Firewall Rules

https://campus.barracuda.com/doc/13305526/

Access rules are used to manage traffic going through the NextGen Firewall X-Series. The firewall service is tightly integrated with Application Control, IPS, and the URL Filter service.

About Firewall Objects

Use firewall objects to reference specific networks, services, user groups, or connections when creating firewall access rules. You can use the firewall objects that are preconfigured on the NextGen Firewall X-Series or create custom firewall objects. The main purpose of firewall objects is to simplify creation and maintenance of access rules. Firewall objects are re-usable, which means that you can use one firewall object in as many rules as required. Each firewall object has a unique name that is more easily referenced than an IP address or a network range (see Firewall Objects).

Video Demo

Watch the video below for a short demo on how to configure access rules.

Access Rule Settings

For each access rule, you can configure the following settings:

- **Name** – The name of the access rule. This name is displayed on the **BASIC > Active Connections**, **Recent Connections**, and **IPS Events** pages.
- **Description** – An additional description field for the access rule.
- **Action** – Specifies how the firewall handles network traffic that matches the criteria of the rule. The following actions are available:

- **Allow/Block** – Allow: The firewall passes all network traffic that matches the access rule. Block: The firewall ignores all network traffic that matches the access rule and does not answer to any packet from this particular network session.
- **Reset** – The firewall dismisses all network traffic that matches the access rule. Matching network sessions are terminated by replying **TCP-RST** for TCP requests, **ICMP Port Unreachable** for UDP requests, and **ICMP Denied by Filter** for other IP protocols.
- **DNAT** – The firewall rewrites the destination IP address, network, or port to a predefined network address. Enter multiple destination IP addresses for load balancing or fallback configurations. To additionally forward to a different port, you can append the port number to the IP address. E.g., 172.16.0.10:80
- **Redirect to Service** – The firewall redirects the traffic locally to one of the following services that are running on the firewall: Caching DNS, SIP Proxy, HTTP Proxy, VPN, SSL VPN, or NTP.

- **Connection** – Defines the outgoing interface and source (NAT) IP address for traffic matching the access rule. The following table lists the five default connection objects:

Predefined Connection Object	Outgoing Interface and IP Address Determined By
Default (SNAT)	Change the source IP address of network packets to the IP address of the interface with the lowest metric according to the routing table.
No SNAT	Connection is established using the original source IP address. Use if simple routing with NAT is desired.
SNAT with DSL IP	Source NAT with the IP address of the DSL uplink.
SNAT with 3G IP	Source NAT with the IP address of the 3G uplink.
SNAT with DHCP IP	Source NAT with the IP address of the DHCP uplink.

  You can also create custom connection objects. For example, multiple source IP addresses and interfaces can be specified in the same connection object. This allows failover or session-based balancing between up to four links. Balancing can be achieved using either a round robin or weighted random algorithm.

- **Service** – Describes the protocol and protocol/port range of the matching traffic. You can define one or more services for the access rule. You can select a predefined service object or create your own service objects (see: Service Objects).
- **Source** – The source IP address/netmask of the connection that is affected by the rule. You can select a network object or explicitly enter a specific IP address/netmask. You can also create your own network objects (see: Network Objects).
- **Destination** – The destination IP address/netmask of the connection that is affected by the rule. You can select a network object or explicitly enter a specific IP address/netmask.

Bandwidth Policies

You can adjust the bandwidth for all matching traffic:

- Bandwidth policies protect the available overall bandwidth of the Internet connection. Network traffic is classified and throttled or prioritized within each access rule. To adjust the overall bandwidth of each network interface, go to the **NETWORK > IP Configuration** page. There are eight predefined bandwidth policies. For additional information, see How to Configure Bandwidth Policies or QoS.
- Bandwidth policies for application traffic are configured in the application policy rules. For more information, see How to Configure an Application Policy.

Users/Time

For more granular control, you can configure access rules that are applied only to specific users or during specific times.

- Users can be used as a criteria for the rule. Use the Barracuda DC Agent to enable the firewall to be aware of which connection belongs to a specific user. You can also create users objects (see: User Objects).
- You can create access rules that are only active for specific times or dates. For example, you can create a time object that includes only Mondays and the hours of 8:00 am to 9:00 am. An access rule including this time object will only allow traffic during the time span defined in the time object (see: Schedule Objects).

Advanced

You can also configure the following advanced firewall settings:

- **Interface Group** – When creating an access rule, you can assign interfaces that the source address is allowed to use. Arriving packets of traffic that match the rule are then processed to the specified network interfaces according to the interface group settings. For more information, see How to Create Interface Groups.
- **SYN Flood Protection** – SYN flood protection protects against a common kind of DoS attack. The firewall can eliminate SYN flooding attacks for inbound or outbound attacks. The firewall completes the handshake and only then performs a handshake with the actual target. This helps to protect the target from SYN flood attacks. Disabling SYN flood protection can cause an overhead in packet transmission, but can speed up interactive protocols like SSH. For optimal protection, **SYN Flood Protection** needs to know the **Maximum Sessions** and the **Maximum Sessions per Source** IP address that can be opened before the firewall takes measures. In **Always On** mode, the firewall compares these two values against the current session values, blocks the source IP if one of the two limits is exceeded, and frees the allocated session resources. In **Automatic** mode, the firewall switches to a different TCP handshake mode to protect the network.