Advanced Firewall Rule Settings

https://campus.barracuda.com/doc/41115741/

In some specific situations, you may have to modify the default behavior of your firewall by changing the advanced firewall 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 Barracuda NG Firewall.

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

Advanced Firewall Rule Settings

Rule Mismatch Policy

Usually, a connection request is required to match the source, service, and destination of a rule. By default, the firewall continues to the subsequent rule in the rule set if one of the three conditions is not met. If you do not want a rule to be bypassed, you can change the policy for mismatches to the rule conditions.

The following policies are available for **Source**, **Destination**, **Service**, **User**, and **MAC** address condition mismatch:

- **CONTINUE on Mismatch** (default) – Continues processing the next firewall rules.
- **BLOCK on Mismatch** – Ignores all traffic and does not answer to any matching packet (= silent drop).
- **DENY on Mismatch** – Dismisses all traffic and sends TCP-RST (for TCP requests), ICMP Port Unreachable (for UDP requests), or ICMP Denied by Filter (for other IP protocols) to the source.

If you want the session to be re–evaluated when the rule set or authentication settings are changed, enable the **Persistence** setting.

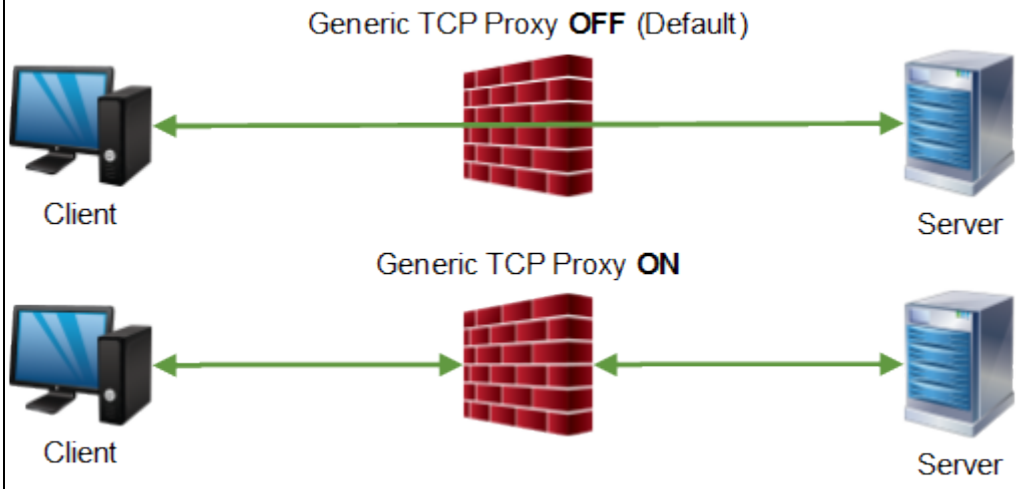
Example Use Case

Two machines in your LAN have access to a database server on a critical port (for example, telnet). You want to ensure that no other rule accidentally allows access for a source other than these two clients. In this case, select **Block on Mismatch** from the **Source** list in the **Rule Mismatch Policy** section of the **Advanced Rule Parameters** window.

The effect of these options is cumulative. If you check two options, you blank out the remaining values for all subsequent rules.

TCP Policy

In the **TCP Policy** section, you can edit the following TCP policy settings for traffic that is handled by the firewall rule:

Setting	Description
Generic TCP Proxy	The firewall engine is capable of two TCP forwarding methods: • **Application Controlled Packet Forwarding (ACPF) / Generic TCP Proxy OFF** – (Default) The firewall does not terminate the TCP connection. The TCP connection is directly established between the source and destination. Malformed packets are filtered by ACPF. • **Generic TCP Proxy ON** – Also called Stream Forwarding. If you want to avoid any direct TCP connection between two TCP partners traversing the firewall, use stream forwarding to build two distinct TCP connections. The destination will not get any packets that are not generated by the firewall TCP stack itself, making it impossible for a potential attacker to exploit a security flaw in the destination servers TCP stack. Selecting this option reduces the performance of the firewall (400 - 500 MBit maximum). The security advantage of stream forwarding is not as important today as it was when firewall engines were less powerful. For detailed performance data, contact Barracuda Networks Technical Support.  **Features not available when using the Generic TCP Proxy:** • Application Detection • High availability (HA) synchronization • Intrusion Prevention System (IPS) • Network Address Translation (NAT) • Plug-ins • TCP State Detection

