General Firewall Configuration

https://campus.barracuda.com/doc/43847248/

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**) of the Barracuda NG Firewall. After changing general firewall configuration settings, perform a **Firmware Restart** (**CONTROL > Box**) for the changes to take effect. Default values vary depending on the NG Firewall model. Check the default value table below for more information.

In this article:

Firewall Sizing

Maximum Number of Connections

- **Max Session Slots** – Set the maximum number of session slots allowed. (min: 512, default: 65536, max: 800000) The amount of memory consumed by the firewall is updated when this value is changed and displayed in the **Firewall Memory [MB]** field. (with the default value the firewall service will consumer about 150MB 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.
- **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 Barracuda NG Firewall systems with more than 768MB 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 128MB, starting at the 384MB. For more information, see How to Configure the Bootloader.
  Reboot the box after setting the parameter and wait if the firewall service successfully starts after the system boot. Do not use vmalloc areas bigger than 640MB. 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 768MB 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 a installed Barracuda NG Firewall box can be determined with the following command: *rpm -q kernel --qf %{ARCH}\\n.*
- **Max UDP (%)** – Defines how many percent of the the **Max Session Slots** are allowed to be UDP sessions. (min: 1; max. 100; default: 30).

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 how many percent of the **Max Session Slots** are allowed to be ICMP sessions. (min: 1, max: 100, default: 30).
  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 how many percent of the **Max Session Slots** are allowed to be of an IP protocol type except TCP, UDP or ICMP. (min:1, max: 100, default: 10).
  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.

Global Limits 1

- **Max SIP Calls** – Set the maximum number of concurrent SIP calls that can be handled by the legacy SIP firewall plugin (min: 64, max: 16384, default: 512).
  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 (min: 64, max: 16384, default: 512).
- **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. (default: 512) 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 rule sets 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 not longer be resolved causing firewall rules using these networks objects to never match.
- **Max Acceptors** – Maximum number of pending accepts for inbound rules (min: 2000; max: 2000000; default: 8192). 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 (min: 2000; max: 262144; default: 16384). This parameter only comes into effect when the TCP accept policy is set to inbound for the firewall rule.
- **Max BARPs** – Defines the maximum number of bridging ARPs allowed (default: 2048). 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 (min: 0, max: 65536, default: 8192).
- **Dyn Service Names (RPC)** – Maximum number of dynamic service name entries (min:0, max: 65536, default: 8192).

Global Limits 2

- **Inbound Mode Threshold (%)** – Threshold of pending accepts, at which the firewall switches to the inbound TCP accept policy to guard against SYN flooding attacks (min:1. max: 100, default: 20).
- **SYN Cookie High Watermark (%)** – Percentage (of maximum pending inbounds) of pending inbound accepts to switch to SYN cookie usage for enhanced SYN flooding protection (min: 0, max: 100, default: 20).
- **SYN Cookie Low Watermark (%)** – Percentage (of maximum pending inbounds) of pending inbound accepts to go back to ordinary SYN handling (min: 0; max: 100; default: 15).
- **Max Dynamic Rules** – Maximum number of dynamically activated rules (min: 1; max: 1024; default: 128).
- **Max Multiple Redirect IPs** – Maximum number of IP addresses in rules with multiple redirect target IPs (min:1, max: 1024, default: 128).
- **Max TCP Proxy Workers** – Total number of available sessions for the Generic TCP proxy mode depends on the number of workers. Each worker can handle up to 400 sessions. Workers are created on demand.
- **Max SOCKS Workers** – Maximum number of available SOCKS worker when Generic TCP proxy mode is enabled.

