How to Configure Audit and Reporting

https://campus.barracuda.com/doc/73719595/

The firewall audit service allows propagating firewall audit events to the Control Center for collection and analysis.

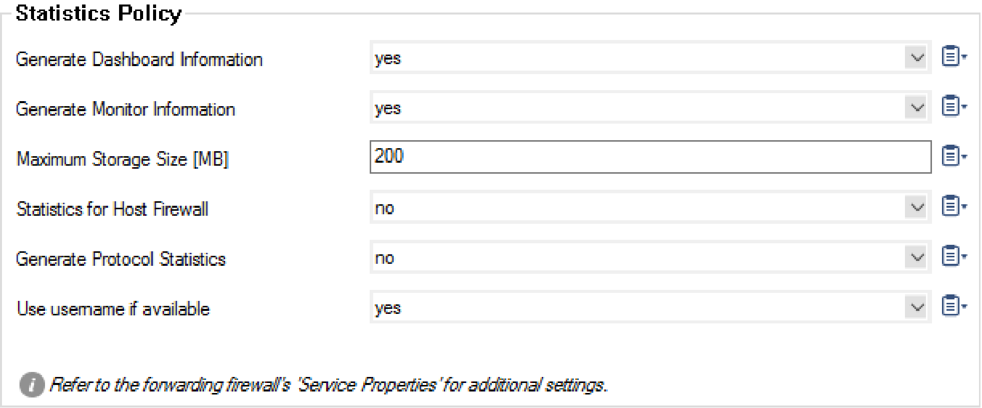
How to Configure Audit and Reporting

---

1. Go to **CONFIGURATION** > **Configuration Tree** > **Box** > **Infrastructure Services** > **General Firewall Configuration** .
2. In the left menu, select **Audit and Reporting**.
3. Expand the **Configuration Mode** menu and select **Switch to Advanced View**.
4. Click **Lock**.

Configure Statistics Policy

In the **Statistics Policy** section, configure the following settings:



Statistics Policy

Generate Dashboard Information	yes
Generate Monitor Information	yes
Maximum Storage Size [MB]	200
Statistics for Host Firewall	no
Generate Protocol Statistics	no
Use username if available	yes

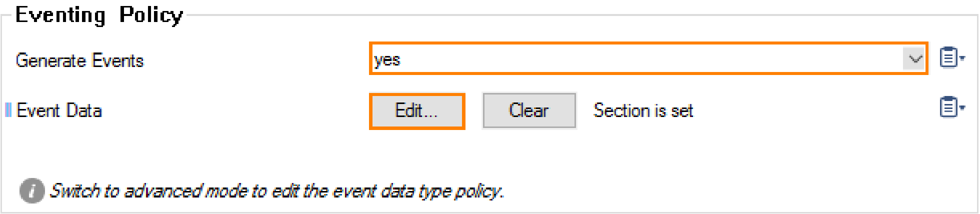
Refer to the forwarding firewall's 'Service Properties' for additional settings.

- **Generate Dashboard Information** – To enable the firewall dashboard, select **yes**.
- **Generate Monitor Information** – To enable the firewall monitor, select **yes**.
- **Maximum Storage Size** – Enter the amount of megabytes [MB] for the maximum size of the storage.
- **Statistics for Host Firewall** – Enable if you want to create statistics for the Host Firewall.
- **Generate Protocol Statistics** – Enable to create protocol- and P2P-specific statistics. These statistic can be seen using the event viewer under `.../server/BOX/proto–stat/.`
- **Use username if available** – Enable if usernames should be used for statistics instead of IP addresses.

