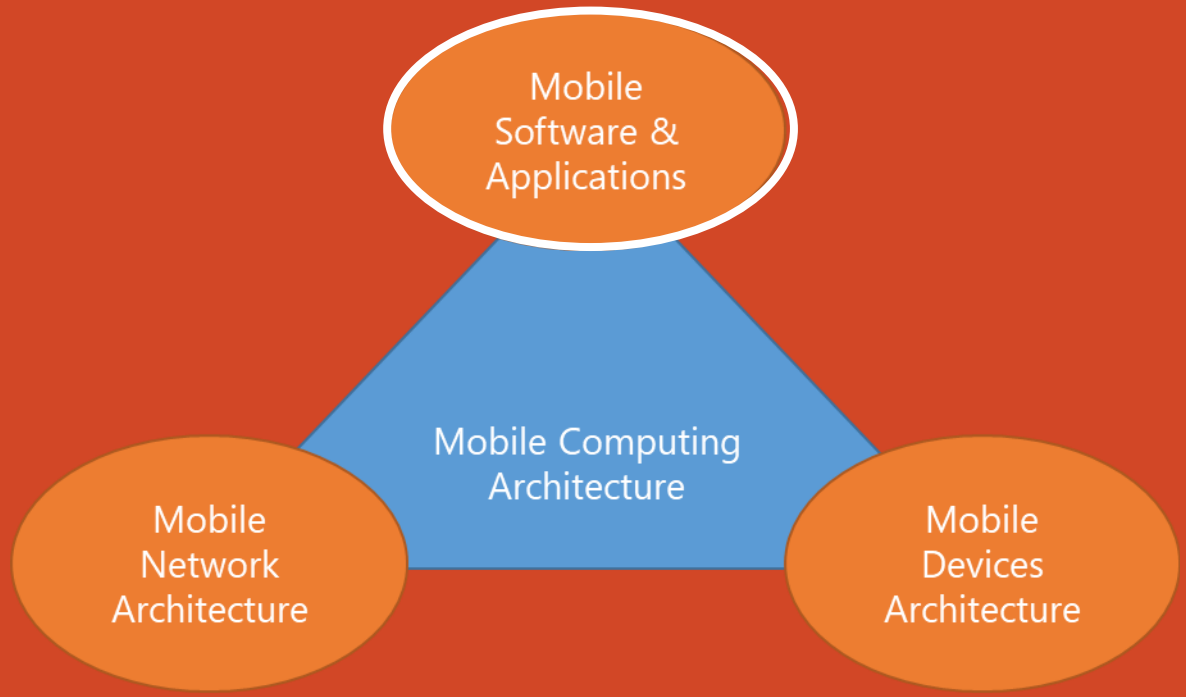
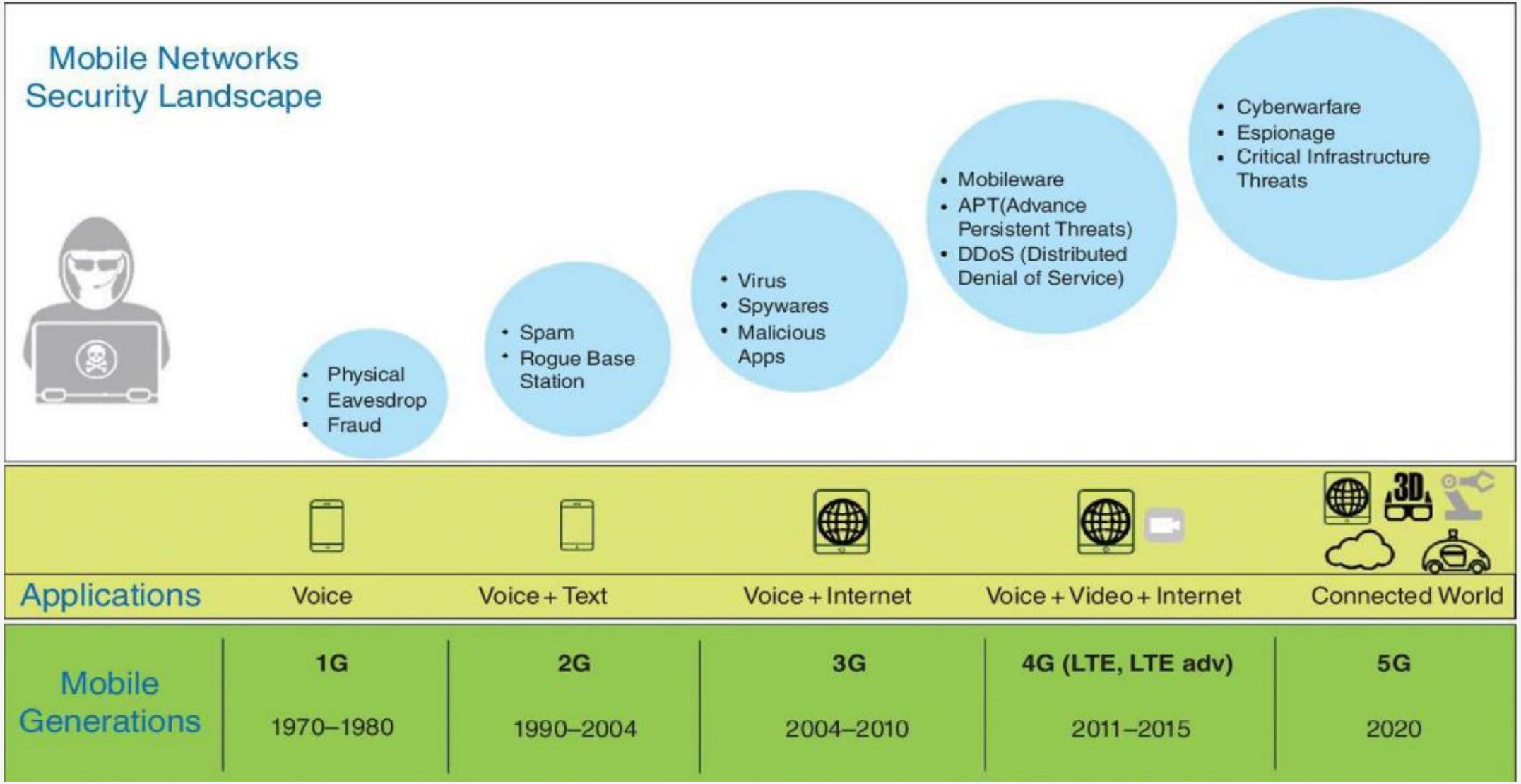
Mobile Computing Architecture

UW Bothell, WA

Mobile Network Security



Mobile Networks Security Landscape



Book: Comprehensive guide to 5G security edited by Madhusanka Liyanage,

Typical 4G Network Security Threats

Threat	Threat description	Impact Severity (Minor, Moderate, Severe, Extreme)	Threat Occurrence (1-5, Low-High)
Insecure Mobile OS (Operating System)	Mobile operating systems carry vulnerabilities that are fixed, using vendor issued patches and updates. If not fixed, can cause attackers to exploit vulnerabilities to hack into mobile systems	Moderate	4
Download unauthorized apps	Users download app from app store that are not verified by the vendor or checked by their IT department, and can be malicious	Moderate	5
Insecure App with sensitive data	A legitimate app that leaks sensitive personal or business data and with no mechanism to encrypt or protect	Severe	5
Virus	Malicious software code with a specific purpose to damage mobile functions or files	Severe	2
Malware	An advanced virus or malicious app that can propagate and self-reproduce causing large-scale, network-wide damage	Extreme	3
Spyware	A malware type used to steal end user data, sensitive information to transmit to remote attackers	Extreme	3
DDoS (Distrusted Denial of Service)	Launched as a coordinated attack involving hundreds of thousands of devices infected with malicious code. Targets the availability of mobile networks	Extreme	2

