Netflow

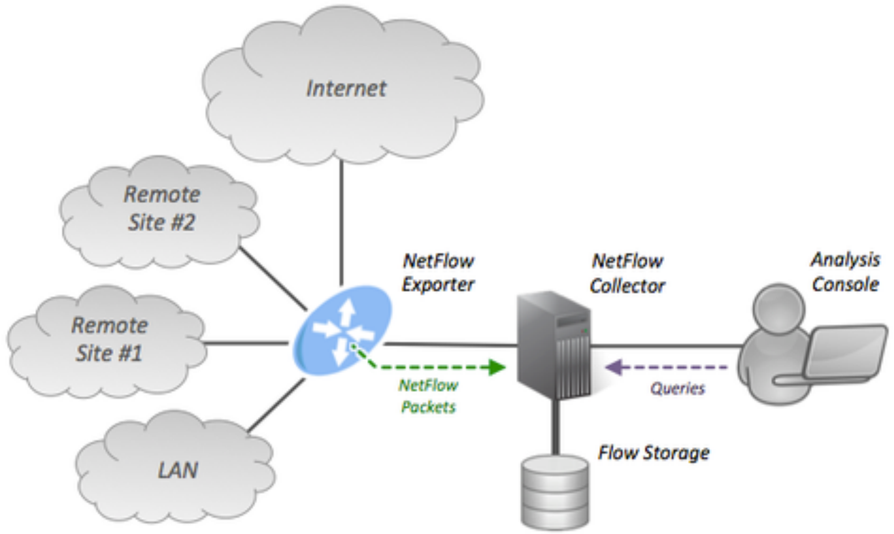
Monitoring and Log Management

Netflow Overview

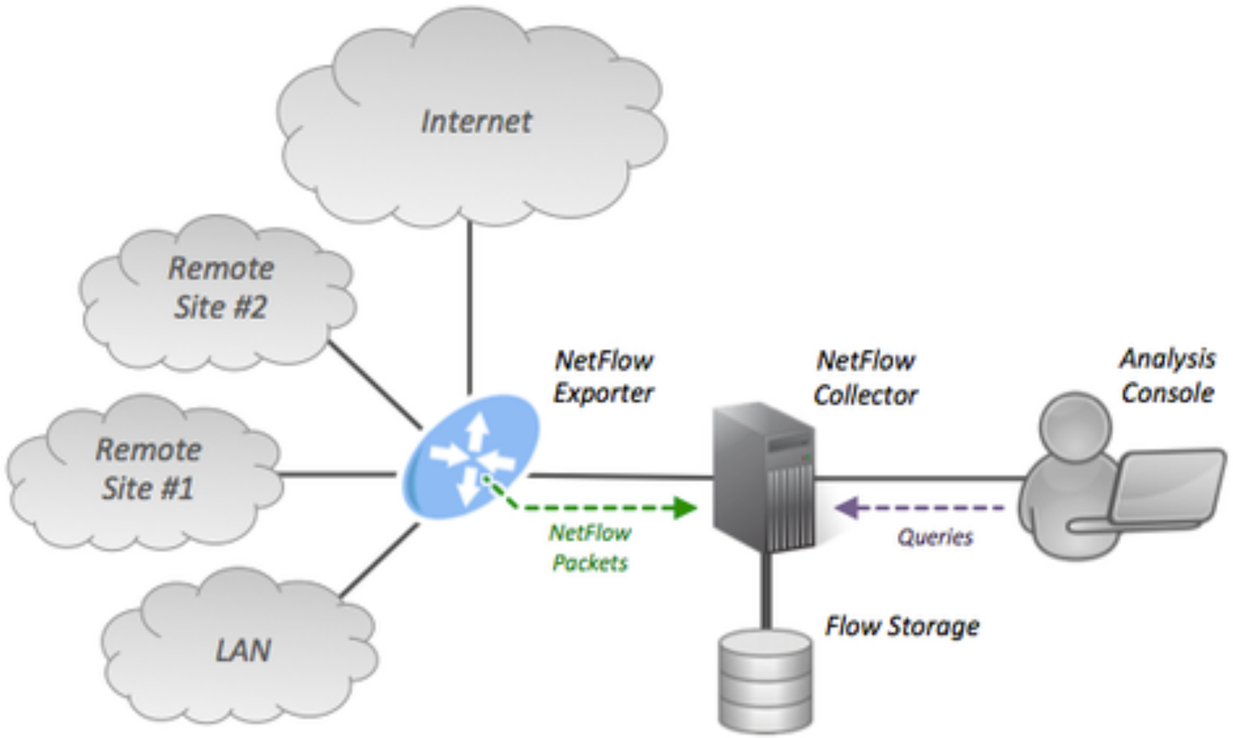
- Netflow is a Cisco feature designed to collect traffic data based on complete exchanges between hosts
- Tools like SNMP provide access to raw data and leave it to the monitoring station to try to figure out what that data means
- When a single action to be monitored occurs in multiple steps or stages over time, it becomes highly problematic to see many of them in a useful way
- With netflow, each data exchange is viewed as an atomic data element and reported as such

