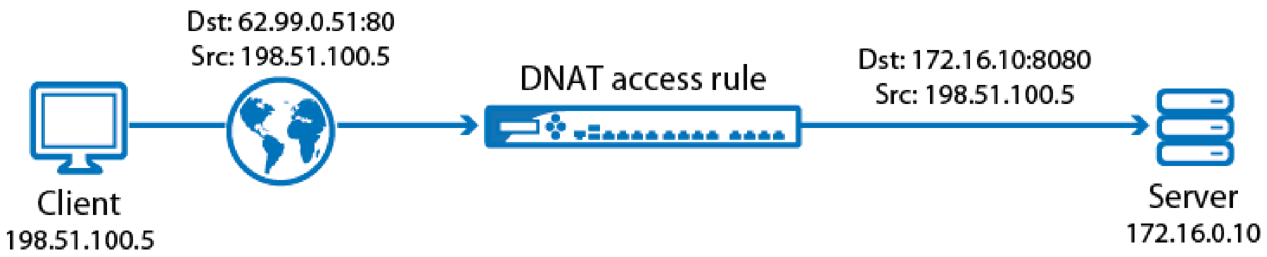
Example - Configuring a DNAT Access Rule

https://campus.barracuda.com/doc/28967159/

To reach services running on servers in the DMZ behind the firewall, configure a **Destination NAT (DNAT)** rule to forward the traffic arriving on the WAN port to the correct server and port in the DMZ.



Before you Begin

- Create a new network object containing the IP addresses of all web servers you want to redirect traffic to. If you want to redirect to a different port, you cannot use network objects.
- Create a network object containing your public IP address. For this example, our public IP address is 62.99.0.51.
- Verify that there is no local firewall service listening on that IP address. To forward IPsec traffic, go to **VPN > Settings** and set **Use Dynamic IPs** to **No**.

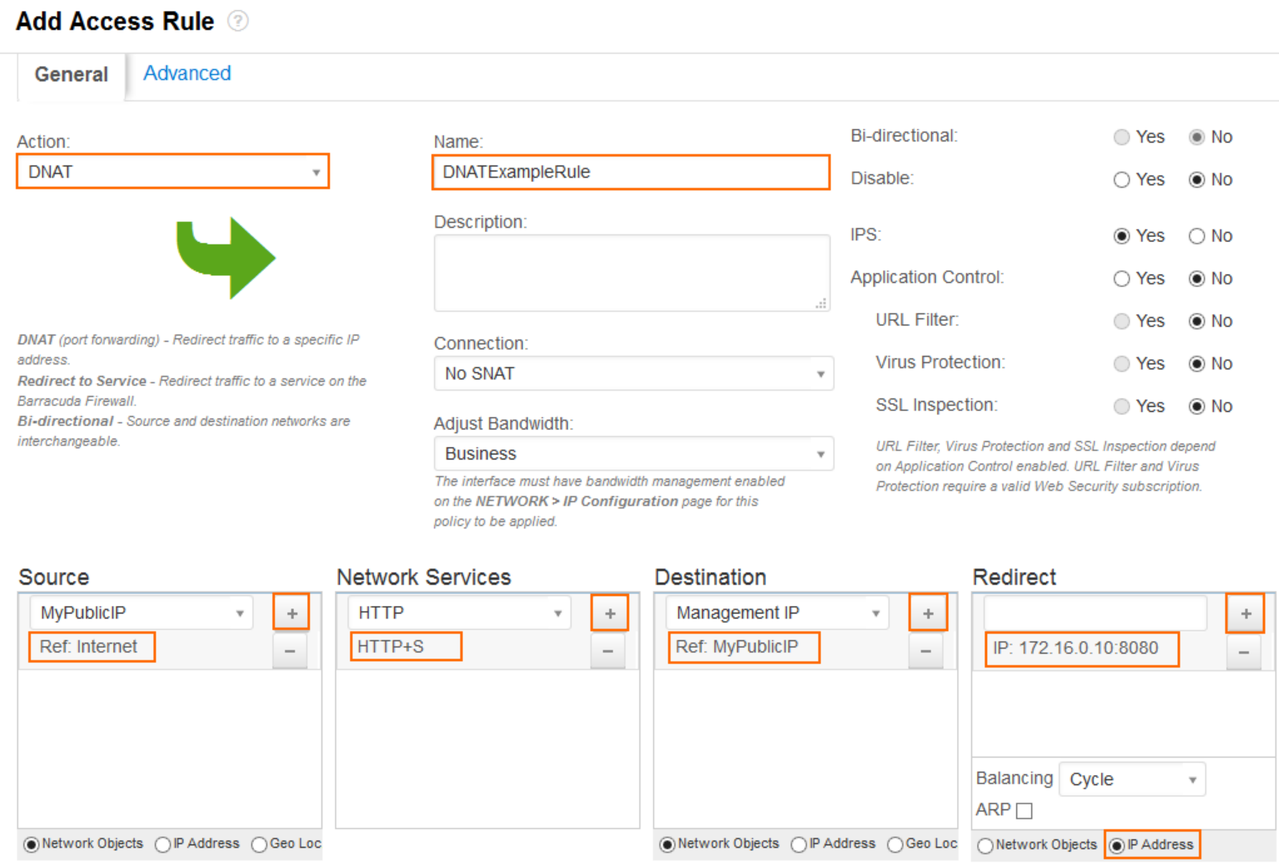
Step 1. Configure a DNAT Access Rule

This example creates a DNAT access rule that allows HTTP traffic from the Internet to the web server residing in the DMZ.

