General Firewall Configuration

https://campus.barracuda.com/doc/96026185/

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 CloudGen 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 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 consume about 150 MB RAM).
- **Max UDP [%]** – (advanced) 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 [%]** – (advanced) 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 [%]** – (advanced) 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 CloudGen Firewalls with more than 768 MB RAM requiring additional vmalloc space to satisfy the increased memory demand of non-default firewall settings, we recommend increasing 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 CloudGen Firewall box can be determined with

the following command: *rpm -q kernel --qf %{ARCH}\\n.*

Global Limits 1

- **Max DNS Entries** – Defines the maximum number of DNS queries that may be triggered by the 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 is exceeded, hostnames can no longer be resolved, causing access rules using these networks objects to never match.
- **Max Acceptors** – (advanced) 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 in addition to 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 comes into effect only when the TCP accept policy is set to inbound for the access rule.
- **Max BARPs** – (advanced) 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** – (advanced) Maximum number of rules using plugins.
- **Dyn Service Names (RPC)** – Maximum number of dynamic service name entries.

Global Limits 2

- **Max. Dynamic Rules** – Maximum number of dynamically activated rules. The default preset value is 128.
- **Max. Multiple Redirect IPs** – Maximum number of IP addresses in rules with multiple redirect target IPs. The default preset value is 128.

Global Inbound Mode Limits

- **Inbound Mode Threshold [%]** – This is the percentage value of the maximum number of sessions in the pending accept state. If the threshold value is reached, the firewall will switch to a general inbound TCP accept policy for SYN flooding protection. The default preset value is 20.
- **SYN Cookie High Watermark [%]** – This is the percentage (of the maximum number of pending inbounds) of pending inbound accepts to switch to TCP SYN cookie usage for enhanced SYN flooding protection. The default preset value is 20.
- **SYN Cookie Low Watermark [%]** – This is the percentage (of the maximum number of pending inbounds) of pending inbound accepts to go back to ordinary SYN handling. The default preset value is 15.

Source-Based Session Limits

- **Max Local-On Session/Src** – (advanced) 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** – (advanced) 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** – (advanced) 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** – (advanced) 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** – (advanced) Maximum number of pending accepts per source IP address.

Firewall History

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.
- **Max. ARP Entries** – Determines the maximum number of ARP 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.
  If many DNS objects are used frequently, disable host resolution in the firewall history to avoid delays and errors in the DNS resolution.

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 (fastest)** – 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 applies only 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 you to define 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.
- **On-demand network objects update** – This option allows you to enable on-demand network objects.
- **Network objects update interval** – Update interval in minutes for on-demand network objects.

IPv6 Settings

- **Block Type 0 Routing Headers** – This option allows you to block type 0 routing headers according to rfc5095.

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**
- **TCP Stream Reassembly** – (advanced) Reassembles the TCP stream before scanning for

vulnerabilities.

