

Alloc8 – How to Guide:  
Adaptive Response

# Adaptive Response Rules

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:

1. Create a static Network Object that defines the subnet(s) that will be monitored.

OR

2. Map an Active Directory group to a Dynamic Network Object.
3. Include the Dynamic Network Object in the Optimizer Policies.

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 10 GB data transfer (uploads and downloads) per month.

## Create a Source Network Object

Create a Network Object that defines the Student subnet as 192.168.0.0/16.

1. In the Web UI go to **Configuration > Objects > Network > Network Objects**.
2. In the Add New Network Object area, type a name for the object.
3. Select whether the subnet is on the LAN side of the appliance (internal) or the WAN side (external). Packets are matched to a Network Object, and the closest subnet within that Network Object determines the location.

There are 3 options for the location field: Inherit, Internal, and External.

- Internal means all subnets/hosts defined by this Network Object exist on the LAN side of the appliance.
- External means all subnets/hosts defined by this Network Object exist on the WAN side of the appliance.
- Inherit means that a subnet/hosts location is determined by closest match to other Network Objects. If

no Network Objects match then the location defaults to external.

4. To include traffic matching this network object in the Subnets Report, select the **Subnet Report** check- box.
5. Type the network IP addresses and netmask length of the subnet in the fields. IPv4 and IPv6 addresses are accepted.
6. Click **Add New Network Object**.

**Note** When creating or editing a network object, you will be presented with 4 input lines. To add more than 4 objects, you need to save and then re-edit to be presented with an extra 4 lines.

## Create an Adaptive Response limit rule

Adaptive Response Limits are rules which are used to create and populate network objects based on amount of data transferred. These dynamic network objects may then be used when creating virtual circuits or filters. For example, create a rule that 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 10 GB in a calendar month. At the end of the calendar month, the Students-Over-Quota Network Object is reset.

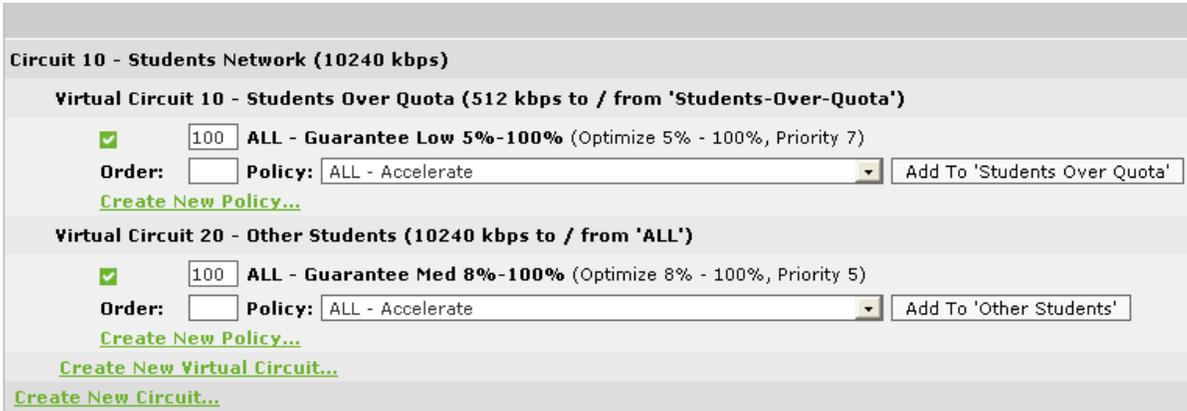
| Add New AR Limit            |                                      |
|-----------------------------|--------------------------------------|
| Name:                       | <input type="text"/>                 |
| Source Network Object:      | <input type="text" value="ALL"/>     |
| Destination Network Object: | <input type="text"/>                 |
| Duration:                   | <input type="text" value="Daily"/>   |
| Direction:                  | <input type="text" value="Inbound"/> |
| Limit Type:                 | <input type="text" value="Both"/>    |
| Amount (MB):                | <input type="text"/>                 |
| Time (Min):                 | <input type="text"/>                 |
| Enable:                     | <input type="text" value="No"/>      |

1. In the Web UI Go to **Configuration > Object > Adaptive Response**.
2. Type a name for the new limit.
3. Specify a **Source Network Object** to use as a list of users for whom to apply the quota.
  - This can be a Static Network Object (such as a subnet) or a Dynamic Network Object (such as an Active Directory group).
4. Specify a name for the **Dynamic Network Object**, which holds the list of users that have exceeded their quota.
5. Specify the duration to use when accounting the quota: **daily**, **weekly**, or **monthly**.
6. Specify which direction should be used when accounting the quota: **inbound**, **outbound**, or **both**.
7. Specify the quota amount (in MB) for this rule.
8. To enable the rule, select **Yes**.
  - When a rule is disabled all IPs will be removed from the Destination Network Object.
9. Click **Add New Limit**.



## Use the Adaptive Response Rule in the Optimizer

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



**Circuit 10 - Students Network (10240 kbps)**

**Virtual Circuit 10 - Students Over Quota (512 kbps to / from 'Students-Over-Quota')**

**ALL - Guarantee Low 5%-100%** (Optimize 5% - 100%, Priority 7)

Order:  Policy:

[Create New Policy...](#)

**Virtual Circuit 20 - Other Students (10240 kbps to / from 'ALL')**

**ALL - Guarantee Med 8%-100%** (Optimize 8% - 100%, Priority 5)

Order:  Policy:

[Create New Policy...](#)

[Create New Virtual Circuit...](#)

[Create New Circuit...](#)

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 512 kbps Virtual Circuit whereas all other students (the ones who have not exceeded their monthly limit) are placed in a 10Mbps Virtual Circuit.

## Use Adaptive Response with Active Directory

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

1. Click **Configuration > Objects > Users & Groups > Network Groups**
2. Beside the "*Students (DEV)*" group click **Edit**
3. Select the **Map to Network Object** and **Ignore Domain** checkboxes.
4. Click **Apply**.

A Network Object named '*Students*' is created that contains all IPs in the Active Directory '*Student*' group. This Network Object can be used when creating an Adaptive Response rule exactly as for the previous example.

## Create Adaptive Response Rules with 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
```

## Add a Dynamic Network Object to Optimizer with CLI

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

## Disable 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
```

## Exclude Hosts or 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>
```

The following 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 Alloc8 appliance. The second example excludes an entire subnet that exists on the WAN-side of the Alloc8 appliance.

### 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
```

## Other Adaptive Response CLI 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 IPs from all Adaptive Response destination Network Objects. The Network Objects will be repopulated when rules are next evaluated.

```
adaptive clear
```