Source Based Session Limits

- **Max Local-On Session/Src** – Maximum number of sessions per source IP address. Can not be set to more than **Max Session Slots** (min: 1; max. **Max Session Slots**; default: 8192).
  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. (min: 1, default: 512).
  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 (min:1, default: 512).
  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 (min: 1, default 128).
  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 (min: 5, max: 1024, default: 64)

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: min: 128; max: 8192; default: 2048.
- **Max. Block Entries** – min: 128; max: 8192; default: 2048.
- **Max. Drop Entries** – min: 128; max: 8192; default: 2048.
- **Max. Fail Entries** – min: 128; max: 8192; default: 2048.
- **Max. ARP Entries** – min: 128; max: 8192; default: 2048.
- **DNS Resolve IPs** – Setting this parameter to **yes** (default: **no**) 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** – Specifies whether an existing connection is terminated (**Terminate-on-change** ; default) or not (**Keep-on-change**) if the rule set changes and the session is no longer allowed by the new rule set.
- **No Rule Update Time Range** – This option allows defining a time range during which firewall 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

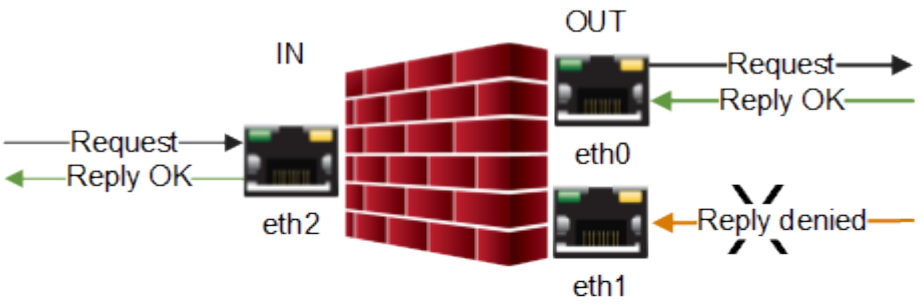
- **RAW TCP Idle Timeout** – Defines the idle timeout value in seconds for RAW TCP mode.
- **RAW TCP Timeout Policy** – Defines the timeout policy that will be used for RAW TCP mode.
  - **Use-global-timeouts (default)** – Sets the timeout value that has been configured in the previous sections.
  -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

Default Anti Spoofing Policy

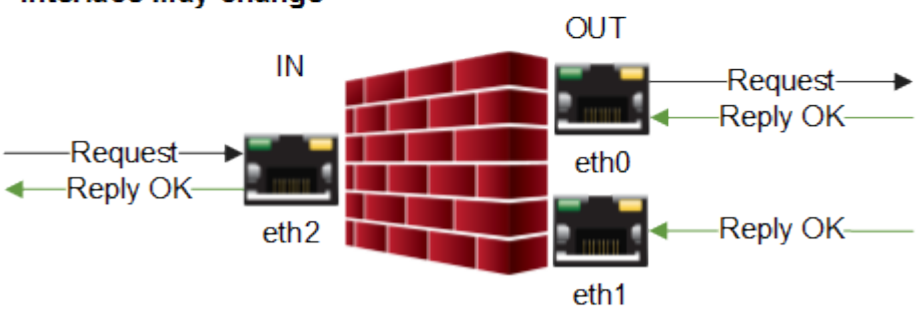
- **ARP Reverse Route Check** – Setting this parameter to **Yes** causes answers to ARP requests to be checked if Source IP and interface match.
- **Reverse Interface Policy** – The options of this parameter specify whether requests and replies must use the same (outgoing) interface (**same-interface**; default 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.

same-interface



interface-may-change



Port Scan Policy

- **Port Scan Threshold** – When the number of blocked request exceed the threshold, a port scan is detected and a port scan event is triggered. (min value: 2 max: 1000000000, default: 10)
- **Port Scan Detection Interval** – Detection interval in seconds to check for not allowed activity (min: 0; max: 1000000000; default: 60). 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 Barracuda NG Firewall 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.

High Availability Related Policies

- **Allow Active-Active Mode** – (advanced) Active-Active firewall operation mode is deactivated by default (**no**). It 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 (default: **Yes**). 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. Only make use of this feature, if you are operating your Barracuda NG Firewall system for routing and NOT for firewall purposes, as generic network forwarding might cause severe security issues.