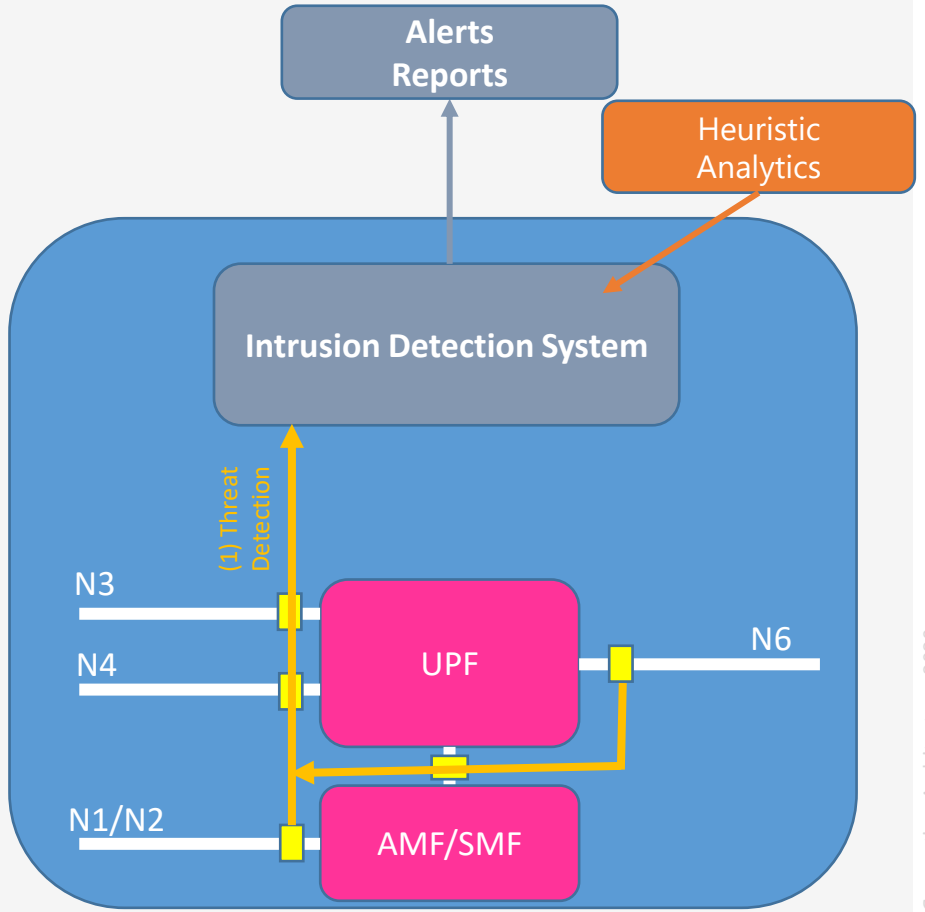
Typical 5G Network Security Threats

Threat	Threat description	Impact Severity (Minor, Moderate, Severe, Extreme)	Threat Occurrence Probability (1-5, Low-High)
Ransomware	Specialized malwares use exploit, encrypt and lock access to critical data. Access granted after paying demanded ransom money	Severe	3
Advance Malware	Advance malwares targeting billions of mobile and IoT devices with capability to exploit the OS and network vulnerabilities	Extreme	3
IoT Botnets	IoT and mobile devices hosting a control agent/bot receiving remote commands and continuously leaking telemetry information to a remote bot-master running a central command and control (C&C) system. Used for both passive and active attacks	Severe	2
Critical Infrastructure Threats	Threats that are focused, damaging critical infrastructure services such as SCADA, i.e. Stuxnet, Shamoon attacks	Extreme	3
Zero-day Attacks	An advance attack exploiting the undiscovered vulnerabilities of a system. Can be a combination or package of multiple attack types, malware, rootkits and botnets	Extreme	1

Intrusion Detection System (IDS)

Intrusion detection is the process of monitoring the events occurring in a local system or network and analyzing them for any sign of violations. An IDS is a software that automates the intrusion detection process. An IDS can typically provide several functions:

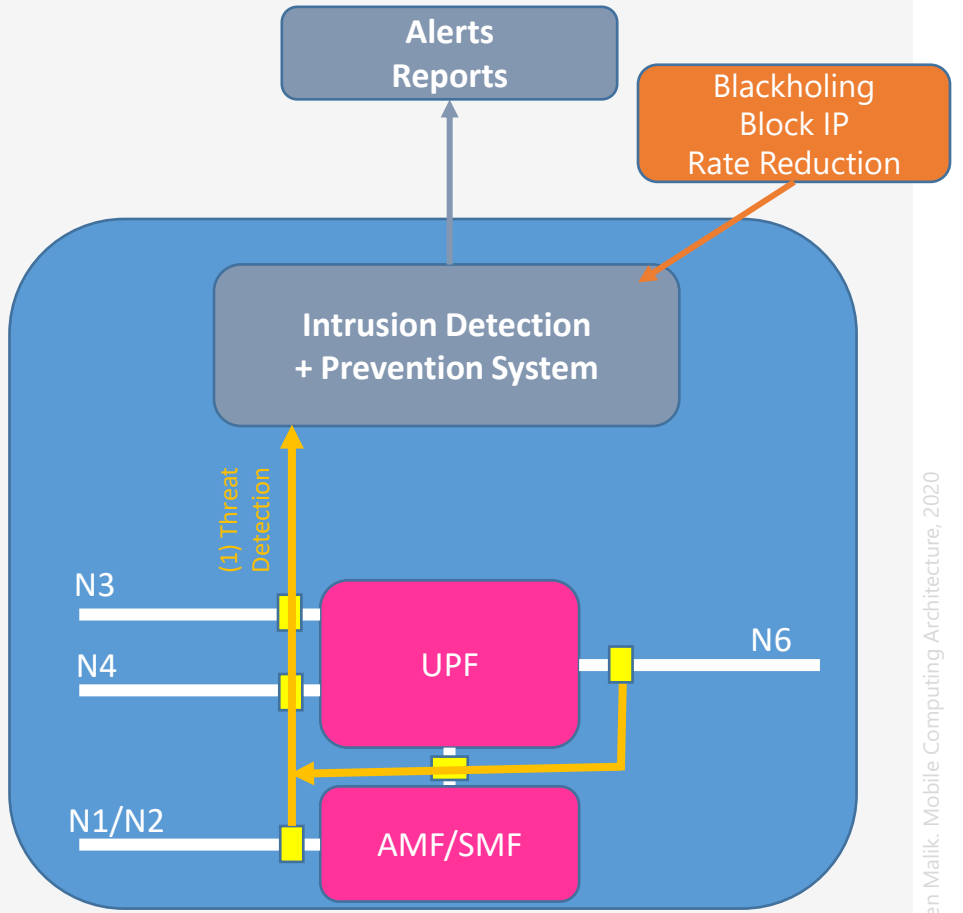
- Monitoring and recording information: Targeted information can be usually recorded either locally or distributed according to concrete settings. For example, IDSs can store the information in an enterprise management server.
- Notifying security team: An alert can be sent to security team if any malicious event is identified.
- Generating reports.:Such reports often summarize the monitored events and provide details on particular interested events.
- There are two major types of IDSs:
    - Host-based IDS (HIDS) for example, Symantec, Norton, etc.
    - Network-based IDS (NIDS), see picture



Intrusion Prevention System (IDS)

An IPS is a software that has all the capabilities of an IDS and can also attempt to stop possible incidents. As compared with an IDS, IPS technologies can respond to a detected threat by attempting to prevent it from succeeding. They can provide the following functions:

