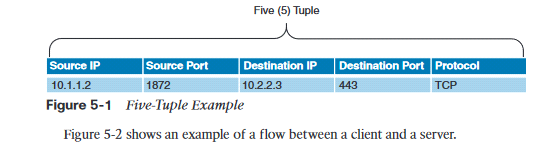
Technologies that can be used to obtain and maintain complete network visibility: **NetFlow, IPFIX, Cisco Stealthwatch, IDS/IPS, Cisco Advanced Malware Protection (AMP) for endpoints and Networks**

**NetFlow**

* It allows administrator to performs the tasks:
* See what is actually happening across the entire network
* Identify DoS attacks
* quickly identify compromised endpoints and network infrastructure devices, monitor network usage of employees, contractors, or partners
* Detect firewall misconfigurations and inappropriate access to corporate resources
* NetFlow supports both IPV4 and IPV6
* We can use NetFlow to detect attack before, during and after they have already taken place

**Flow:** unidirectional series of packets between a given source and destination.

Five-tuple is used to identify the flow in the NetFlow database of flows kept on the device



Cisco next-generation NetFlow can track information such as : source and destination MAC addresses, source and destination ipv4/ipv6 addresses, source and destination ports, TOS, DSCP, routing information (next-hop, AS number, prefix mask etc) etc.

NetFlow database is called **NetFlow cache**

We have three caches:

**Normal cache**: this is the default cache type in many infrastructure devices enabled with NetFlow and Flexible NetFlow. The entries in the flow cache are removed based on the configured timeout active seconds and timeout inactive seconds settings.

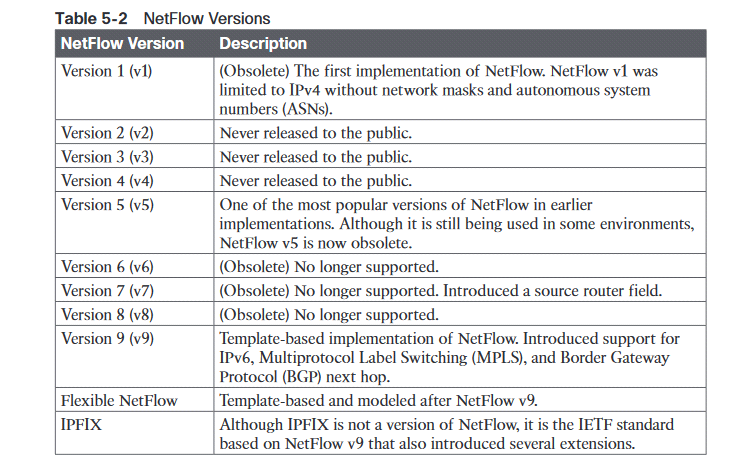
**Immediate cache**: flow accounts for a single packet, used when only very small flows are expected

**Permanent cache**: used to track a set of flows without expiring the flows from the cache.

**NetFlow roles**: network security, traffic engineering, Network planning, Network troubleshooting

**NetFlow for Security and Visibility**

* The first step to successfully identify security threats is achieving complete network visibility.
* We cannot protect against or mitigate what we cannot view/detect
* We can use NetFlow for Anomaly Detection and DDoS Attack Mitigation
* NetFlow provides information about all network activity that can be very useful for incident response and network forensics
* You can use NetFlow in combination with DNS records to help you detect suspicious and malicious traffic
* You can deploy NetFlow in: router, switch, cisco ASA, cisco FTD

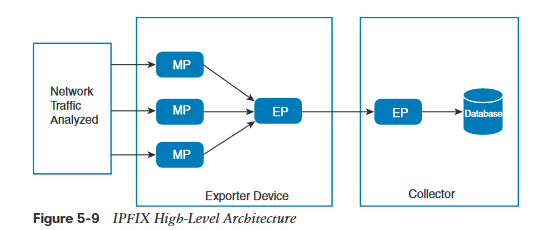


**IP Flow Information Export (IPFIX)**

* Network flow standard led by Internet Engineering Task Force (IETF)
* IPFIX is created for common, universal, standard of export the flow information from routers, switches, firewalls and other infrastructure devices
* It defined how flow should be formatted and transferred from an exporter to a collector

**IPFIX Architecture**

Metering process (MP), EP, CP



**IPFIX Templates**: describes the structure of flow data records within a data set.

**SCTP: Stream Control Transmission Protocol** provides reliable transport with a mechanism to skip packet retransmissions. SCTP ensures that IPFIX templates are sent reliably by improving end-to-end delay.

**Cisco Application Visibility AVC** solution is a collection of services available in several cisco network infrastructure devices to provide application-level classification, monitoring, and traffic control. AVC is supported by cisco ISR, Cisco ASR,1000 series, WLC.

**AVC capabilities**: application recognition, metrics collection and exporting, management and reporting systems, network traffic control.

