Adaptive Response

Exinda ExOS Version 6.3

Table of Contents

Part I Introduction 4
1 Using this Guide 4
Part II Overview 6
Part III Creating Adaptive Response Rules (Web UI) 8
1 Create a Source Network Object 8
2 Create an Adaptive Response Rule 9
3 Use the Adaptive Response Rule in the Optimizer 10
4 Using Adaptive Response with Active Directory 11
Part IV Creating Adaptive Response Rules (CLI) 14
1 Other Commands 14
2 Add Dynamic Network Object to Optimizer 15
3 Disabling an Adaptive Response Rule 15
4 Excluding Hosts/Subnets from the Quota 15

Part

1 Introduction

Adaptive Response

Exinda Firmware Version: 6.3

1.1 Using this Guide

Throughout the manual the following text styles are used to highlight important points:

- Useful features, hints and important issues are called "notes" and they are identified in a light blue background.

Note: This is a note.

- Practical examples are presented throughout the manual for deeper understanding of specific concepts. These are called "examples" and are identified with a light green background.

This is an example.

- Warnings that can cause damage to the device are included when necessary. These are indicated by the word "caution" and are highlighted in yellow.

Caution: This is a caution.

Part II

2 Overview

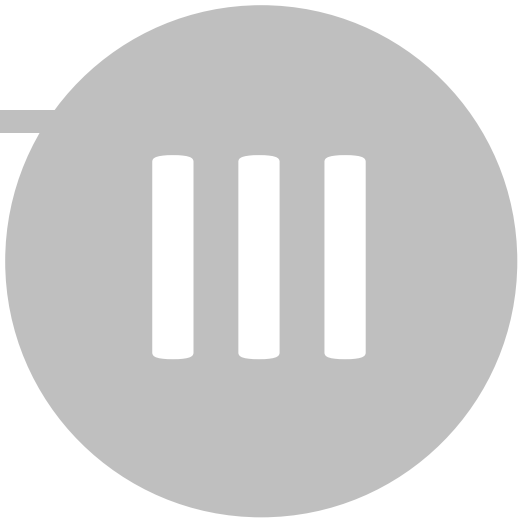
Adaptive Response allows administrators to specify rules based on data transfer which dynamically populate Network Objects. These Dynamic Network Objects may then be used when configuring Optimizer Policies.

This functionality allows the system administrator to create policies which automatically restrict a user's bandwidth once a set transfer limit has been exceeded within a specified period of time. Users are identified by IP address.

The following steps are required to implement such policies:

- Create a static Network Object that defines the subnet(s) that will be monitored OR map an Active Directory group to a Dynamic Network Object.
- Create an Adaptive Response limit rule (which implicitly creates a Dynamic Network Object).
- Include the Dynamic Network Object in the Optimizer Policies.

Part



3 Creating Adaptive Response Rules (Web UI)

In order to demonstrate how to configure Adaptive Response using the Web UI, the following example will be used as a guide.

Example: An educational institution has a group of students who have IP addresses in the subnet 192.168.0.0/16. Each student shall be allowed 10GB data transfer (uploads and downloads) per month.

3.1 Create a Source Network Object

Using the Web UI - Advanced Mode, navigate to System | Objects | Network Objects and create a Network Object that defines the Student subnet as 192.168.0.0/16.