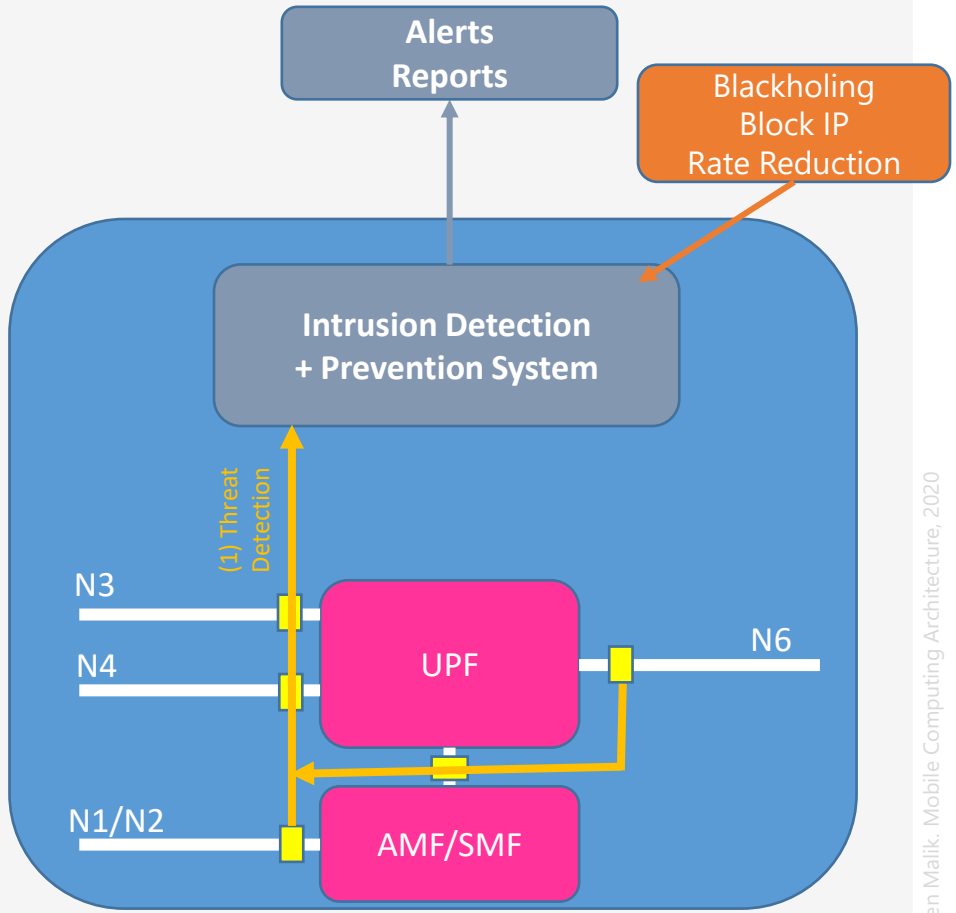
- Stopping the attack: IPSs can react to existing attacks, such as terminating the network connection or user session that is being used for the attack, and blocking access to the target from the offending user account, IP addresses, etc.
- Changing the security environment: An IPS can change the configuration of other security controls to disable an attack (i.e., reconfiguration of a device), or even launch patches to be applied to a host if the host has detected vulnerabilities.
- Changing the attack's content: Some IPSs can remove or replace malicious portions of an attack/program to make it benign. For instance, an IPS can remove an infected file attachment from an email and then permit the cleaned email to reach its recipient.



Network Malware/Ransomware/Spyware Prevention (IDS/IDP)

- Combination of IDS + IPS
- Encrypted Traffic: pattern recognition
- GTP Tunnels: IDS should have the capability
- Malware database
- Monitor Internet facing Interface (N6)
- Monitor Roaming traffic
- Monitor Control traffic

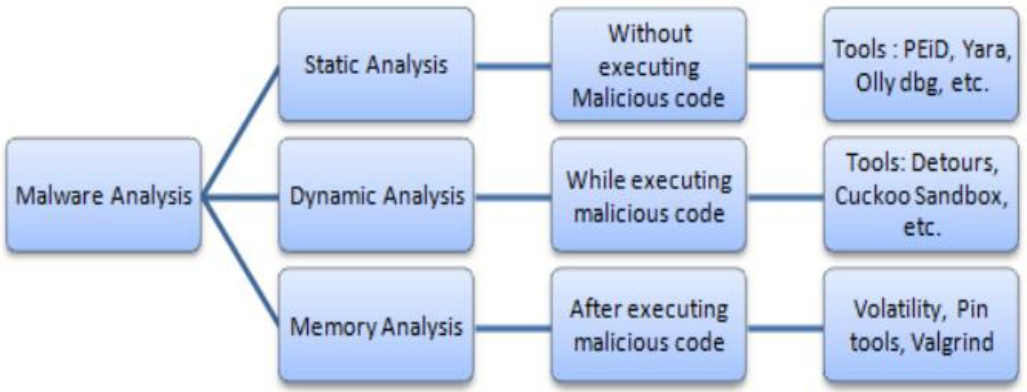
Note: For Mobile Devices, typically software like Norton, Symantec, etc. are used for detection and protection



Malware Analysis – Three Types – I

1- Static Analysis

- The process of detecting or examining the malicious code without executing it is defined as static malware analysis.
- It is a signature-based methodology
- Metadata strings, code, and import libraries are extracted and used in the feature selection or feature extraction phase in the machine learning classification
- File types: Exe, DLL, documents, Assembly code, byte code, etc., from these file types static features are extracted as output.
- The tools used for static malware analysis are PEiD, ssdeep, pafish, Yara, strings,

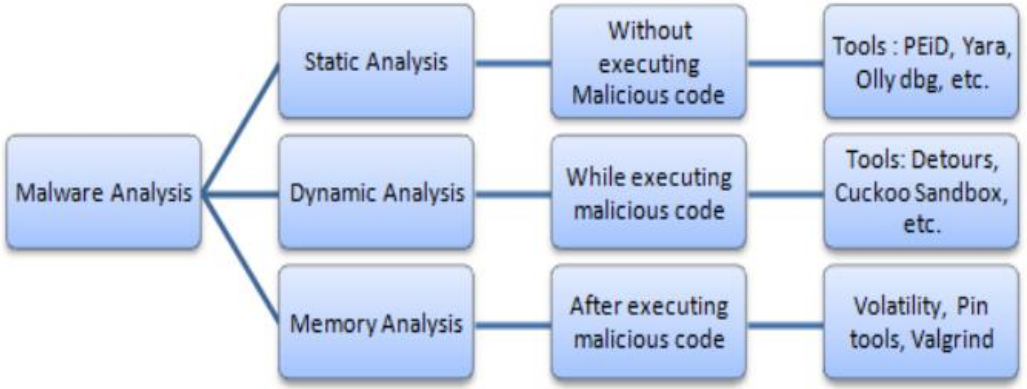


Reading assignment: last slide #4

Malware Analysis – Three Types - II

2- Dynamic Analysis

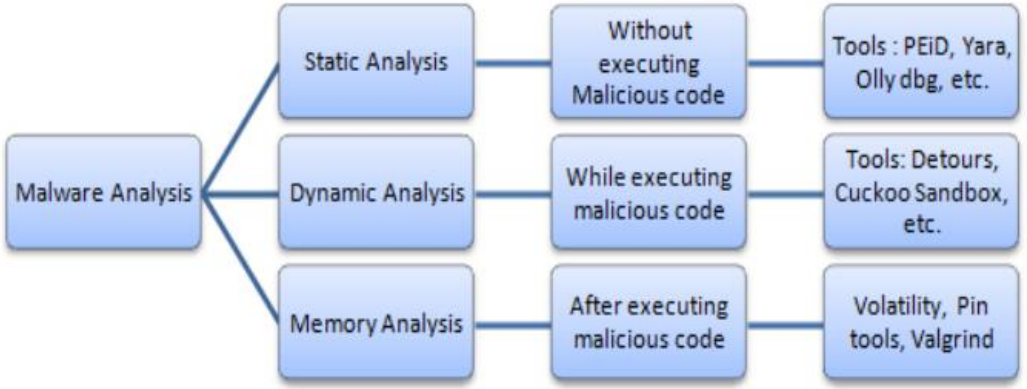
- Detecting the behavior and functionality of malicious code *while* executiing the code
- Dynamic features are system calls, file activities, process activities, and network activities.
- The dynamic malware analysis tools are used to extract the dynamic features of malicious code, tools are Sandbox, Comodo automated analysis, ThreatTrack etc.
- The monitoring tools for dynamic malware analysis are Process Explorer, Process Monitor, Capture-BAT, RegShot, etc.