Configure Eventing Policy

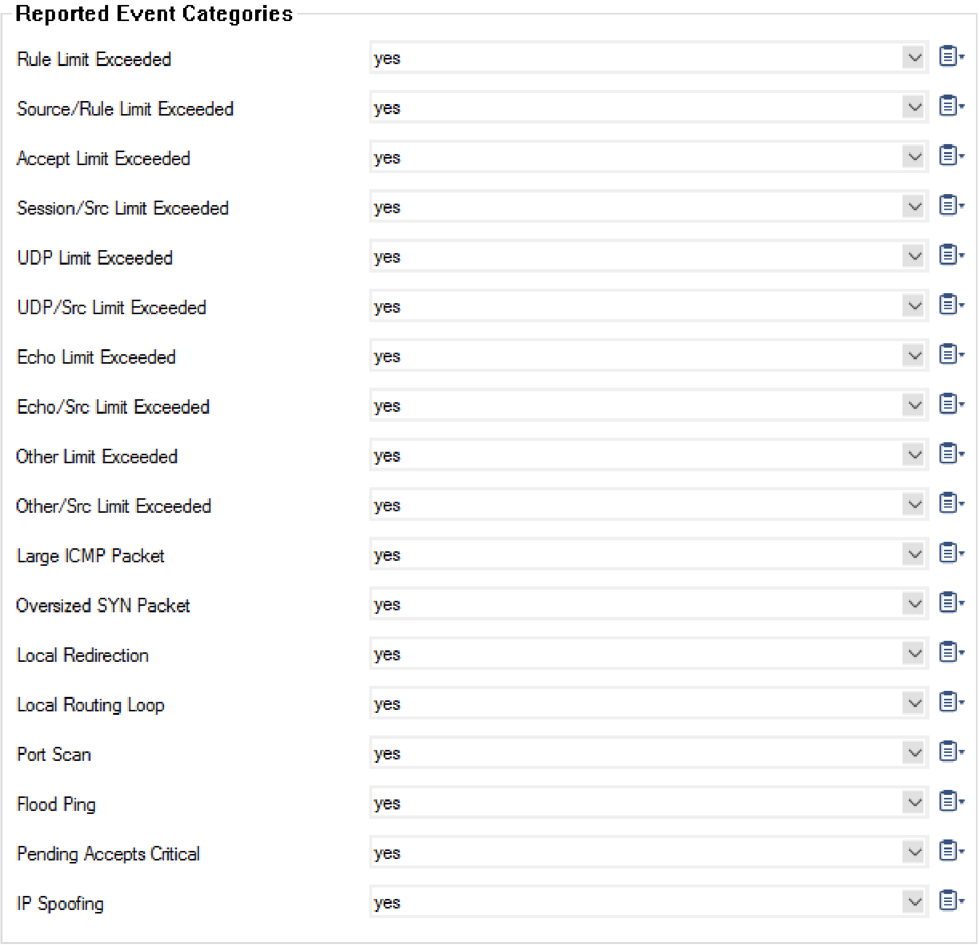
In the **Eventing Policy** section, configure the following settings:

- **Generate Events** – To generate events, select **yes**.
- **Event Data** – Click **Show.../Edit...** to enable or disable specific events:



    - **Rule Limit Exceeded** – Triggers event 'FW Rule Connection Limit Exceeded' [4016] when the allowed maximum number of connections for a rule has been exceeded.
    - **Source/Rule Limit Exceeded** – Triggers event 'FW Rule Connection per Source Limit Exceeded' [4018] when the allowed maximum number of connections/src for a rule has been exceeded.
    - **Accept Limit Exceeded** – Triggers event 'FW Pending TCP Connection Limit Reached' [4006] when the limit for 'Max Pending Accepts/Src' has been exceeded.
    - **Session/Src Limit Exceeded** – Triggers event 'FW Global Connection per Source Limit Exceeded' [4024] when the limit for either 'Max Local-In Sessions/Src' or 'Max. Forwarding Sessions/Src' has been exceeded.
    - **UDP Limit Exceeded** – Triggers event 'FW UDP Connection Limit Exceeded' [4009] when the limit for 'Max UDP (%)' has been exceeded.
    - **UDP/Src Limit Exceeded** – Triggers event 'FW UDP Connection per Source Limit Exceeded' [4008] when the limit for either 'Max Local-In UDP/Src' or 'Max. Forwarding UDP/Src' has been exceeded.
    - **Echo Limit Exceeded** – Triggers event 'FW ICMP-ECHO Connection Limit Exceeded' [4027] when the limit for either 'Max Echo (%)' has been exceeded.
    - **Echo/Src Limit Exceeded** – Triggers event 'FW ICMP-ECHO Connection per Source Limit Exceeded' [4026] when the limit for either 'Max Local-In Echo/Src' or 'Max. Forwarding Echo/Src' has been exceeded.
    - **Other Limit exceeded** – Triggers event 'FW OTHER-IP Session Limit Exceeded' [4029] when the limit for either 'Max Other (%)' has been exceeded.
    - **Other/SrcLimit exceeded** – Triggers event 'FW OTHER-IP Connection per Source Limit Exceeded' [4028] when the limit for either 'Max Local-In Other/Src' or 'Max. Forwarding Other/Src' has been exceeded.
    - **Large ICMP Packet** – Triggers event 'FW Large ICMP Packet Dumped' [4012] when the service object specific limit of 'Max Ping Size' has been exceeded.
    - **Oversized SYN Packet** – Triggers event 'FW Oversized SYN Packet Dumped' [4010] when an oversized SYN packet has been detected and dropped.
    - **Local Redirection** – Triggers event 'FW Local Redirection Suppressed' [2502] when the firewall redirects traffic to itself.
    - **Local Routing Loop** – Triggers event 'FW Forwarding Loop Suppressed' [2500] when the firewall detects a routing loop.
    - **Port Scan** – Triggers event 'FW Port Scan Detected' [4000] when the 'Port Scan Threshold' has been exceeded by a particular source.
    - **Flood Ping** – Triggers event 'FW Flood Ping Protection Activated' [4002] when the service object specific limit of 'Min Delay' has been violated.
    - **Pending Accepts Critical** – Triggers event 'FW Activating Perimeter Defence (inbound

mode)' [4004] when limit for 'Inbound Threshold (%)' has been exceeded.
  - **IP Spoofing** – Triggers events 'FW IP Spoofing Attempt Detected' [4014] or 'FW Potential IP Spoofing Attempt' [4015]. This only applies to firewall rules where 'Source/Reverse Interface' policies have been set to 'matching'.

