CYBER SECURITY MARATHON 2018

Network Infrastructure Security

By Michael Takeuchi

Cyber Security Marathon

25 February 2018, Hotel Bumi Wiyata (Depok)

Little Things About Me

- My name is **Michael Takeuchi**
- Was MikroTik Certified on MTCNA, MTCRE, MTCINE, MTCUME, MTCWE, MTCTCE, MTCIPv6E
- MikroTik Certified Consultant on mikrotik.com
- Was Juniper Certified on JNCIA-Junos
- Was Cisco Cerfied on CCNA-RS
- January 2017 – June 2017 Work as Remote Network Engineer at Middle East
- July 2017 – Now Work as Network Analyst at Internet Service Provider (AS38320)

Objective

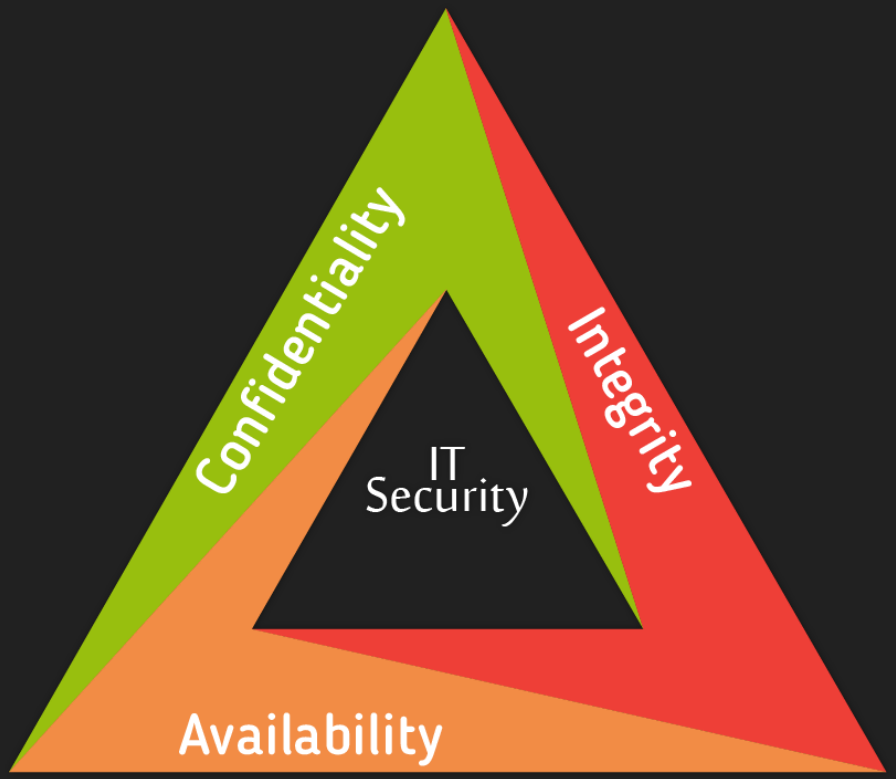
- Understand information security aspect
- Understand What is Network Infrastructure
- Helps minimize the cost of security incidents
- Understand how to defend yourself & your network
- Understand the difference between conventional & hardened network infrastructure
- Educate users on their responsibility to help protect the confidentiality, availability and integrity of their organization's information and information assets

Presentation Outline

- IT Security Basic Architecture
  - Confidentiality
  - Integrity
  - Availability
- Network Infrastructure Security
  - Network? / Computer Network
  - Infrastructure? / IT Infrastructure
  - Why need to be secured?
  - How?
- Network Infrastructure Topology
  - Conventional Network Infrastructure
  - Hardern Network Infrastructure

IT Security Basic Architecture

IT Security Basic Architecture



http://whatis.techtarget.com/definition/Confidentiality-integrity-and-availability-CIA

Confidentiality

- Confidentiality is roughly equivalent to privacy. Measures undertaken to ensure confidentiality are designed to prevent sensitive information from reaching the wrong people, while making sure that the right people can in fact get it: Access must be restricted to those authorized to view the data in question. It is common, as well, for data to be categorized according to the amount and type of damage that could be done should it fall into unintended hands. More or less stringent measures can then be implemented according to those categories.

