Reporting of Network Flow Information with IPFIX

https://campus.barracuda.com/doc/96026569/

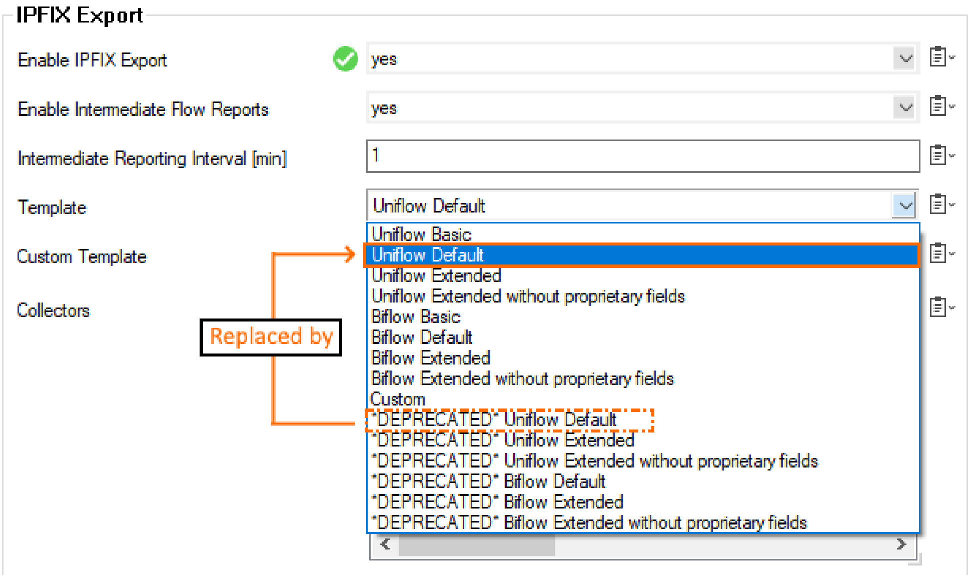
On the Barracuda CloudGen Firewall, you can stream audit and reporting information to multiple external collectors based on the IPFIX protocol. Enable IPFIX, add collectors, and, optionally, enable IPFIX streaming for your HTTP proxy service.

Handling IPFIX Templates

Starting with firmware version 8.0.5 / 8.2.0, IPFIX now works completely independent of the audit infrastructure. In order to use IPFIX, you now just need to enable/disable IPFIX in the configuration. The audit configuration does not need to be changed in any way and has no effect on IPFIX.

Also, previous IPFIX templates have been updated to newer versions. When updating the firmware to 8.0.5 / 8.2.0, IPFIX will run in 'backward compatibility mode', that is, previous IPFIX template settings remain in their current state and now (8.0.5 / 8.2.0) have names with the prefix ***DEPRECATED***. These settings remain activated to preserve the configured behavior and can be updated to their corresponding new names.

It is recommended to change such settings by selecting the corresponding new names. In this example, switch from ***DEPRECATED* Uniflow Default** to **Uniflow Default** in the respective menu list in the UI.



IPFIX Export

Enable IPFIX Export: yes

Enable Intermediate Flow Reports: yes

Intermediate Reporting Interval [min]: 1

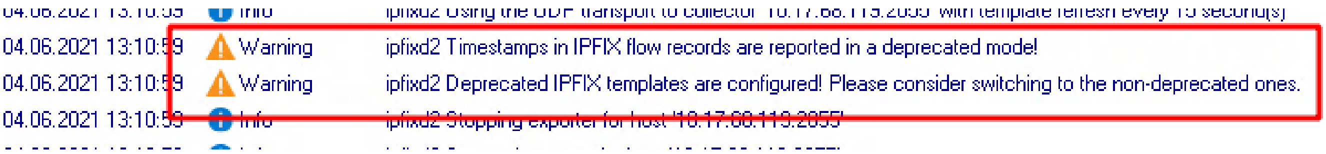
Template: Uniflow Default

Custom Template

Collectors

Uniflow Basic
Uniflow Default
Uniflow Extended
Uniflow Extended without proprietary fields
Biflow Basic
Biflow Default
Biflow Extended
Biflow Extended without proprietary fields
Custom
DEPRECATED Uniflow Default
DEPRECATED Uniflow Extended
DEPRECATED Uniflow Extended without proprietary fields
DEPRECATED Biflow Default
DEPRECATED Biflow Extended
DEPRECATED Biflow Extended without proprietary fields
Replaced by

