Access Rules

https://campus.barracuda.com/doc/53248318/

By default, without any access rules in the ruleset, all traffic is blocked by the firewall. To allow traffic, you must create rules for IPv4 and IPv6 traffic in the firewall ruleset and place them in the correct order. Both host and firewall services have their own dedicated rulesets. These rulesets determine the order in which incoming traffic is matched against the access rules. Rules are processed from the top to the bottom; the first access rule that matches is executed. If the traffic does not match the first rule, the next rule is then evaluated, continuing in this way from top to bottom until a matching rule is found. If none of the rules match, the connection is blocked. Place the more granular, specific rules toward the top of the ruleset, and the broader, general rules toward the bottom. An access rule will not match if a rule before it matches the same traffic.

Access-rule Matching Criteria

For an access rule to match, you must configure the following matching criteria:

- **Service** – 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 to be handled by the rule. You can select a network object or explicitly enter a specific IP address/netmask.
- **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.
- **(optional) Schedule/Time** – Use a schedule object as a matching criteria. For more information, see Schedule Objects.
- **(optional) User** – Use a user object as as a matching criteria. For more information, see User Objects.

IPv4 Access Rule Actions

The action specifies how the firewall handles network traffic that matches the criteria of the rule. The following actions are available

- **Pass** – All traffic matching the access rule is forwarded.
- **Block** – All traffic matching the access rule is ignored. Matching connection attempts are not answered.
- **Deny**– All traffic matching this access rule is dismissed. 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.
- **Dst NAT** – The firewall rewrites the destination IP address, network, or port to a predefined network address.

- **Map** – The firewall rewrites IP ranges or networks to a predefined network or IP range.
- **App Redirect** – The firewall redirects the traffic locally to one of the services running on the F-Series Firewall.
- **Broad Multicast** – Broadcasts matching this rule are forwarded. This is used for bridged networks.
- **Cascade** – Jump to and evaluate a different rule list.
- **Cascade Back** – Jump back to the global rule list and resume evaluation of the access rules below the cascade rule.

IPv6 Access Rule Actions

- **Bock**
- **Deny**
- **Pass**
- **Cascade**

Fore more information, see How to Create IPv6 Access Rules.

Connection Methods

The settings in the connection object determine the outgoing interface of the packet. For IPv4 traffic, you can also configure source NAT and PAT. The connection object also contains the policies of how traffic is distributed over the available interfaces in the **Failover and Load Balancing** section.

For more information, see Connection Objects.

Troubleshooting Blocked Connections Video

To get a feel for how to use access rules, and how NextGen Admin allows you to determine which rules to create, watch the following video: