Network monitoring and Security analysis

Dr. Mohammed Anbar

National Advanced IPv6 Centre of Excellence (NAv6)
UNIVERSITI SAINS MALAYSIA

ASIACONNECT
DISTRIBUTED AND CLOUD-BASED NETWORK DEFENSE SYSTEM FOR NRENs

Asi@Connect

TEIN COOPERATION CENTER

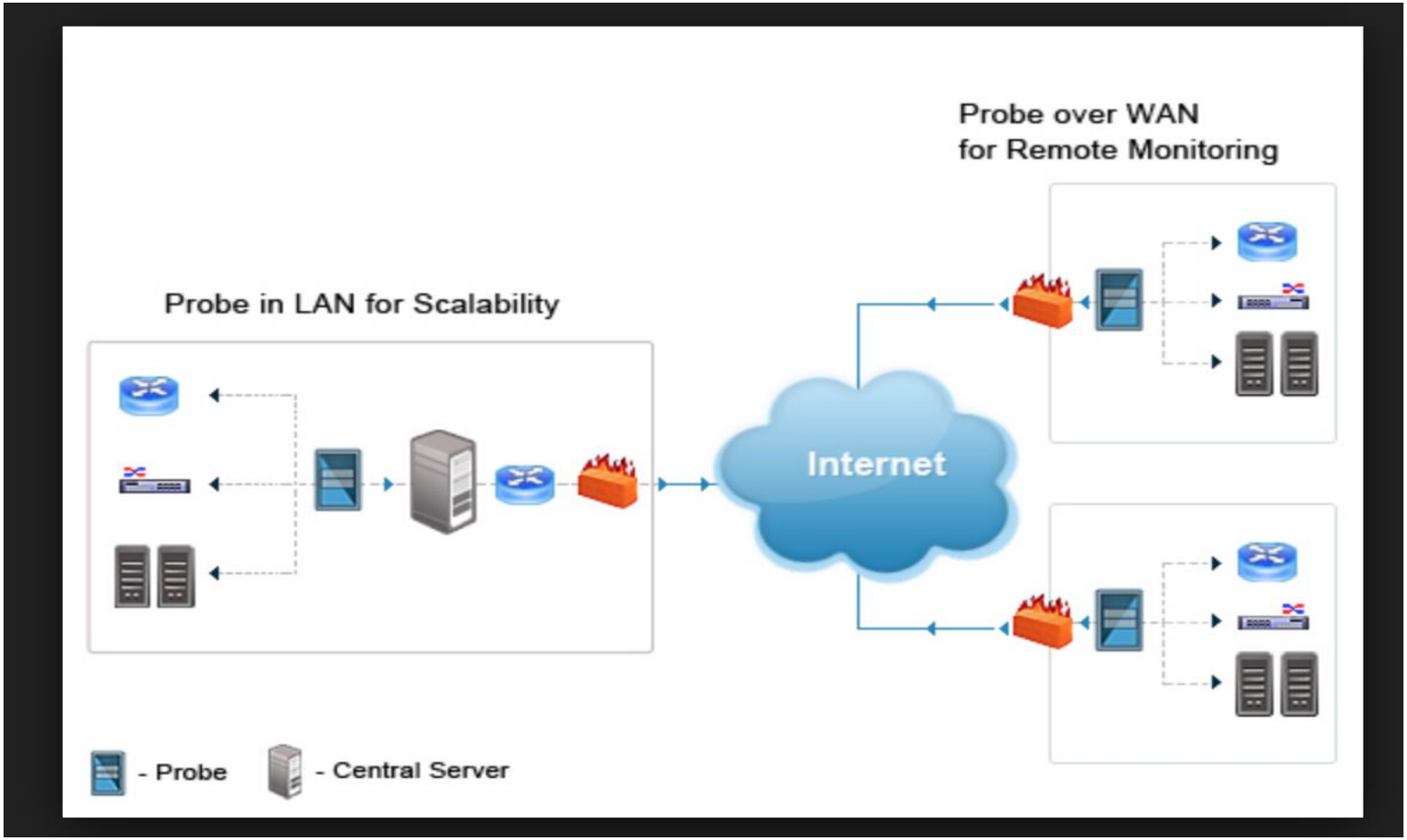
What is network monitoring?

The term network monitoring describes the use of a system that constantly monitors a computer network for slow or failing components and that notifies the network administrator in case of outages via email, pager or other alarms. It is a subset of the functions involved in network management.

Who? What? Where? How? When?

- **Who is accessing your network?**
  - students, academics, staff, visitors or others
- **What are they accessing your network for?**
  - academic study, social use, business use, illegal use
- **Where are they accessing your network from?**
  - internal, external
- **How are they accessing your network?**
  - remote user, local Ethernet, WAN, dial-up, Wi-Fi, VPN
- **When did they access your network?**
  - today, yesterday, last week, last month…

Types of network monitoring tools



Network Monitoring Techniques

- Active Measurement
- Passive Measurement

Network Traffic monitoring Approaches

- The passive approach uses devices to watch the traffic as it passes by.
- The passive monitoring devices are polled periodically and information is collected to assess network performance and status.
- The passive approach does not increase the traffic on the network for the measurements. It also measures real traffic.
- The passive approach is extremely valuable in network trouble-shooting, however they are limited in their ability emulate error scenarios or isolating the exact fault location.
- Since the passive approach may require viewing all packets on the network, there can be privacy or security issues about how to access/protect the data gathered.

Network Traffic monitoring Approaches

- The active approach relies on the capability to inject test packets into the network or send packets to servers and applications, following them and measuring service obtained from the network.

- As such it does create extra traffic, and the traffic or its parameters are artificial. The volume and other parameters of the introduced traffic is fully adjustable and small traffic volumes are enough to obtain meaningful measurements

- On the other hand, the active approach provides explicit control on the generation of packets for measurement scenarios. This includes control on the nature of traffic generation, the sampling techniques, the timing, frequency, scheduling, packet sizes and types (to emulate various applications), statistical quality, the path and

A few Open Source solutions…

Performance

- Cricket
- IFPFM
- flowc
- mrtg
- netflow
- NfSen
- ntop
- pmacct
- rrdtool
- SmokePing

Change Mgmt

- Mercurial
- Rancid (routers)
- RCS
- Subversion

Security/NIDS

- Nessus
- OSSEC
- Prelude
- Samhain
- SNORT
- Untangle

Net Management

- Big Brother
- Big Sister
- Cacti
- Hyperic
- Munin
- Nagios*
- Netdisco
- Netdot
- OpenNMS
- Sysmon
- Zabbix

what is cloud monitoring ?

- Cloud monitoring is primarily part of cloud security and management processes, and it is generally implemented through automated monitoring software that provides central access and control over cloud infrastructure. Cloud administrators can review the operational status and health of any cloud-based device or component.

- In addition to monitoring and ensuring cloud infrastructure/solution/service availability, cloud monitoring data also helps in evaluating the performance of the entire infrastructure.

- Cloud computing metrics such as server uptime and response rate report can help in evaluating customer/user experience.

Cloud Computing Cloud: the need for monitoring

- Monitoring of Cloud is a task of paramount importance for both Providers and Consumers.

- The continuous monitoring of the Cloud and of its SLAs supplies both the Providers and the Consumers with information such as the workload generated by the latter and the performance and QoS offered through the Cloud.

- Allowing to implement mechanisms to prevent or recover violations

Cloud Computing Cloud: the need for monitoring

- Capacity and resource planning
- Capacity and resource management
- Data center management
- SLA management
- Billing
- Troubleshooting
- Performance management
- Security management

Cloud Monitoring: basic concepts

- **Layers** (Facility, Network, Hardware, Operating System (OS), Middleware, Application and user).
- **Abstraction levels** (low level and high level).
- **Tests and metrics** (Computation-based and network-based)

Cloud Monitoring: basic concepts Layer

- **Facility**: This layer considers the physical infrastructure comprising the data centers that host the computing and networking equipment.
- **Network**: This layer considers the network links and paths both in the Cloud and between the Cloud and the user.
- **Hardware**: This layer considers the physical components of the computing and networking equipment.
- **Operating System (OS):** This layer considers the software components forming the operating system of both the host and user

Cloud Monitoring: basic concepts Layer (cont.)

- **Middleware**: This layer considers the software layer between the OS and the user application. It is typically present only in the Cloud systems offering SaaS and PaaS service models.
- **Application**: This considers the application run by the user of the Cloud system.
- **User**: This is the final user of the Cloud system and the applications that run outside the Cloud (e.g. a web browser running on a host at the user's premise).

Cloud Monitoring: basic concepts Abstraction levels

- In the case of SaaS, high-level monitoring information is generally of more interest for the Consumer than for the Provider (being closely related to the QoS experienced by the former).

- On the other hand, low-level monitoring is related to information collected by the Provider and usually not exposed to the Consumer, and it is more concerned with the status of the physical infrastructure of the whole Cloud (e.g. servers and storage areas, etc.).

- In the context of IaaS, both levels are of interest for both Consumers and Providers.

Cloud Monitoring: basic concepts Tests and metrics

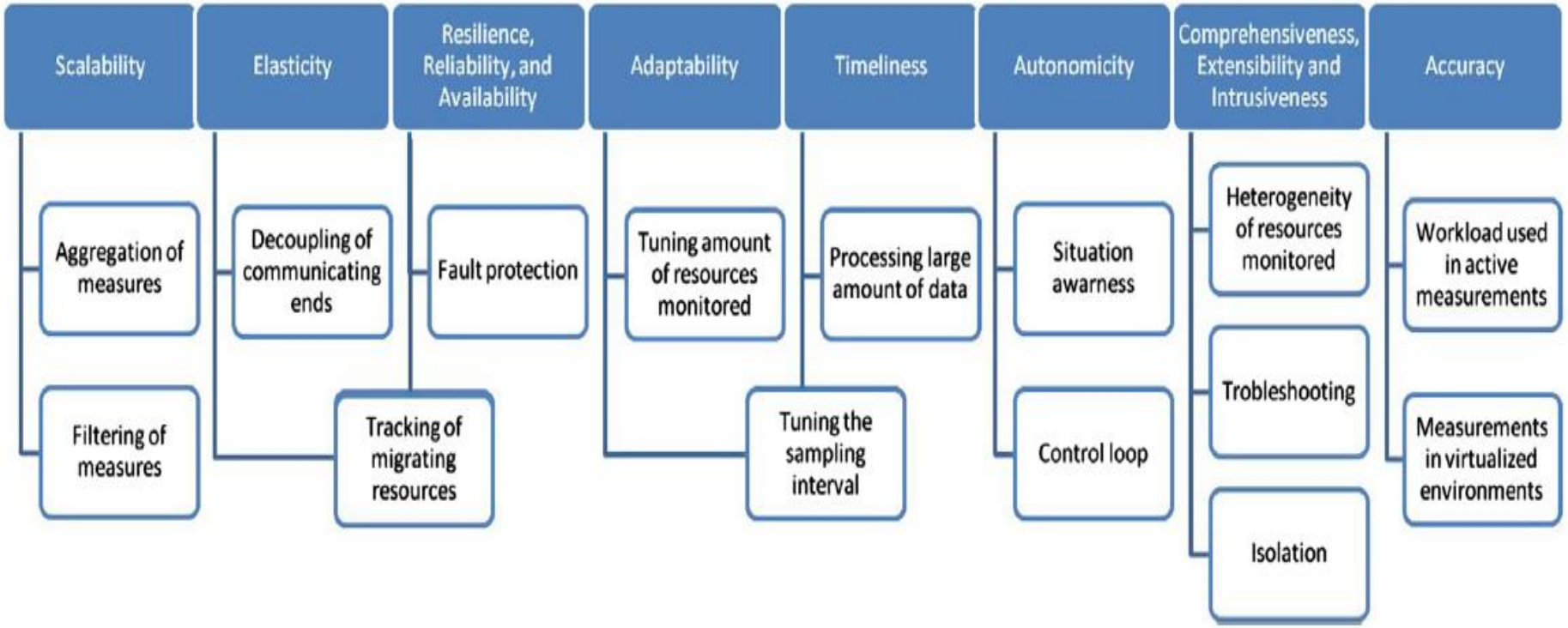
- **Computation-based**

  Tests are related to the following metrics: server throughput, defined as the number of requests (e.g. web page retrieval) per second; CPU Speed; CPU time per execution.

- **Network-based**

  Tests are related to the monitoring of network-layer metrics. This set includes round-trip time (RTT), jitter, throughput, packet/data loss, available bandwidth, capacity, traffic volume, etc

Cloud monitoring: Properties and related issues



Source: Aceto, G., Botta, A., De Donato, W., & Pescapè, A. (2013). Cloud monitoring: A survey. *Computer Networks*, *57*(9), 2093-2115.

Options for Cloud monitoring

- CSP-provided network monitoring tools
- Traditional network monitoring tools
- Cloud-focused network performance monitoring

CSP-provided network monitoring tools

- By far the cheapest and fastest way to get network monitoring up in running in the cloud is to leverage tools provided by your cloud provider.

- The primary drawback to using CSP-provided tools is that they only work within a single cloud.

Traditional network monitoring tools

- Most enterprise organizations opt to deploy traditional network monitoring tools such as ping, SNMP polling, and NetFlow within a public cloud network -- when possible.

- The benefit here is that it allows network administrator to utilize the same tools within their cloud instances as they use to monitor network components on the private corporate LAN and **WAN**.

- For IaaS clouds, it's easily accomplished, but for PaaS and SaaS deployments, many of the traditional network management tools won't work.

Cloud-focused network performance monitoring

- Many IT departments require even more visibility into the network than has traditionally been provided across the enterprise LAN.
- Because a certain level of trust has been handed over to CSPs, IT teams need added visibility to keep closer tabs on the network performance inside and between clouds.
- Cloud-focused network performance monitoring platforms from companies such as Cisco, ExtraHop and ThousandEyes.
- Many of these platforms include network probes, cloud agents, and in-depth routing and policy change notifications. These tools can be used to provide granular detail to the health of the network, down to the end-user perspective.

Cloud monitoring platforms and services

Commercial platforms	Open source platforms	Services
CloudWatch	Nagios	CloudSleuth
AzureWatch	OpenNebula	CloudHarmony
CloudKick	CloudStack ZenPack Cloudstone	Cloudstone
CloudStatus	Nimsoft	CloudClimate
Nimsoft	PCMONS	Cloud CMP
Monitis	PCMONS	CloudClimate
LogicMonitor	DARGOS	Up.time

Cloud security

- Cloud security is considered as one of the most significant obstacles to the spread of Cloud Computing, especially considering certain kinds of applications (e.g. business critical ones) and Consumers (e.g. governments).
- For managing the security in Cloud infrastructures and services, proper monitoring systems are needed.
- Moreover, for hosting critical services for public agencies, Clouds have to satisfy strict regulations and prove it. And this can be done through a monitoring system that enables auditing

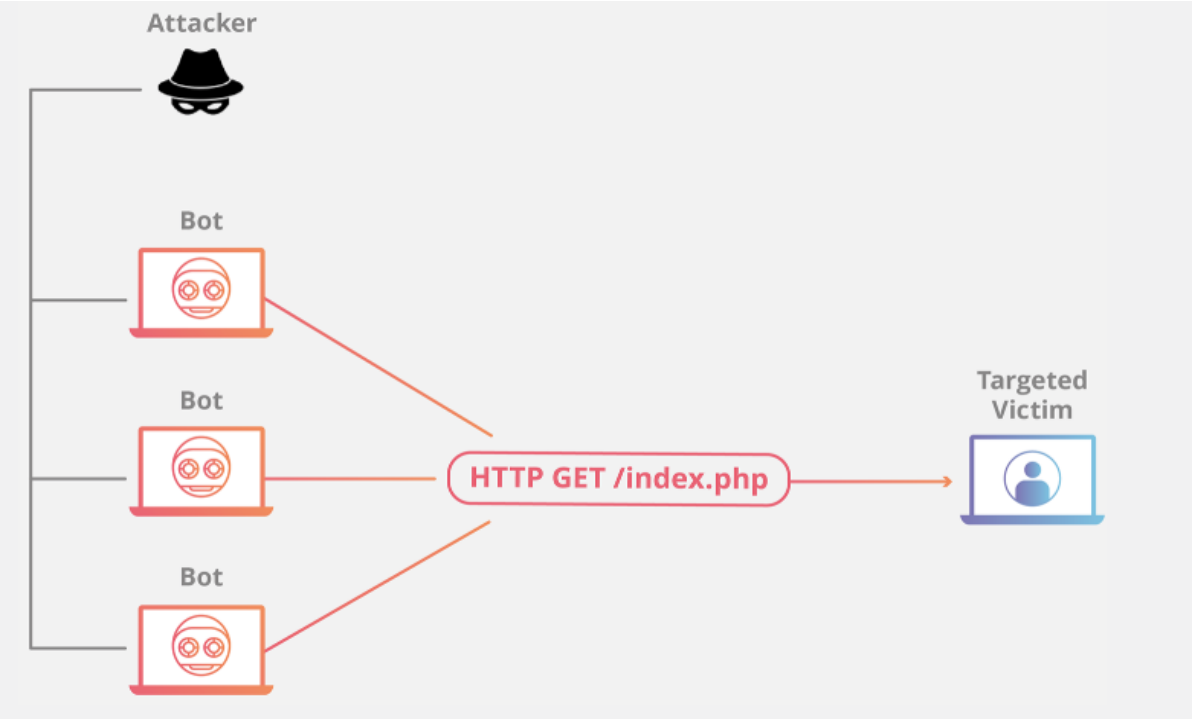
Distributed Denial of Service

- In network security, there are various types of attacks available which can affect the network resources and services. Distributed Denial of Service (DDoS) is foremost notable attacks.

- Main focus is to deny access to the legitimate user from accessing the network resources or restrict the availability of the network resources by exhausting bandwidth (Kumar et al., 2012).