Integrity

- Integrity involves maintaining the consistency, accuracy, and trustworthiness of data over its entire life cycle. Data must not be changed in transit, and steps must be taken to ensure that data cannot be altered by unauthorized people (for example, in a breach of confidentiality). These measures include file permissions and user access controls. Version control maybe used to prevent erroneous changes or accidental deletion by authorized users becoming a problem.

Availability

- Availability is best ensured by rigorously maintaining all hardware, performing hardware repairs immediately when needed and maintaining a correctly functioning operating system environment that is free of software conflicts. It's also important to keep current with all necessary system upgrades. Providing adequate communication bandwidth and preventing the occurrence of bottlenecks are equally important. Redundancy, failover, RAID even high-availability clusters can mitigate serious consequences when hardware issues do occur.

Network Infrastructure Security

Network?

Aman | https://en.wikipedia.org/wiki/Network

Languages

Bân-lâm-gú
Deutsch
Français
Italiano
Nederlands
Română
Tagalog

Edit links

Science, technology, and mathematics [edit]

Science [edit]

- Network science, an academic field which studies complex networks
- Network theory, the study of graphs as a representation of relations between discrete objects
- Biological network, networks found in ecological, evolutionary, and physiological contexts
- Social network, in social science research
  - Scientific collaboration network, a social network where nodes are scientists and links are co-authorships

Technology and communications [edit]

- Artificial neural network, a computing system inspired by animal brains
- Electrical network, an interconnection of electrical components
- Social networking service, an online platform which people use to build social networks
- Telecommunications network, allowing communication between separated nodes
  - Computer network or data network, a digital telecommunications network
  - Radio network, including both broadcast and two-way communications
  - Television network, used to distribute television program content

Mathematics [edit]

- Scale-free network, a network whose degree distribution follows a power law
- Small-world network, a mathematical graph in which most nodes are not neighbors, but have neighbors in common

Computer Network

- A **computer network**, or **data network**, is a digital telecommunications network which allows nodes to share resources.

- Wikipedia,

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

Nodes = PC/Networking Devices

Resources = Data/Information

Infrastructure?

- **Infrastructure** is the fundamental facilities and systems serving a country, city, or other area, including the services and facilities necessary for its economy to function. It typically characterises technical structures such as roads, bridges, tunnels, water supply, sewers, electrical grids, **telecommunications (including Internet connectivity and broadband speeds)**, and so forth, and can be defined as "the physical components of interrelated systems providing commodities and services essential to enable, sustain, or enhance societal living conditions.

- Wikipedia,

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

IT Infrastructure

- **Information technology infrastructure** is defined broadly as a set of information technology (IT) components that are the foundation of an IT service: typically physical components (computer and networking hardware and facilities), but also various software and network components

- Wikipedia,

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

Why need to be secured?

- Network infrastructure can be a good investment if you know how to take care of it. Keeping it secure may not be an easy task, but its' well worth it in the end and **Why need to be secured?** The answer is **"Because all of your data is pass through the network"**

How?

- Understand your network design.
- Review your applications.
- Find holes in your network.
- Build a firewall.
- Control circumventors.
- Use Secure Socket Layer.
- Don’t overcomplicate your network.
- Protect your network inside and out.
- Combat problems before they come.

How?

