Web Control

Feature Overview and Configuration Guide

Introduction

This guide describes AlliedWare Plus™ Web Control and its configuration.

AlliedWare Plus™ Web Control provides a new level of service for business productivity management, compliance and web security. It offers an easy way to monitor and control the types of websites viewed by employees. It stops staff members visiting inappropriate websites that:

- Drain their productivity
- Contain questionable content
- Are bandwidth intensive and hence put a strain on resources
- Pose potential security threats to the organization

Contents

Products and software version that apply to this guide

This Guide applies to AlliedWare Plus™ products that support Web Control, running version **5.4.5** or later. Web Control configuration default action on a per entity basis is available from **5.4.6-2** onwards.

However, implementation varies between products. To see whether a product supports a feature or command, see the following documents:

- The product's Datasheet
- The AlliedWare Plus Datasheet
- The product's Command Reference

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

Feature support may change in later software versions. For the latest information, see the above documents.

How Web Control works

Integrated with Digital Arts' Active Rating System (ARS), AlliedWare Plus Web Control provides comprehensive and dynamic website coverage with high accuracy of categorization. AlliedWare Plus™ Web Control is capable of accurately assigning millions of websites or pages into around 100 categories and allowing or blocking website access in real-time.

AlliedWare Plus Web Control provides the following features:

- Categorizes a vast number of websites in multiple languages
- Covers millions of the most relevant websites in around 100 categories
- Supports multiple categorizations for a single website
- Supports management and configuration of categories, rules and website categorization provider, including on a per Firewall entity basis.

AlliedWare Plus Web Control uses a website classifier engine and caching mechanism to filter HTTP traffic.

When an HTTP request passes through the device, the associated TCP session transporting the HTTP data is proxied. The embedded URL of the website is intercepted and sent to the website classifier engine to retrieve the category the website belongs to.

To categorize the website, the website classifier engine queries Digital Arts' constantly updated Active Rating System (ARS) which contains about 100 pre-defined categories. The categorization provider then returns the category of the website. The website classifier engine also queries the custom static engine, which can be customized to suit individual business needs. The custom categorization is used in preference to, and can, override Digital Arts categorization. This means if a website matches match criteria from custom categories, then the website will not be sent for categorization by Digital Arts.

Once the website has been categorized, the device can filter the website according to a set of rules defined per category. The user is unable to visit the blocked website and will get a notification page if the website is blocked. Conversely, the user can get the resulting page from the website if the website is allowed. The default action to take on uncategorized websites, and categorized websites that don't hit any user defined Web Control filter rules is to **deny** access to the website. This default action can be optionally changed to **permit** via the Web Control **action {permit | deny}** command.

Categorized websites are cached within the device. The device can check its local cache for a matching website against the HTTP request passing through it.