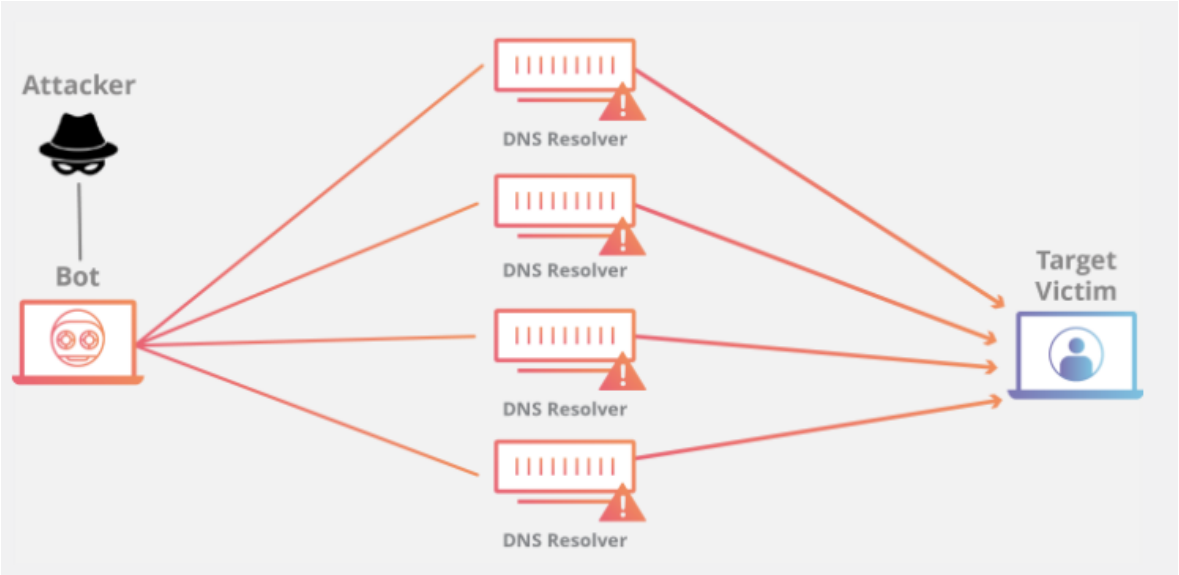
- A Denial of Service (DoS) attack is one in which a server or service is “overwhelmed” by traffic and consequently either disabled or made unavailable to its customers. Typically the effect on the target of a DoS attack is a loss of business, or in the less critical cases, just failure to get his/her message out.

DDoS Attack



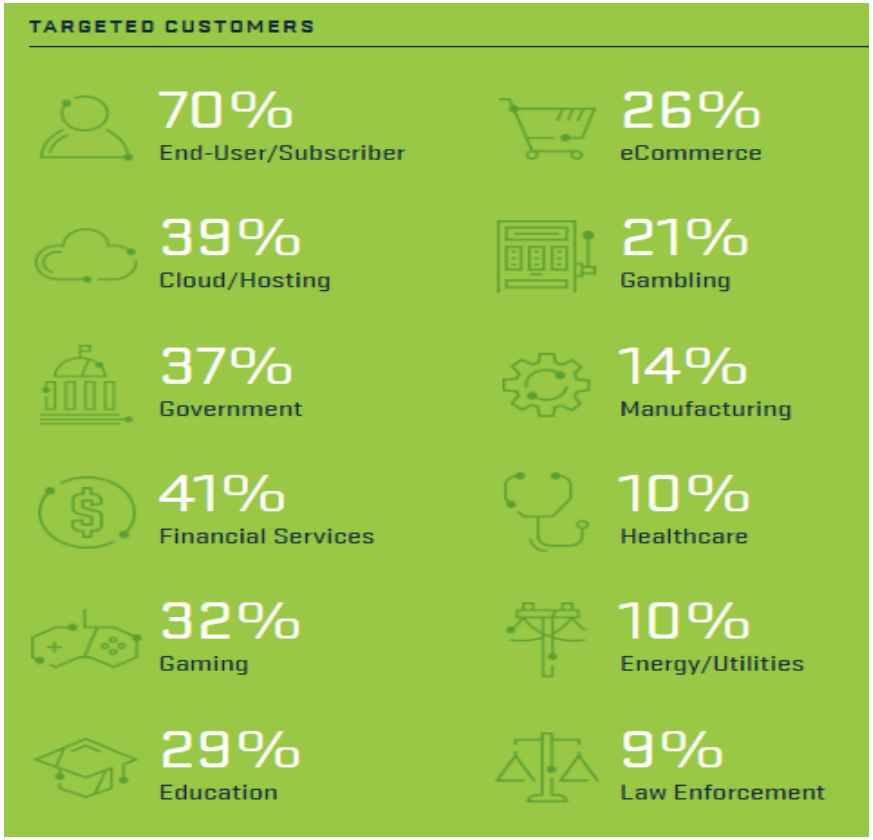
Source : cloudflare, 2018
https://www.cloudflare.com/

DDoS Attack-Amplification Attack



Source : cloudflare, 2018
https://www.cloudflare.com/

DDoS attacks statics



Source : Arbor, 2018
https://www.netscout.com/report/

Economical Denial of Sustainability (EDoS)

- To emphasize on the impact of DDoS, a new variant of DDoS attack known as Economical Denial of Sustainability (EDoS) was introduced.

- EDoS can be classified as packet flood that can extend the elasticity of metered-services provisioned via cloud infrastructure, EDoS attack can be formulated by remotely run bots to flood the targeted cloud service by fake requests at slow rate to hide themselves from the security devices.
- Therefore, the cloud service will pump up additional resources to satisfy the on-demand requests. Public cloud services offered on pay-as-use bases. In case of EDoS attack, client will be charged for these fake requests, making the service not viable to afford.