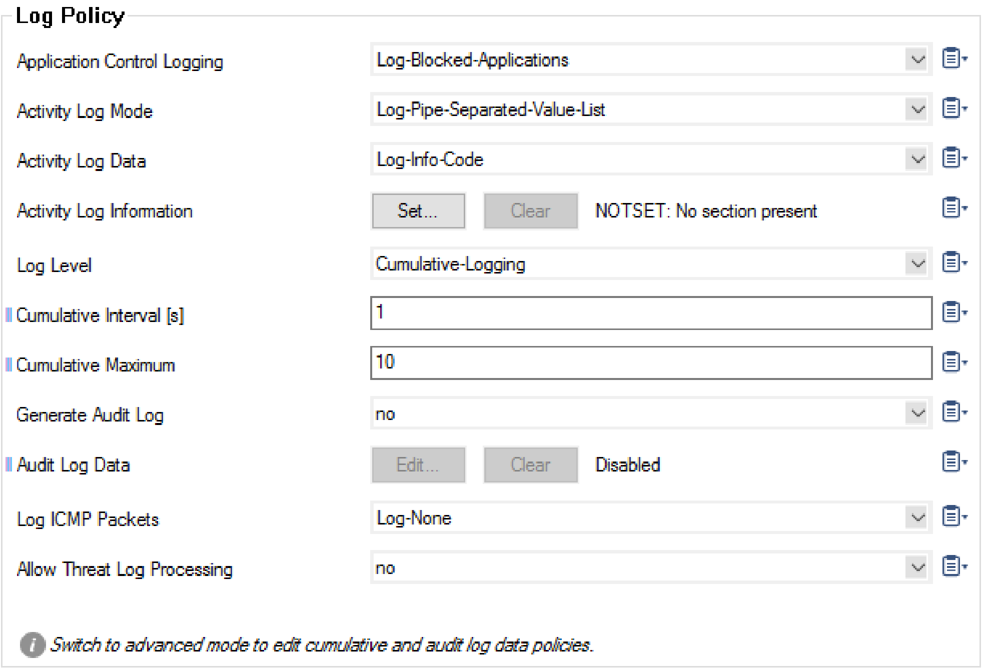


Reported Event Categories

Rule Limit Exceeded	yes
Source/Rule Limit Exceeded	yes
Accept Limit Exceeded	yes
Session/Src Limit Exceeded	yes
UDP Limit Exceeded	yes
UDP/Src Limit Exceeded	yes
Echo Limit Exceeded	yes
Echo/Src Limit Exceeded	yes
Other Limit Exceeded	yes
Other/Src Limit Exceeded	yes
Large ICMP Packet	yes
Oversized SYN Packet	yes
Local Redirection	yes
Local Routing Loop	yes
Port Scan	yes
Flood Ping	yes
Pending Accepts Critical	yes
IP Spoofing	yes

Configure Log Policy

In the **LogPolicy** section, configure the following settings:



Log Policy

Application Control Logging: Log-Blocked-Applications

Activity Log Mode: Log-Pipe-Separated-Value-List

Activity Log Data: Log-Info-Code

Activity Log Information: NOTSET: No section present

Log Level: Cumulative-Logging

Cumulative Interval [s]: 1

Cumulative Maximum: 10

Generate Audit Log: no

Audit Log Data: Disabled

Log ICMP Packets: Log-None

Allow Threat Log Processing: no

Switch to advanced mode to edit cumulative and audit log data policies.

- **Application Control Logging** – Select which Application Control data should be logged.
    - **No-Log-Entry** – No information about applications will be logged.
    - **Log-Blocked-Applications** – Blocked applications will be logged.
    - **Log-Allowed-Applications** – Allowed applications will be logged.
    - **Log-All-Applications** – All applications will be logged.
      Notifications for application ruleset blocks which were logged with type "Detect" and only contain the block information in the info-text are now logged with type "Block". See the following tables with the correspondig codes and reasons:

Code	Meaning
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

Code	**Meaning**
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

Code	**Meaning**
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 Incomlete
3040	High Level Protocol Header is Invalid
3041	High Level Protocol Version is Invalid
3042	High Level Protocol Packet is Incomlete
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 Nexthop 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

Code	Meaning
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 fai
4043	URL Domain Explicitly not Allowed by URL Categorizatio

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 fai
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

Code	Meaning
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

Code	Meaning
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 Protcol 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

Code	**Meaning**
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 fai
7043	URL Domain Explicitly not Allowed by URL Categorizatio
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 fai
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

- **Activity Log Mode**
  - **Log-Pipe-Separated-Value-List** – Select this option if you require value based log entries separated by a pipe symbol, e.g.

