JASON DION

TRAINING THE CYBER SECURITY WORKFORCE

Network Event Monitoring

CYBER INCIDENT RESPONSE

Network Event Monitoring

- Network event analysis is a common task for cybersecurity analysts
- Gather, correlate, and analyze data from different systems/sensors on network
- Used to detect or prevent incidents

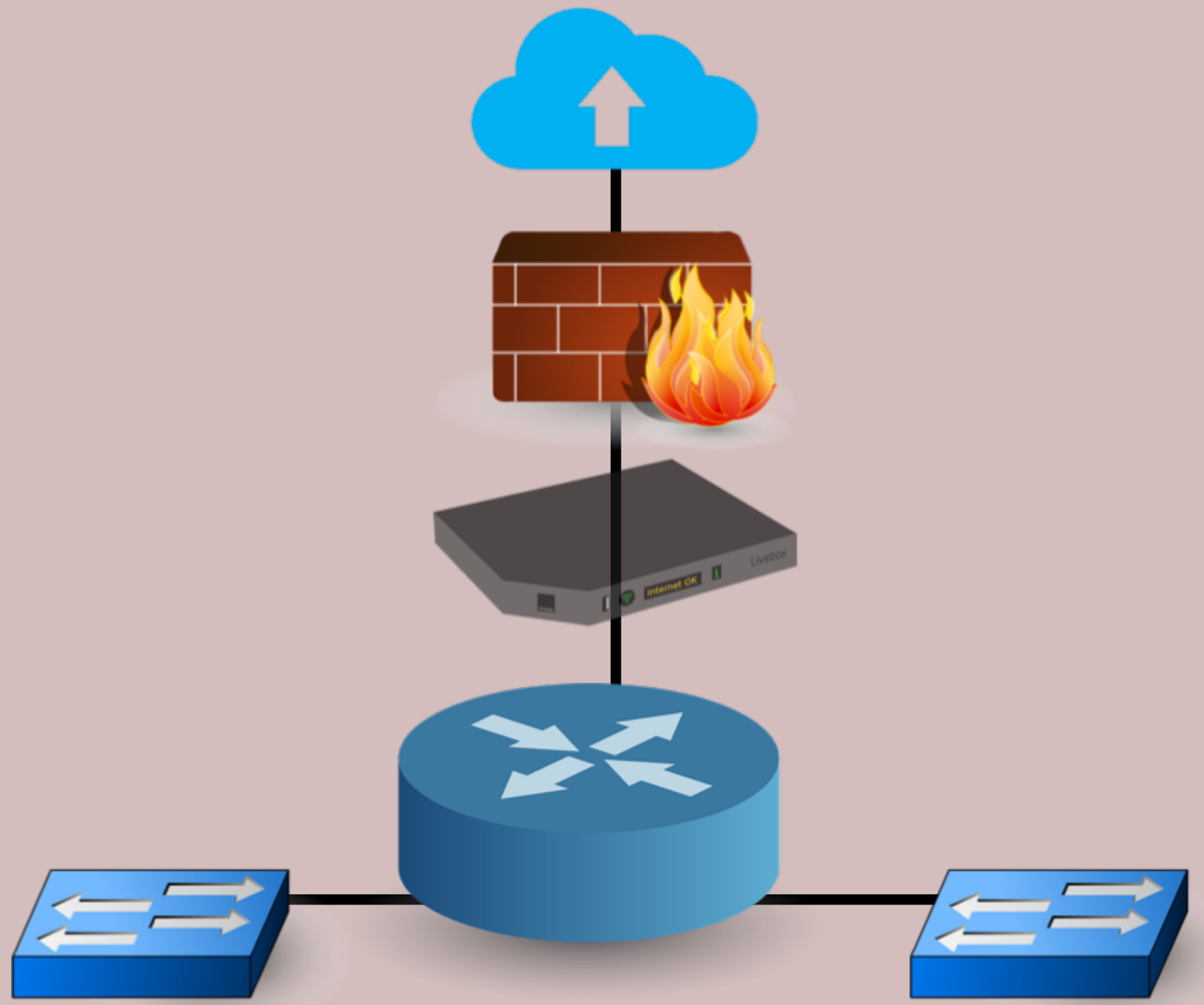
Router-based Monitoring

- Provides data flow on the network and information on the status of the device
- Relies on capturing the data about the traffic passing through a router
- Called *network flows*