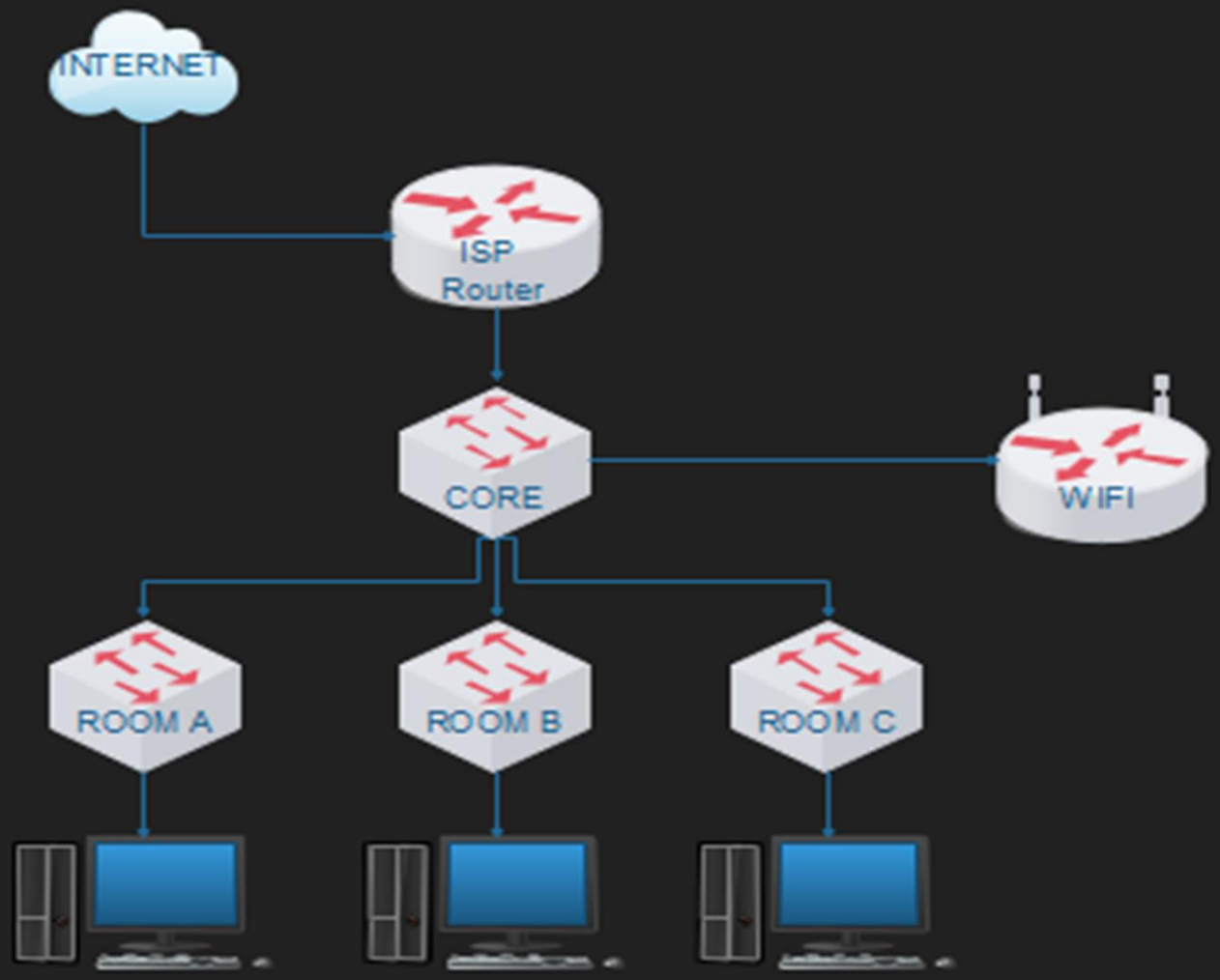
- Perform auditing and mapping
- Keep the network up-to-date
- Physically secure the network
- Consider MAC address filtering
- Implement VLANs to segregate traffic
- Use 802.1X for authentication
- Use VPNs to encrypt select PCs or servers
- Encrypt the entire network

How? (My Version)

- 1. Audit your network
- 2. Hardern your network
- 3. Do a Penetration Testing to your network
- 4. Go to number 1 until your network be hard

