General Firewall Configuration

https://campus.barracuda.com/doc/53248706/

To adjust resources used by your firewall service, you can change the sizing parameters in the **General Firewall Configuration** (**CONFIGURATION > Configuration Tree > Box > Infrastructure Services**) section of the Barracuda NextGen Firewall F-Series. After changing general firewall configuration settings, perform a **Firmware Restart** (**CONTROL > Box**) for the changes to take effect. Default values vary depending on the model.

Firewall Sizing

Maximum Number of Connections

- **Max Session Slots** – Set the maximum number of session slots allowed. The amount of memory consumed by the firewall is updated when this value is changed and displayed in the **Firewall Memory [MB]** field. (When set to the default value, the firewall service will consumer about 150 MB RAM.)

  If you set this parameter to the maximum allowed value, you will need to add vmalloc=896M to the the kernel boot parameters and execute a reboot. For more information, see How to Configure the Bootloader.
- **Max UDP (%)** – Defines the percentage of the **Max Session Slots** allowed to be UDP sessions.

  With eventing activated (parameter **UDP Limit Exceeded** set to *yes*), the event *FW UDP Connection Limit Exceeded [4009]* is generated when the limit is exceeded.
- **Max Echo (%)** – Defines the percentage of the **Max Session Slots** allowed to be ICMP sessions.

  With eventing activated (parameter **Echo Limit Exceeded** set to *yes*), the event *FW ICMP-ECHO Connection Limit Exceeded [4027]* is generated when the limit is exceeded.
- **Max Other (%)** – Defines the percentage of the **Max Session Slots** allowed to be an IP protocol type, except TCP, UDP, or ICMP.

  With eventing activated (parameter **Other Limit Exceeded** set to *yes*), the event *FW OTHER-IP Session Limit Exceeded [4029]* is generated when the limit is exceeded.
- **Firewall Memory [MB]** – Displays the estimated memory requirement according to the current firewall configuration settings. If the value exceeds 200 MB, an additional bootloader parameter may be required. On i686-based F-Series Firewalls with more than 768 MB RAM requiring additional vmalloc space to satisfy the increased memory demand of non-default firewall settings, we recommend to increase the vmalloc area in steps of 128 MB, starting at 384 MB. For more information, see How to Configure the Bootloader .

  Reboot the box after setting the parameter, and wait until the firewall service successfully starts after the system boot. Do not use vmalloc areas larger than 640 MB. The vmalloc area is shared among several kernel subsystems. Therefore, the exact size of the allocated vmalloc area that is required to load the firewall cannot be predetermined. Setting the **vmalloc** parameter to **enable increased acpf memory operation** is discouraged on systems with 768 MB of RAM or on "i386" architecture systems. Setting

this parameter on those boxes could negatively affect the system performance and/or stability. The architecture of an installed F-Series Firewall box can be determined with the following command: *rpm -q kernel --qf %{ARCH}\\n.*

Global Limits 1

- **Max SIP Calls** – Set the maximum number of concurrent SIP calls that can be handled by the legacy SIP firewall plugin.
  Barracuda Networks recommends using the SIP proxy service instead of the SIP firewall plugin.
- **Max SIP Transactions** – Set the maximum amount of SIP transactions that can be handled by the legacy SIP firewall plugin.
- **Max SIP Media** – Define the maximum amount of SIP Media (RTP) connections allowed for the legacy SIP firewall plugin. The inactivity timeout for the media connections can be configured by setting the **Balanced Timeout** for the service object.
- **Max DNS Entries** – Defines the maximum number of DNS queries that may be triggered by use of network objects containing hostnames. 75% of the queries are reserved for the forwarding firewall and 25% for the host firewall. Network objects used in both forwarding and host firewall rulesets will trigger two DNS queries and be counted twice.
  The firewall can only match on IP addresses. When the maximum amount of allowed DNS queries are exceeded, hostnames can no longer be resolved, causing access rules using these networks objects to never match.
- **Max Acceptors** – Maximum number of pending accepts for inbound rules. An acceptor is a dynamic implicit rule that is generated by plugins handling dynamic connection requests. The FTP protocol, for example, uses a data connection beside the control connection on TCP port 21 to perform the actual file transfer. By analyzing the FTP protocol, the firewall knows when such data connections occur and creates an acceptor to allow the corresponding data transfer session.
- **Max Pending Inbounds** – Maximum number of pending TCP inbound requests. This parameter only comes into effect when the TCP accept policy is set to inbound for the access rule.
- **Max BARPs** – Defines the maximum number of bridging ARPs allowed. A bridging ARP entry (BARP) stores the information that specifies which bridge interface corresponds to a certain MAC address. Additionally, associated IP addresses are stored along with the BARP entry. Modifying this value may be useful for large bridging setups.
- **Max Plugins** – Maximum number of rules using plugins.
- **Dyn Service Names (RPC)** – Maximum number of dynamic service name entries.