Network Flows

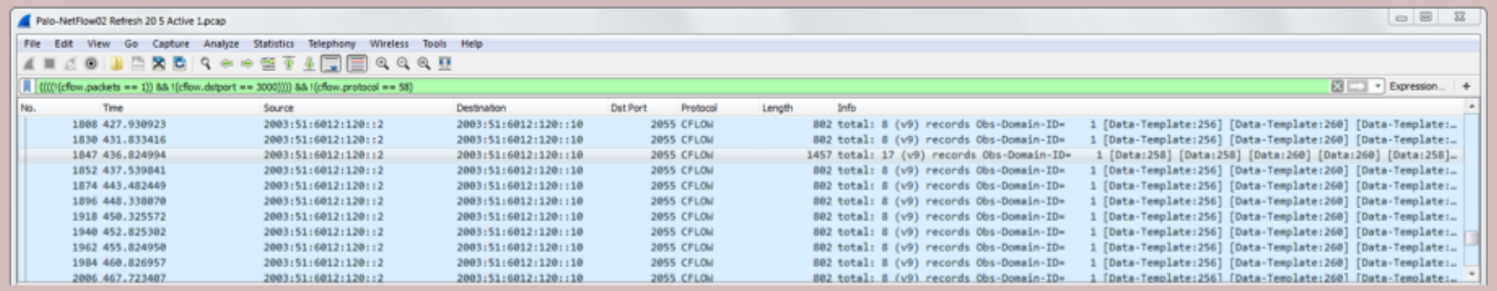
- Netflow, sFlow, J-Flow, …
  - All are standards for monitoring traffic flows
  - Count information about the traffic at the interface
  - Samples traffic (1:100, 1:1000, etc)
- RMON
  - Operates at layers 1, 2, 3, 4 of the OSI model
  - Operates as client/server model with probes
  - Provides statistics, history, alarms, and events to a Management Information Base (MIB)
- SNMP (Simple Network Management)
  - Collects information about routers/switches
  - Information is about the devices themselves, not the traffic crossing those devices

Network Flows



JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

Example Network Flows



No.	Time	Source	Destination
1808	427.930923	2003:51:6012:120::2	2003:51:6012:120::10
1830	431.833416	2003:51:6012:120::2	2003:51:6012:120::10

Dst Port	Protocol	Length
2055	CFLOW	802
2055	CFLOW	802

Info
total: 8 (v9) records Obs-Domain-ID= 1 [Data-Template:256] [Data-Template:260] [Data-Template:…
total: 8 (v9) records Obs-Domain-ID= 1 [Data-Template:256] [Data-Template:260] [Data-Template:…

JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

Example Network Flows

NetFlow Collection Status | Interface Status

Filter Domain : NinjaNet Time : Today
Exporter : lchqgw01 (10.201.0.1)

Interface Status - 16 records

Exporter	Interface	Direction	Interface ...	Current Utilization	Current Traffic (...	Maximum Utilization	Maximum Traffic (...
lchqgw01 (10.201.0.1)	Vl1	Inbound	1G	10.87%	108.74M	10.9%	108.96M
lchqgw01 (10.201.0.1)	Vl240	Outbound	10M	4.13%	413.43k	5.35%	535.14k
lchqgw01 (10.201.0.1)	Vl240	Inbound	10M	3.58%	358.25k	48.48%	4.85M
lchqgw01 (10.201.0.1)	Vl203	Inbound	1G	1.19%	11.92M	1.25%	12.46M
lchqgw01 (10.201.0.1)	Vl202	Outbound	1G	1.09%	10.89M	1.09%	10.89M
lchqgw01 (10.201.0.1)	Vl202	Inbound	1G	0.6%	6.02M	0.72%	7.17M
lchqgw01 (10.201.0.1)	Vl1	Outbound	1G	0.4%	4M	0.82%	8.17M
lchqgw01 (10.201.0.1)	ifIndex-0	Outbound	1G	0.29%	2.94M	0.31%	3.08M
lchqgw01 (10.201.0.1)	Vl203	Outbound	1G	0.27%	2.69M	0.27%	2.69M
lchqgw01 (10.201.0.1)	Vl232	Outbound	1G	0.14%	1.42M	0.14%	1.42M
lchqgw01 (10.201.0.1)	Vl210	Outbound	1G	0.08%	829.14k	0.11%	1.06M
lchqgw01 (10.201.0.1)	Vl232	Inbound	1G	0.05%	457.91k	0.06%	554.58k
lchqgw01 (10.201.0.1)	Vl210	Inbound	1G	<0.01%	56.75k	0.01%	100.87k

JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

SNMP v3

- Simple Network Management Protocol
- Adds encryptions, authentication, and user capabilities to SNMP traffic
- SNMP v1 and SNMP v2 are considered obsolete and a security risk

Active Monitoring

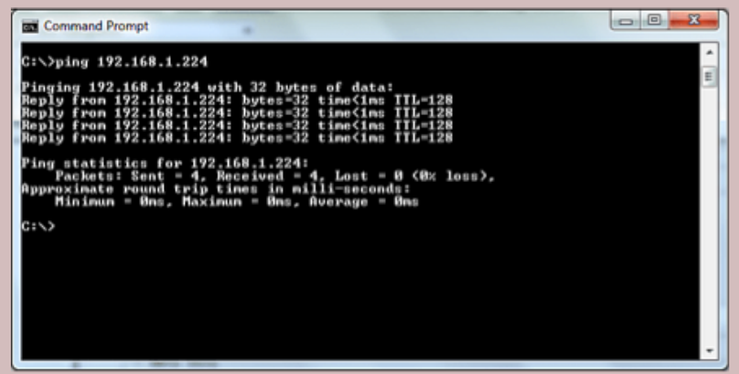
- Request is sent to a remote system and data is collected from the end point

- Data contains information about:
  - Availability
  - Routes
  - Packet delays
  - Packet loss
  - Bandwidth

Active Monitoring (Examples)

JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

- Ping
  - Data acquired by using ICMP on remote system
  - Basic up and down information and latency only
- iPerf
  - Measures maximum bandwidth of a given network
  - Remote testing of a link
  - Useful to determine a baseline of the network



Passive Monitoring

- Uses a network tap to copy all traffic between two devices
- Useful for after-the-fact analysis
- Detailed information about:
  - Rate of traffic
  - Protocols used
  - Content