Syn Flood Protection (Forward/Reverse)	Defines the behavior of the firewall with regard to the TCP three-way-handshake. You can select the following options: • **Server Default** – Uses the default configuration. • **Outbound** – Passes the SYN untouched through to the target address. • **Inbound** – 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 this option may speed up interactive protocols like SSH. For more information, see Best Practice - Protect Against TCP SYN Flooding Attacks with TCP Accept Policies.
Accept Timeout (s)	Length of time that the firewall waits until the destination has to answer. After this timeout, the firewall sends a TCP RST packet to both partners (default: 10).
Last ACK Timeout (s)	Length of time in seconds that the firewall waits after an ACK to terminate the connection (default: 10).
Retransmission Timeout (s)	Length of time in seconds that the firewall waits until the source has to retransmit packets. If nothing happens, the firewall registers the session as a hijacking attempt (default: 300 seconds).
Halfside Close Timeout (s)	Length of time in seconds that the firewall waits after conscious termination of the connection to close the socket (default: 30).
Disable Nagle Algorithm	Enables TCP_NODELAY. This option is only available when the **Generic TCP Proxy** is enabled.
Force MSS (Maximum Segment Size)	Checks the SYN and SYN–ACK TCP packets for an MSS that is larger than the configured MSS. If the MSS TCP attribute is smaller, the packet is rewritten with the configured MSS. Use this feature for VPNs to force a TCP MSS that fits the MTU of the VPN tunnel device. For IPv4, the maximum transmission size must be at least 40 bytes smaller than the MTU.
Raw TCP mode	Handles sole chunks of TCP traffic without analyzing the entire contiguous TCP stream to allow routing loops. However, this mode is limited in terms of intrusion prevention, application detection, overall TCP state tracking, and other aspects. Raw TCP mode must be explicitly enabled in a forwarding firewall rule. Raw TCP sessions are not synchronized. You must only use this feature when it is absolutely necessary. It does not replace Traffic Intelligence or the Graphical Tunnel Interface. Raw TCP mode can also decrease the overall performance of the system. The following features are ***not*** available in Raw TCP mode: • Application Control 2.0 • Legacy Level 7 Application Detection • High Availability (HA) Synchronization • Intrusion Prevention System (IPS) • Network Address Translation (NAT) • Firewall Plugin Modules • TCP State Detection • WAN Optimization

Resource Protection

In the **Resource Protection** section, you can specify the following session limits to conserve your system resources:

Setting	Description
Allow to exceed global session limits	Allow this access rule to override the global session limits defined in the General Firewall Configuration.
Max Number of Sessions	Maximum number of accepted concurrent connections for this rule on a global basis (default: `0` = unlimited). If the **Rule Limit Exceeded** setting is enabled in your event monitor settings, the FW Rule Connection Limit Exceeded [4016] event is generated when the **Max Number of Sessions** limit is exceeded.
Max Number of Sessions per Source	Maximum number of accepted concurrent connections per source address (default: `0` = unlimited). You must only specify this limit if your system is susceptible to Denial of Service (DoS) attacks. If the **Source/Rule Limit Exceeded** setting is enabled in your event monitor settings, the FW Rule Connection per Source Limit Exceeded [4018] event is generated when the **Max. Number of Sessions per Source** limit is exceeded.
Session Duration Limit (s)	Maximum length of time in seconds that the session can stay active. By default, there is no duration limit for the session. This setting is only executable in the forwarding firewall; it does not affect the local firewall.

Counting / Eventing / Audit Trail

In the **Counting / Eventing / Audit Trail** section, define when events are logged or written to the access cache.

Setting	Description
Firewall History Entry	Save the connection information to the firewall history. (default: **Yes**).
Log File and FW Audit Entry	Obtains log file entries (default: **Yes**).
Transparent Failover State Sync	Synchronizes the session on a high availability system (default: **Yes**).

Statistics Entry	Obtains statistics (default: **Yes**). If you select **No**, global firewall statistics are not generated and information is not displayed in the firewall dashboard.
Log Session State Changed	Logs changes of session states (default: **No**).
Own Log File	Saves all log events in an extra log file (default: **No**).
Service Statistics	Generates service statistics for this rule (default: **No**).
Eventing	The severity level of the rule's event messages. Host firewall rules are not affected by this setting. You can select the following event levels to be generated if a forwarding firewall rule matches: • **None (default)** – No events are generated. • **Normal** – Generates the FW Rule Notice [4020] event. • **Notice** – Generates the FW Rule Warning [4021] event. • **Alert** – Generates the FW Rule Alert [4022] event. In the event settings, you can specify actions for these event messages. For more information, see How to Configure Event Settings. Regardless of this setting, forwarding as well as host firewall rules will generate event messages if *BLOCK on Mismatch* is selected for any of the **Rule Mismatch Policy** settings.
Application Log Policy	• **Default** – No detected applications are logged. • **Log Blocked Applications** – Only blocked applications are logged. • **Log Allowed Applications** – Allowed applications are logged. • **Log All Applications** – All detected applications are logged.