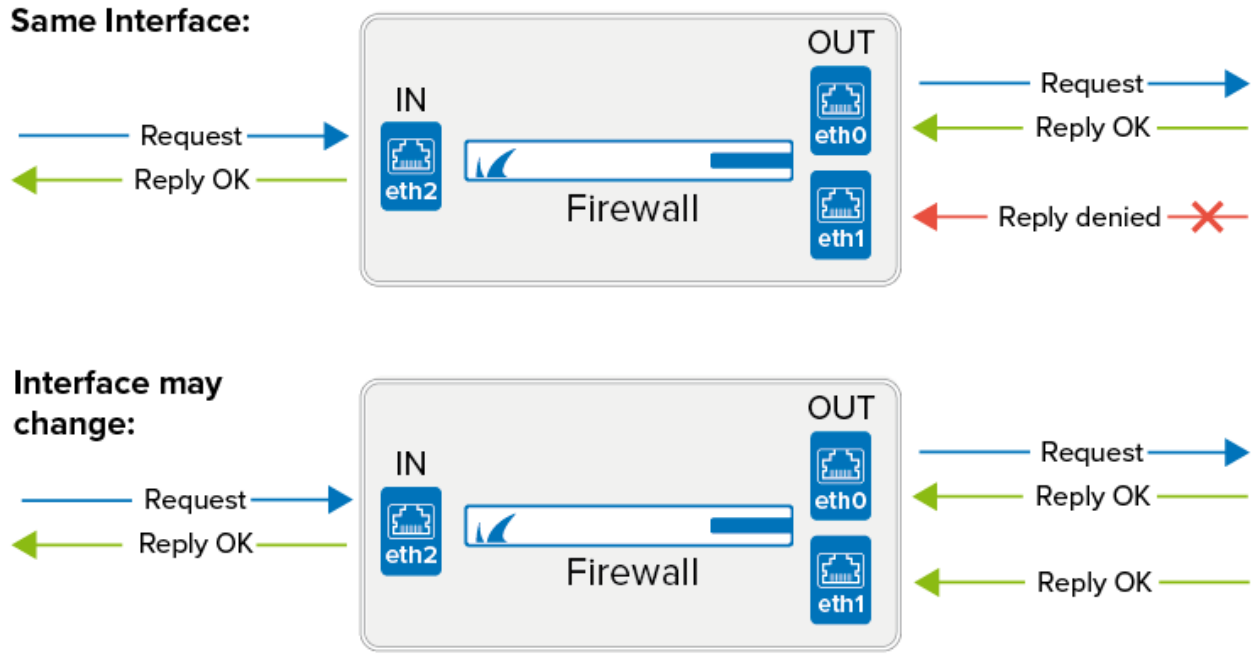
Raw TCP Mode Policy

- **RAW TCP Idle Timeout [s]** – 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 [s]** – 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) This option, if enabled, improves shaping tree evaluation.
  - **Disabled** – Disables this option.
  - **Enabled** – Improves shaping tree evaluation.
  - **Enable-MultiQueue-Only** (default) – 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 must 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.
- **Enable Authentication Sync** – (advanced) This option allows you to enable authentication data synchronization between HA partners.

  Do not change unless otherwise stated from Barracuda Networks Technical Support.
  - **Auto** – Automatically detects if a direct synchronization is required, or if synchronization is done over an authentication synchronization zone.
  - **Yes** – Enables direct synchronization between HA partners.
  - **No** – Disables direct synchronization between HA partners.
- **Log Synced Sessions** – (advanced) This setting determines logging of access cache sessions that have been synchronized between HA partners. Set to **No** to disable logging. Set to **Auto** to check if a trustzone synchronization is in place. If yes, the sync is done via trustzone, and direct synchronization gets disabled automatically. If no trustzone sync is configured, **Auto** will enable direct authentication sync.
- **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 CloudGen Firewall only for routing and NOT for firewall purposes because generic network forwarding might cause severe security issues.

Operational IPS

This menu point in **General Firewall Configuration** is accessible only in **Advanced Configuration Mode**.

Intrusion Prevention System (IPS) Engine Settings

- **IPS Scan Mode** – (advanced) Select the scanning mode for IPS. You must reboot for the changes to take effect.
  - **Auto** – (advanced) The firewall automatically chooses the best suited mode.
  - **Fast-Scan** – (advanced) With this option enabled, only the beginning of a session is scanned as most attacks occur within the first few packets regardless of the protocols used (TCP, UDP).
  - **Full-Scan** – (advanced) Scan all packets.

Intrusion Prevention System (IPS) Decoder Settings

- **HTML Parsing for IPS** – Toggles HTML obfuscation detection. If this setting is changed, you must reboot for the changes to take effect.
- **HTML content-encoding decompression** – Enables HTTP content-encoding decompression (gzip, deflate). A reboot is required.
- **HTML content-disposition decompression** – Enables HTTP content-disposition decompression (zip). A reboot is required.
- **PDF decoder** – Enables decoding of PDF documents. A reboot is required.
- **RPC decoder** – Enables an RPC decoder. This is used for DCERPC and SMB connections. A reboot is required.

Operational VPN

- **Enable Assembler Ciphers** – (advanced) 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).
  Reboot for this setting to take effect.
- **Globally clear DF Bit** – (advanced) Clears the DF bit for each ipv4 packet routed through a VPN tunnel. For more information on MTU, see Advanced 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

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.
- **Log Verbosity** – (advanced) The log level of the URL Filter engine.
  Increasing this value may produce huge URL Filter log files. Increase only in case of debugging.