Global Limits 2

- **Inbound Mode Threshold (%)** – Threshold of pending accepts, at which point the firewall switches to the inbound TCP accept policy to guard against SYN flooding attacks.
- **SYN Cookie High Watermark (%)** – Percentage (of maximum pending inbounds) of pending inbound accepts to switch to SYN cookie usage for enhanced SYN flooding protection.
- **SYN Cookie Low Watermark (%)** – Percentage (of maximum pending inbounds) of pending inbound accepts to go back to ordinary SYN handling.
- **Max Dynamic Rules** – Maximum number of dynamically activated rules.

- **Max Multiple Redirect IPs** – Maximum number of IP addresses in rules with multiple redirect target IPs.
- **Max SOCKS Workers** – Maximum number of available SOCKS workers when the Generic TCP proxy mode is enabled.

Source-Based Session Limits

- **Max Local-On Session/Src** – Maximum number of sessions per source IP address. Cannot be set to more than **Max Session Slots**.
  With eventing activated (parameter **Session/Src Limit Exceeded** set to *yes*), the event *FW Global Connection per Source Limit Exceeded [4024]* is generated when the limit is exceeded.
- **Max Local-In UDP/Src** – Maximum number of UDP sessions per source IP address.
  With eventing activated (parameter **UDP/Src Limit Exceeded** set to *yes*), the event *FW UDP Connection per Source Limit Exceeded [4008]* is generated when the limit is exceeded.
- **Max Local-In Echo/Src** – Maximum number of ICMP Echo sessions per source IP.
  With eventing activated (parameter **Echo/Src Limit Exceeded** set to *yes*), the event *FW ICMP-ECHO Connection per Source Limit Exceeded [4026]* is generated when the limit is exceeded.
- **Max Local-In Other/Src** – Maximum number of sessions for all other IP protocols (not TCP, UDP, ICMP) per source IP address.
  With eventing activated (parameter **Other/Src Limit Exceeded** set to *yes*), the event *FW OTHER-IP Connection per Source Limit Exceeded [4028]* is generated when the limit is exceeded.
- **Max Pending Local Accepts/Src** – Maximum number of pending accepts per source IP address.

History Cache

The firewall history stores connection information for troubleshooting purposes. You can configure how many and how long connections are stored in the **General Firewall Configuration** settings. Use the **Advanced View** to configure these settings.

- **Max. Access Entries** – Determines the size of the visualization caches.
- **Max. Block Entries** – Determines the maximum number of block entries.
- **Max. Drop Entries** – Determines the maximum number of drop entries.
- **Max. Fail Entries** – Determines the maximum number of fail entries.
- **Max. Scan Entries** – Determines the maximum number of scan entries.
- **DNS Resolve IPs** – Setting this parameter to **yes** will resolve IPs to hostnames on the firewall history. This may cause excessive load on the DNS servers.

Operational

Ruleset-Related Settings

- **Rule Matching Policy** – Selects the way in which a rule lookup is performed.
  - **Kernel space** – linear lookup – adequate for small rulesets.
  - **Kernel space** – tree lookup – preferred option for large rulesets with hundreds of rules. As a rule of thumb, for about 1000 session/s the Kernel space should be enabled for better firewall performance. Additionally, if many firewall objects (> 200) are used, the Kernel space - tree option is recommended.
- **Rule Change Behavior** – This setting only applies to the forwarding firewall and not to the host firewall, because the host firewall generally does not allow re-evaluation of a session upon a rule-change. The setting specifies whether an existing connection is terminated (**Terminate-on-change** or not (**Keep-on-change**) if the ruleset changes and the session is no longer allowed by the new ruleset.
- **No Rule Update Time Range** – This option allows defining a time range during which access rules may not be updated. Use international time format. For example, to disallow rule update from 14:00 through 22:00, insert 14-22.

