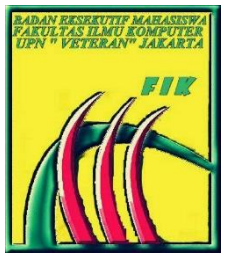
Survival 101:
How To Defend Your Territory Against The Endless Cyber Attacks

Presented by Michael Takeuchi
UPN Veteran Jakarta, 20 November 2017



Little Things About Me

- My name is **Michael Takeuchi**
- Was MikroTik Certified on MTCNA, MTCRE, MTCINE, MTCUME, MTCWE, MTCTCE, MTCIPv6E
- Was Juniper Certified on JNCIA-Junos
- MikroTik Certified Consultant on mikrotik.com
- January 2017 – June 2017 Work as Remote Network Engineer at Middle East
- July 2017 – Now Work as Network Analyst at Internet Service Provider (AS38320)
- Not Hacker, Just Networker ☺

Presentation Outline

- Cyber Attacks?
  - What is Cyber Attacks?
  - Type of Attacks
  - Who is Attacking?
  - Past, Now & Future
  - Endless?
- Territory Mean on Cyber Attacks Cases
- In-Depth with Your Territory (Network)
  - Network?
  - Network Addressing (IP Address)
  - Public IP Addressing & Private IP Addressing
  - Network Address Translation
  - Introduction to Routing
  - What We Need to Do?
- Simple Firewall Implementation (Explanation & Demo)
- Summary

Objective

- educate users on their responsibility to help protect the confidentiality, availability and integrity of their organization's information and information assets
- understand how their actions can greatly impact the overall security position of an organization
- reinforce security policy and other information security practices that are supported by the organization
- helps minimize the cost of security incidents, helps accelerate the development
- of new application systems, and helps assure the consistent implementation of controls across an organization’s information systems

Cyber Attacks?

What is Cyber Attacks?

- A **cyberattack** is any type of offensive manoeuvre employed by nation-states, individuals, groups, or organizations that targets computer information systems, infrastructures, computer networks, and/or personal computer devices by various means of malicious acts usually originating from an anonymous source that either steals, alters, or destroys a specified target by hacking into a susceptible system.

- Wikipedia

https://en.wikipedia.org/wiki/Cyberattack

Type of Attacks

- Phising
- Malware
- Bruteforce
- Defacement
- Denial of Service
- Remote Access Trojan
- Man in The Middle Attack
- Advanced Persistent Threat (APT)

and many more...

Who is Attacking?

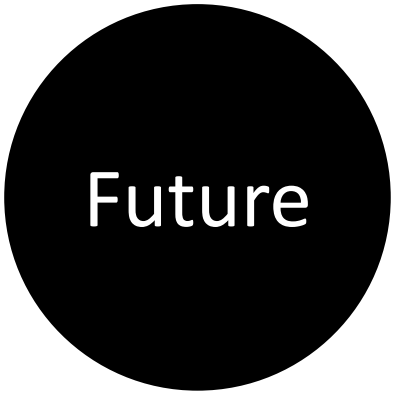
- https://threatmap.checkpoint.com/ThreatPortal/livemap.html
- https://www.fireeye.com/cyber-map/threat-map.html
- https://cybermap.kaspersky.com/stats/
- http://www.digitalattackmap.com
- http://map.norsecorp.com
- http://public.honeynet.id (Made in Indonesia)

The attacks you are seeing are actually on Vendor's infrastructure, not all attack are detected and please be aware, maybe the attacker is your friends or yourself ☺

Past, Now & Future

Defacement, Bank Hacking, Frequency Hijacking, Botnet Denial of Service

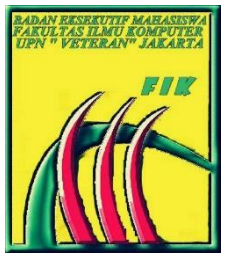
Ransomware, Credit Card Fraud (scam), Denial of Service Attack



IoT Hacking, Human Hacking, Denial of Service

Endless?

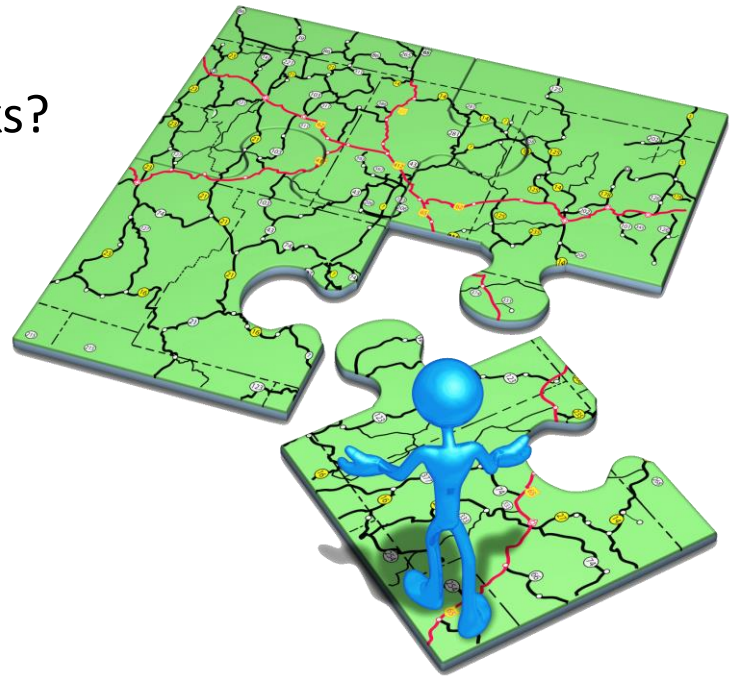
Territory Mean
on Cyber Attacks Cases



What is Territory?

- Wikipedia said that A **territory** is an administrative division, usually an area that is under the jurisdiction of a state.
- In my opnion, A **territory** is an area or district that managed by ourselves

So? What the relation with cyber attacks?



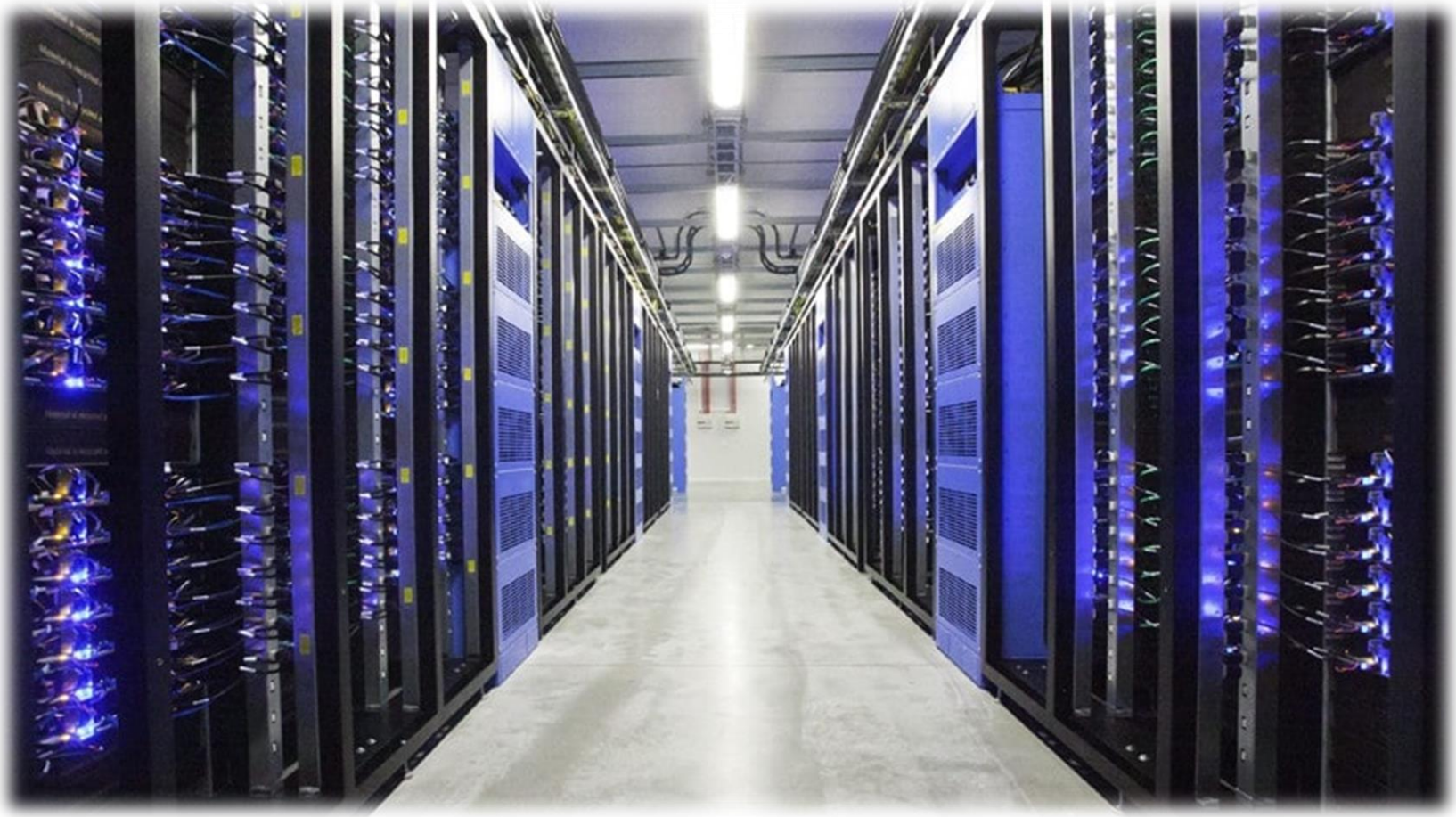
Where is it?