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 Networks 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).
- **SCADA Dump Size [MB]** – (advanced) A value of 0 means disabled. Enable to write a dump file for further analysis if SCADA protocol detection is enabled without parsing log support.

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 to monitor information data. A value of 0 enables automatic assignment based on the device. This parameter relates to the virtual disk size of the APPID_stat database and is set to 'auto' per default. 'Auto' means:
  - `/phion0` partition size-dependent calculation.
  - Below 20GB: 10 MB for all database files.
  - Between 20 GB and 100 GB: 100 MB for all database files.
  - Greater than 100 GB: 200 MB for all database files.
- **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 .../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** – (advanced) Use this section to selectively enable or disable event generation.
  - Click **Edit** and define the events data should be generated for.

Log Policy

- **Application Control Logging** – Select the global policy for Application Control 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. For more information, see Available Log Files and Structure
- **Activity Log Data** – Configure whether the Firewall Activity logs uses full text or encoded information according to the list below. The encoded format is typically used to reduce the size of the log files.

4000	Unknown Block Reason
4001	Forwarding is disabled
4002	Block by Rule
4003	Block no Rule Match
4004	Block by Rule Source Mismatch
4005	Block by Rule Destination Mismatch
4006	Block by Rule Service Mismatch
4007	Block by Rule Time Mismatch

4008	Block by Rule Interface Mismatch
4009	Block Local Loop
4010	Block by Rule ACL
4011	Block Rule Limit Exceeded
4012	Block Rule Source Limit Exceeded
4013	Block Pending Session Limit Exceeded
4014	Block Size Limit Exceeded
4015	Block by Dynamic Rule
4016	Block No Address Translation possible
4017	Block Broadcast
4018	Block Multicast
4019	Block Source Session Limit Exceeded
4020	Block UDP Session Limit Exceeded
4021	Block Source UDP Session Limit Exceeded
4022	Block Echo Session Limit Exceeded
4023	Block Source Echo Session Limit Exceeded
4024	Block Other Session Limit Exceeded
4025	Block Source Other Session Limit Exceeded
4026	Block Total Session Limit Exceeded
4027	Block no Route to Destination
4028	Block Invalid Protocol for Rule Action
4029	Block Protected IP Count Exceeded Licensed Limit
4030	Block Device not available
4031	Block by Rule User Mismatch
4032	Block Bridged Destination MAC Unknown
4033	Block by Rule MAC Mismatch
4034	Send Authentication Required
4035	Block Invalid Local Redirection to Non Local Address
4036	Block Invalid Redirection to Local Address
4037	Block Slot Creation Failed
4038	Block by Rule Quarantine Class Mismatch
4039	Local IPv6 traffic is disabled
4040	WANOPT Protocol Negotiation Mismatch
4041	Block by Rule App mismatch
4042	URL Categorization not available and policy set to fail
4043	URL Domain Explicitly not Allowed by URL Categorization

4044	URL Category not Allowed by Policy
4045	URL Category Blocked by Policy
4046	Block due to ATP Quarantine
4047	Block Unauthorized ATP File Download Access
4048	URL Categorization not available and policy set to fail
4049	URL Category must be acknowledged by user
4050	Custom URL domain must be acknowledged by user
4051	URL Category must be acknowledged by supervisor
4052	Detected Content not allowed by policy
4053	Detected Browser Agent not allowed by policy
4054	Untrusted self-signed certificate
4055	Certificate not trusted
4056	Certificate Revoked
4057	Expired or not yet valid certificate
4058	Certificate content invalid
4059	Certificate revocation check failure
7000	Unknown Block Reason
7001	Forwarding is disabled
7002	Block by Rule
7003	Block no Rule Match
7004	Block by Rule Source Mismatch
7005	Block by Rule Destination Mismatch
7006	Block by Rule Service Mismatch
7007	Block by Rule Time Mismatch
7008	Block by Rule Interface Mismatch
7009	Block Local Loop
7010	Block by Rule ACL
7011	Block Rule Limit Exceeded
7012	Block Rule Source Limit Exceeded
7013	Block Pending Session Limit Exceeded
7014	Block Size Limit Exceeded
7015	Block by Dynamic Rule
7016	Block No Address Translation possible
7017	Block Broadcast
7018	Block Multicast
7019	Block Source Session Limit Exceeded