1. Go to the **FIREWALL > Firewall Rules** page.
2. Click **Add Access Rule** to create a new access rule.
3. In the **Add Access Rule** window, enter a name and description for the rule.
4. Specify the following settings:

Action	Connection	Source	Network Services	Destination	Redirect

DNAT	**No SNAT**	**Internet**	**HTTP+S**	Either `62.99.0.51` or the **WAN-ISP1** Network Object	network object containing one or more IP addresses or `IP address:port` 172.16.0.10:8080 To enter a combination of `address:port`, paste it from the clipboard into the edit field.



Add Access Rule

Action: DNAT

DNAT (port forwarding) - Redirect traffic to a specific IP address.
Redirect to Service - Redirect traffic to a service on the Barracuda Firewall.
Bi-directional - Source and destination networks are interchangeable.

Name: DNATExampleRule

Description:

Connection: No SNAT

Adjust Bandwidth: Business

The interface must have bandwidth management enabled on the NETWORK > IP Configuration page for this policy to be applied.

Bi-directional: ○ Yes ● No

Disable: ○ Yes ● No

IPS: ● Yes ○ No

Application Control: ○ Yes ● No

URL Filter: ○ Yes ● No

Virus Protection: ○ Yes ● No

SSL Inspection: ○ Yes ● No

URL Filter, Virus Protection and SSL Inspection depend on Application Control enabled. URL Filter and Virus Protection require a valid Web Security subscription.

Source: MyPublicIP; Ref: Internet; ● Network Objects ○ IP Address ○ Geo Loc

Network Services: HTTP; HTTP+S

Destination: Management IP; Ref: MyPublicIP; ● Network Objects ○ IP Address ○ Geo Loc

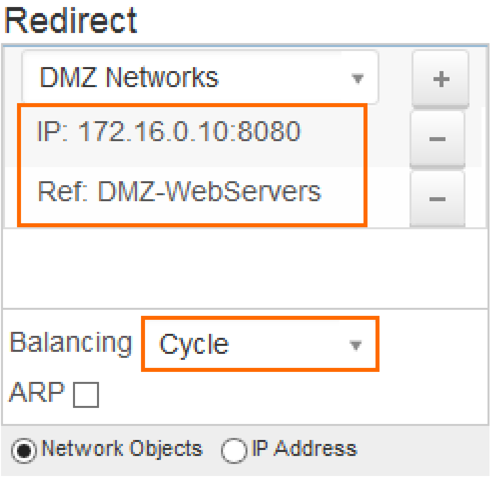
Redirect: IP: 172.16.0.10:8080; Balancing: Cycle; ARP □; ○ Network Objects ● IP Address

5. Click **Save**.

Step 2. (optional) Load Balancing Additional Web Servers in the DMZ

To redirect to more than one web server in cycle (round robin) or fallback mode, you can either add additional IP addressees to the network object, or enter additional IP addresses to the **Redirect** list. In fallback mode, all traffic is sent to the first IP address in the list (or network object). If that IP address is no longer reachable, traffic is sent to the second, and so forth. In cycle mode, the traffic is distributed to all IP addresses in the **Redirect** list based on the source IP address of the traffic. In this example, we used a network object containing 2 IP addresses (172.16.0.11 and 172.16.0.12) and left the original IP address 172.16.0.10 on port 8080 from step 2. HTTP and HTTPS traffic is now cycled between:

- 172.16.0.10:8080
- 172.16.0.11 port 80 or 443 as the chosen network services **HTTP+S** allows for those ports
- 172.16.0.12 port 80 or 443 as the chosen network services **HTTP+S** allows for those ports



Redirect

DMZ Networks

IP: 172.16.0.10:8080

Ref: DMZ-WebServers

Balancing: Cycle

ARP □

● Network Objects ○ IP Address

Step 3. Verify the Order of the Access Rules

New rules are created at the bottom of the firewall ruleset. Rules are processed from top to bottom in the ruleset. Drag your access rule to a slot in the rule list, so that no access rules before it matches this traffic. Verify that your rules are placed above the BLOCKALL rule. Otherwise, the rule never matches.

After adjusting the order of the rules in the ruleset, click **Save**.

Figures