Malware Analysis – Three Types - III

3- Memory Analysis

- Detecting the behavior and functionality of malicious code *after* eecutiing the code
- The features for memory analysis are shared libraries, running processes, hooking detection, network connections, rootkit connection, hidden artifacts, code injection, etc.
- The tools for memory analysis are volatility, pin tools, Valgrind, etc.



Network Security Threats - DDoS

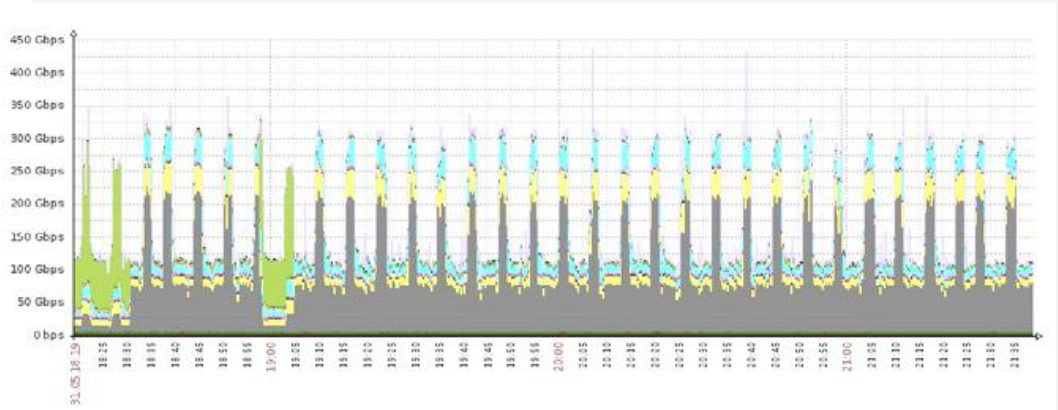
Miria attacks against Brian Krebs, OVH and DynDNS introduced – **on top of the record-breaking volumes** – sophisticated vectors such as **GRE floods** and **DNS water torture**.

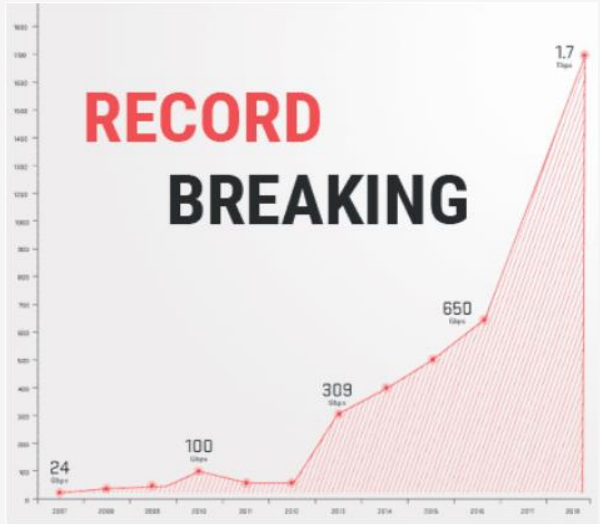
Mirai is **open-source code** means hackers can potentially mutate and customize it—resulting in an untold variety of new attack tools that can only be detected **by intelligent automation** such as behavioral analysis or machine learning.

DDoS as a Service (DDoSaaS)

*Hackers are abandoning "old school" tools and opting to **pay for attacks** via stressor services.*

For just **$19.99 a month**, an attacker can run **20-minute bursts for 30 days** using a number of attack vectors, such as DNS, SNMP and SSYN, and slow GET/POST application-layer DoS attacks.

