HTTP Proxy
Surf Protection Guide
For ASL V5

(Version 0.1 – Date: 5/23/2004 5:18 PM)

by Gert Hansen <ghansen@astaro.com>

Table of Contents

1 Introduction

As there has been some misunderstanding, confusion and lack of documentation about the HTTP Proxy functionality and how to configure it, I took the opportunity to explain it.

I will cover 5 topics:
1) Describe the different parts of the configuration, what they do and how they work.
2) Outline each possible scenario (combination of parts of the configuration), if it works or not, and what to do to get it working.
3) Explain the two common problems and how to fix them
4) Interpreting Common Error messages

2 Parts of the HTTP Proxy Configuration

The Main Parameters of the HTTP Proxy and Content Filter functionality are:

2.1 Proxy Mode

This config option defines in which mode the proxy operates.
We support three possible Modes:

- Standard
- Transparent
- User Authentication

2.2 User Authentication Mechanism

This option is only available if you configured the proxy to run in 'User authentication' Mode.

It defines which mechanism should be used in order to authenticate the user information to allow the usage of the proxy.
You can also define multiple mechanisms, the mechanisms than get processed from top to bottom.
If one says ok, he his authenticated, if none says ok, it is blocked.

This option has nothing to do with the profile assignment, those are two different parts.

Possible Values:

- None
- Local
- Radius
- LDAP

If you don't see LDAP and/or Radius you need to configure them in WebAdmin > System > User Authentication.

For debugging of the authentication you find information in the logfile /var/log/aua.log.

2.3 Surf Protection Profile

A Surf Protection Profile describes which kind of content is allowed, this includes White list, Blacklist, Cobion URL Filtering, Content Removal and Virus Protection.
You can create multiple profiles to match different surfing behaviors.

i.e: create one profile for the sales division and one for the management, or one for the 'kids' and one for 'parents'

In order to use a profile you need to assign it to users.

Important Note:
There must always be at least one profile configured! If this is not the case, the proxy will block every request, as this is the default behavior, block all.

2.4 Surf Protection Profile Assignment

The SP Profile Assignment defines which user or which network or host gets assigned to which Surf Protection Profile.

There are three different Assignment types:

- Local Assignments
- Assign by Radius
- Assign by LDAP

You only see the Radius and LDAP option if you successfully configured Radius and LDAP user authentication.

If you operate the proxy in Standard or Transparent Mode, you will automatically use the Local Assignment.

All assignments are processed from top to bottom.

2.4.1 Local Assignment

You can configure Local Assignment to Assign different profiles either based on the network or host where the request comes from or the username the request has been authenticated with.

It is important to understand that it must match both, the user AND the network. Plz take a look at the scenarios in Section 2.

2.4.2 Assign by Radius

With this mechanism we Assign the SP Profile by the Group a user is in.
<to be added>

2.4.3 Assign by LDAP

With this mechanism we Assign the SP Profile by certain attributes a user has.
<to be added>

3 Outline HTTP Surf Protection Scenarios

In this section we describe the different common scenarios you can your HTTP proxy with.

3.1 Proxy Mode: Standard or Transparent

3.1.1 Assign Profile only by Network

All ok.

3.1.2 Assign Profile only by User

Does not work, as we don't do User Authentication -> do not use

3.1.3 Assign Profile by User and Network

Does not work, as we don't do User Authentication -> do not use

3.2 Proxy Mode: UserAuth, UserAuth: Local Users

3.2.1 Profile assignment: Local, Assign Profile only by Network

All Ok, but the user information's are not relevant in this assignment.

3.2.2 Profile assignment: Local, Assign Profile only by User

Does not work, we always need a network, if unsure add 'Any'

3.2.3 Profile assignment: Local, Assign by User and Network

The profile only matches if both parameters are true, the user AND the network.

3.3 Proxy Mode: UserAuth, UserAuth: Radius

If you are using Radius Authentication in order to validate the user credentials against a central user database, you are still able to select your Assignment method, either Local or Radius.

3.3.1 Profile assignment: Local, Assign by Network

All Ok, but the user information's are not relevant in this assignment.

3.3.2 Profile assignment: Local, Assign by User

Does not work, we always need a network, if unsure add 'Any'

3.3.3 Profile assignment: Local, Assign by User and Network

The profile only matches if both parameters are true, the user AND the network

3.3.4 Profile assignment: radius

See Radius HowTo

3.4 Proxy Mode: UserAuth, UserAuth: LDAP

If you are using LDAP Authentication in order to validate the user credentials against a central user database, you are still able to select your Assignment method, either Local or Radius.

3.4.1 Profile assignment: Local, Assign by Network

All Ok, but the user information are not relevant in this assignment.

3.4.2 Profile assignment: Local, Assign by User

Does not work, we always need a network, if unsure add 'Any'

3.4.3 Profile assignment: Local, Assign by User and Network

The profile only matches if both parameters are true, the user AND the network

3.4.4 Profile assignment: LDAP

See the LDAP HowTo

Current Limitation/Bugs: only one profile supported ;), first one matches always.
If a user is matched in multiple profiles, there are known issues...

4 Explain the two common problems and how to fix them

- User Auth and Local profile assignment enabled but no network configured in the assignment.
  Fix: Add the network 'Any' to the assigned networks

- Selected a user assignment even if we do not user authentication at all.
  Fix: Remove the assigned users.

5 Interpreting Common Error messages

5.1 'no matching profile'

This tells you that the Surf protection was not able to assign your request to a valid Surf Protection Profile.
The most common failures are mentioned above:

- a missing network assignment if user authentication is used.
- A user assignment even when using standard or transparent mode