Who Have The Responsibility?

Why You?

When it’s (Cyber Attacks) Happens?

How?



In-Depth with Your Territory (Network)

Network?

- A **computer network** or **data** network is a telecommunications network which allows nodes to share resources. In computer networks, networked computing devices **exchange data** with each other using a data link. The connections between nodes are established using either cable media or wireless media. **The best-known computer network is the Internet.**

Network Addressing (IP Address)

- An **Internet Protocol address** (**IP address**) is a numerical label assigned to each device connected to a computer network that uses the Internet Protocol for communication.
- The IP address space is managed globally by the Internet Assigned Numbers Authority (IANA), and by five regional Internet registries (RIR) responsible in their designated territories for assignment to end users and local Internet registries, such as Internet service providers.
- IP addresses are usually written and displayed in human readable notations, such as 172.16.254.1 in IPv4, and 2001:db8:0:1234:0:567:8:1 in IPv6.

Public IP Addressing & Private IP Addressing

- **Public IP** is an IP that distributed on internet
- **Private IP** is an IP that used on Private Network (such as LAN)
- **Public IP** should not be used on **Private Network** and this is ***Vice Versa***
- When user on Private Network want to have a communication with Internet, they must have (at least) one Public IP which will become a mask on the Internet (read: Network Address Translation)
- You can check your Private IP using:
  - ipconfig (on windows)
  - ifconfig (on linux, mac os, BSD Family)
- You can check your Public IP using: https://whatismyipaddress.com/

Public IP Addressing & Private IP Addressing

- Private IP Allocation:

10.0.0.0 – 10.255.255.255 (10.0.0.0/8)

172.16.0.0 – 172.31.255.255 (172.16.0.0/12)

192.168.0.0 – 192.168.255.255 (192.168.0.0/16)

- Public IP Allocation: All address excluded reserved address
- Reserved Address: https://en.wikipedia.org/wiki/Reserved_IP_addresses

Network Address Translation (NAT)

- Network address translation (NAT) is a method of remapping one IP address space into another by modifying network address information in Internet Protocol (IP) datagram packet headers while they are in transit across a traffic routing device.[1]
- The technique was originally used for ease of rerouting traffic in IP networks without readdressing every host.
- In more advanced NAT implementations featuring IP masquerading, it has become a popular and essential tool in conserving global address space allocations in face of IPv4 address exhaustion by sharing one Internet-routable IP address of a NAT gateway for an entire private network.