Operational IPS

Per default TCP stream reassembly and HTML parsing is 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 your Barracuda NG Firewall 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 (default)** – The Barracuda NG Firewall automatically chooses the mode best suited for your Barracuda NG Firewall.
  - **Fast Scan** – Scan select packets to improve performance and throughput.
  - **Full Scan** – Scan all packets.

Operational TAP

TCP Proxy Settings

- **TCP Proxy Version** – Select the TCP proxy version. Default: **V2.**
  You must restart the boxfw service for a change of the TCP proxy version to take effect.

TCP Proxy V1 Settings

- **Max Worker Processes** – Set the maximum number of workers created when using the TCP proxy mode (stream forwarding). Each worker can handle up to 400 sessions.
  You must restart the boxfw service for changes to the number of workers to take effect.

TCP Proxy V2 Settings

- **Number of Threads** – Set the number of thready manually or enter `0` for the NG Firewall to handle creating and removing threads automatically. Default: 0
  You must restart the boxfw service for changes to the number of threads to take effect.
- **Log Level** – Choose how verbose the logs should be. Default: info
- **Log Rate Limit** – Enter the maximum number of log entries per second for a single log message. Set to `0` to disable the log rate limit. Default: 5

Operational VPN

- **VPN Rate Limit (Mbps) –** Limits how fast VPN traffic is encrypted and decrypted. If you experience excessive CPU load in an environment with many VPN tunnels, then change this value. The default 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 –** By default these assembler ciphers are enabled. 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 (default: no) –** 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

- **Working Mode** – Enable/disable URL categorization.
- **Max. Cache Entries –** The maximum number of entries in the kernel cache. 0 is auto selection depending on RAM size.
- **Categorization Timeout (sec) –** Set the maximum timeout to wait for categorization response.
- **Cache Entry Expiration (sec) –** After the configured time the cached entries category will be updated.

Application and Port Protocol Protection

- **Enable Port Protocol Detection –** Enable this option to use Application Detection and/or Port Protocol Protection.

Application Detection Default Policy (Legacy)

- **Application Policy –** The default action upon application detection. This policy can be referenced as the default policy within the application control view of a firewall rule. Alternatively an explicit setting can be adopted on a per firewall rule basis for all policy actions except for traffic bandwidth limitation and QoS band assignment which needs to be set here.
- **Application Bandwidth [kbit/s] –** Select an explicit maximum bandwidth that will be assigned to a traffic flow upon detection of an application as defined by the default policy or a firewall rule specific policy. Note that a bandwidth of 10kitb/s can be used to render many evasive peer-to-peer applications useless.
- **Application QoS Band –** Select a QoS band that will be assigned to a traffic flow upon detection of an application as defined by the default policy or a firewall rule specific policy. Note that you can choose a band from the predefined basic QoS profile template but you will still need to activate the overall use profile on the various network interfaces within the traffic

shaping config.

Application Detection Default Selection (Legacy)

- **Use Preselected Applications –** Select **yes** to include the list of preselected applications into the scope of application detection. You can add and exclude specific applications using the list selections below.
- **Explicitly Add Applications –** Explicitly specify applications that will be added to the list of preselected.
- **Explicitly Skip Applications –** Explicitly specify applications that will be skipped.

Audit and Reporting

Statistics Policy

- **Generate Dashboard Information** – Enable/disable the firewall dashboard.
- **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 statistic if available, otherwise the source IP address.

Eventing Policy

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

Log Policy

- **Appid logging** – Global application control log policy. This setting can be overridden on a per access rule basis. Default: **Log-Blocked-Applications**
- **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. Minimum 1, maximum 60 sec.
- **Cumulative Maximum** – Maximum of similar log entries to start cumulative logging. Minimum 1, maximum 1000.
- **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.

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**.
- **Settings** – Opens the **IPFIX Exporter Setup** window where you can configure IPFIX 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.

Default Values for all Hardware Barracuda NG Firewall Models

Barracuda NG Firewall models use different default values depending on the hardware capabilities of the system.