7020	Block UDP Session Limit Exceeded
7021	Block Source UDP Session Limit Exceeded
7022	Block Echo Session Limit Exceeded
7023	Block Source Echo Session Limit Exceeded
7024	Block Other Session Limit Exceeded
7025	Block Source Other Session Limit Exceeded
7026	Block Total Session Limit Exceeded
7027	Block no Route to Destination
7028	Block Invalid Protocol for Rule Action
7029	Block Protected IP Count Exceeded Licensed Limit
7030	Block Device not available
7031	Block by Rule User Mismatch
7032	Block Bridged Destination MAC Unknown
7033	Block by Rule MAC Mismatch
7034	Send Authentication Required
7035	Block Invalid Local Redirection to Non Local Address
7036	Block Invalid Redirection to Local Address
7037	Block Slot Creation Failed
7038	Block by Rule Quarantine Class Mismatch
7039	Local IPv6 traffic is disabled
7040	WANOPT Protocol Negotiation Mismatch
7041	Block by Rule App mismatch
7042	URL Categorization not available and policy set to fail
7043	URL Domain Explicitly not Allowed by URL Categorization
7044	URL Category not Allowed by Policy
7045	URL Category Blocked by Policy
7046	Block due to ATP Quarantine
7047	Block Unauthorized ATP File Download Access
7048	URL Categorization not available and policy set to fail
7049	URL Category must be acknowledged by user
7050	Custom URL domain must be acknowledged by user
7051	URL Category must be acknowledged by supervisor
7052	Detected Content not allowed by policy
7053	Detected Browser Agent not allowed by policy
7054	Untrusted self-signed certificate
7055	Certificate not trusted

7056	Certificate Revoked
7057	Expired or not yet valid certificate
7058	Certificate content invalid
7059	Certificate revocation check failure
2000	Session Idle Timeout
2001	Balanced Session Idle Timeout
2002	Last ACK Timeout
2003	Retransmission Timeout
2004	Halfside Close Timeout
2005	Unreachable Timeout
2006	Connection Closed
2007	Connection Reset by Source
2008	Connection Reset by Destination
2009	Connection Reset by Administrator
2010	Allow time interval expired
2011	Connection no Longer Allowed by Rule
2012	Dynamic Rule Expired
2013	Terminated due to content
2014	Forward Destination is a Local Address
2015	Unsyncable Session and Passive Sync Mode
2016	Network Device no Longer Available
2017	Dynamic Service not Allowed by Rule
2018	Session Duration Timeout
2019	Application Control
2020	Unallowed Protocol Detected
2021	IPS Policy Requested Termination
2022	WANOPT Policy Negotiation Failed
2023	None of the Allowed Protocols Detected
2024	Session diverted to dynamic mesh VPN tunnel
2025	Internal SSL Error
2026	Self Signed Cert Found
2027	No Issuer Found
2028	Certificate Revoked
2029	Certificate Validation Failed
2030	No Local Socket Present
2031	Out of Memory Fail Close"

6000	Unknown Scan Reason
6001	Terminate due to Pattern Detection
6002	Pattern Detection
6003	Application Control
6004	Drop due to Application Control
6005	Shape due to Application Control
6006	Unallowed Port Protocol Detected
6007	Reset due to Unallowed Port Protocol Detection
6008	Drop due to Unallowed Port Protocol Detection
6009	IPS Log
6010	IPS Warning
6011	IPS Alert
6012	IPS Drop Log
6013	IPS Drop Warning
6014	IPS Drop Alert
6015	Web Access
6016	Application/Protocol Detection
6017	Application/Protocol Warning
6018	Application/Protocol Alert
6019	Application/Protocol Denied
6020	Application/Protocol Denied with Warning
6021	Application/Protocol Denied with Alert
6022	URL Categorization
6023	URL Categorization Warning
6024	URL Categorization Alert
6025	URL Category Denied
6026	URL Category Denied with Warning
6027	URL Category Denied with Alert
6028	Virus Blocked
6029	Malicious File Blocked by Advanced Threat Protection
6030	Virus Scan not possible - Blocked
6031	Virus Scan not possible - Passed
6032	Virus Scan Error - Blocked
6033	Virus Scan Error - Passed
6034	Malicious Content Detected in Delivered File
6035	DNS Request for a Hostname with bad Reputation