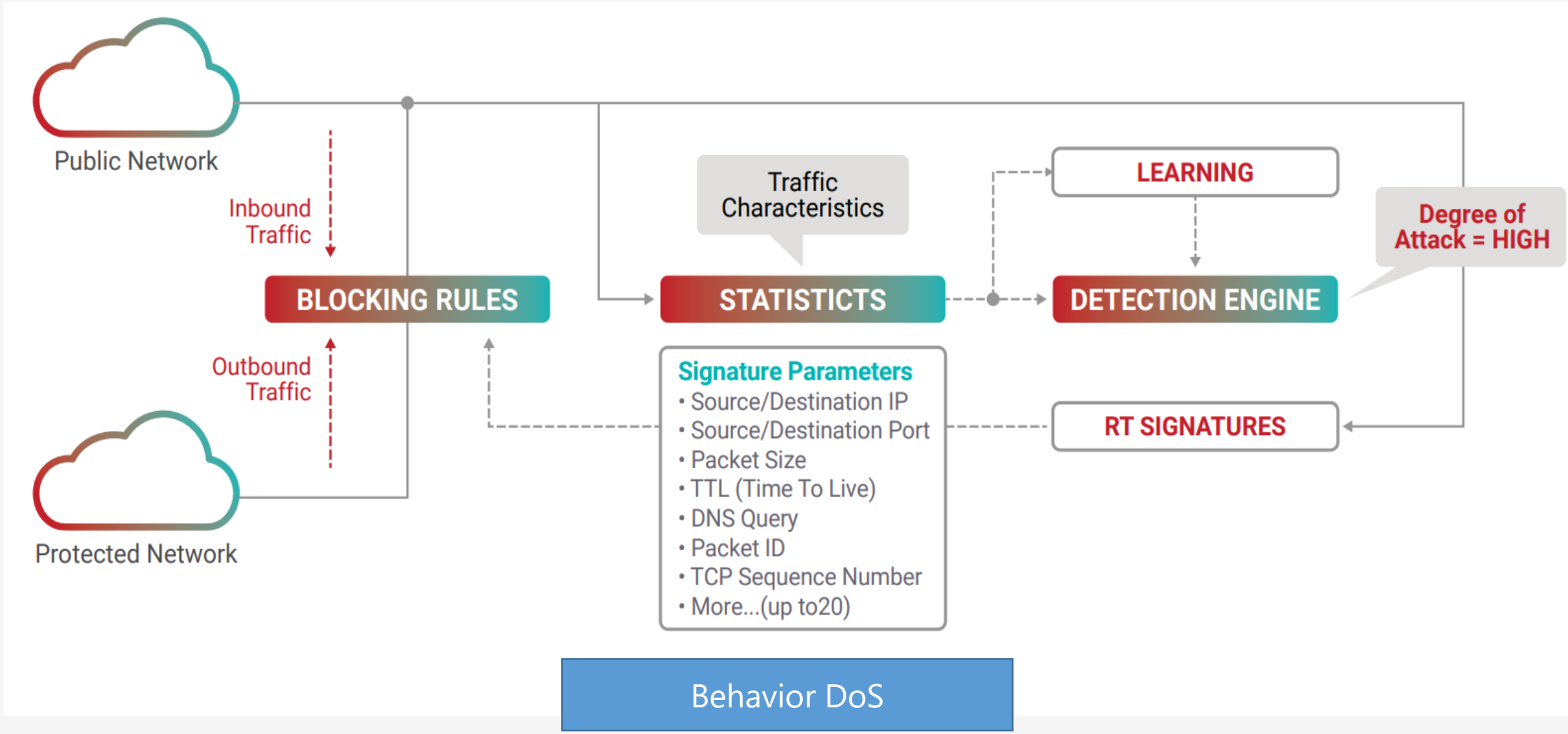




Radware – Hackers and Companies Agree, Data Is Lucractive – 2017

Source: Qualcomm

Network Security Threats – DDoS Mitigation

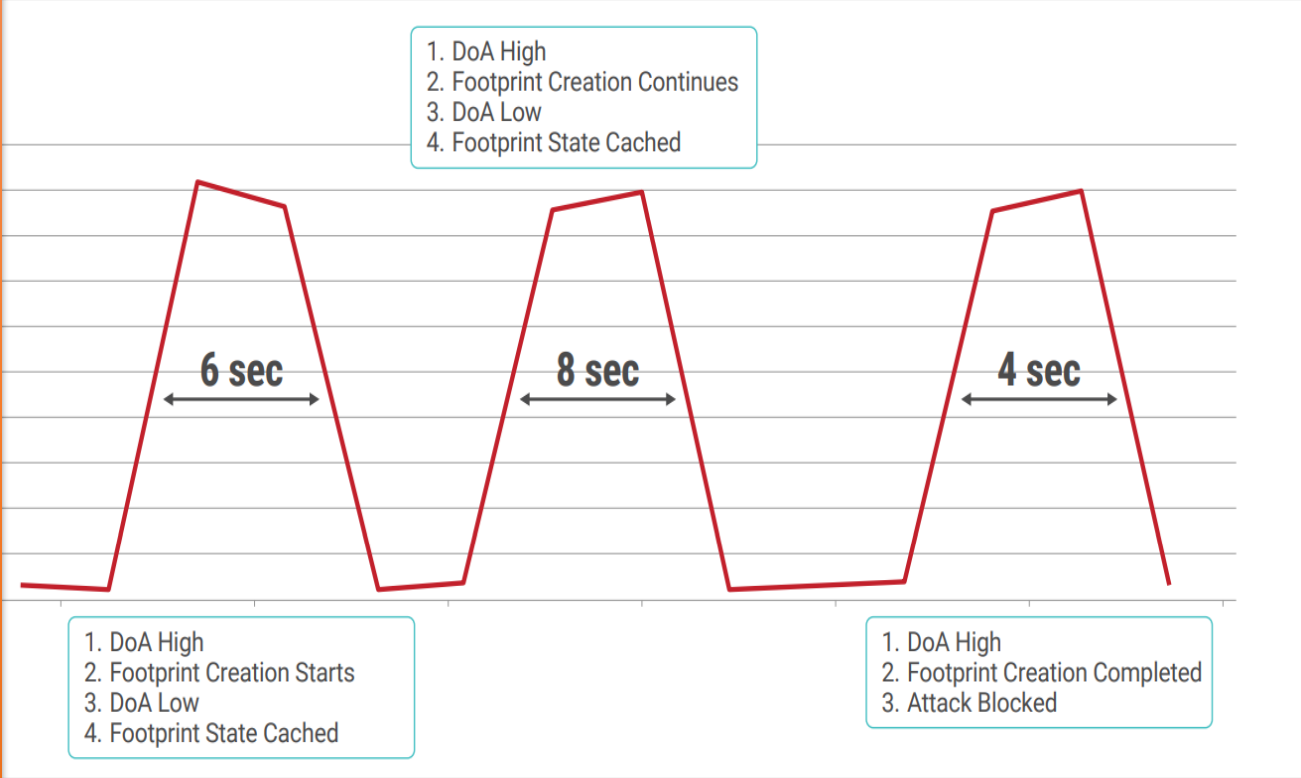


Source: Radware

Network Security Threats – Behavior-DoS Mitigation

- Attack detection in BDoS Protection combines two parameters. (1) rate of a specific traffic type. (2) rate-invariance, such as the portion of the specific traffic type out of the entire traffic distribution.
- An analytics engine measures the degree-of-attack (DoA) surface.
- BDoS considers an attack to have started only when both parameters are high
- A high volume of traffic caused by a flash crowd will have a high rate anomaly, but the rate-invariant parameter will remain normal. As a result, the combined DoA surface will not cause BDoS to trigger mitigation
- However, if both parameters show an anomalous score, the combined DoA surface will trigger attack handling, and BDoS will start creating a blocking signature in real-time.

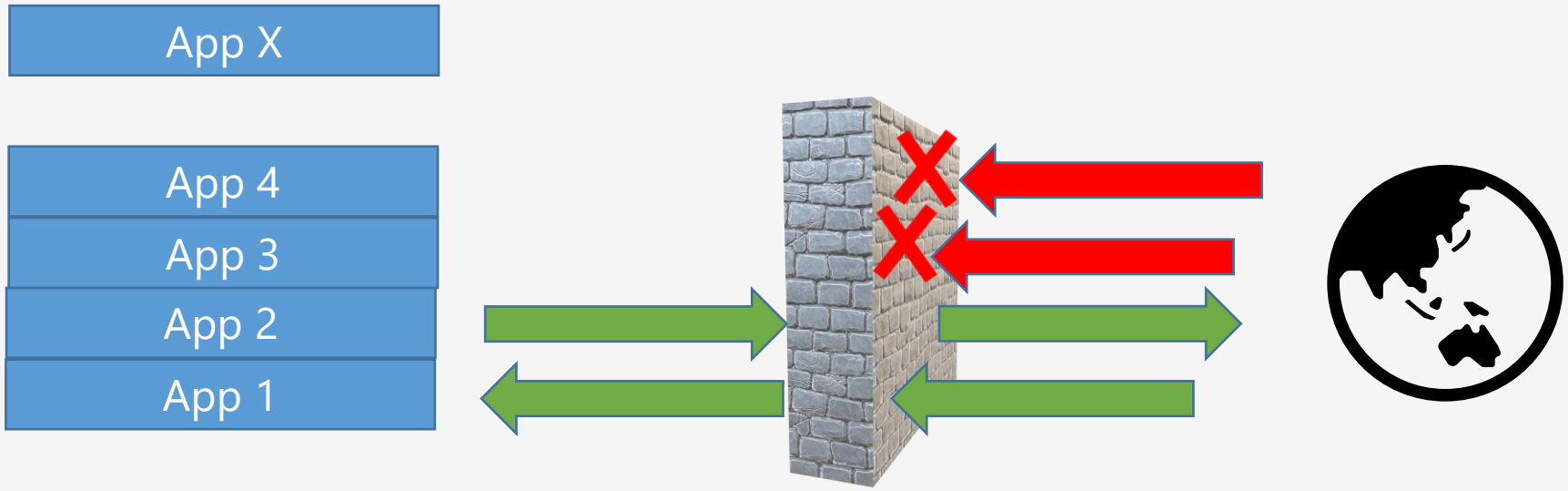
Degree-of-Attack (DoA)



Dynamic nature of DDoS requires Realtime Analysis and Generation of Prevention Signatures