Figure 1: Web Control block action

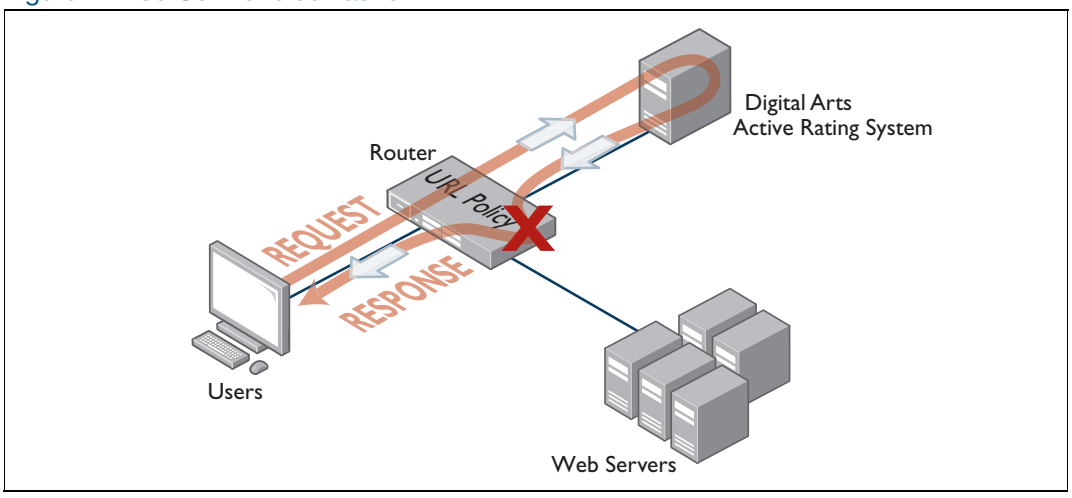
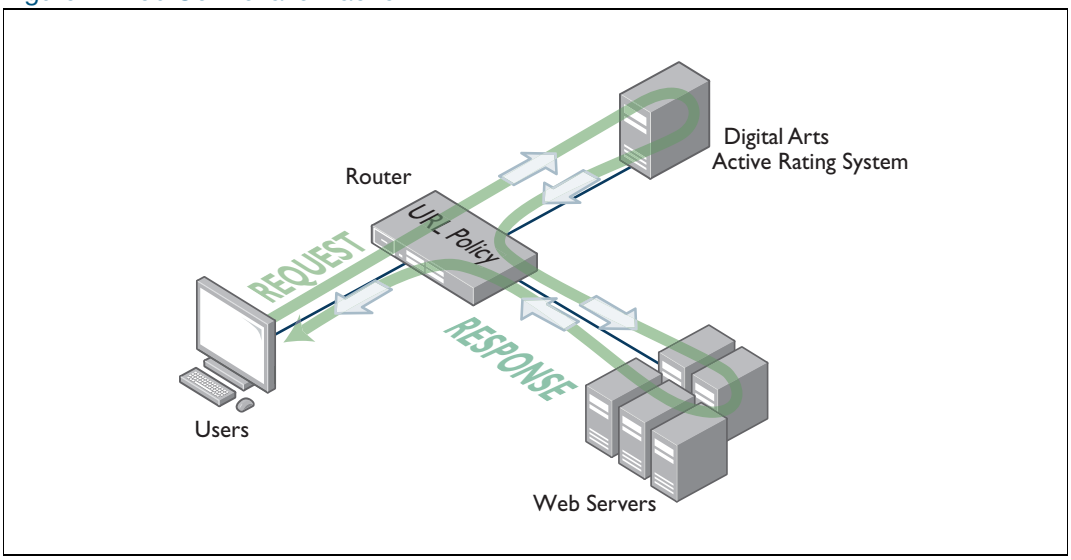


Figure 2: Web Control allow action



Configuration Examples

How to configure basic Web Control

By default, Web Control protection is disabled and you need to explicitly enable it.

Step 1: Enter the Web Control Configuration mode.

```
awplus#configure terminal
awplus(config)#web-control
```

Step 2: Set the website categorization provider and enable Web Control protection.

```
awplus(config-web-control)#provider digitalarts
awplus(config-web-control)#protect
```

The command **show web-control categories** displays a list of predefined categories. You can optionally create your own named custom categories.

Step 3: Configure a category and match criteria.

To configure match criteria for the named custom category **movie**, use the Web Control command **match <word>** as follows:

```
awplus(config-web-control)#category movie
awplus(config-category)#match imdb
awplus(config-category)#match youtube
awplus(config-category)#match rottentomatoes
```

Match criteria are case-insensitive and matched up to the first appearance of '?' (query string marker) or '#' (fragment identifier) in a website URL. For example, URL

www.alliedtelesis.com/search.aspx?keyword=routers does not match the match criterion match router but www.alliedtelesis.com/routers does match that criterion.

When a URL matches a match criterion, the URL is categorized to the match criterion's category. A URL can be matched to more than one category. Custom match criteria override and precede provider categorization. If a URL or website matches custom criteria, then the URL will not be further sent for categorization by the provider criteria.

The provider performs the categorization of URLs into the appropriate category, so there is no need to configure specific match criteria for pre-defined categories.

You can create your own custom categories which will match any website URLs against text strings in that category, see Step 3 **Configure a category and match criteria.** This allows custom categories to be created to suit business needs.

You can create up to 50 match criteria in total, so a category can have a maximum of 50 match criteria, or 50 categories can each have one match criterion, as long as the total number of the match criteria does not exceed 50.

Note: This feature cannot be used to filter SSL encrypted website URLs (HTTPS).

