

Distributed Architecture Overview

Large and demanding network infrastructures contain many flow data sources in various locations. Processing large amounts of flow data on a single Flowmon Collector might be feasible, however this solution does not scale. In a large or expanding network the capacity of single processing unit will be eventually depleted. Distributed architecture (DA) provides high scalability and load balancing for such demanding environments. Flow data is distributed among multiple units for profiles computation and other flow data processing. More units can be simply added to increase both performance and storage capacity. Distributed Architecture provides central console for management and configuration of all units remote geographical locations as well as data aggregation and visualization in one place.

Table of Content

Components	2
Master Unit	2
Slave Unit	2
Proxy Unit	2
Groups	2
Proxy Group	2
Source Group	2
Query Processing	3
Deployment Modes	3
Master – Slave Mode	3
Master – Proxy – Slave Mode	4
Sample Deployment	4
Flow Distribution Models	5
Round-Robin Model	5
Flow Source Related	5
Flow Sources Management	5
Profiles Management	6
Network and Bandwidth Requirements	6
Communication Port Numbers	6
Bandwidth Utilization of DA Components	6
Flowmon Modules and Distributed Architecture	7
Module Deployment	7
Flowmon ADS	7
Flowmon DDoS Defender	7
Flowmon APM	7
Flowmon Traffic Recorder	7

Components

There are 3 types of units in DA: Master, Proxy and Slave units. Master and Proxy units are dedicated hardware or virtual appliances. Slave Units are traditional Flowmon Collectors (hardware or virtual appliances). For hardware specification of Master and Proxy units see Flowmon Collectors [specification document](#).

Master Unit

Central console for management and configuration of other units. It provides central interface to all data from all connected Flowmon Collectors. It provides web application for data visualisation, querying, reporting and analysis. Master Unit gathers data from other units and assembles final result.

There can be multiple instances of Master Unit. Users work with and perform configuration changes only on the top-priority instance called the Top Priority Master Unit (TPM). Slave Units, Proxy Units and groups are configured on TPM. TPM can initiate data queries on Proxy Units and obtain results. Other Master Units are synchronized and kept consistent with the TPM and can be set as TPM if the current TPM fails.

Slave Unit

Slave Units are storing and processing assigned part of flow data (see Flow Distribution Models below). More Slave Units can be added when needed. Slave Units are managed by Proxy Units. Slave Units can work in two ways as Standalone Slave or Proxy Group Slave. Proxy Group Slave operates as described above (Master – Proxy – Slave deployment mode). Standalone Slave is a Slave Unit which operates also as a Proxy Unit. In this mode there is only one Slave Unit in the Proxy Group (Master – Slave deployment mode).

Proxy Unit

Proxy Units are necessary for configurations with multiple Slave Units (Standalone Slaves) in one group. Master Unit communicates with Proxy Units only (to save bandwidth between different locations and for easier firewall configuration). Proxy Unit forwards all its requests to and from Slave Units in Proxy Group. Proxy Unit is used as a single target of flow export (eg. in one geographical location) and distributes flow data to its Slave Units. For groups with single Slave Unit no Proxy Unit is needed and Slave acts as Proxy for itself (Proxy Group Slave). One Proxy Unit and one or more Slave Units assigned to it creates a Proxy Group. Only one Proxy Unit is allowed in a Proxy Group.

Groups

Proxy Group

Proxy Unit and its Slave Units form a Proxy Group. Each Slave Unit can be assigned to a single Proxy Group only. Proxy Group enables scalability – if the group is overloaded, a new Slave Unit can be simply added to take over part of the data and tasks. All Proxy Group Slaves in Proxy Group must be licensed as the same collector model. Only Proxy Groups assigned into the Source Group are able to operate in the DA.

Source Group

Source Group is formed by one Proxy Group (mode without High Availability) or more Proxy Groups (High Availability mode). All Proxy Groups in a Source group are identical, deployed in the same location and receive flow data from the same flow sources (therefore a Source group). In High Availability (HA) mode, Proxy Groups are able to recover data between each other.

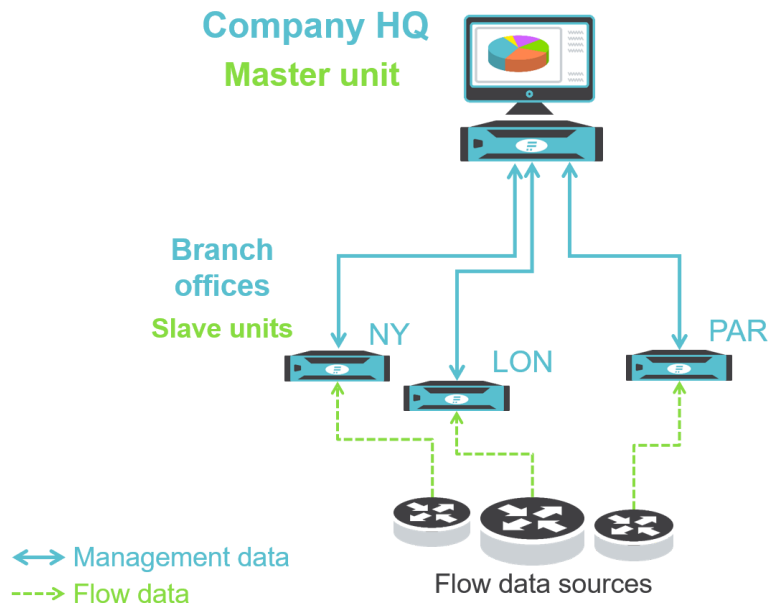
Query Processing

Flow data is stored on Slave Units. Master Unit stores only aggregated results and metadata. Queries are initiated at Master Unit and forwarded to Proxy Units. Each Proxy Unit will forwards queries to its Slave Units. Results from Slave Units are aggregated by Proxy if possible and then the results from all Proxy Units are sent to Master Unit. Master Unit then aggregates partial results into the final result provided to user.

Deployment Modes

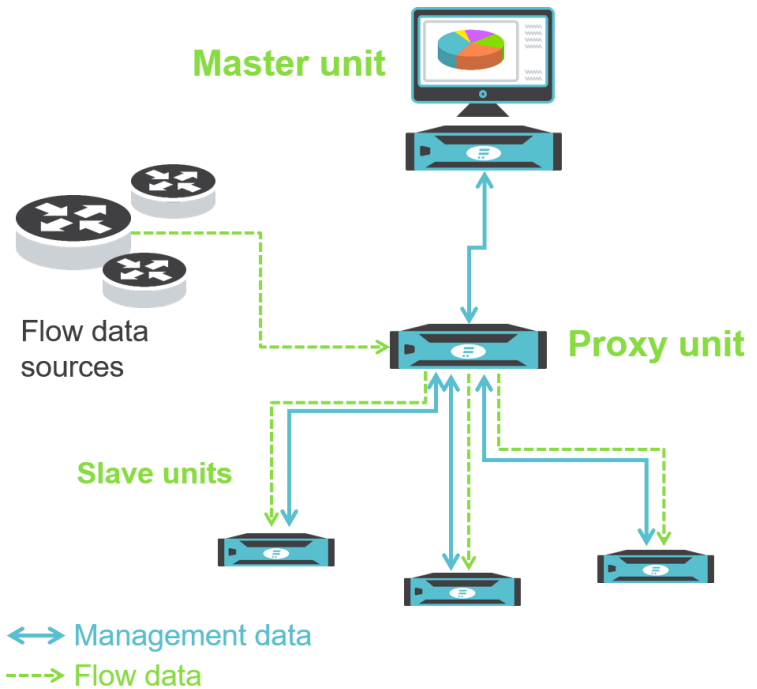
Master – Slave Mode

In this mode Master Unit communicates directly with Slave Units (Standalone Slaves). Each Slave Unit is set as a target of flow export for different flow data sources. In the example diagram below, each Slave Unit is storing and processing flow data in the different branch office (New York, London and Paris). Master Unit provides central reporting and data visualization. Slave Units are managed with Master Unit from the company HQ.

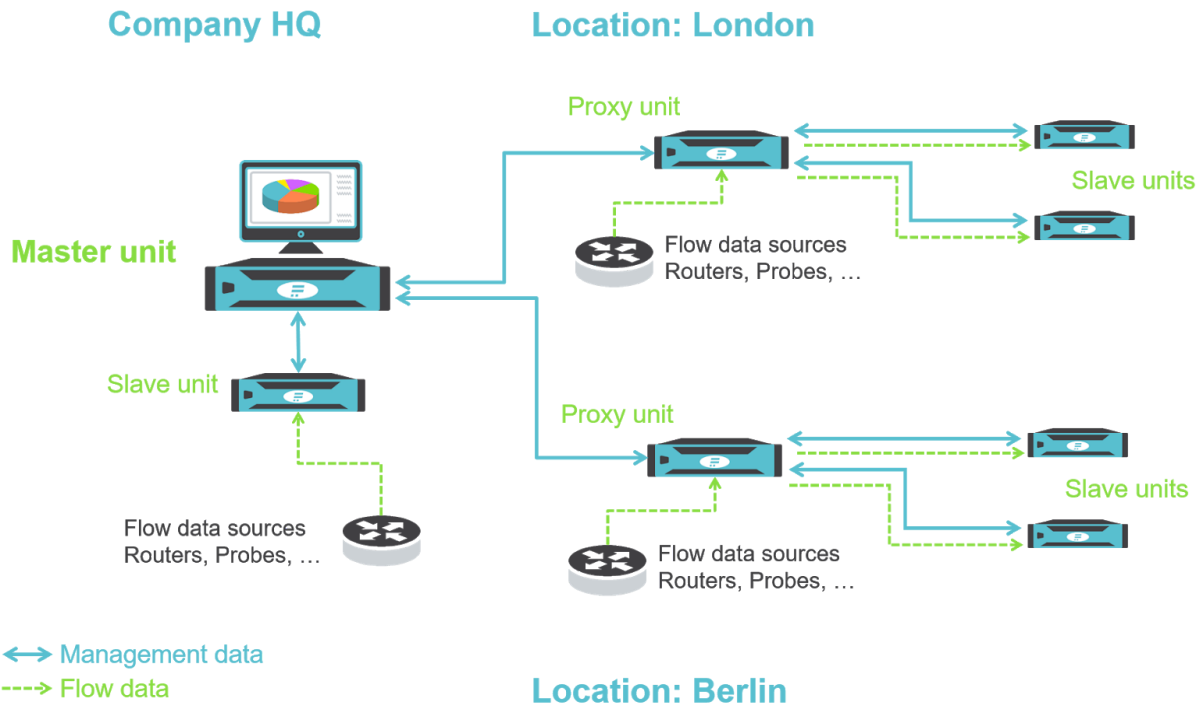


Master – Proxy – Slave Mode

In this mode Master Unit communicates only with Proxy Units. Proxy is set as a target for flow export and distributes flow data to Slave Units (Proxy Group Slaves). Slave Units and Proxy Unit form Proxy Group. Slave Units can be easily added to Proxy Groups will fully automated provisioning of all configuration needed.



Sample Deployment



Company headquarters is in Master – Slave mode. Slave Unit collects and processes data from flow data sources in HQ. Remote locations in London and Berlin are in Master – Proxy – Slave mode. Master Unit communicates with

Proxy Units and it distributes flow data and management changes to Slave Units. When Master Unit requests data, it queries Slave Unit in HQ or Proxy Units in remote locations.

Flow Distribution Models

This chapter describes flow distribution models which are the ways how is flow data distributed among Slave Units in a Proxy Group. Models have their advantages and disadvantages.

Round-Robin Model

Every Proxy Unit distributes flows in round-robin manner to all Slave Units in its group. Incoming flow packets are de-assembled, templates are sent to all Slaves units and flows are distributed in round robin manner. New flow packet assembled by Proxy Unit must have source IP of the original flow source.

Advantages:

- Perfect scalability in group (“just add a new device to group”)
- All slaves in the group are utilized equally

Disadvantages:

- More complicated data recovery

Flow Source Related

Every Proxy Unit maps flow packets from specific flow source to specific Slave Unit in its group. Incoming flow packets are distributed to Slave Units according to flow source address. Flow packets are forwarded as they are.