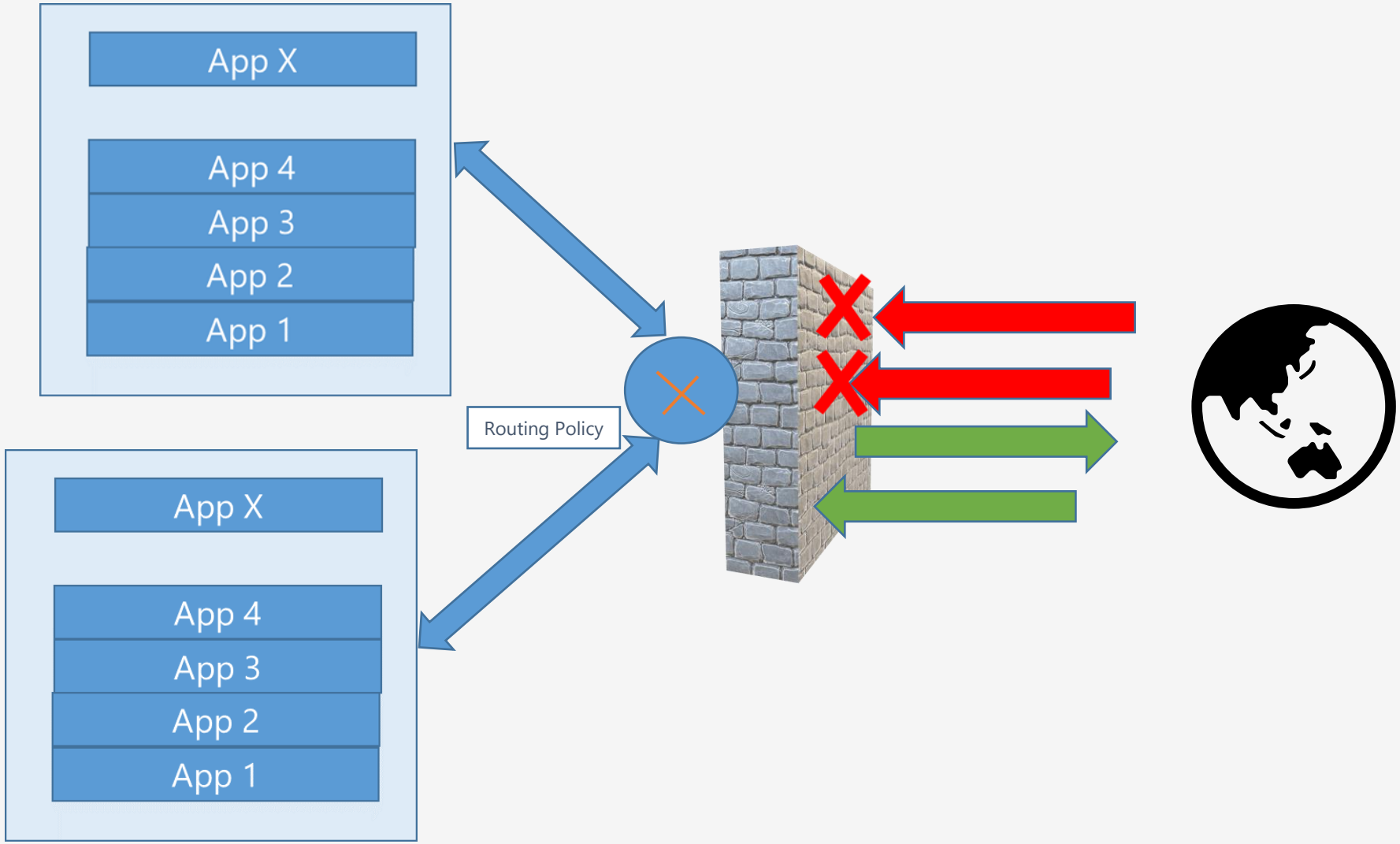
Source: Radware

Firewalls – I



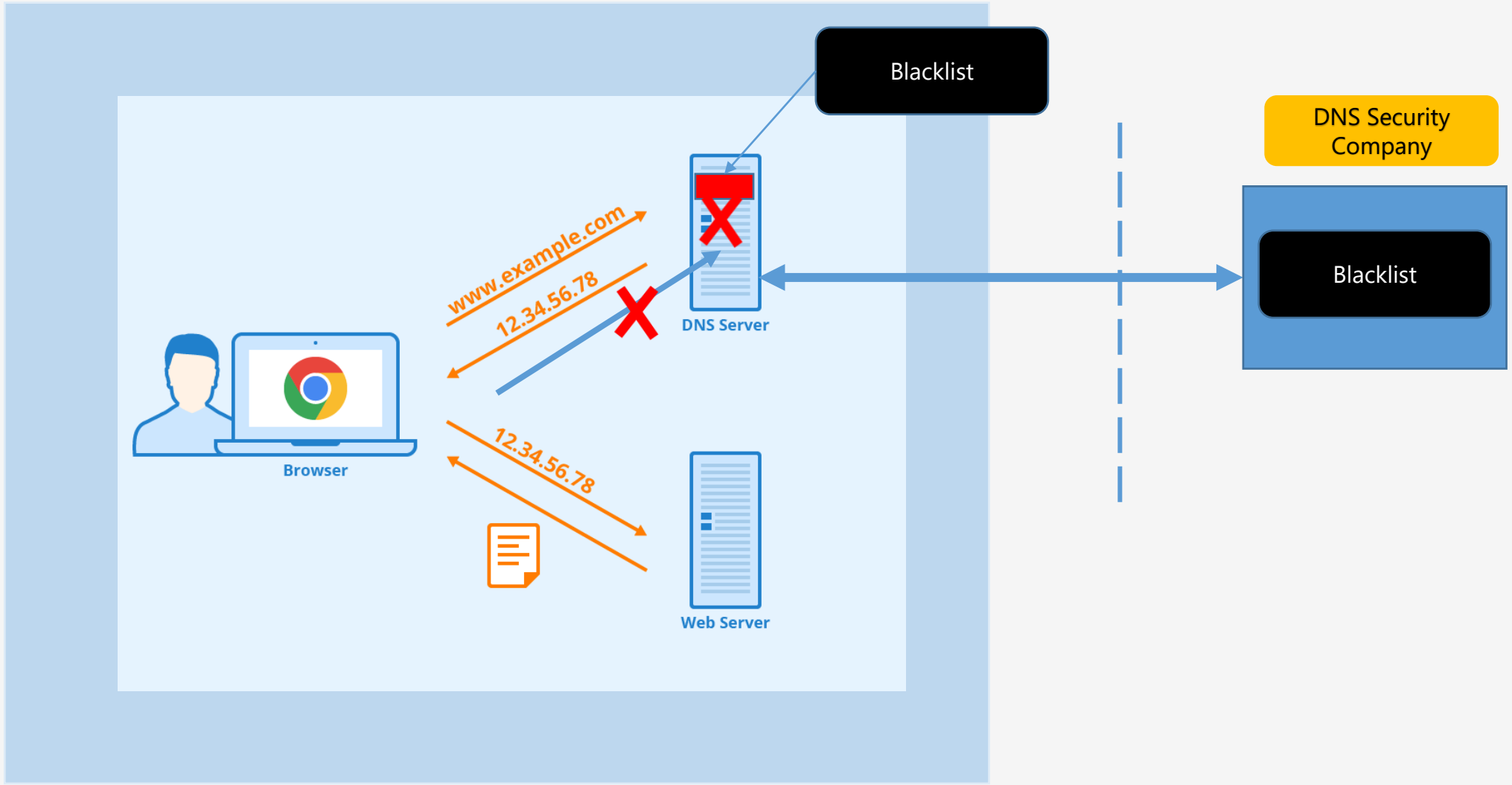
Source: Qualcomm

Firewalls – II (Virtual Private Network Routing)