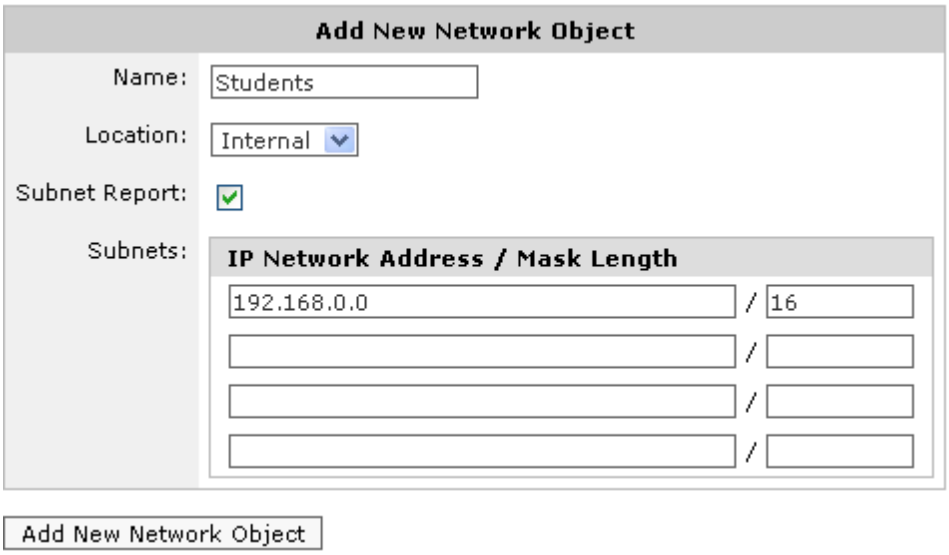


Figure 1: The 'Students' Network Object.

3.2 Create an Adaptive Response Rule

Using the Web UI - Advanced Mode, navigate to System | Objects | Adaptive Response.

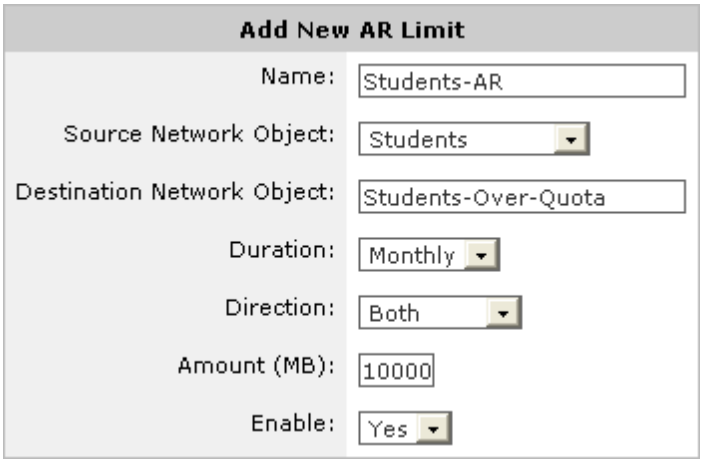


Figure 2: The Adaptive Response Web UI form.

Name	Give the rule a name
Source Network Object	The Network Object used as a source of IP addresses
Destination Network Object	This Dynamic Network Object will be created and will contain all the IPs from the Source Network Object that have exceeded the Adaptive Response limit.
Duration	Over what period the limit will apply : Daily, Weekly or Monthly.
Direction	In which direction should data be accounted? Inbound (WAN -> LAN) , Outbound (LAN -> WAN) or Both.
Amount	The data limit (quota) in MB.
Enable	Enable or disable this rule. When a rule is disabled all IP's will be removed from the Destination Network Object.

To configure an Adaptive Response limit for the example above, the rule should look like this:

Name	Source Network	Destination Network	Duration	Direction	Amount	Enabled	Edit	Delete
Students-AR	Students	Students-Over-Quota	monthly	both	10000	☑	Edit	Delete

Figure 3: A configured Adaptive Response rule.

This rule ensures that any user in the Students Network Object, gets placed in the Students-Over-Quota Dynamic Network Object once they have transferred (uploaded and downloaded) more than 10GB in a calendar month.

At the end of the calendar month, the Students-Over-Quota Network Object is reset.

Once you are satisfied with the rule, click the “Add New Limit” button. This will load and activate the rule and begin populating the Destination Network Object.

To view the IP addresses added to the Dynamic Network Object, navigate to the System | Network Object | Dynamic page using the Advanced Web UI and select the Dynamic Network Object associated with your Adaptive Response rule from the drop down.

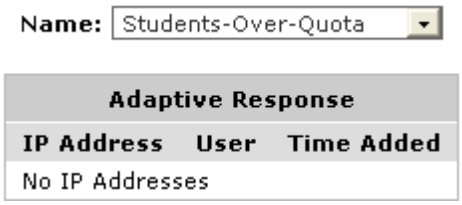


Figure 4: View current list of IP addresses in the Dynamic Network Object.

This will show which users were added to the Dynamic Network Object and when they were added.

3.3 Use the Adaptive Response Rule in the Optimizer

Add the new Dynamic Network Object to the Optimizer Policies using the Advanced Web UI and navigated to the Optimizer page.

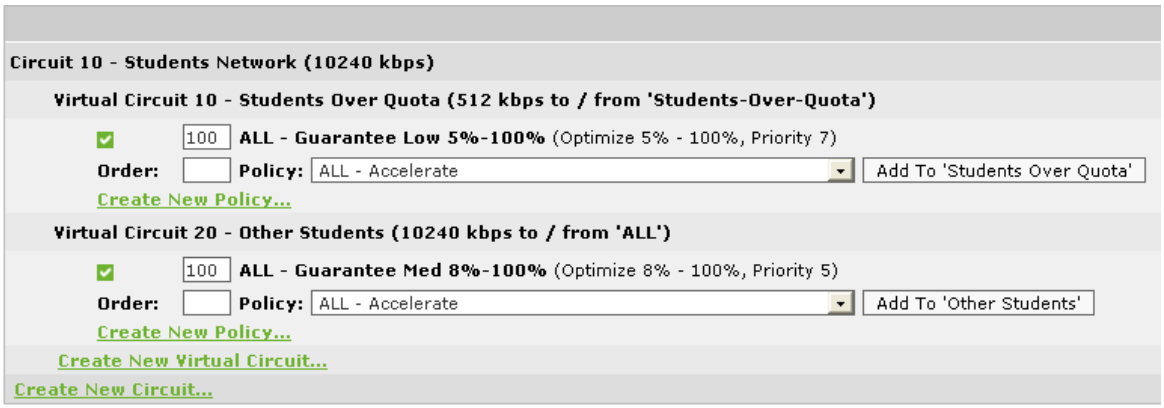


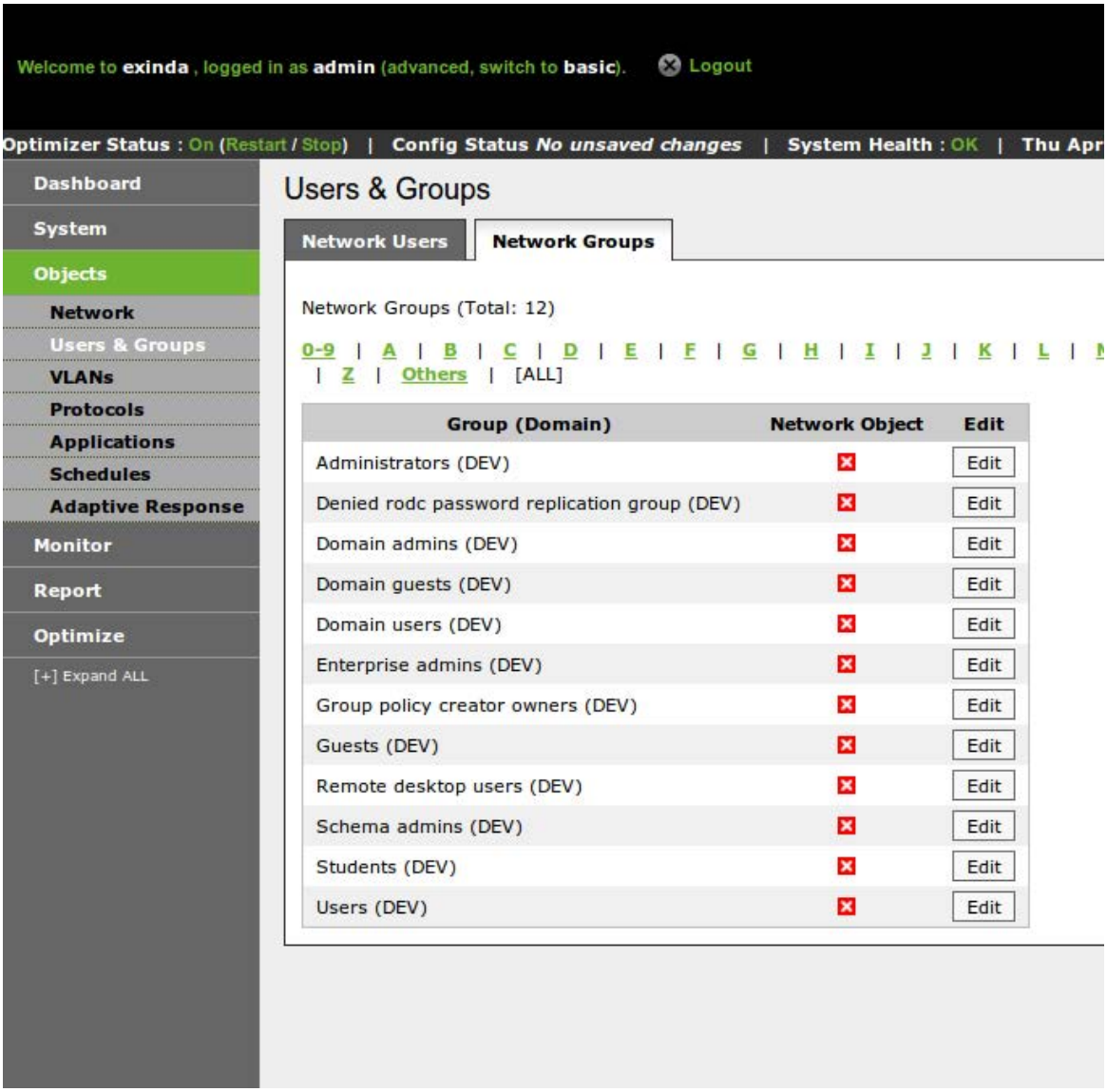
Figure 5: The Students-Over-quota Dynamic Network Object used in an Optimizer Virtual Circuit.