Network Address Translation (NAT)

- **IP masquerading** is a technique that hides an entire IP address space, usually consisting of private IP addresses, behind a single IP address in another, usually public address space. The address that has to be hidden is changed into a single (public) IP address as "new" source address of the outgoing IP packet so it appears as originating not from the hidden host but from the routing device itself. Because of the popularity of this technique to conserve IPv4 address space, the term *NAT* has become virtually synonymous with IP masquerading.

Introduction to Routing

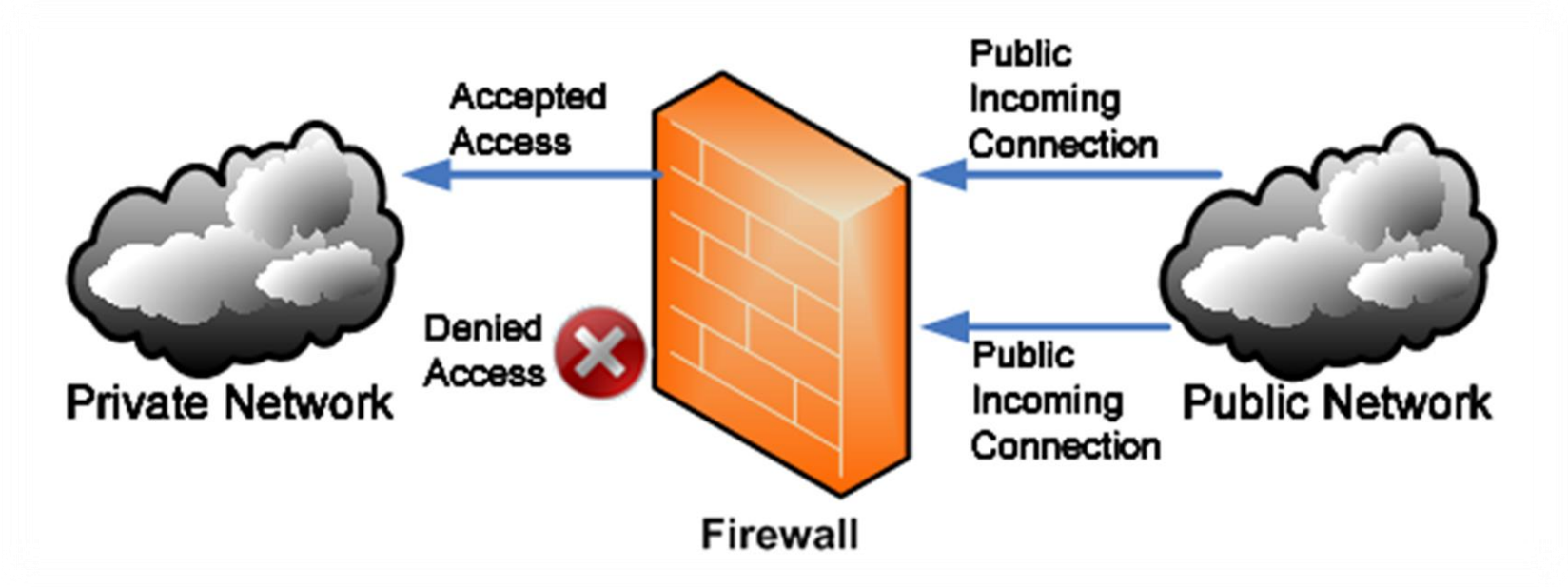
- **Routing** is one of many feature that support the internet
- **Routing** is the process of selecting a path for traffic in a network, or between or across multiple networks by **Router**
- For the example when we sent some request packet to http://www.upnvj.ac.id, the packet will be routed by your devices to some node that become *Gateway (*usually Gateway is a Router) and will processed by the Router that we setup before

What We Need to Do?

