnet:      2603:1056::/36
  Subnet:      2603:1096::/38
  Subnet:      2603:1096:400::/40
  Subnet:      2603:1096:600::/40
  Subnet:      2603:1096:a00::/39
  Subnet:      2603:1096:c00::/40
  Subnet:      2603:10a6:200::/40
  Subnet:      2603:10a6:400::/40
  Subnet:      2603:10a6:600::/40
  Subnet:      2603:10a6:800::/40
  Subnet:      2603:10d6:200::/40
  Subnet:      2620:1ec:4::152/128
  Subnet:      2620:1ec:4::153/128
  Subnet:      2620:1ec:c::10/128
  Subnet:      2620:1ec:c::11/128
  Subnet:      2620:1ec:d::10/128
  Subnet:      2620:1ec:d::11/128
  Subnet:      2620:1ec:8f0::/46
  Subnet:      2620:1ec:8f8::/46
  Subnet:      2620:1ec:900::/46
  Subnet:      2620:1ec:908::/46
  Subnet:      2620:1ec:a92::152/128
  Subnet:      2620:1ec:a92::153/128
  Subnet:      2a01:111:f400::/48
  Subnet:      2a01:111:f402::/48
  Host:        URL_Offload.include_entries.fqdn_entries
   FQDN IPv4: outlook.office365.com
   FQDN IPv4: *.sharepoint.com
   FQDN IPv4: example.com
   FQDN IPv4: outlook.office.com
   FQDN IPv6: outlook.office365.com
   FQDN IPv6: *.sharepoint.com
   FQDN IPv6: example.com
   FQDN IPv6: outlook.office.com
```

C613-22122-00 REV B