Advantages:

- Flows from same flow source are stored on the same Slave Unit – they can be used for flow source related detections etc. (e.g. anomaly detection)
- Easy data recovery

Disadvantages:

- Slaves in group are not utilized equally
- Limited scalability - flows from heavy utilized source cannot be distributed to multiple Slave Unit

Flow Sources Management

Each new flow source detected on Proxy Unit is reported to Master Unit. Master maps this flow source to Source Group, where it was detected and requests primary Proxy Group to obtain flow source metadata via SNMP. Flow source metadata update is requested by Master in regular manner.

Deleting flow source means to delete a channel of live profile – this is automatically propagated to all sub-profiles and their channels. Delete operation is performed on Master – it will delete a live profile channel (standard profile operation propagated to Proxies and Slaves) and it will also remove flow source from database and from list of flow sources of its Source Group. So deleting source will discard all its data in live profile. In sub-profiles, the data will stay intact.

Profiles Management

Profiles are managed by user on Master Unit. Profiles configuration remains the same as in the single system architecture. Selecting parent channels will assign each channel to specific flow sources (as each flow source is representing a root of its channel tree) and hence to a Source Groups. The profile is then created/modified on all Slave Units in selected Source Groups.

For Flow Sources Related distribution model, profile is created on all Slave Units in selected Source Groups as well, even if flow sources are not assigned to all Slaves in Source Group.

This is necessary in order to:

- keep unified configuration of all Slaves
- allow easy replacement and recovery
- allow changing list of parent channels of existing profile (subprofile of live)

When a profile is created, selected Source Groups then notify all Master Units, that the profile was created/modified. Every Slave is managing its profiles in same manner as in non-distributed architecture.

Network and Bandwidth Requirements

Communication Port Numbers

DA components use ports 2210 and 4210 for communication between each other. Port number **2210** is used for configuration and control, port **4210** for sending queries and results. For proper functionality of Distributed Architecture these ports needs to be allowed on the firewall.

Bandwidth Utilization of DA Components

Following bandwidth utilization is valid for communication between Master Unit and one Source Group. The communication between individual components in Distributed Architecture is not encrypted currently.

Operation	Bandwidth
Normal operations User is working with top statistics, list flow and other data with reasonable result size	0,1 Mbps
Large data set delivery User is receiving unlimited list of flows result for large set of data	10 Mbps
Major configuration updates exchange	0,5 Mbps

Delivery of update packages

Update package transmission between Master and Proxy Unit is not considered time-critical and will use only the available bandwidth.

Flowmon Modules and Distributed Architecture

Flowmon Modules are software components extending functionality of Flowmon Solution with advanced flow data analysis and other features (anomaly detection, application performance monitoring and traffic capture).

Module Deployment

Each module requires different approach when deployed in Distributed Architecture. This chapter describes these specifics for each extension module.

Following table describes on which units should be each module installed:

	Flowmon ADS	Flowmon APM	Flowmon Traffic Recorder
Master Unit	✓	✓	✓
Proxy Unit	* ✓ / x	x	x
Slave Units	✓	x	x
Flowmon Probes	x	✓	✓

*Flowmon ADS must be deployed on Proxy Units to forward regular Master-Slave communication (events, configuration and queries/responses) when it's not possible to establish direct connection between Master and Slave Units. Flowmon ADS on Proxy Units does not do any processing or data storage and does not have any user interface.

Flowmon ADS

Multiple Flowmon ADS systems are deployed on multiple Slave Units (each Slave needs to be licensed and there has to be same Flowmon ADS license on each processing unit). Flowmon ADS Master Unit (GUI) is deployed on Master Unit, which provides central interface to all data and detected events from all connected Flowmon ADS systems (only one Master is supported).

Flowmon DDoS Defender

Flowmon DDoS Defender does not support Distributed Architecture at the moment.

Flowmon APM

Multiple Flowmon APM licenses are deployed on Flowmon Probes. Flowmon APM (regular APM licence) is licensed and installed on the Master Unit (only one Master is supported).

Flowmon Traffic Recorder

Multiple Flowmon TR licenses are deployed on Flowmon Probes and one on the Master Unit (GUI). Only one Master is supported.