Default TCP Policy

- **Syn Flood Protection** – Defines the default behavior of the firewall with regard to the TCP three-way handshake.
  - **Outbound** – Passes on the SYN 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 will cause an overhead in packet transmission, but may speed up interactive protocols like SSH.
- **Nagle Algorithm** – This parameter enables/disables the Nagle algorithm. This option is only available when using stream forwarding.
- **Perform TCP Sequence Check** – This parameter enables/disables TCP sequence checks.You can select one of the following options:
  - **RST-Packets-Only**
  - **All Packets**
  - **None**

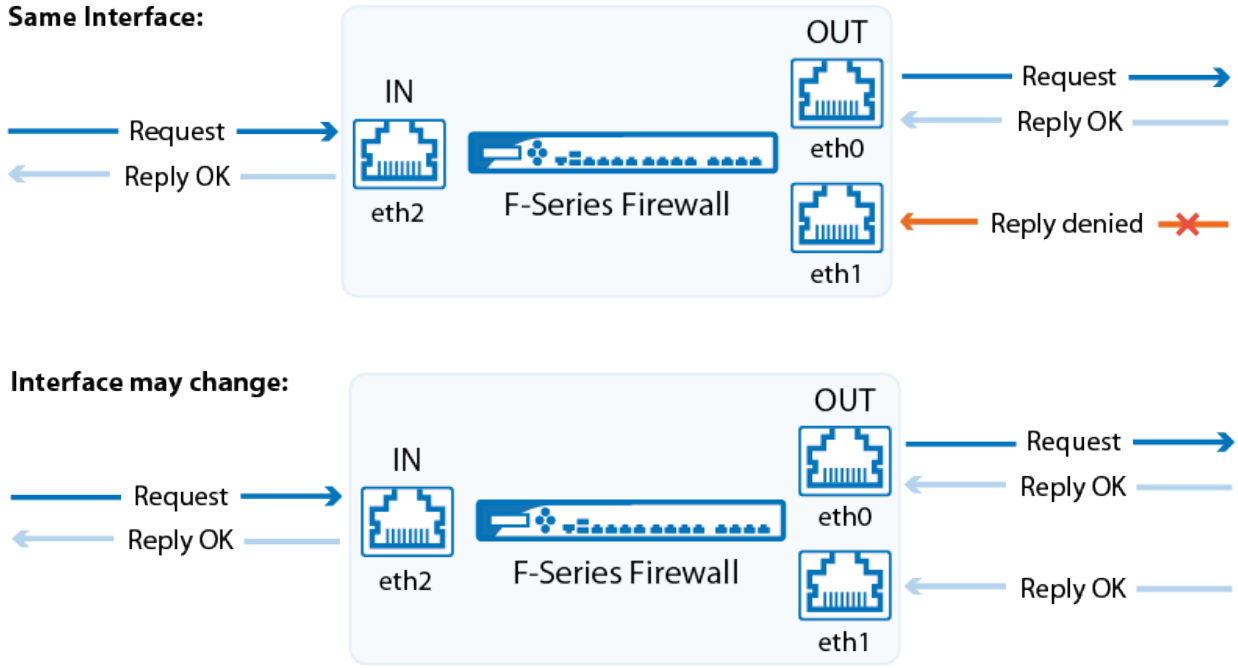
Raw TCP Mode Policy

- **RAW TCP Idle Timeout** – Defines the idle timeout value in seconds for RAW TCP mode.
- **RAW TCP Timeout Policy** – Defines the timeout policy that will be used for RAW TCP mode.
  - **Use-global-timeouts** – Sets the timeout value that has been configured in the previous sections.
  - **Use-tcp-timeouts** – Uses the timeout values from standard TCP set in the matching rule.

Default Anti-Spoofing Policy

- **ARP Reverse Route Check** – Setting this parameter to **Yes** causes answers to ARP requests to be checked if source IP and interface match.
- **Reverse Interface Policy** – The options of this parameter specify whether requests and replies must use the same (outgoing) interface (**same-interface** or not (**interface-may-change**).

  This parameter specifies the global policy. You may change the policy per rule, though it is NOT recommended to do so.



Port Scan Policy

- **Port Scan Threshold** – When the number of blocked requests exceed the threshold, a port scan is detected and a port scan event is triggered. To not generate an event, see How to Configure Basic, Severity, and Notification Settings for Events .
- **Port Scan Detection Interval** – Detection interval in seconds to check for not allowed activity. In combination with the parameter **Port Scan Threshold,** it defines the condition when to report a port scan.