If IPFIX is working in backward compatibility mode, the use of former templates is indicated by corresponding messages in the log line:



```
04.06.2021 13:10:59   Info      ipfixd2 Using the UDP transport to collector '10.17.68.113:2055' with template refresh every 15 second(s)
04.06.2021 13:10:59   Warning   ipfixd2 Timestamps in IPFIX flow records are reported in a deprecated mode!
04.06.2021 13:10:59   Warning   ipfixd2 Deprecated IPFIX templates are configured! Please consider switching to the non-deprecated ones.
04.06.2021 13:10:59   Info      ipfixd2 Stopping exporter for host '10.17.68.113:2055'
```

Changes to IPFIX Templates

With firmware 8.0.5 / 8.2.0, several changes have been made to the Information Elements.

For an overview of the current information templates, see the tables below.

Standardized Fields

Some standardized fields (Information Elements) in predefined templates have changed:

- All templates now include *flowStartMilliseconds* and *flowEndMilliseconds*.
- *octetTotalCount* and *packetTotalCount* are now only included in the **Extended** templates.
- A new basic template (**Uniflow Basic**) has been introduced that offers the best compatibility with various collectors.
- Except in the basic template, *firewallEvent* is now included in all templates.
- The *systemInitTimeMilliseconds* has been added and is included in the **Extended** templates.

Barracuda Proprietary Fields

Some proprietary fields were replaced with standardized ones and apply to the deprecated templates only:

- *bindIPv4Address* has been replaced with *postNATSourceIPv4Address*
- *connIPv4Address* has been replaced with *postNATDestinationIPv4Address*
- *bindTransportPort* has been replaced with *postNAPTSourceTransportPort*
- *connTransportPort* has been replaced with *postNAPTDestinationTransportPort*
- *auditCounter* has been removed without replacement, because similar information can be derived from the IPFIX header
- *timestamp* has been removed without replacement, because similar information can be derived from the IPFIX header

Reporting Timestamps

The reporting of timestamps for intermediate flow records has been adapted to improve the compatibility with various collectors. Instead of reporting the flow's overall start and end times, the flow record now includes the start and end times of the corresponding intermediate interval. This change takes effect only when a non-deprecated template is configured.

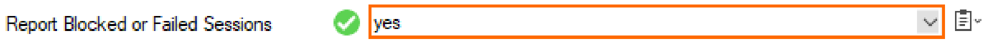
The reporting timestamps now work as follows:

- If there is a preceding flow report for a flow, the report's 'end time' is used as the new 'start time'. Otherwise, the slot creation time is used.
- The timestamp of the last packet that was forwarded through the slot is sent as 'end time'.

Blocked Traffic

Blocked traffic is no longer reported by default for improved compatibility with various collectors. If reporting of blocked traffic is desired and there are no compatibility concerns, it can be re-enabled as follows:

1. Go to **CONFIGURATION > Configuration Tree > Box > Infrastructure Services > General Firewall Configuration**.
2. In the left menu, select **Audit and Reporting**.
3. In the left menu, expand **Configuration Mode** and click **Switch to Advanced View**.
4. Click **Lock**.
5. In the section IPFIX Export, set **Report Blocked or Failed Sessions** to **yes**.
6. Click **Send Changes / Activate**.



Report Blocked or Failed Sessions ✓ yes

Configuring IPFIX

To configure audit & reporting with IPFIX, see How to Configure IPFIX.

To create custom information templates, see How to Create Custom IPFIX Templates.

Tables

Basic Template

ID	Name	Size (octets)	Type
1	octetDeltaCount	8	unsigned64
2	packetDeltaCount	8	unsigned64
4	protocolIdentifier	1	unsigned8
7	sourceTransportPort	2	unsigned16
8	sourceIPv4Address	4	ipv4Address

10	ingressInterface	4	unsigned32
11	destinationTransportPort	4	unsigned16
12	destinationIPv4Address	4	ipv4Address
14	egressInterface	4	unsigned32
152	flowStartMilliseconds	8	dateTimeMilliseconds
153	flowEndMilliseconds	8	dateTimeMilliseconds

Default Template

ID	Name	Size (octets)	Type
1	octetDeltaCount	8	unsigned64
2	packetDeltaCount	8	unsigned64
4	protocolIdentifier	1	unsigned8
7	sourceTransportPort	2	unsigned16
8	sourceIPv4Address	4	ipv4Address
10	ingressInterface	4	unsigned32
12	destinationIPv4Address	4	ipv4Address
14	egressInterface	4	unsigned32
148	flowID	8	unsigned64
152	flowStartMilliseconds	8	dateTimeMilliseconds
153	flowEndMilliSeconds	8	dateTimeMilliseconds
161	flowDurationMilliseconds	4	unsigned32
233	firewallEvent	1	unsigned8
Barracuda Proprietary Information Elements **Private Enterprise Number Barracuda Networks: 10704**			
2	cudaLogOperation	1	unsigned8
3	cudaTrafficType	1	unsigned8
4	cudaFirewallRule	variable	string
5	cudaServiceName	variable	string
6	cudaFirewallReason	variable	string
7	cudaFirewallReasonText	variable	string

Extended Template

ID	Name	Size (octets)	Type
1	octetDeltaCount	8	unsigned64
2	packetDeltaCount	8	unsigned64
4	protocolIdentifier	1	unsigned8
7	sourceTransportPort	2	unsigned16
8	sourceIPv4Address	4	ipv4Address
10	ingressInterface	4	unsigned32
12	destinationIPv4Address	4	ipv4Address
14	egressInterface	4	unsigned32
21	flowEndSysUpTime	4	unsigned32
22	flowStartSysUpTime	4	unsigned32
148	flowID	8	unsigned64
152	flowStartMilliseconds	8	dateTimeMilliseconds
153	flowEndMilliSeconds	8	dateTimeMilliseconds
161	flowDurationMilliseconds	4	unsigned32
233	firewallEvent	1	unsigned8
Barracuda Proprietary Information Elements **Private Enterprise Number Barracuda Networks: 10704**			
2	barracudaLogOperation	1	unsigned8
3	barracudaTrafficType	1	unsigned8
4	barracudaFirewallRule	variable	string
5	barracudaServiceName	variable	string
6	barracudaFirewallReason	variable	string
7	barracudaFirewallReasonText	variable	string

Extended Template without Proprietary Barracuda Fields

ID	Name	Size (octets)	Type
1	octetDeltaCount	8	unsigned64
2	packetDeltaCount	8	unsigned64
4	protocolIdentifier	1	unsigned8
7	sourceTransportPort	2	unsigned16

8	sourceIPv4Address	4	ipv4Address
10	ingressInterface	4	unsigned32
12	destinationIPv4Address	4	ipv4Address
14	egressInterface	4	unsigned32
21	flowEndSysUpTime	4	unsigned32
22	flowStartSysUpTime	4	unsigned32
148	flowID	8	unsigned64
152	flowStartMilliseconds	8	dateTimeMilliseconds
153	flowEndMilliSeconds	8	dateTimeMilliseconds
161	flowDurationMilliseconds	4	unsigned32
233	firewallEvent	1	unsigned8

Valid Values for the cudaLogOperation Information Field

ID	Name
0	Unknown
1	Allow
2	LocalAllow
3	Block
4	LocalBlock
5	Remove
6	LocalRemove
7	Drop
8	Terminate
9	LocalTerminate
10	Change
11	Operation
12	Startup
13	Configuration
14	Rule
15	State
16	LocalState
17	Process
18	AdminAction
19	Deny

20	LocalDeny
21	SecurityEvent
22	Sync
23	Fail
24	LocalFail
25	ARP
26	Detect
27	LocalDetect
28	IntermediateReport

Values for the cudaTrafficType Information Field

ID	Name
0	Forwarding
1	Local In
2	Local Out
3	Loopback

Figures