    ```
    2018 01 30 08:14:47 Info     +00:00 Detect:
    IPRX|TCP|eth0|10.17.33.202|29289|00:00:00:00:00:00|74.208.236.242|8
    0||eth0||0|10.17.33.201|74.208.236.242|0|1|0|0|0|0|user15|HTTP
    direct|Web browsing|www.noiseaddicts.com||Social Networking
    ```

    Log-Pipe-Separated-Key-Value-List – Select this option if you require key-value pairs of log entries separated by a pipe symbol, e.g.

    ```
    2018 01 30 13:12:21 Security +01:00 Block:
    type=FWD|proto=UDP|srcIF=eth0|srcIP=10.17.34.12|srcPort=54915|srcMA
    C=18:db:f2:13:ca:9c|dstIP=10.17.34.255|dstPort=54915|dstService=|ds
    tIF=|rule=BLOCKALL|info=Block by
    Rule|srcNAT=0.0.0.0|dstNAT=0.0.0.0|duration=0|count=1|receivedBytes
    =0|sentBytes=0|receivedPackets=0|sentPackets=0|user=|protocol=|appl
    ication=|target=|content=|urlcat=
    ```

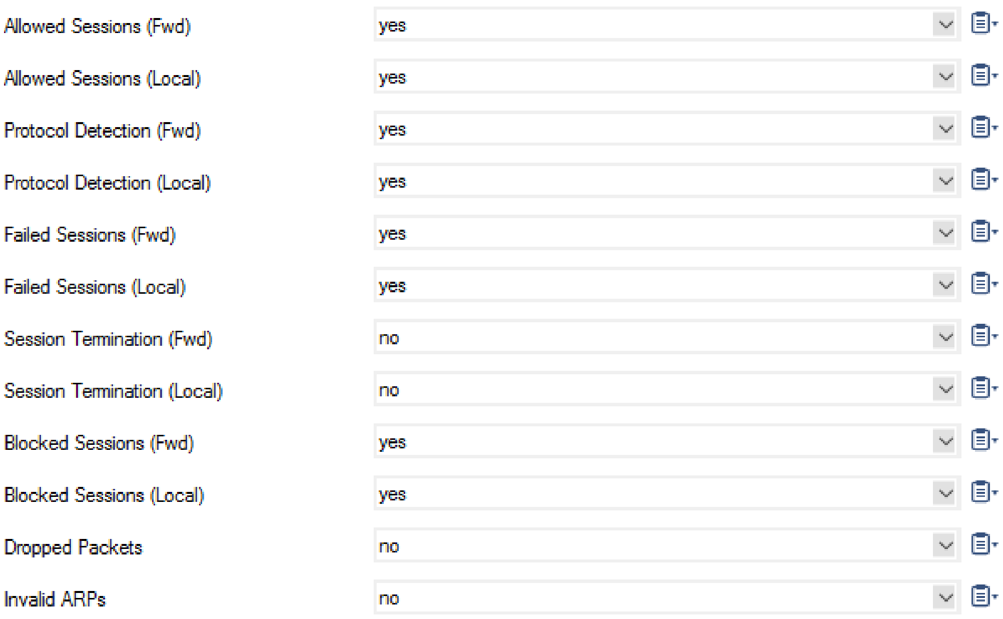
- **Activity Log Data**
  - **Log-Info-Code** – In "**Log-Info-Code**" mode, additional information is written as a number, e.g.

2018 01 30 12:58:09 Info +00:00 Detect: FWD|TCP|eth0|10.17.33.202|44973|00:00:00:00:00:00|74.208.236.242|80||eth0|| ***4045*** |10.17.33.201|74.208.236.242|0|1|0|0|0|0|user11|HTTP direct|Web browsing|www.noiseaddicts.com||Social Networking (46)

  - **Log-Info-Text** – In "**Log-Info-Text**" mode, the additional information is written as full text, e.g. IPRX|TCP|eth0|10.17.33.202|57037|00:00:00:00:00:00|31.13.84.36|443||eth0|| ***URL Category Blocked by Policy*** |10.17.33.201|31.13.84.36|0|1|0|0|0|0|user2|HTTPS direct|Facebook Base| facebook.com ||Social Networking (46)

> logd daemon is automatically translating numbers to text, so in Firewall admin (formerly NGadmin) the reason text is shown also for "Log-Info-Code" mode!