Miscellaneous

In the **Miscellaneous** section, you can edit the following settings:

Setting	Description
Authentication	The required user authentication method for HTTP and HTTPS connections. You can select the following authentication methods: • **No Inline Authentication (default)** • **Login+Password Authentication** • **X509 Certificate Authentication** • **X509 Certificate & Login+Password Authentication** For more information about authentication, see Firewall Authentication and Guest Access.

IP Counting Policy	You can select the following policies: • **Default Policy** – Uses the interface realm settings that are assigned in the network configuration for the local networks and interface routes. Depending on the specified realm, the source or destination IP counts. The **Default Policy** is hard-coded and cannot be changed in the Barracuda NG Firewall configuration. • **Count Source IP** – Counts source IP addresses towards license limits. • **Count Destination IP** – Counts destination IP addresses towards license limits. For more information on protected IP addresses, see Licensing.
Time Restriction	Applies a time restriction to rules that are configured with a feature level that is equal to or lower than 3.2.
Clear DF Bit	The DF bit determines whether a packet can be fragmented or not. In networks where packet size is limited to an MTU, packet fragmentation may become vital when packets sent to this network exceed the MTU (for example, as may frequently occur with SAP applications). Because the firewall must not override the DF bit setting, fragmentation is up to the client. When the DF bit is set and the target network's MTU specification requires fragmentation, the firewall responds with an ICMP `Destination Unreachable` message (`Code 4: Packet too large. Fragmentation required but DF bit in the IP header is set`). If the client does not understand the answer code, data transmission fails and data loss may occur if packet sizes exceed the MTU of the network. Before enabling this setting, consider the following points: • The fragmentation and packet reassembling process might lead to significant performance loss at high traffic rates. • The maximum segment size (MSS) is automatically decreased as necessary when traffic is routed through the respective VPN. • Encapsulating packets reduces the available MTU size. The DF bit is automatically cleared from traffic, which is forwarded towards a VPN interface. • Only enable this setting when experiencing transport problems that are clearly associated with packet size restrictions. To clear the DF bit from the IP header and fragment packets if necessary regardless of the setting in the packet's IP header, select *Yes*. By default, this setting is disabled.
Set TOS Value	The TOS value. By default, the value is set to *0* (TOS unchanged).
Prefer Routing over Bridging	Controls the routing behavior of routed transparent Layer 2 bridges. To route traffic over bridges that are configured on the Barracuda NG Firewall, select **Yes**. Enable this setting when an external router connects the bridges and traffic should not be directed to this router. If traffic is first routed to the external router, it is rejected because it passes the gateway twice. By default, this setting is disabled. For more information on routed transparent Layer 2 bridges, see How to Configure Routed Layer 2 Bridging.
Color	The color of the rule in the rule set.

Quarantine Policy

In the **Quarantine Policy** section, you can select one of the following rule matching policies for evaluating sessions to and from a specific quarantine class:

- **Match** – The rule matches.
- **Block** – The rule blocks the request.
- **Deny** – The rule denies the request.
- **Continue** – Rule evaluation continues with the next rule in the rule set.

A session is only evaluated when it matches the specified policy for the following settings:

Setting	Description
LAN Rule Policy	Matching policy for sessions to and from a non–quarantine net.
Quarantine Class 1 Rule Policy	Matching Policy for sessions to and from a Quarantine class 1 net.
Quarantine Class 2 Rule Policy	Matching Policy for sessions to and from a Quarantine class 2 net.
Quarantine Class 3 Rule Policy	Matching Policy for sessions to and from a Quarantine class 3 net.

Dynamic Interface Handling

Setting	Description
Source Interface	Restricts rule processing to the specified dynamic network interface (if installed and configured).
Continue on Source Interface Mismatch	Continues with rule processing, even if no matching interface can be found. The subsequent rule is then used for rule evaluation.
Reverse Interface (Bi-directional)	The interface that the destination address is allowed to use. Only applicable for bi-directional rules.
Interface Checks After Session Creation	Disables interface checks. Only applicable for bi-directional rules.

Figures