Network Infrastructure Topology

Conventional Network



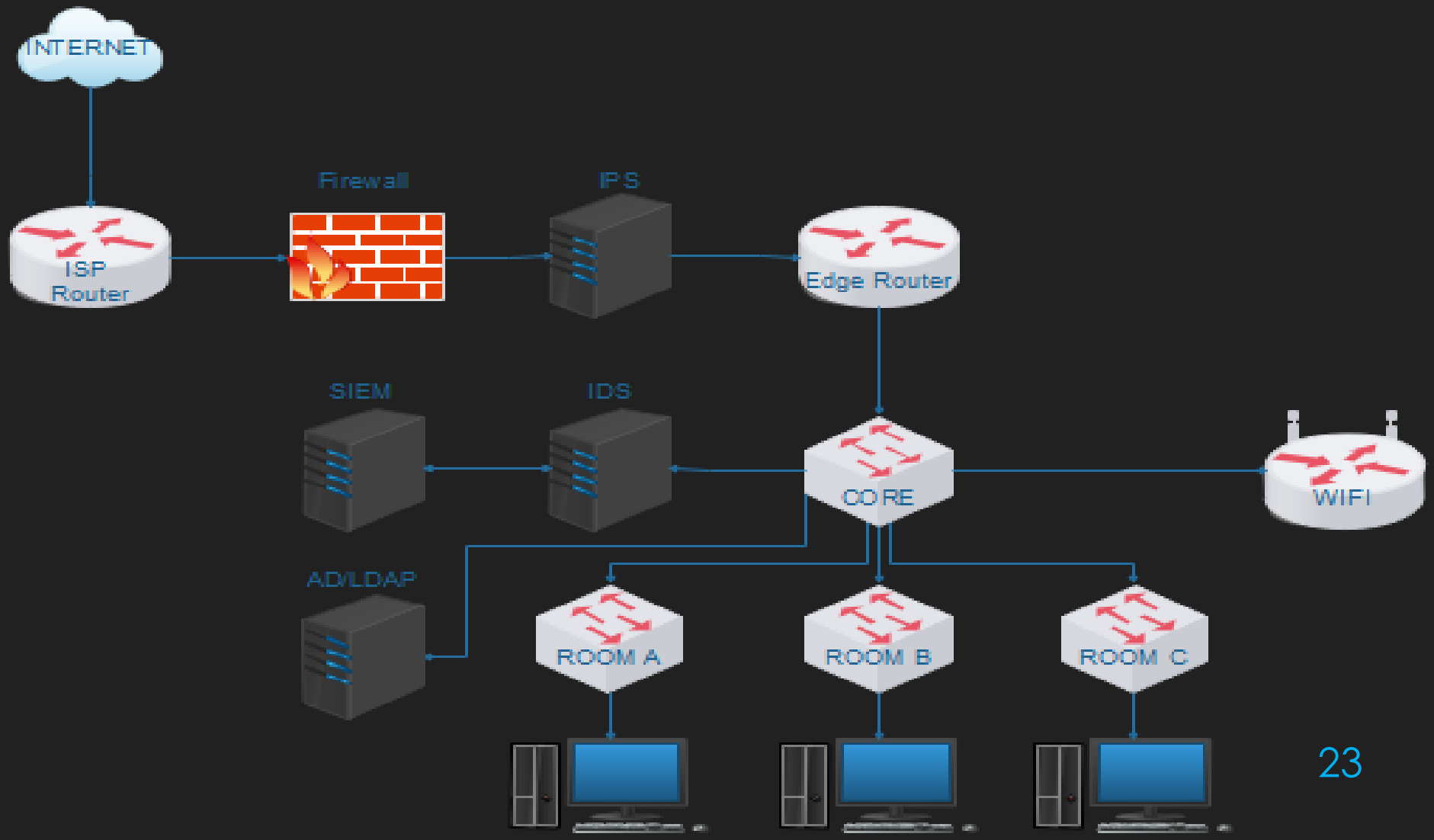
Services Installed

- ISP Router
  - Routing
  - NAT
- Core Switch
  - Switching
- End-user
  - Routing
  - Networking

Pro & Con

- Pro
  - Simple
  - Low Cost
- Con
  - Unmanageable
  - Data can be sniffed
  - All in one broadcast domain
  - Encryption must be applied on the end-user
  - Firewall setup must be applied on the end-user

Hardern Network (1)



Services Installed (1)

- ISP Router
  - Routing
- Firewall
  - NAT
- IPS
  - Filtering Malicious Traffic
- Edge Router
  - Inter-VLAN Routing
  - VLAN Trunking

Services Installed (2)

- Core Switch
  - VLAN
  - Switching
  - Port Mirroring
- IDS
  - Catch All Traffic
  - Give Alert If Intrusion Detected
- SIEM
  - Log Management
  - Convert From RAW Log to Human Readable