- **Activity Log Information** – Click **Set.../Edit** to enable or disable specific activities:
  - **Allowed Sessions (Fwd)** – Log each newly established forwarding session.
  - **Allowed Sessions (Local)** – Log local traffic, e.g., HTTP proxy or DNS.
  - **Protocol Detection (Fwd)** – Log protocol detection for each newly established forwarding session.
  - **Protocol Detection (Local)** – Log protocol detection for each newly established local session, e.g., HTTP proxy or DNS.
  - **Failed Sessions (Fwd)** – Log each allowed request that failed to be established.
  - **Failed Sessions (Local)** – Log local traffic.
  - **Session Termination (Fwd)** – Log each finished forwarding session.
  - **Session Termination (Local)** – Log finished local sessions.
  - **Blocked Sessions (Fwd)** – Log each blocked forward session request. This is relevant for auditing.
  - **Blocked Sessions (Local)** – Log blocked local traffic.
  - **Dropped Packets** – Log each silently dropped packet.
  - **Invalid ARPs** – Log each invalid ARP request.



Allowed Sessions (Fwd)	yes
Allowed Sessions (Local)	yes
Protocol Detection (Fwd)	yes
Protocol Detection (Local)	yes
Failed Sessions (Fwd)	yes
Failed Sessions (Local)	yes
Session Termination (Fwd)	no
Session Termination (Local)	no
Blocked Sessions (Fwd)	yes
Blocked Sessions (Local)	yes
Dropped Packets	no
Invalid ARPs	no

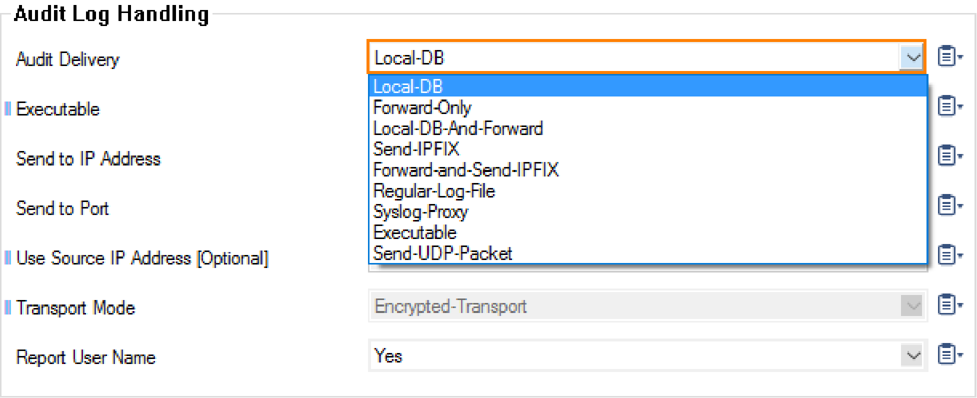
> "**Session Termination (Fwd)**", "**Session Termination (Local)**", "**Dropped Packets**" and "**Invalid ARPs**" are disabled by default!

- **Log Level** – Select the log level. Cumulative logging allows some reduction of log file lengths and tries to avoid indirect denial of service (DoS) attacks.
- **Cumulative Interval [s]** – Interval in seconds for which cumulative logging is activated for either matching or similar log entries. To enter cumulative logging, the entries need to be identical in all of the identifiers of a log entry except the source port (min: 1; max: 60; default: 1).
- **Cumulative Maximum** – Maximum number of log entries within the same rule and which results in cumulative logging to be triggered (default: 10).
- **Generate Audit Log** – Enables Firewall Audit.
  An audit event entry consists of a CR-terminated line of ASCII characters. Each line holds 23 pipe ("|") separated values. The values can be built up as a pipe-separated-value-list or as a pipe-separated-key-value-pair-list.
  Example: *1129102500|Block:|FWD|eth0|ICMP|BLOCKALL|10.0.3.80|0|10.0.3.73|0||4002|Block by Rule|0.0.0.0|0|0.0.0.0|0||00:07:e9:09:04:30|0|0|0|0|0|4552264444*

Column	Value	Type
1	Time	Unix seconds
2	Log Operation	Log Operations (Unknown, Allow, LocalAllow, Block, LocalBlock, Remove, LocalRemove, Drop, Terminate, LocalTerminate, Change, Operation, Startup, Configuration, Rule, State, LocalState, Process, AdminAction, Deny, LocalDeny, SecurityEvent, Sync, Fail, or LocalFail)
3	Session Type	Session Type (Forwarding, Local In, Local Out, or Loopback)
4	Input Network Device	String
5	IP Protocol	String
6	Firewall Rule	String
7	Source IP Address	IP Address
8	Source Port Number	0–65535
9	Destination IP Address	IP Address
10	Destination Port Number	0-65535
11	Service Name	String
12	Reason Code	Number
13	Reason	String
14	Bind IP Address	IP Address
15	Bind Port Number	0-65535
16	Connection IP Address	IP Address
17	Connection Port Number	0–65535
18	Output Network Device	String
19	MAC Address	6 colon-separated hex bytes
20	# of Input Packets	Number

