Advanced Access Rule Settings

https://campus.barracuda.com/doc/72516172/

In some cases, you may have to modify the default behavior of your firewall by changing the advanced access rule parameters. Some of these parameters can be used to increase the security level while others provide rarely needed exceptions to the strict default security policy of the firewall. Bandwidth policy settings are located in the access rule **General** tab. To configure other advanced access rule settings, click the **Advanced** tab in the rule, and select the required option.

> The advanced parameters of an access rule can impact security if not properly configured. Ensure that you fully understand the functionality of a parameter before you change it.

Bandwidth Policies

You can adjust the bandwidth for all matching traffic.

Bandwidth policies protect the overall available 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 **NETWORK > IP Configuration**. There are eight predefined bandwidth policies. To adjust the bandwidth in an access rule, select the bandwidth policy from the **Adjust Bandwidth** list.

For more information, see Traffic Shaping.

User Restrictions

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. To limit an access rule to a specific user or user group, click the **Advanced** tab in the rule, add one or more user objects from the **Valid for Users** list, and click **+**.

For more information, see User Objects.

Time Restrictions

You can create access rules that are active only for specific times or dates. For example, you can create a schedule object that includes only Mondays and the hours of 8:00 a.m. to 9:00 a.m. An access rule including this schedule object will only allow traffic during the time span defined in the object. To let the access rule apply only during the specified time, select the schedule object from the **Apply only during this time** list.

For more information, see Schedule Objects.

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. Choose an interface group as configured in **NETWORK > Interface Groups**. Select **Any** to match all interfaces.

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.

To configure SYN flood protection in an access rule, select an option from the **SYN Flood Protection** list:

- **Automatic** – Detects SYN flood attacks when a threshold is exceeded and then protects the system against them. The threshold is 20% of the maximum sessions/requests supported by the firewall.
- **Always On** – Protection is always on. This is more resource–intensive and can cause session flow issues.

Maximum Sessions

You can restrict the maximum number of accepted concurrent connections for this access rule. If set to 0, the number of allowed sessions for this rule is unlimited. Otherwise, sessions exceeding this limit

are blocked.

Maximum Sessions per Source

You can restrict the maximum number of accepted concurrent connections per source address. If set to 0, the number of allowed sessions per source IP allowed for this rule is unlimited. Otherwise, additional sessions from the same source IP exceeding this limit are blocked. This setting can be used to prevent Denial of Service (DoS) attacks against a specific server.

Transparent Redirect

Enable to transparently forward traffic to the destination without changing the header info.

Google Accounts

Enable **Google Accounts** to activate Google Accounts filtering for this access rule. If enabled, only accounts that belong to the Google Apps Domains specified in **Firewall > Settings** are allowed to log on to Google. Private Google accounts using the gmail.com domain are always blocked when this option is enabled.