In this example, the Students that have exceeded their monthly limit get placed in a 512kbps Virtual Circuit whereas all other students (the ones who have not exceeded their monthly limit) are placed in a 10Mbps Virtual Circuit.

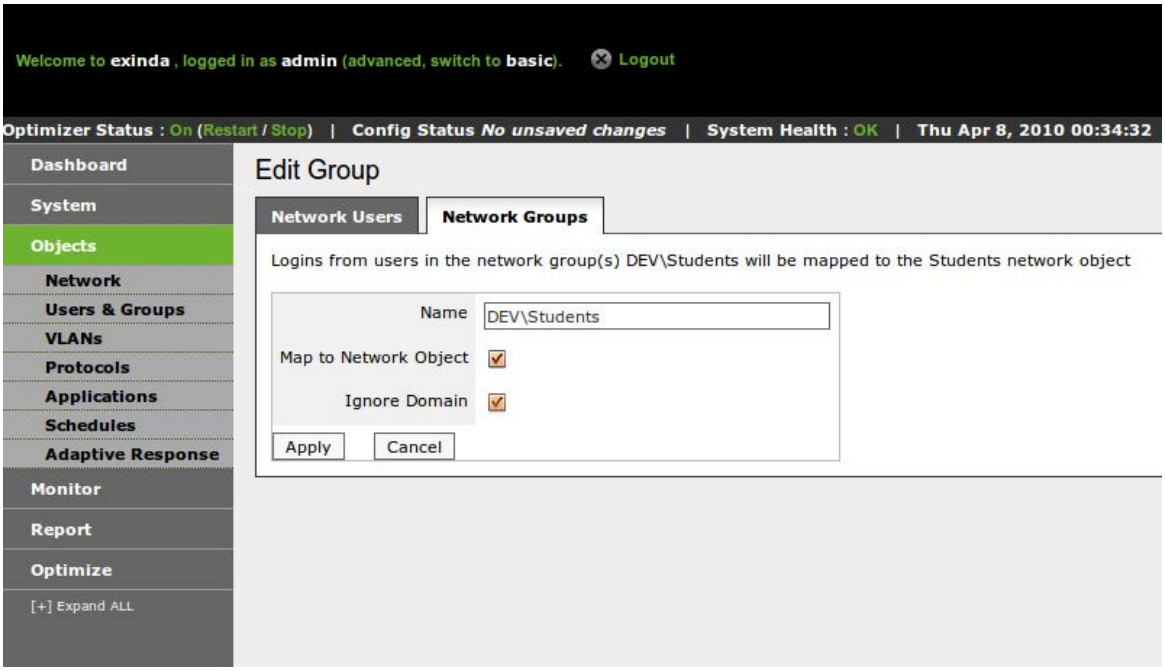
3.4 Using Adaptive Response with Active Directory

In the last example, a static Network Object was used as the source of IP's. It is also possible to use a Dynamic Network Object mapped from an Active Directory group as a source.

Using the Web UI - Advanced Mode, navigate to Objects | Users & Groups. Edit the **"Students (DEV)"** group.