21	# of Output Packets	Number
22	# of Input Bytes	Number
23	# of Output Bytes	Number
24	Duration	In seconds
25	ID	Audit entry number

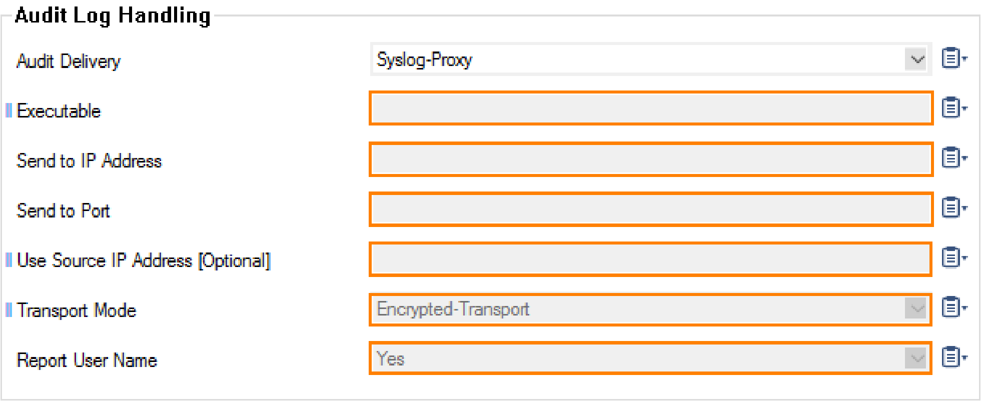
- **Audit Log Data** – Click **Set.../Edit** to configure **Firewall Audit** settings:
  - **Audit Delivery** – Select how audit log data is stored or transferred:
    - **Local-DB** – Store audit data within a local sqlite3 DB.
    - **Forward-Only** – Forward natively to an audit collector service.
    - **Local-DB-And-Forward** – The combination of both.
    - **Send-IPFIX** – Hand off data to separate IPFIX exporter.
    - **Forward-and-Send-IPFIX** – Combination of forwarding and send data to an IPFIX exporter.
    - **Regular-Log-File** – Plain ascii based log file.
    - **Syslog-Proxy** – Generate syslog messages.
    - **Executable** – Feed into custom executable on stdin.
    - **Send-UDP-Packet** – Send via plain UDP stream.



Audit Log Handling

Audit Delivery: Local-DB
Executable
Send to IP Address
Send to Port
Use Source IP Address [Optional]
Transport Mode: Encrypted-Transport
Report User Name: Yes

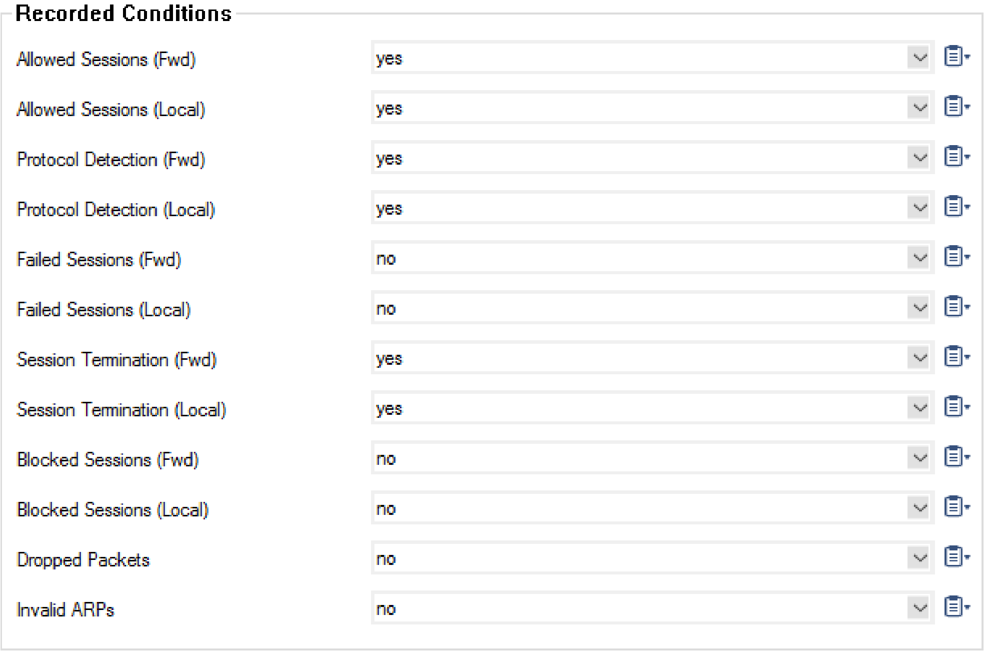
  - **Executable** – Enter the path of the executable file the data is sent to.
  - **Send to IP Address** – Enter the IP address of the audit service the data is sent to.
  - **Send to Port** – Enter the port the data is sent to. If not specified, port 680 is used.
  - **Use Source IP Address [Optional]** – Enter the source IP address. If not specified, the management IP / Virtual IP address is used.
  - **Transport Mode** – Select whether transported data should be encrypted or not.
  - **Report User Name** – Optionally include the username into the session information if available.