Performance-Related Policies

- **Session Creation CPU Limit (%)** – (advanced) Reserves a specific amount of CPU resources for the Barracuda OS to prevent the firewall from becoming unmanageable in case of a high amount of concurrent sessions being initiated. Barracuda Networks recommends to keep the **Default** value.
- **Validate TCP Checksum** – (advanced) Enables an additional TCP packet consistency check. This will reduce performance.
- **Validate UDP Checksum** – (advanced) Enables an additional UDP packet consistency check. This will reduce performance.

- **Parallel Shaping Tree Evaluation** – (advanced)
  - **Disabled** – Disables this option.
  - **Enabled** – Improves shaping tree evaluation.
  - **Enable-MultiQueue-Only** – Enables this feature only for shaping trees built on top of interfaces with multiple hardware-queues or with RPS enabled.

High Availability Related Policies

- **Allow Active-Active Mode** – (advanced) Active-Active firewall operation mode has to be enabled in preparation for operation of multiple active firewalls on one box with a load balancer connected upstream.
- **Enable Session Sync** – (advanced) All currently established sessions will be synced to the HA partner to improve failover performance.
- **Log Synced Sessions** – (advanced) This setting determines logging of access cache sessions, which have been synchronized between HA partners. Set to **No** to disable logging.
- **Generically Forwarded Networks** – (advanced) Traffic between networks inserted into this field will be excluded from firewall monitoring and will be forwarded without source and destination differentiation, even if no forwarding firewall is installed.

  Local sessions are not reevaluated on rule change. This parameter only effects forwarding sessions. Workflow for enforcing changed local rules: manually terminate local sessions in the **Firewall Live** tab. Make use of this feature if you are operating your F-Series Firewall only for routing and NOT for firewall purposes because generic network forwarding might cause severe security issues.

Operational IPS

When TCP stream reassembly and HTML parsing are set to **auto** the operating system enables or disables these features to best match your current configuration and performance.

- **TCP Stream Reassembly for IPS** – Reassembles the TCP stream before scanning for vulnerabilities.
- **HTML Parsing for IPS** – Toggles HTML obfuscation detection. If this setting is changed, you must reboot for the changes to take effect.
- **IPS Scan Mode** – Select the scanning mode for IPS. You must reboot for the changes to take effect.
  - **Auto** – The firewall automatically chooses the best suited mode.
  - **Fast Scan** – Scan select packets to improve performance and throughput.
  - **Full Scan** – Scan all packets.

Operational VPN

- **VPN Rate Limit (Mbps)** – Limits how fast VPN traffic is encrypted and decrypted. Change this

value if you experience excessive CPU load in an environment with many VPN tunnels. The value 0 does not impose any restriction.

Restart the VPN service after changing this value. (**CONTROL > Server**). All active VPN connections will be terminated when restarting the VPN service.

- **Enable Assembler Ciphers** – Using the assembler implementation for AES/SHA/MD5 increases VPN performance significantly.
- **Enable Intel AVX Extensions** – Enables or disables the usage of Intel's AVX extension (also valid on AMD processors).
- **Enable VIA PadLock** – Enables or disables the usage of VIAs PadLock Security Engine.
- **Enable Cavium** – Enable or disable Cavium crypto acceleration cards.

  Reboot for this setting to take effect.
- **Globally clear DF bit** – Clears the DF bit for each ipv4 packet routed through a VPN tunnel. For more information on MTU, see Routing.

Application Detection

Resource Failure Policy

- **Out of Memory Policy** – An out of memory condition may disable protocol and application detection. As a consequence, all deeper analysis will be disabled as well.
  - **Fail-Open** – Select to continue forwarding.
  - **Fail-Close** – Select to terminate the affected sessions.

Url Categorization (URL Filter)

Always reboot the firewall after changing one of the following values!

- **Max. Cache Entries** – The maximum number of entries in the kernel cache. 0 is auto selection depending on RAM size.
- **Categorization Timeout [s]** – Set the maximum timeout to wait for categorization response.
- **Cache Entry Expiration [s]** – After the configured time, the cached entries category will be updated.
- **Cache Entry Expiration (no cat.) [s]** – After the specified time in seconds, the cached entries' category, with category 'not categorized' will be updated.
- **Cache Entry Expiration (err cat.) [s]** – After the specified time in seconds, the cached entries' category, with category 'assigning error' will be updated.