Step 4: Configure an entity the rule applies to.

```
awplus(config-web-control)#exit
awplus(config)#zone private
awplus(config)#network engineering
awplus(config-network)#ip subnet 192.168.1.0/24 interface eth1
```

Step 5: Create a rule for the category.

```
awplus(config-network)#exit
awplus(config-zone)#exit
awplus(config)#web-control
awplus(config-web-control)#rule permit movie from
private.engineering
awplus(config-web-control)#exit
awplus(config)#exit
```

URLs containing the match criteria associated with the custom category **movie** can now be accessed from the engineering network. Access to other URLs that do not match the custom category **movie** will be blocked by the default Web Control action.

Step 6: Display the information about the state of Web Control.

```
awplus#show web-control
```

Output 1: Example output for basic web control configuration:

```
awplus#show web-control
Web Control protection is enabled
Web Control default action is deny
Web Control is licensed
Categorization provider is Digital Arts
Statistics:
 Categorization hits: 0/0  (0.0%)
 Rule hits:   0/0  (0.0%)
 Cache hits:  0/0  (0.0%)
 Cache size:  0
```

How to configure Web Control default action on a per entity basis

The default action to take on uncategorized websites, and categorized websites that don't hit any user defined Web Control filter rules is to **deny** access to the website.

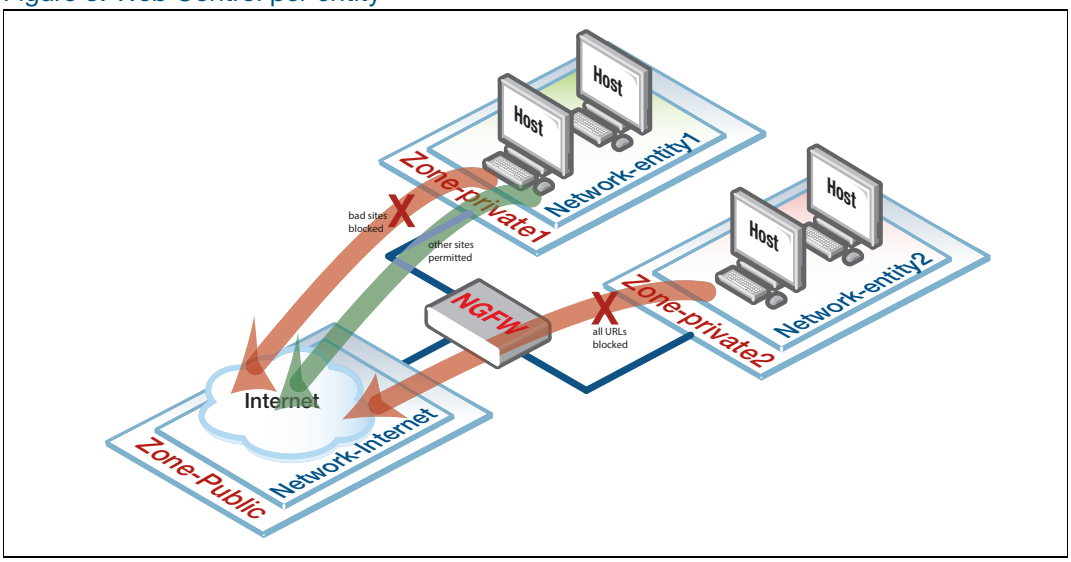
However, if there is multiple firewall entities configured in the device (such as multiple firewall zones), then you may wish to configure different default actions for each individual entity for any URLs that do not match filter rules.

A new reserved keyword **any** has been added to the parameter **<category>** in the rule command from release 5.4.6-2 onwards.

This reserved Web Control keyword overrides the default Web Control action for the specific entity that it is associated with. Rules containing this reserved keyword can be applied to all types of firewall entities, including zone, network and host entities.

This new reserved keyword allows you to configure multiple firewall entities, with each entity having its own unique default action to apply to uncategorized URLs.