Audit Log Handling

Audit Delivery	Syslog-Proxy
Executable	
Send to IP Address	
Send to Port	
Use Source IP Address [Optional]	
Transport Mode	Encrypted-Transport
Report User Name	Yes

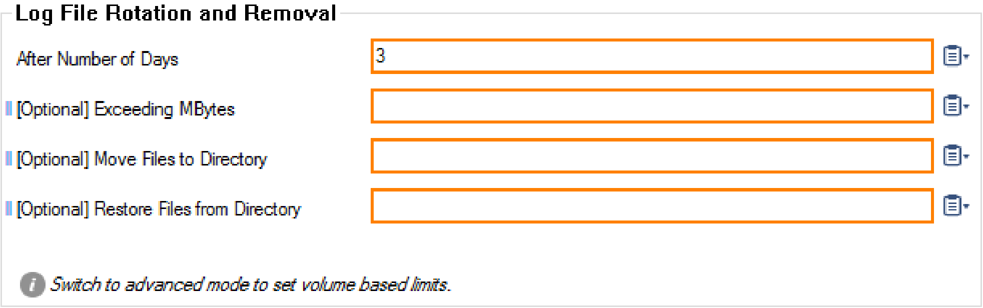
  - **Allowed Sessions (Fwd)** – Create a record for each newly established forwarding session. This is relevant for auditing.
  - **Allowed Sessions (Local)** – Same for local traffic, e.g., HTTP proxy or DNS.
  - **Protocol Detection (Fwd)** – Enable protocol detection for each newly established forwarding session.
  - **Protocol Detection (Local)** – Enable protocol detection for each newly established local session, e.g., HTTP proxy or DNS.
  - **Failed Sessions (Fwd)** – Create an entry for each allowed request that failed to be established. This is relevant for troubleshooting.
  - **Failed Sessions (Local)** – Same for local traffic.
  - **Session Termination (Fwd)** – Create a record on session removal for each finished forwarding session.
  - **Session Termination (Local)** – Create a record on session removal for each finished local session.
  - **Blocked Sessions (Fwd)** – Create a record for each blocked forward session request. This is relevant for auditing.
  - **Blocked Sessions (Local)** – Create a record for each blocked local session request. This is relevant for auditing.
  - **Dropped Packets** – Create an entry for each silently dropped packet.
  - **Invalid ARPs** – Create an entry for each invalid ARP request.



Recorded Conditions

Allowed Sessions (Fwd)	yes
Allowed Sessions (Local)	yes
Protocol Detection (Fwd)	yes
Protocol Detection (Local)	yes
Failed Sessions (Fwd)	no
Failed Sessions (Local)	no
Session Termination (Fwd)	yes
Session Termination (Local)	yes
Blocked Sessions (Fwd)	no
Blocked Sessions (Local)	no
Dropped Packets	no
Invalid ARPs	no

- **After Number of Days** – Number of days until log file entries will be purged.
- **[Optional] Exceeding MBytes** – Enter the maximum size of log files in MB until purging starts.
- **[Optional] Move Files to Directory** – Specify the directory where purged log data is moved to.
- **[Optional]Restore Files from Directory** – If required, specify the directory from where to restore previously purged log data.

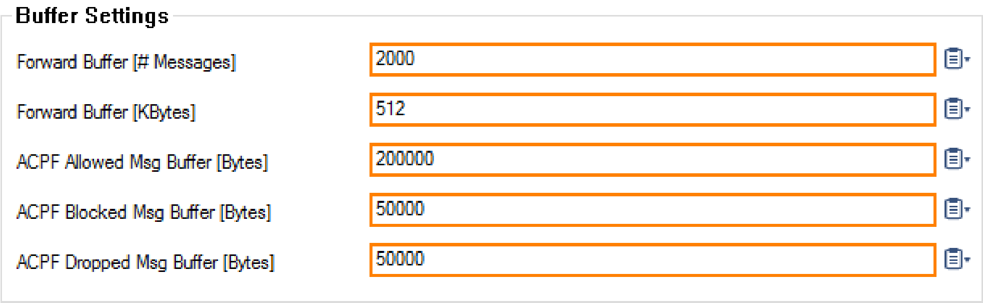


Log File Rotation and Removal

After Number of Days	3
[Optional] Exceeding MBytes	
[Optional] Move Files to Directory	
[Optional] Restore Files from Directory	

Switch to advanced mode to set volume based limits.