Application and Port Protocol Detection

- **Enable Port Detection** – Set to **yes** to use deep packet inspection to enforce the used protocol on a port. For more information, see How to Configure Port Protocol Protection

Application Detection Destination Tracking

- **Enable Destination Tracking** – Set to **no** unless specifically instructed otherwise by

Barracuda technical support.

Supervisory Control and Data Acquisition (SCADA)

- **SCADA Protocol Detection** – Enable to detect SCADA protocols.
  - **Disabled** – Detection is disabled.
  - **Enable without Parsing Log** – Detected SCADA protocols are included in the Firewall Activity log.
  - **Enable with Parsing Log** – Enabled with detailed logs (box/SCADA/parsing).

Audit and Reporting

Statistics Policy

- **Generate Dashboard Information** – Enable/disable the firewall dashboard.
- **Generate Monitor Information** – Enable the firewall monitor.
- **Maximum Storage Size [MB]** – Specify the storage size in megabytes to be used for monitor information data. A value of 0 enables automatic assignment based on the device.
- **Statistics for Host Firewall** – This option enables statistics for connections passing through the host firewall.
- **Generate Protocol Statistics** – If enabled, protocol and P2P-specific statistics are created and listed within the statistics viewer under .../server/BOX/proto-stat/...
- **Use username if available** – If set to **yes**, usernames are used for statistics, if available. Otherwise, the source IP address is used.

Eventing Policy

- **Generate Events** – Enable/Disable event generation.
- **Event Data** – Use this section to selectively enable or disable event generation.

Log Policy

- **Application Control Logging** – Select the global policy for Application Control 2.0 logging.
  This setting will be replaced by the rule log policy if specified.
- **Activity Log Mode** – Configure whether the Firewall Activity logs use key-value pairs or only log the values. Default: only values are logged.
- **Log Level** – Decides whether log messages are accumulated to avoid too large log files.
- **Cumulative Interval [s]** – Interval (in sec) for which cumulative logging is activated for either matching or similar log entries.
- **Cumulative Maximum** – Maximum of similar log entries to start cumulative logging.
- **Generate Audit Log** – Enable the generation of structured firewall audit data that can be stored locally and/or forwarded. If enabled, the 'Audit Log' tab of the firewall UI will get populated with data.
- **Audit Log Data** – Use this section to selectively enable or disable audit log generation.

- **Log ICMP Packets** – Select the log policy for ICMP packets.
  - **Log-All** – Log all ICMP packets except type *ECHO*.
  - **Log-Unexpected** – Log all ICMP packets except *ECHO* and *UNREACHABLE*.
  - **Log-None** – Disable ICMP logging.
- **Allow Threat Log Processing** – Allow other processes to access threat log information for further processing.

IPFIX Streaming

- **Enable IPFIX/Netflow** – Internet Protocol Flow Information Export (IPFIX, RFC 3917) is based on NetFlow Version 9. You can use this setting to stream the FW audit log via IPFIX. Note that using this also requires an adjustment of **Audit Delivery** within section **Audit Log Data** to **Send-IPFIX**.
- **Enable intermediate reports** – Enable sending of intermediate reports with delta counters. (Use the **IPFIX reporting interval [m]** option to determine how often intermediate reports are sent.)
- **IPFIX reporting interval [m]** – Interval in minutes between two intermediate IPFIX flow reports for each active flow.
- **IPFIX Template** – If set to *Extended*, includes additional information such as delta counters, to the IPFIX export. If your collector does not support reverse flows, select Uniflow templates, these templates will duplicate the traffic against the collector.
- **Collectors** – Add external IPFIX collectors.
- **Settings** – Click **Set/Edit** to configure connection tracing settings.

Out of Session (OOS) Packet Policy

- **Interfaces to Send TCP RST** – The firewall sends TCP RST packets to these network interfaces if it detects packets not belonging to an active session. This is useful to avoid timeouts on certain servers.
- **IPV4 Networks to Send TCP RST** – The firewall sends TCP RST packets to these IPv4 networks if it detects packets not belonging to an active session.
- **IPV6 Networks to Send TCP RST** – The firewall sends TCP RST packets to these IPv6 networks if it detects packets not belonging to an active session.

Figures