6036	Client access to a DNS Sinkhole Address
6037	Client access to a Hostname with bad Reputation"
1000	Network Unreachable
1001	Host Unreachable
1002	Protocol Unreachable
1003	Port Unreachable
1004	Fragmentation Needed
1005	Source Route Failed
1006	Network Unknown
1007	Host Unknown
1008	Source Host Isolated
1009	Network Access Denied
1010	Host Access Denied
1011	Network Unreachable for TOS
1012	Host Unreachable for TOS
1013	Denied by Filter
1014	Host Precedence Violation
1015	Host Precedence Cutoff
1016	Connect Timeout
1017	Accept Timeout
1018	No Route to Host
1019	Unknown Network Error
1020	Routing Triangle
1021	TTL Expired
1022	Defragmentation Timeout
1023	No Route To Destination
1024	Communication Prohibited
1025	Unknown Code 2
1026	Address Unreachable
1027	Port Unreachable
1028	WANOPT Protocol Negotiation Mismatch
1029	WANOPT Out of descriptors
1030	WANOPT Partner protocol missing
1031	WANOPT No VPN
1032	Internal SSL Error
1033	Untrusted self-signed certificate

1034	Certificate not trusted
1035	Certificate Revoked
1036	Expired or not yet valid certificate
1037	Certificate content invalid
1038	Certificate revocation check failure
1039	Flex connection timeout
1040	Flex connection error
1041	Out of Memory Fail Close"
3000	Reverse Routing MAC Mismatch
3001	Reverse Routing Interface Mismatch
3002	Source is Multicast
3003	Source is Broadcast
3004	Source is an Invalid IP Class
3005	Source is Loopback
3006	Source is Local Address
3007	IP Header is Incomplete
3008	IP Header Version is Invalid
3009	IP Header Checksum is Invalid
3010	IP Header has Invalid IP Options
3011	IP Header Contains Source Routing
3012	IP Packet is Incomplete
3013	TCP Header is Incomplete
3014	TCP Header Checksum is Invalid
3015	TCP Header has an Invalid Cookie
3016	TCP Header has an Invalid SEQ Number
3017	TCP Header has an Invalid ACK Number
3018	TCP Header has Invalid TCP Options
3019	TCP Header has Invalid TCP FLAGS
3020	TCP Packet Belongs to no Active Session
3021	UDP Header is Incomplete
3022	UDP Header Checksum is Invalid
3023	ICMP Header is Incomplete
3024	ICMP Header Checksum is Invalid
3025	ICMP Type is Invalid
3026	ICMP Reply Without a Request
3027	No socket for packet

3028	Forwarding not Active
3029	No Device for source IP address
3030	ARP request device mismatch
3031	ARP reply duplicate and MAC differs
3032	Size Limit Exceeded
3033	Rate Limit Exceeded
3034	TTL Expired
3035	Unknown ARP Operation
3036	ICMP Packet Belongs to no Active Session
3037	ICMP Packet is Ignored
3038	ICMP Packet is Ignored by Rule Settings
3039	High Level Protocol Header is Incomplete
3040	High Level Protocol Header is Invalid
3041	High Level Protocol Version is Invalid
3042	High Level Protocol Packet is Incomplete
3043	High Level Protocol Packet is Invalid
3044	Source MAC Mismatch
3045	Destination MAC Mismatch
3046	Bridge ACL violation
3047	ARP Burst Detected
3048	Static bridge ARP mismatch
3049	Change of locked ARP entry
3050	Possible MAC Spoofing
3051	No Next hop Allowed on Bridge Segment
3052	Decompression failed
3053	Session Creation Load Exceeded
3054	Failed to update/create QARP entry
3055	Failed to retrieve routing information for quarantine setup
3056	Cannot send packets between different quarantine groups
3057	QARP device entry does not match device to be used
3058	Drop guessed TCP RST
3059	Invalid SYN for Established TCP Session
3060	Received Packet Exceeds NIC MTU (Invalid TCP-Segmentation-Offload ?)
3061	TCP Header ACK Sequence Number out of Window Size
3062	Unsupported IPV6 header
3063	No Ruleset loaded