- **Forward Buffer [Messages]** – Number of messages that can be buffered when forwarding.
- **Forward Buffer [KBytes]** – Number of KBytes that can be buffered when forwarding.
- **ACPF Allowed Msg Buffer [Bytes]** – Number of ACPF buffered bytes for allow messages.
- **ACPF Blocked Msg Buffer [Bytes]** – Number of ACPF buffered bytes for block messages.
- **ACPF Dropped Msg Buffer [Bytes]** – Number of ACPF buffered bytes for drop messages.



Buffer Settings

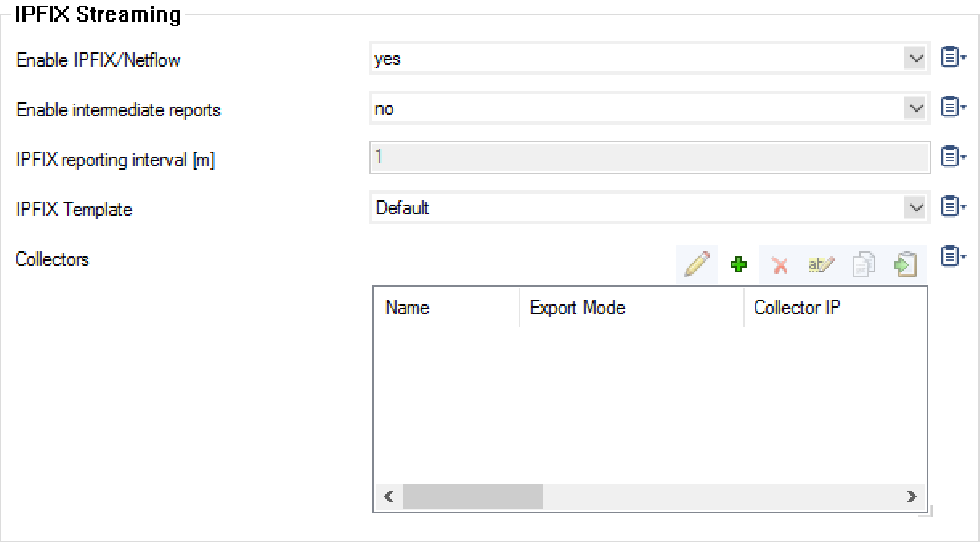
Forward Buffer [# Messages]	2000
Forward Buffer [KBytes]	512
ACPF Allowed Msg Buffer [Bytes]	200000
ACPF Blocked Msg Buffer [Bytes]	50000
ACPF Dropped Msg Buffer [Bytes]	50000

- **Log 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.

Configure IPFIX Streaming

In the **IPFIX Streaming** section, configure the following settings:

- **Enable IPFIX/Netflow** – Internet Protocol Flow Information Export (IPFIX, RFC 3917) is based on NetFlow version 9. You can use this to stream the Firewall Audit logs via IPFIX.
- **Enable intermediate reports** – Select yes to enable sending of intermediate reports with delta counters.
- **IPFIX reporting interval [m]** – Use the IPFIX reporting interval [m] option to determine how often intermdiate reports are sent.
- **IPFIX Template** – If set to Extended, includes additional information, such as delta coutners, 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** – Click **+** to add collectors.



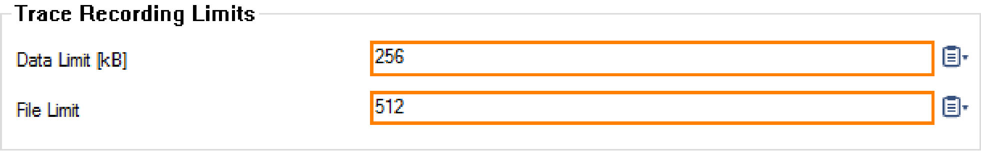
IPFIX Streaming

Enable IPFIX/Netflow	yes
Enable intermediate reports	no
IPFIX reporting interval [m]	1
IPFIX Template	Default
Collectors	

Name	Export Mode	Collector IP

Configure Connection Tracing

- Click **Set.../Edit** to configure the **Connection Tracing** settings.
  - **Data Limit [kB]** – Maximum number of bytes of a traced connection (max. 4096kB).
  - **File Limit** – Maximum number of traced connections (max. 1024).



Data Limit [kB]: 256

File Limit: 512

Activation

To activate changes made to the audit and reporting configuration, you must perform a firmware restart.

1. Click **Send Changes** and **Activate**.
2. Go to the **CONTROL > Box**.
3. Expand the **Operating System** section.
4. Click **Firmware Restart**.

All active connections will be terminated when performing a firmware restart.

Figures