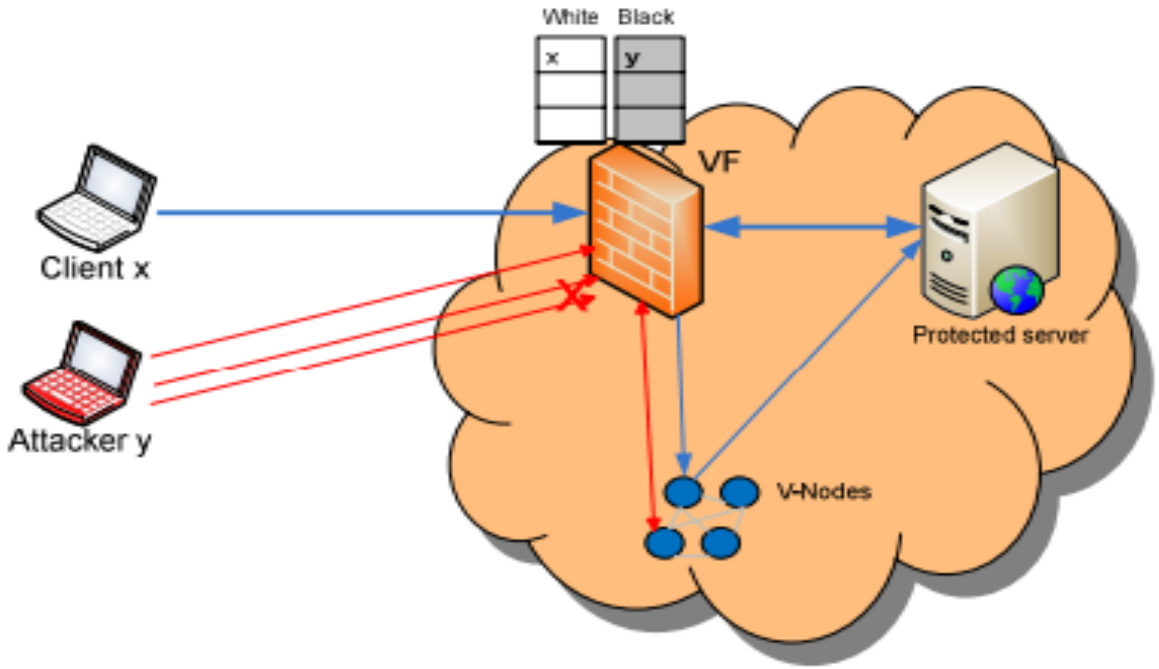
- As a result, the cloud provider will lose its customers and it will be more viable to run in-house data centre, cheaper than the cloud. Hence, the cloud service providers are affected negatively by EDoS attacks more than their customers.

EDoS Mitigation techniques
EDoS-Shield

- This mechanism has two main components, the cloud verifier node and virtual firewall.
- Firewall does the packet filtering based on the White list and Black list method. and the verifier cloud node updates the lists based on the results of the verification process
- verifier nodes which are represented by a pool of virtual machine nodes implemented based on the cloud infrastructure.
- A V-Node has the capabilities to verify legitimate requests at the application level using graphic Turing tests , such as CAPTCHA.
- If the application request gets verified successfully, then the source IP address of that request will be added to the whitelist and the request will be forwarded to the destined service in the cloud.

Source: M. H. Sqalli, F. Al-Haidari and K. Salah, "EDoS-Shield - A Two-Steps Mitigation Technique against EDoS Attacks in Cloud Computing," *2011 Fourth IEEE International Conference on Utility and Cloud Computing*, Victoria, NSW, 2011, pp. 49-56. doi: 10.1109/UCC.2011.17

EDoS-Shield (Cont.)