Figure 3: Web Control per entity



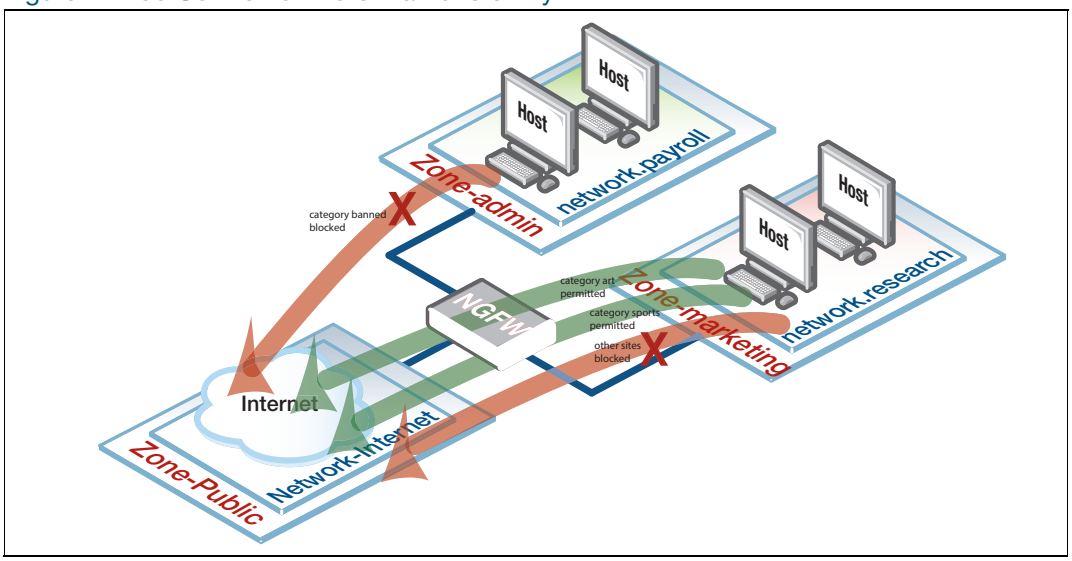
Example 1 Basic configuration to create a rule using the category keyword **any**:

```
awplus#configure terminal
awplus(config)#web-control
awplus(config-web-control)#rule deny badsites from private
awplus(config-web-control)#rule permit any from private
```

Rules are processed in order. In this example above the access to URLs associated with the named category **badsites** being accessed from the named firewall entity **private** will be blocked via the **deny** rule. Access to all other URLs originating from that specific firewall entity will be allowed via the subsequent **permit any** rule.

However, access to URLs from any other entity will not match the rules above, and so will be blocked via the Web Control default action.

Figure 4: Web Control for more than one entity



Example 2 The following shows how to configure two firewall entities, with a different default action being applied for each entity.

Access from the research network entity (within marketing zone) to URLs matching the **art** and **sports** categories are permitted, whilst access to any other URLs is denied.

Conversely, access from the payrol network entity (within the admin zone) to URLs matching the **banned** category are denied, whilst access to any other URLs is permitted.

Step 1: **Create the admin zone entity containing the payrol network entity and assign its ip subnet address.**

```
awplus#configure terminal
awplus(config)#zone admin
awplus(config-zone)#network payrol
awplus(config-network)#ip subnet 192.168.1.0/24
```

Step 2: Create the marketing zone entity containing the research network entity and assign its ip subnet address.

```
awplus(config-host)#zone marketing
awplus(config-zone)#network research
awplus(config-network)#ip subnet 192.168.2.0/24
```

Step 3: Enter into Web Control configuration mode and set the website categorization provider.

```
awplus(config-host)#web-control
awplus(config-web-control)#provider digitalarts
```

Step 4: Configure custom categories and associated match criteria.

```
awplus(config-control)#category banned
awplus(config-category)#match youtube
awplus(config-category)#match movies
awplus(config-category)#match gambling

awplus(config-category)#category art
awplus(config-category)#match contemporary
awplus(config-category)#match classic

awplus(config-category)#category sports
awplus(config-category)#match rugby
```

Step 5: Create rules for the categories.

```
awplus(config-category)#rule 10 permit art from marketing.research
awplus(config-web-control)#rule 20 permit sports from
marketing.research
awplus(config-web-control)#rule 30 deny any from marketing.research
awplus(config-web-control)#rule 40 deny banned from admin.payrol
awplus(config-web-control)#rule 50 permit any from admin.payrol
```

Step 6: Enable Web Control protection.

```
awplus(config-web-control)#protect
```

C613-22009-00 REV C

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