Netflow Data Handling

- Agent programs, either embedded or add-on, monitor network interfaces and summarize traffic as flows
- Agents report these to a collector, known as exporting flows



Netflow Data Handling



- Collectors can store the flow data for retrieval by analysis software
- Analysis software provides visualization of the data and can analyze it to create reports, logs, and alerts
- A hierarchy of agents, collectors and analysis devices can be created for large networks - a simple network might use a single host and program to perform all 3 functions

Netflow Concerns

- Netflow records are constructed in one of several versions, the collector and exporter must support compatible versions - v1, v5, v7, v8, v9 are all possible
- Netflows are typically exported using UDP and are therefore subject to loss, they are not tracked or retransmitted
- Netflow protocol has been superseded by IPFIX, based on netflow v9
- IPFIX could be viewed as being "v10" but it is not driven by Cisco; it is intended to be a vendor-agnostic standard for flow data management and provides for much more flexibility in what is captured and what it means for vendor-specific components of the flow data

Netflow Concerns

- Many vendors have equivalent functionality with similar names such as sflow, jflow, cflow, netstream, conntrack, etc.
- High-end routers and switches often use sampled flows which produces extrapolated data in return for reduced load on the device
- Packet capture appliances or hosts running probe software on tapped or spanned ports may be used to capture packets for flow data creation - may not have the same view of the flows as the source or destination devices in return for performance and storage wins

Netflow Data Generation

- Most enterprise routers and switches have built-in flow data generation capability (softflowd package adds it to pfsense)
- nfprobe, pmacct, nprobe and many others can be used as agents on various types of hosts
- ntopng is a good example of an analysis software package that includes the netflow data generation, collection and analysis in a single application - it can also export flows to a collector

NtopNG

- ntop has been around for quite some time as a way of viewing network activity similar in concept to the UNIX top program
- ntop is web-based and network-oriented
- ntopng is a successor to ntop and adds flow visualization among other things
- ntopng is available as a package for many Linux distributions, or as a download from ntopng.org

Installation

- ntopng in package form can be installed with package tools like apt, version may not be current and will be community version
- non-free pro version has improved graphing, additional data views
- nbox complete system management tool is derived from ntop project
- ntopng runs its own web service on port 3000 by default
- /etc/default/ntopng is the file where you add any command line options or environment variables to modify the default behaviour of ntopng
  e.g. INTERFACES, HTTP_PORT, ADD_ARGS="-i tcp://a.b.c.d:5556"
- ntopng is enabled and disabled using systemctl or service commands

Flow Exporting With pfSense

- pfSense, like most managed equipment can add capabilities dynamically
- For pfSense it is done by adding packages, such as ntopng
- softflowd is a netflow gathering and exporting package
- It is installed under System->Packages and configured under Services->softflowd once installed
- The typical port is 2055/udp for the listener for netflow v1, v5, and v9

CLI flow monitoring

- Netflow is not intended to be used from a command line
- Other tools can monitor traffic flows and give quick and dirty views into current activity
- iftop has a top-style interface
- nethogs is intended to highlight heavy network-using programs/users

Netflow Lab

- netflow setup on pfsense
- netflow setup on webhost