	F10	F18	F80	F100	F180	F200	F280	F300	F380	F400	F600	F800	F900	F1000	C400	C610
General Firewall Configuration																
Max. Session Slots	2048	8192	8192	8192	8192	8192	70000	8192	70000	131072	131072	256000	512000	768000	8192	8192
Max. UDP (%)	30	30	30	30	30	30	30	30	30	30	30	30	30	30	30	30
Max. Echo [%]	30	30	30	30	30	30	30	30	30	5	5	5	5	5	30	30
Max. Other [%]	15	15	15	15	15	15	10	15	10	10	10	10	10	10	10	10
Max. SIP Calls	32	32	32	32	32	32	32	32	32	1024	1024	1024	1024	1024	32	32
Max. SIP Transactions	32	32	32	32	32	32	32	32	32	1024	1024	1024	1024	1024	32	32
Max. SIP Media	64	64	64	64	64	64	64	64	64	2048	2048	2048	2048	2048	64	64
Max. Pending Inbounds	512	512	512	512	512	512	512	512	512	32768	32768	32768	32768	32768	512	512
Max. Plugins	1024	1024	1024	1024	1024	1024	1024	1024	1024	8192	8192	8192	8192	8192	1024	1024
Dyn. Service Names (RPC)	1024	1024	1024	1024	1024	1024	1024	1024	1024	131072	131072	131072	131072	131072	1024	1024

Inbound Mode Threshold [%]	20	20	20	20	20	20	20	20	20	20	20	20	20	20	20	20
Max. Dynamic Rules	32	32	32	32	32	32	32	32	32	128	128	128	128	128	32	32
Max. Multiple Redirect IPs	32	32	32	32	32	32	32	32	32	128	128	128	128	128	32	32
Max. Local-In Sessions/Src	256	256	256	256	256	256	256	256	256	8192	8192	8192	8192	8192	256	256
Max. Local-In UDP/Src	128	128	128	128	128	128	128	128	128	512	512	512	512	512	128	128
Max. Local-In Echo/Src	128	128	128	128	128	128	128	128	128	512	512	512	512	512	128	128
Max. Local-In Other/Src	128	128	128	128	128	128	128	128	128	128	128	128	128	128	128	128
Max. Pending Local Accepts/Src	32	32	32	32	32	32	32	32	32	64	64	64	64	64	32	32
Max. Access Entries	512	512	512	512	512	512	512	512	512	4096	4096	4096	4096	4096	512	512
Max. Block Entries	512	512	512	512	512	512	512	512	512	4096	4096	4096	4096	4096	512	512
Max. Drop Entries	512	512	512	512	512	512	512	512	512	8192	8192	8192	8192	8192	512	512
Max. Fail Entries	512	512	512	512	512	512	512	512	512	4096	4096	4096	4096	4096	512	512
Max. Acceptors	1024	1024	1024	1024	1024	1024	1024	1024	1024	8192	8192	8192	8192	8192	1024	1024
Max. ARP Entries	128	128	128	128	128	128	128	128	128	4096	4096	4096	4096	4096	128	128
VPN Rate Limit (Mbps)	30	50	100	80	150	130	200	130	750	700	-	-	-	-	-	-
Enable Protocol Detection	1	1	1	1	1	1	1	1	1	4096	4096	4096	4096	4096	1	1
Forwarding Settings																
Max. Forwarding Session/Src	8192	8192	8192	8192	8192	8192	8192	8192	8192	8192	8192	8192	8192	8192	-	-
Max. Forwarding UDP/Src	512	512	512	512	512	512	512	512	512	512	512	512	512	512	-	-
Max. Forwarding Echo/Src	512	512	512	512	512	512	512	512	512	512	512	512	512	512	-	-
Max. Forwarding Other/Src	128	128	128	128	128	128	128	128	128	128	128	128	128	128	-	-

Max. Pending Forward Accept/Src	64	64	64	64	64	64	64	64	64	64	64	64	64	64	-	-

Figures