3064	Source Barp Unknown
3065	Source and destination Barp on the same device
3066	Drop Otherhost
3067	Firewall not active
3068	Payload linearization failed
3069	Reevaluation failed
3070	Unknown fragment
3071	Bridge Loop Detected
3072	Interface is set to discard by RSTP"
5000	Unknown Deny Reason
5001	Deny by Rule
5002	Deny by Rule Source Mismatch
5003	Deny by Rule Destination Mismatch
5004	Deny by Rule Service Mismatch
5005	Deny by Rule Time Mismatch
5006	Deny Local Loop
5007	Deny by Rule ACL
5008	Deny by Dynamic Rule
5009	Deny No Address Translation possible

- **Activity Log Information** – Click **Set/Edit** to define what type of information is included in the firewall activity log. Click **Clear** to reset to factory default values.
- **Log Level** – Decides whether log messages are accumulated to avoid too large log files.
- **Cumulative Interval [s]** – (advanced) Interval in seconds for which cumulative logging is activated for either matching or similar log entries.
- **Cumulative Maximum** – (advanced) 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** – (advanced) Click **Set/Edit** to selectively enable or disable audit log generation. Click **Clear** to reset to factory default values.
- **Log ICMP Packets** – Select the logging 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 Export

- **Enable IPFIX Export** – Set to **yes** to enable sending of IP flow information using the IP flow

information export (IPFIX) protocol.

- **Enable Intermediate Flow Reports** – Enable sending of intermediate reports with delta counters. (Use the **Intermediate Reporting Interval [min]** option to determine how often intermediate reports are sent)
- **Intermediate Reporting Interval [min]** – Interval in minutes between two intermediate IPFIX flow reports for each active flow.
- **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.

  Starting with firmware version 8.0.5 / 8.2.0, former IPFIX templates were updated to newer versions. It is recommended to change the former settings by selecting the related new names, in example, switch from ***DEPRECATED* Uniflow Default** to **Uniflow Default** in the respective menu list in the UI.
- **Custom Templates** – If **Custom** is selected for **Template**, you can configure your own set of information elements in the window **Custom Template** after you clicked **Edit...** .
- **Collectors** – Click + to add external IPFIX collectors.
- **Report Blocked or Failed Sessions** – If set to **yes**, this option enables sending of flow records for packets that were not forwarded by the firewall, e.g., because they were blocked or the respective session could not be established.

Connection Tracing

- **Settings** – Click **Set/Edit** to configure connection tracing settings.

Out of Session Packets

This menu point in **General Firewall Configuration** is accessible only in **Advanced Configuration Mode**.

Out of Session [OOS] Packet Policy

- **Interfaces to Send TCP RST** – (advanced) 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** – (advanced) 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** – (advanced) The firewall sends TCP RST packets to these IPv6 networks if it detects packets not belonging to an active session.

Global Safe Search

Search Engine Log

- **Enable Search Engine Log** – (advanced) Set to **yes** to enable logging of search strings. The log file will be created as soon as the firewall detects a query. You can inspect the log file **searchString** in your firewall on **LOGS > Log Viewer > Assigned Services > NGFW**.

Safe Search Settings

You can protect users behind a Barracuda CloudGen Firewall from undesired content in search results. To achieve this, enable the following options:

- **Enable Youtube Safe Search** – Set this option to **yes** to enable YouTube safe search.
- **Enable Bing Safe Search** – Set this option to **yes** to enable Bing safe search.
- **Enable Google Safe Search** – Set this option to **yes** to enable Google safe search.
- **Enable Yahoo Safe Search** – Set this option to **yes** to enable Yahoo safe search.

Advanced Log Settings

This menu point in **General Firewall Configuration** is accessible only in **Advanced Configuration Mode**.

- **Security Policy Facility Loglevels** – (advanced) Specify the general log level for services running on the firewall.

Figures