1. Auditing your network
2. Harderning your network
3. Penetration Testing your network
4. Go to number 1 until your network be hard

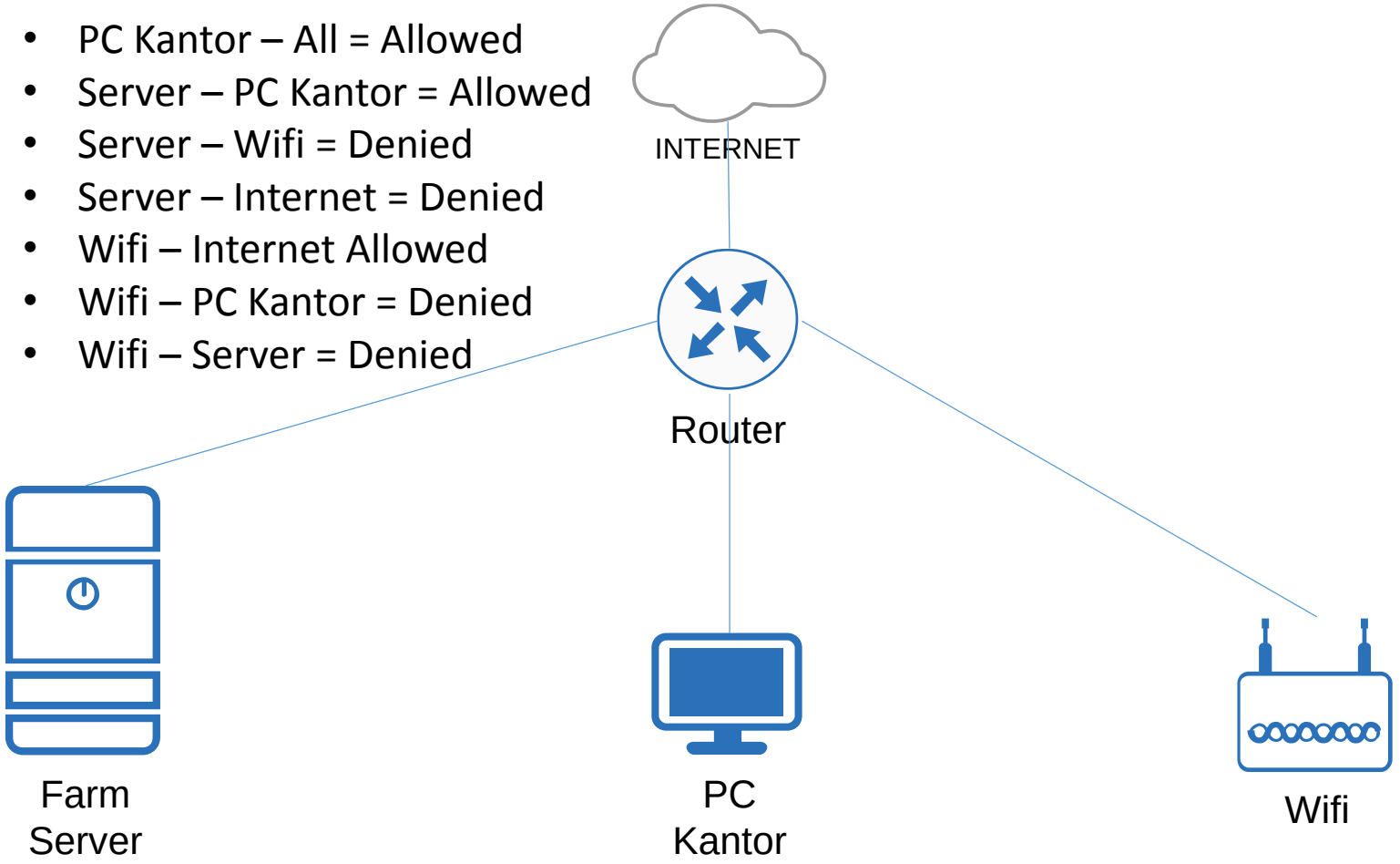
Simple Firewall Implementation

What is Firewall?



Simple Firewall Implementation

- PC Kantor – All = Allowed
- Server – PC Kantor = Allowed
- Server – Wifi = Denied
- Server – Internet = Denied
- Wifi – Internet Allowed
- Wifi – PC Kantor = Denied
- Wifi – Server = Denied



Demo

Summary

Secure ≠ Easy

Feel So Hard To Securing, Auditing, Hardening Your Network?

Let Me Help You !

michael@takeuchi.id

http://www.facebook.com/mict404

https://www.linkedin.com/in/michael-takeuchi

Come to
Cyber Security Marathon !
24 – 25 February 2018
@Depok, Jawa Barat
https://depokcybersec.org


Thank
you