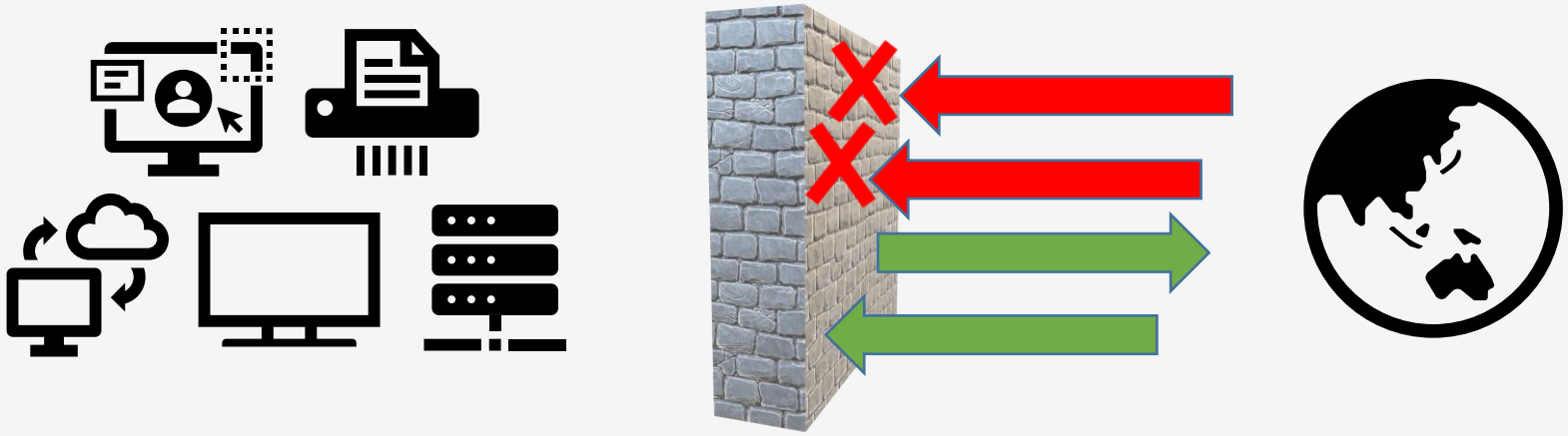
Source: Qualcomm

DNS Protection



Source: Qualcomm

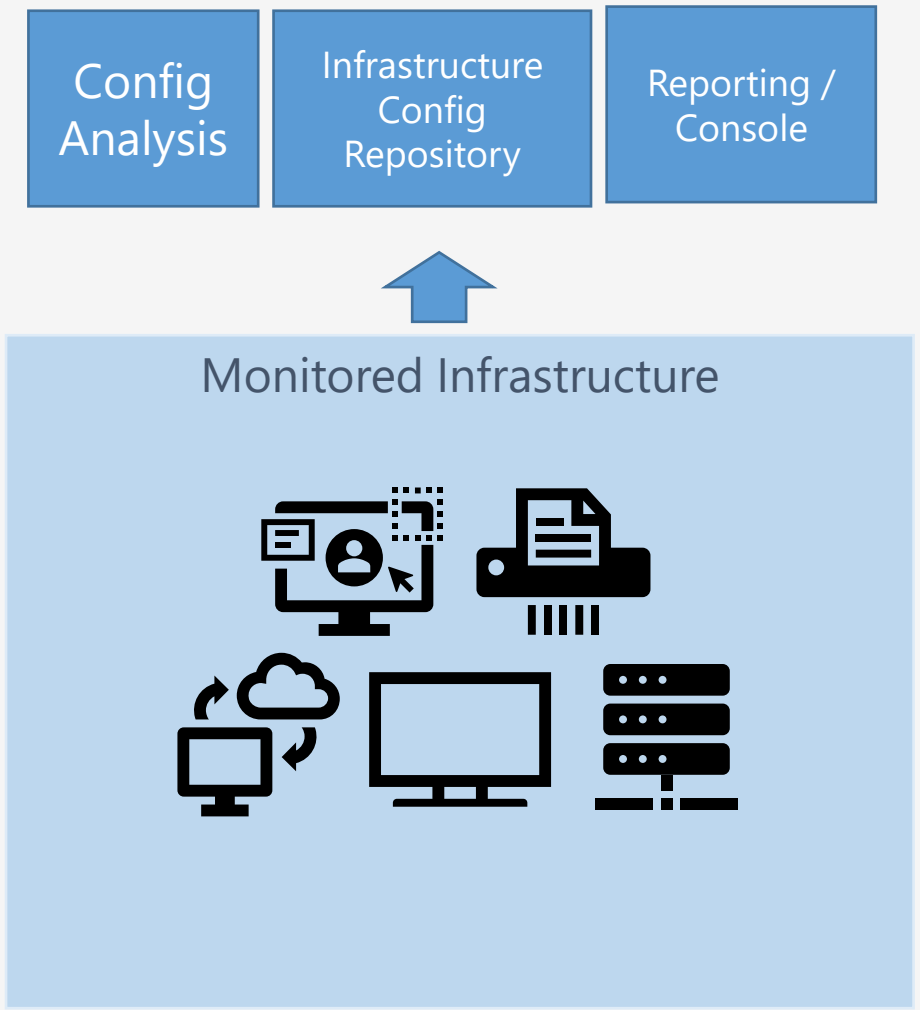
Infrastructure Integrity – Behind Firewall Protection



Source: Qualcomm

Infrastructure Integrity – Configuration Management

- System Integrity (Operating system, configuration, parameters, admin passwords, etc.)
- Any changes in System Integrity without authorization can be potentially a security breach
- Capture the Integrity state of the systems
- Monitor
- Catch delta / discrepancies
- Report



Source: Qualcomm

Infrastructure Integrity – Device Certificates

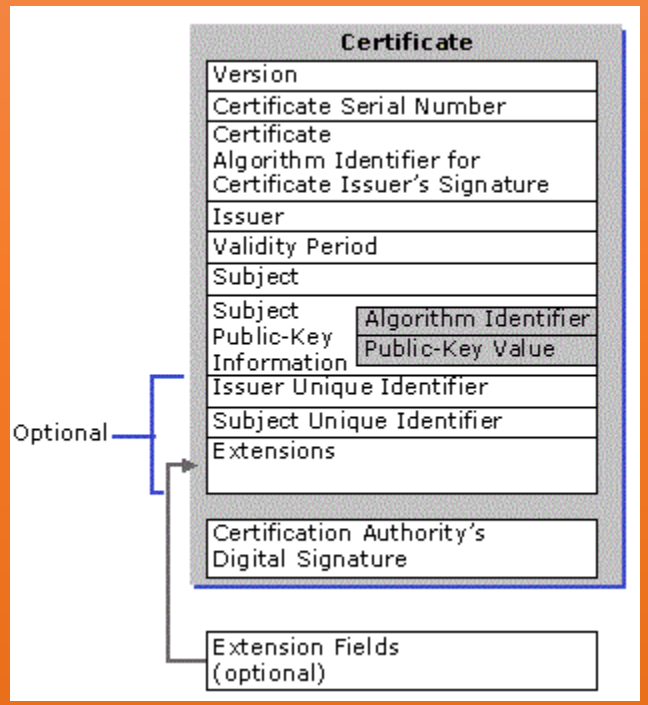
A device certificate is an electronic document that is embedded into a hardware device and can last for the life of the device. The certificate's purpose is similar to that of a driver's license or passport: it provides proof of the device's identity and, by extension, the identity of the device owner

Let’s take a look at Public Key Infrastructure (PKI) first…

Public Key Infrastructure – Digital Certificate (Cert)

A digital certificate is used to associate a public key to a uniquely identified owner. The standard for digital certificates is X.509, which identifies the fields and values to be used in the certificate. These fields include:

- Version of the certificate
- Unique serial number associated with the certificate
- Algorithm ID used to sign the certificate
- Name of the certificate issuer
- Validity dates of the certificate
- Name of the owner of the certificate
- Public key of the owner
- ID of the issuing certificate authority
- ID of the owner
- Optional extensions