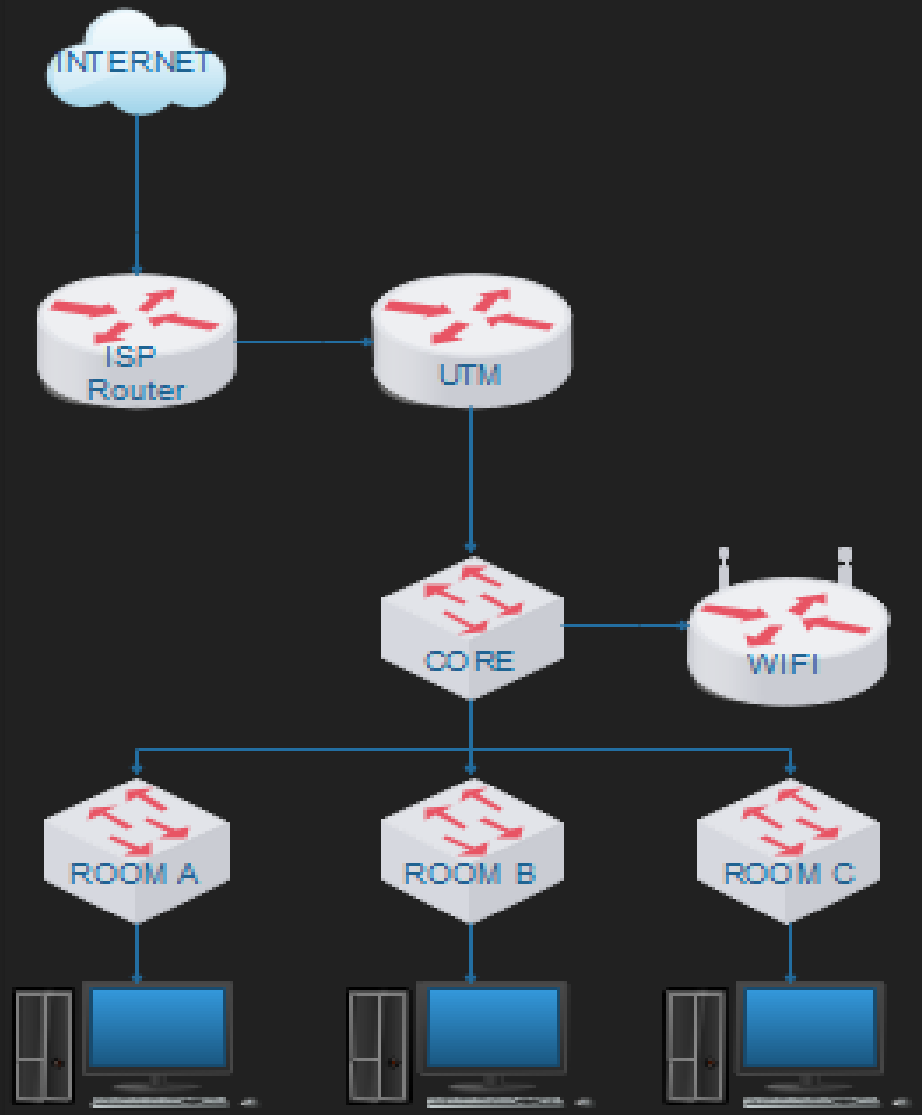
Services Installed (3)

- Active Directory/LDAP
  - Domain Controller
  - Access Control for end-user
- End-user
  - Routing & Networking
  - Domain Group
  - Anti Virus
  - Anti Malware
  - Inernet Security

Pro & Con

- Pro
  - Manageable
  - Different Broadcast Domain (make management easier)
  - More be secure (but not 100%)
  - Encryption can be applied on the network easier
  - Firewall can scan entire network
  - All of traffic can be monitored
- Con
  - Cost
  - Complex
  - Qualified HR Needed

Hardern Network (2)



Services Installed (1)