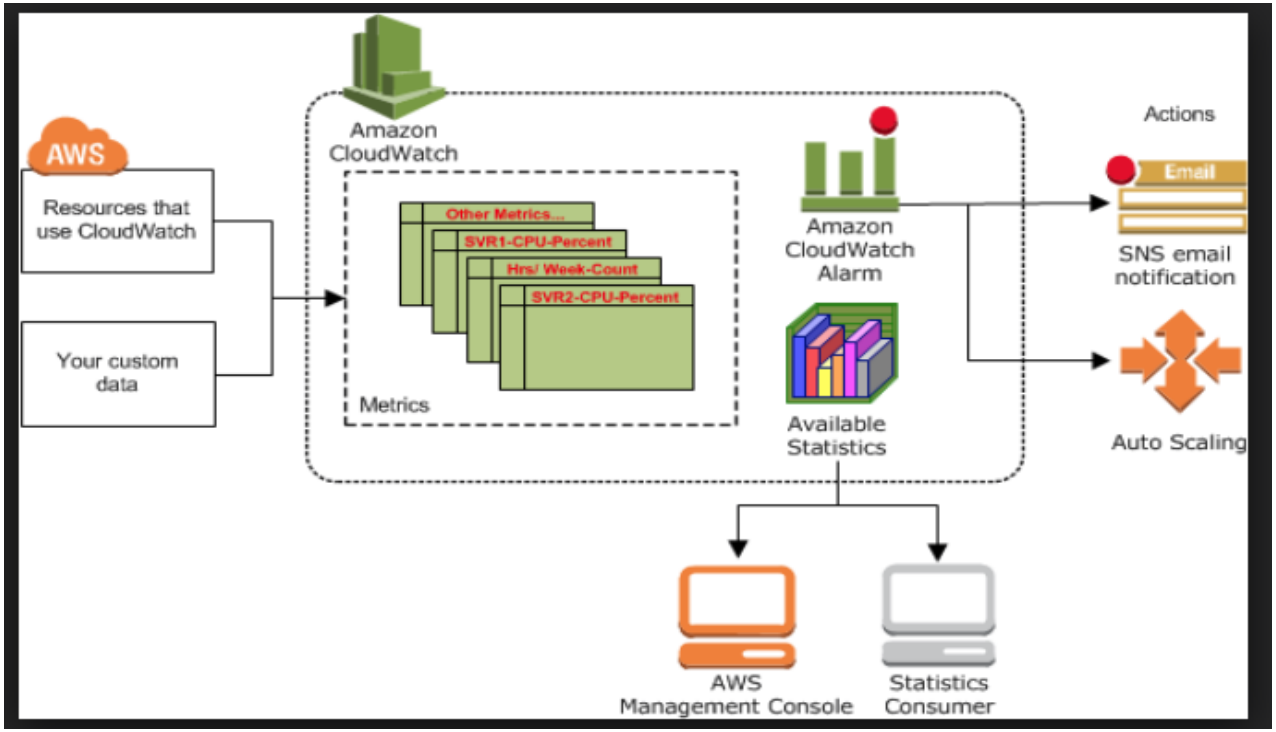
Source: M. H. Sqalli, F. Al-Haidari and K. Salah, "EDoS-Shield - A Two-Steps Mitigation Technique against EDoS Attacks in Cloud Computing," *2011 Fourth IEEE International Conference on Utility and Cloud Computing*, Victoria, NSW, 2011, pp. 49-56. doi: 10.1109/UCC.2011.17

EDoS Mitigation techniques CloudWatch

- CloudWatch is professional service from Amazon to reduce the impact of the EDoS attacks by providing monitoring service for cloud resources, which enable organisations to define upper limits to the elastic resource utilization of their cloud infrastructure.
- This is an inefficient solution against the EDoS as user can still be charged for over utilization in case of DDoS attempt
- Also it defeats the purpose of cloud computing as the elasticity touches the upper limit, the cloud service freezes and users service access will not be available.
- As this passive approach only provides the monitoring and alert service, final decision will be dependent on the client's administrator to look into the problem and take action accordingly.

CloudWatch (Cont.)

- In most of the cases, client responds only after the cloud commits the resources using auto scaling and customer has to pay for the time they use the resource.
- In case of volumetric DDoS attack, cloud expands itself to the max limit defined by the end user before admin get any attention on it.



Source: https://aws.amazon.com/cloudwatch

CSP-provided network monitoring tools (Cloudwatch)

(Demo)

Traditional network monitoring tools (Demo)