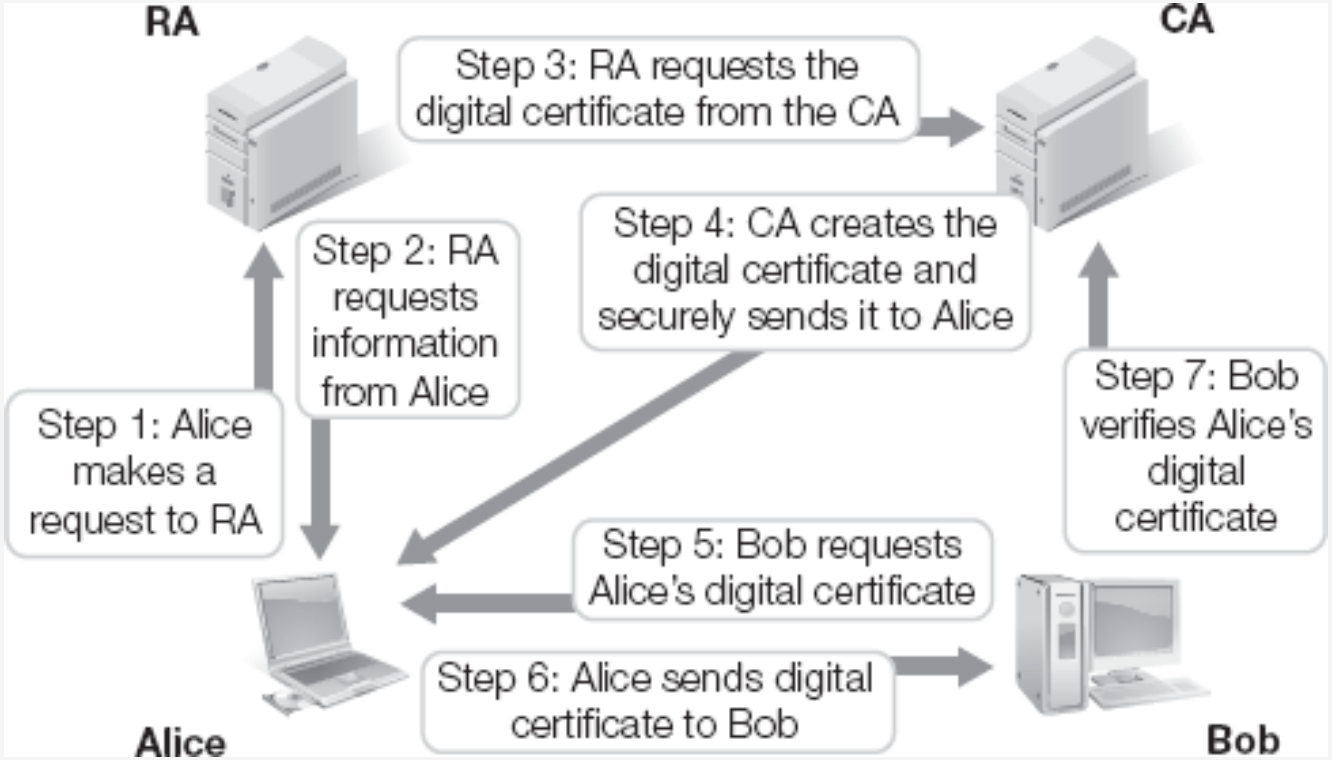


Public Key Infrastructure – PKI

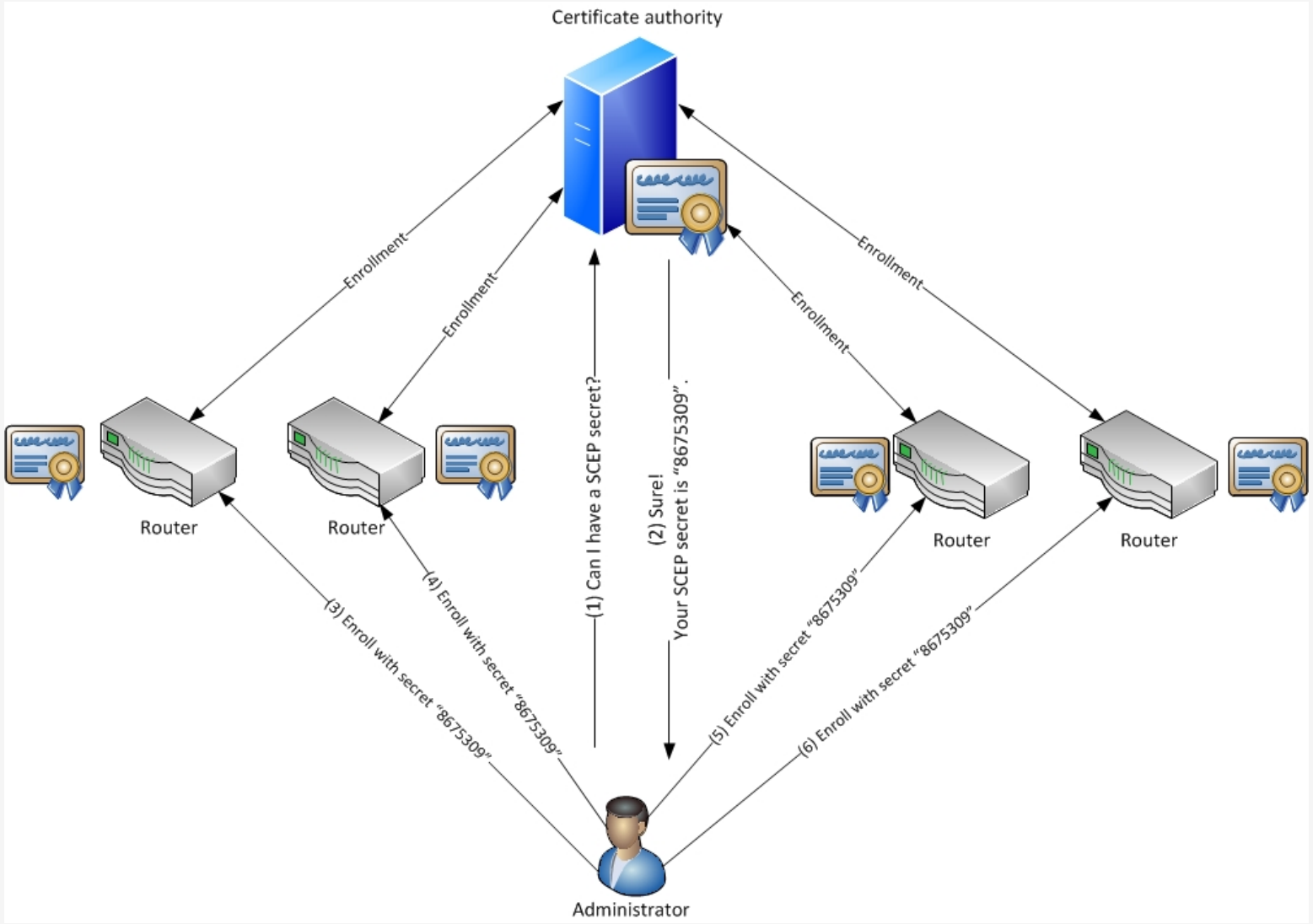
Components of a public key infrastructure are:

- Certificate authority (CA) — issues digital certificates for identities. A certificate associates the identity of a person or server with the corresponding public key.
- Registration authority (RA) — responsible for the registration and initial authentication of users who are issued certificates after a registration request is approved.
- Certificate server (CS) — responsible for issuing digital certificates based on the information provided at the registration process. CS in part of CA.
- Certificate repository (CR) —A database that stores the digital certificates
- Certificate validation—a certificate is valid

Public Key Infrastructure - Process



Infrastructure Integrity – Device Certificates



Source: Juniper

Reading Material

Moblie Networks Security Landscape.pdf

IDS and IPS.pdf

Radware_Behavioral_Burst_Attack_Protection_WP.pdf

Classification-Of-Malware-Detection-Using-Machine-Learning-Algorithms-A-Survey.pdf