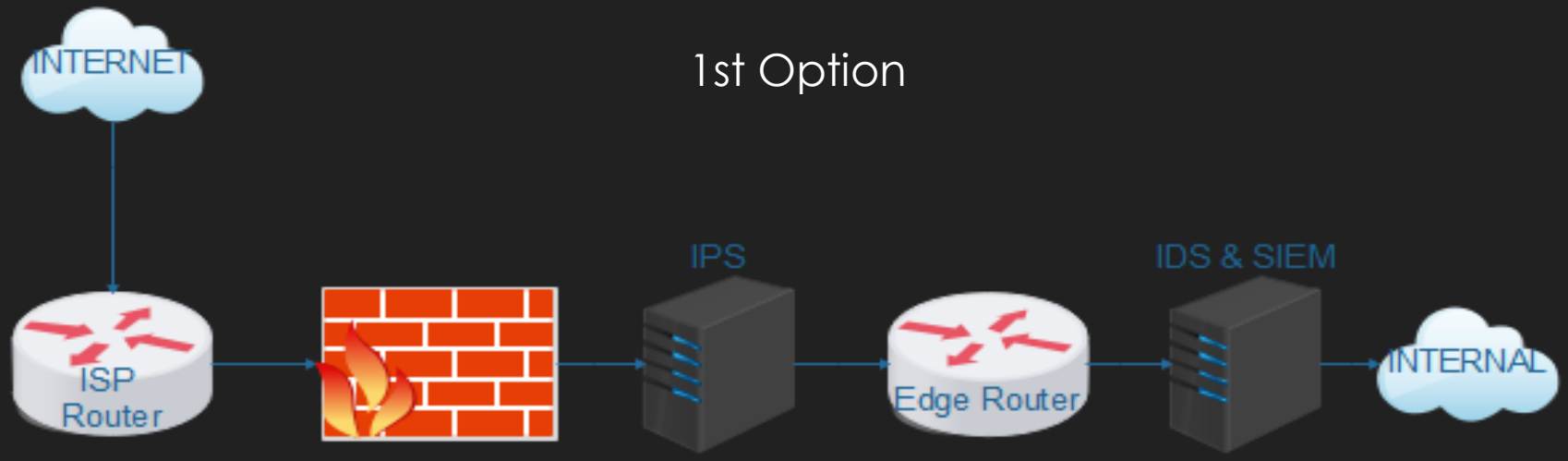
- ISP Router
  - Routing
- Unified Threat Management (UTM) a.k.a. All in One Box
  - Firewall
  - AD/LDAP
  - NAT
  - IDS
  - IPS
  - VLAN Trunking
  - Routing & Inter-VLAN Routing

Services Installed (2)

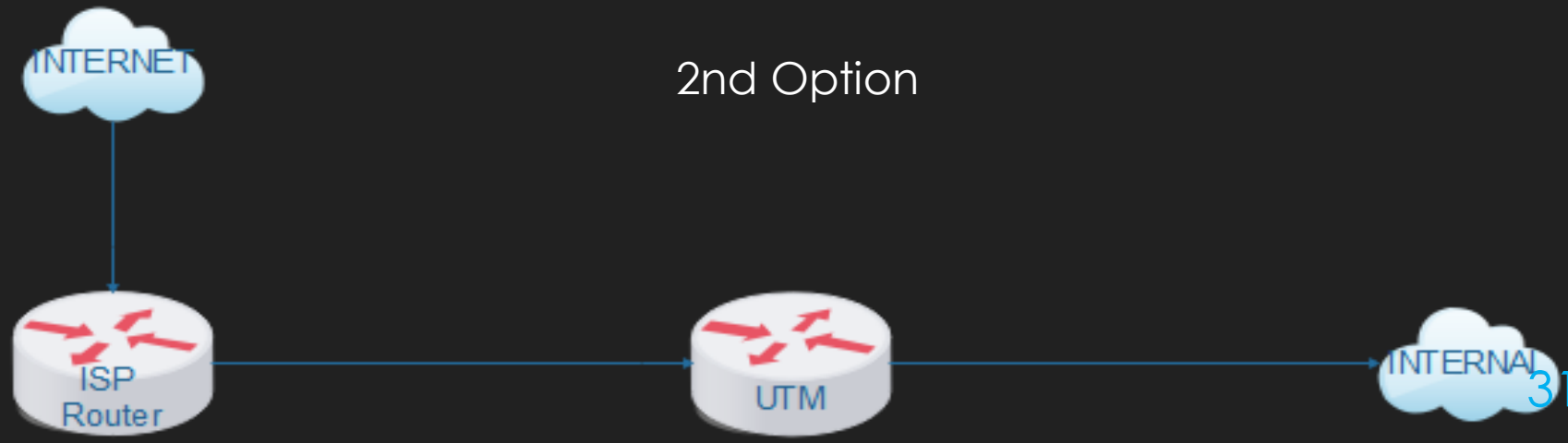
- Core Switch
  - VLAN
  - Switching
- End-user
  - Routing & Networking
  - Domain Group
  - Anti Virus
  - Anti Malware
  - Inernet Security

(FW, IDS, IPS, SIEM) VS UTM

1st Option



2nd Option



Summary

What **Y**ou **S**ee **I**s **W**hat **Y**ou **G**et

&

Secure ≠ Easy

Frequently Asked Question

1. Am i need to buy UTM and all of these services?
   - No, just buy what you need
2. If i want to buy a devices, what brand is good?
   - See gartner survey
3. Am i need to hardening my network?
   - No, if you don't care about your privacy, it's just wasting your money

Help

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


thank
you