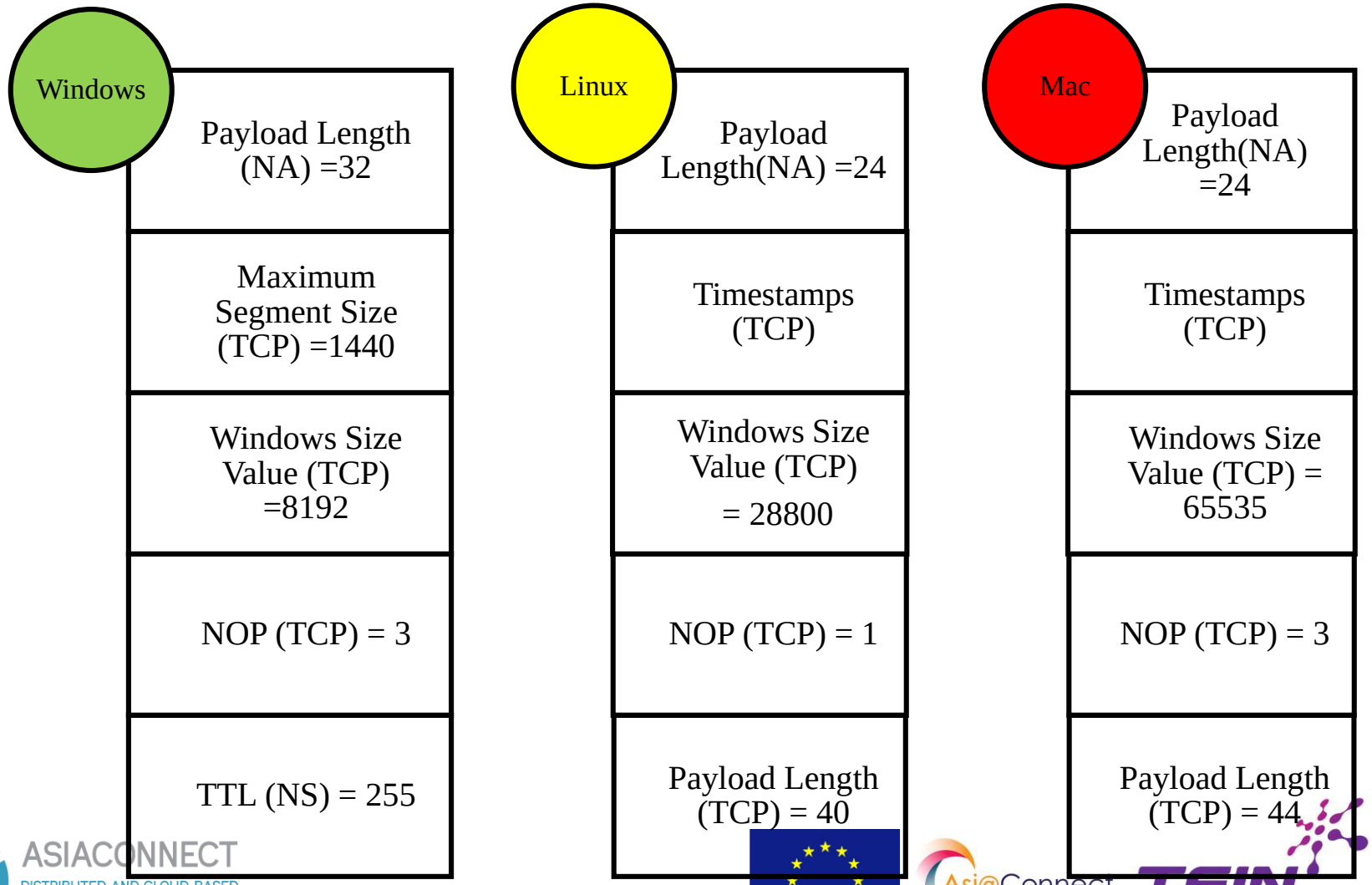
TCP port scanning

OS Fingerprinting (IPv4)

Operating System (OS)	IP Initial TTL	TCP window size
Linux (kernel 2.4 and 2.6)	64	5840
Google's customized Linux	64	5720
FreeBSD	64	65535
Windows XP	128	65535
Windows 7, Vista and Server 2008	128	8192
Cisco Router (IOS 12.4)	255	4128

OS Fingerprinting (IPv6)

FIRST LAYER DATABASE : OS FAMILY



OS Fingerprinting (IPv6)

SECOND LAYER DATABASE : OS TYPES

Windows

Windows 7

- Windows Scale (TCP)= 2(Multiply by 4)
- Windows Size Value (TCP) = 8192
- Payload Length (NA) (TCP) = 32
- TCP Option Bytes (TCP) = 12 Bytes
- No Timestamp

Windows 8.1/ Windows 10

- Windows Scale (TCP) = 8(Multiply by 256)
- Windows Size Value (TCP) = 8192
- Payload Length (NA) (TCP)= 32
- TCP Option Bytes (TCP) = 12 Bytes
- No Timestamp

Linux

Ubuntu 16.04

- Windows Scale (TCP) = 7(Multiply by 128)
- Windows Size Value (TCP) = 28800
- TTL (TCP) = 64
- TCP Option Bytes (TCP) = 20 Bytes
- Timestamps (TCP)

Android 6.0.1

- Windows Scale (TCP) = 7(Multiply by 128)
- Windows Size Value (TCP)=65535
- TTL (TCP) = 255
- TCP Option Bytes (TCP) = 20 Bytes
- Timestamps (TCP)

Mac

Mac OS 10.11

- Windows Scale (TCP) = 7(Multiply by 128)
- Windows Size Value (TCP) =65535
- End of List (TCP)
- TCP Option Bytes (TCP) = 24 Bytes
- Timestamps (TCP)

Links

- https://www.wireshark.org/
- https://nmap.org/
- https://console.aws.amazon.com/console/home

Thank you

Dr. Mohammed Anbar
anbar@usm.my