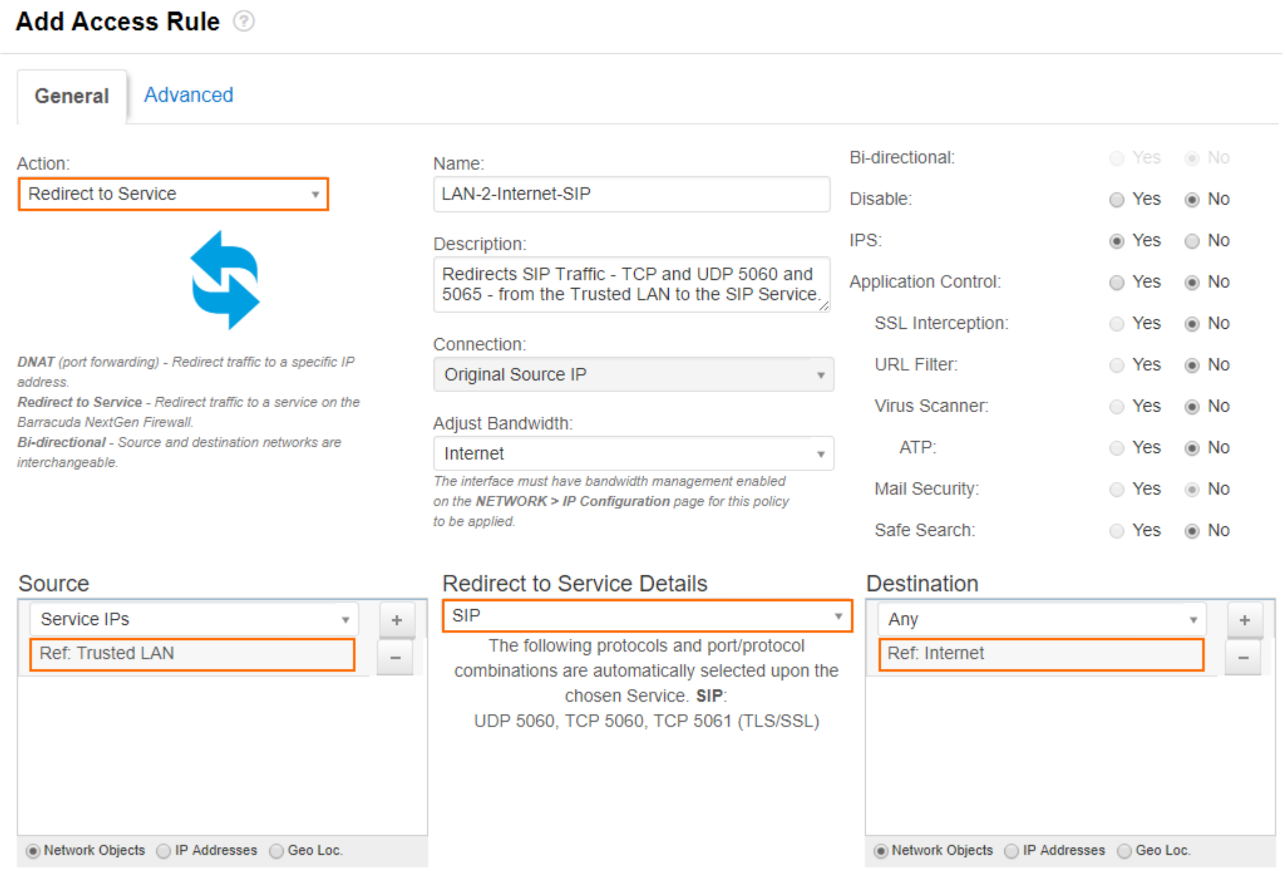
How to Create a Redirect-to-Service Access Rule

https://campus.barracuda.com/doc/73698498/

The Redirect to Service access rule rewrites the destination IP address and forwards the traffic to a service running on the firewall. For example, you can use an app redirect rule to transparently redirect all web traffic over the SIP proxy service.

Create a Redirect-to-Service Access Rule

1. Go to **FIREWALL > Access Rules**.
2. Click **Add Access Rule** to create a new rule. The **Add Access Rule** window opens.
3. Select **Redirect to Service** as the action.
4. Enter a name for the rule. E.g., `LAN-2-Internet-SIP`
5. Specify the following settings that must be matched by the traffic to be handled by the access rule, and click **+** after each entry:
    - **Source** – The source addresses of the traffic.
    - **Redirect to Service Details** – Select the service the traffic should be redirected to.
    - **Destination** – The destination address(es) of the traffic.
6. (optional) Configure **Advanced** settings. For more information, see Advanced Access Rule Settings.



Add Access Rule

Action: Redirect to Service

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

Name: LAN-2-Internet-SIP

Description: Redirects SIP Traffic - TCP and UDP 5060 and 5065 - from the Trusted LAN to the SIP Service.

Connection: Original Source IP

Adjust Bandwidth: Internet

*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
SSL Interception: ○ Yes ● No
URL Filter: ○ Yes ● No
Virus Scanner: ○ Yes ● No
ATP: ○ Yes ● No
Mail Security: ○ Yes ● No
Safe Search: ○ Yes ● No

Source
Service IPs
Ref: Trusted LAN
● Network Objects ○ IP Addresses ○ Geo Loc.

Redirect to Service Details
SIP
The following protocols and port/protocol combinations are automatically selected upon the chosen Service. **SIP**:
UDP 5060, TCP 5060, TCP 5061 (TLS/SSL)

Destination
Any
Ref: Internet
● Network Objects ○ IP Addresses ○ Geo Loc.

7. Click **Save**.
8. Drag and drop the access rule so that it is the first rule that matches the traffic that you want it to forward. Ensure that the rule is located above the BLOCKALL rule; rules located below the BLOCKALL rule are never executed.

Additional Matching Criteria

- **Valid for Users** – For more information, see User Objects.
- **Apply only during this time** – For more information, see Schedule Objects.

Additional Policies

- **IPS** – For more information, see Intrusion Prevention System (IPS).
- **Application Control** – For more information on Application Control features, see Application Control.
- **Adjust Bandwidth** – For more information, see Traffic Shaping.

Figures

1. redir_rule.png