Click on the 'Edit' button for Students (DEV)



Enable the 'Map to Network Object' and 'Ignore Domain' checkboxes. When the 'Apply' button is clicked a Network Object named 'Students' will be created that will be contain all IP's in the Active Directory 'Student' group. This Network Object can be used when creating an Adaptive Response rule exactly as for the previous example.

Part IV

4 Creating Adaptive Response Rules (CLI)

Adaptive Response rules can be created using the CLI (in configure terminal mode):

```
adaptive limit <limit-name> network-object source <src> destination <dst>
adaptive limit <limit-name> amount <N (mb)>
adaptive limit <limit-name> duration <daily|weekly|monthly>
adaptive limit <limit-name> direction <inbound|outbound|both>
adaptive limit <limit-name> enable
```

Example: Create an Adaptive Response rule which adds IP addresses from the static Students Network Object to the Dynamic Network Object Students-Over-Quota, once 200 MB has been downloaded per day.

```
adaptive limit Students-AR network-object source Students destination Students-Over-Quota
adaptive limit Students-AR amount 200
adaptive limit Students-AR duration daily
adaptive limit Students-AR direction inbound
adaptive limit Students-AR enable
```

4.1 Other Commands

The following command may be used to show Adaptive Response rules:

```
show adaptive limit <limit-name>
```

Adaptive Response evaluates rules every 5 minutes by default. IP addresses are added to destination dynamic Network Objects when the amount of traffic for the specified direction and duration exceeds the specified amount. Network Objects are cleared at the end of the duration (e.g. daily, weekly or monthly). The following command can be used to change the frequency at which the rules are evaluated:

```
adaptive update-time <seconds>
```

Use the following command to show network objects created by Adaptive Response:

```
show network-object <network object>
```

The following command will clear all IP's from all Adaptive Response destination Network Objects. The Network Objects will be repopulated when rules are next evaluated.

```
adaptive clear
```

4.2 Add Dynamic Network Object to Optimizer

The aim of this step is create a virtual circuit which references a dynamic network object created above.

Example: Assuming we have created a Virtual Circuit named "Wan Inbound Choke" with reduced bandwidth, we can now reference the Dynamic Network Object created above using the following CLI command.

```
(config) # circuit default vcircuit "WAN Inbound Choke" destination Students-Over-Quota
```

4.3 Disabling an Adaptive Response Rule

To disable an Adaptive Response rule, run the following command. No IPs will belong to the destination Network Object, so any Optimizer Virtual Circuits or Policies using the destination Network Object will effectively do nothing.

```
(config) # no adaptive limit Students-AR enable
```

4.4 Excluding Hosts/Subnets from the Quota

It is possible to configure Adaptive Response rules to exclude both internal or external hosts and subnets from the data transfer limits. This configuration option is available using the following CLI commands:

```
adaptive limit <limit-name> except network-object {internal|external} <network object>
```

Example: Create an Adaptive Response rule which adds IP addresses from the static Students Network Object to the Dynamic Network Object Students-Over-Quota once 200 MB has been downloaded per day, **except for the IP address 192.168.0.50**.

```
network-object IgnoreUser subnet 192.168.0.50 /32
network-object IgnoreUser location internal

adaptive limit Students-AR network-object source Students destination Students-Over-Quota
adaptive limit Students-AR amount 200
adaptive limit Students-AR duration daily
adaptive limit Students-AR direction inbound
adaptive limit Students-AR enable

adaptive limit Students-AR except network-object internal IgnoreUser
```

Example: Create an Adaptive Response rule which adds IP addresses from the static Students Network Object to the Dynamic Network Object Students-Over-Quota once 200 MB has been downloaded per day **except for the DMZ subnet 203.122.212.128 /27**.

```
network-object IgnoreDMZ subnet 203.122.212.128 /27
network-object IgnoreDMZ location external
```

```
adaptive limit Students-AR network-object source Students destination Students-Over-Quota
adaptive limit Students-AR amount 200
adaptive limit Students-AR duration daily
adaptive limit Students-AR direction inbound
adaptive limit Students-AR enable


adaptive limit Students-AR except network-object external IgnoreDMZ
```

The above examples illustrate how to exclude IP addresses or subnets from the Adaptive Response quota. The first example excludes an internal IP address that exists on the LAN-side of the Exinda appliance. The second example excludes an entire subnet that exists on the WAN-side of the Exinda appliance.