**Application recognition:**

Cisco AVC use existing Cisco Network Based Application Recognition Version 2 (NBAR 2) to provide deep packet inspection (DPI) technology to identify a wide variety of applications within the network traffic flow using layer3 to layer 7 data

**Metrics Collection and Exporting:**

Cisco AVC includes an embedded monitoring agent that is combined with Netflow to provide a wide variety of network metrics data

Type of metrics: TCP performance metrics such as bandwidth usage, response time, and latency

VoIP performance metrics such as packet loss and jitter

**NetFlow Deployment Scenarios**

User access layer, wireless LAN, Internet Edge, Data center, Site to site VPN

**Cisco Stealthwatch**

It solution that allows network administrators and cybersecurity professionals to analyze network telemetry in a timely manner to defend against advanced cyber threats (like network reconnaissance, malware proliferation across the network, data infiltration.

It aggregates and normalizes considerable amounts of NetFlow data to apply analytics to detect malicious and suspicious activity.

Primary Components of the Cisco Stealthwatch solution

* **FlowCollector**: physical or virtual appliance that collects NetFlow data from infrastructure devices
* **Stealthwatch** Management Console (SMC): main management application that provides detailed dashboards and the ability to correlate network flow and event
* **Flow licenses**: define the volume of flows that may be collected

Optional components

* **FlowSensor:** physical or virtual appliance that can generate NetFlow data when legacy Cisco network infrastructure components are not capable of producing line-rate,unsampled NetFlow data
* **FlowReplicato**r: physical or virtual appliance used to forward NetFlow data as a single data stream to other devices.

**Stealthwatch Cloud**

* Software as a service SaaS cloud solution
* It is used to monitor many different public cloud environments, such as Amazon’s AWS, Google Cloud Platform, and Microsoft Azure.
* Amazon AWS: Netflow = VPC Flow logs
* Microsoft Azure : traffic are collected in network Security Group (NSG) flow logs

On-premises monitoring with cisco stealwatch cloud

* We can monitor on-premise networks in your organizations using Cisco Stealthwatch cloud
* To do this we need to deploy at least one cisco stealthwatch cloud sensor appliance (virtual/physical)
* Two modes we can used to deploy cisco stealthwatch cloud sensor appliance: processing network metadata from a SPAN or a network TAP and processing metadata out of Netflow or ipfix flow records

Threat hunting: concept of proactively or actively searching for advanced threats that may evade your security products and capabilities

Methodologies for threat hunting with cisco stealthwatch:

* Threat intelligence-driven hunting using threat intelligence feeds and reports, malware analysis, and other vulnerability assessment methods
* Machine learning-based or analytics-driven methods
* Situational or “Crown Jewel” analysis, where you start with a critical system or  
  network in mind and base your “hypothesis” of what an attacker can do to those  
  resources and what indicators should be collected

Cisco ETA: Cisco Encrypted Traffic Analytics: can identify malicious communications in encrypted traffic through passive monitoring, the extraction of relevant data element, and a combination of behavioral modeling and machine learning

Cisco ETA components: NetFlow, Cisco Stealthwatch, Cisco Cognitive Threat Analytics

Cisco CTA is a cloud-based cisco solution that uses machine learning and statistical modeling of networks

Cisco CTA creates a baseline of traffic in your network and identifies anomalies

Cisco CTA can also analyze user and device behavior as well as web traffic to uncover malicious command-and-control communications and data exfiltration

We can combine Cisco CTA, Cisco ETA and Cisco Stealthwatch to provide a very comprehensive visibility solution within your organization

NetFlow collection considerations and best pratices

Several best pratices and recommendations

* Minimizing NetFlow overhead: NetFlow collection should be done as close to the NetFlow generator as possible (Netflow can be enabled close to servers or assets you want to monitor
* Asymmetric routing considerations: all devices in the asymmetric route should send NetFlow records to the same collector, not different collectors
* Distributed deployment: FlowCollectors are deployed at multiple sites and are usually placed close to the source producing the highest number of NetFlow records. Advantage: limiting the overhead introduced by netflow
* Centralized deployment: all netflow collectors are placed in a single location; Advantage: benefit of a single collection location and possibly a single IP address globally for NetFlow collection
* Bandwidth consideration

Introduction to Network Segmentation

process of logically grouping network assets, resources and applications.

Segmentation provides the flexibility to implement a variety of services, authentication requirements, and security controls.

Type of networks segments:

enclave network: segment of internal network that requires a higher degree of protection. internal accessibility is further restricted through the use of firewalls, VPNs, VLANs and network access control (NAC) devices

Trusted network (wired or wireless): internal network that is accessible to authorized users. external accessibility is restricted through the use of firewalls, VPN, and IDS/IPS devices:

Semi-trusted network, perimeter network or DMZ: hosts such as web servers and email gateways are generally located in DMZ. Internal and external is restricted through the use of firewalls, VPNs, and IDS/IPS devices

Guest network: A network that is designed for use by visitors to connect to the internet

Untrusted network: network outside your security controls. The internet is an untrusted network.