Departamento de ENGENHARIA INFORMÁTICA
Instituto Superior de Engenharia do Porto

Systems and Information Security SEGSI

Topic 4

Infrastructure Security

Pinto Leite, Jorge (jpl@isep.ipp.pt)

Infrastructure Security

- When talking about infrastructure security, there are plenty of considerations one is more than probably thinking about
  - Physical access
  - Logical access
  - Running software
  - The infrastructure as a whole
    - Cabled
    - Wi-Fi
    - Actives (routers, switches, etc.)
- Some of the previous points have been discussed previously

Infrastructure Security

- There are some principles to achieve in order to mitigate the risks
  1. Weakest Link Security
  2. Defense in Depth
  3. Secure Failure
  4. Minimal Privilege
  5. Compartmentation
  6. Simplicity
  7. Promote Privacy
  8. Saving Secrets is Hard
  9. Distrust by Default
  10. Use Public Information Sources

Infrastructure Security

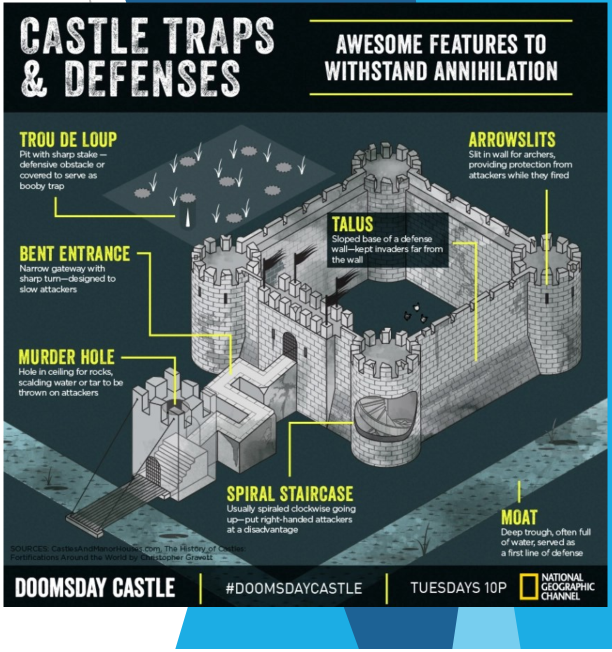
- Before looking more deeply on these principles, consider how one defend their own goods (house, car, etc.)
- The most common defense line is at the border of what is being defended
  - House: doors, windows
  - Car: doors, key, car boot
  - Internet access at home: in the router that divides the internal network from the external
- This kind of security is called *Perimeter Defense*
- The drawback of Perimeter Defense is that if it is breached, all that is inside is compromised
  - Implementing several layers of security provides a better and stronger security as a whole

Infrastructure Security

- Weakest Link Security
  - System and infrastructure security equals the security of the weakest link
    - What is stolen more often? A bank or a supermarket?
    - An attacker tends to look for the weakest points
  - The components that have the greatest risk must be identified
  - Those components should raise the level of safety in order to achieve the best possible and reduce the risk to an acceptable level

Infrastructure Security

- Defense in Depth
  - Defense in Depth is the opposite of perimeter defense
  - In perimeter defense a single layer of security is implemented, usually in the gateway of the perimeter
    - Note that *perimeter* can be thought as a part of the internal infrastructure, does not need to be only the border between internal and external network
  - A single defense can fail or be avoided (or compromised) so it cannot be looked as a strong one
  - Implementing several defense mechanisms allows a more defensible infrastructure because if one mechanism fails, other(s) are in use keeping the infrastructure secure


CASTLE TRAPS & DEFENSES
AWESOME FEATURES TO WITHSTAND ANNIHILATION
TROU DE LOUP
Pit with sharp stake — defensive obstacle or covered to serve as booby trap
ARROWSLITS
Slit in wall for archers, providing protection from attackers while they fired
TALUS
Sloped base of a defense wall—kept invaders far from the wall
BENT ENTRANCE
Narrow gateway with sharp turn—designed to slow attackers
MURDER HOLE
Hole in ceiling for rocks, scalding water or tar to be thrown on attackers
SPIRAL STAIRCASE
Usually spiraled clockwise going up—put right-handed attackers at a disadvantage
MOAT
Deep trough, often full of water, served as a first line of defense
SOURCES: CastlesAndManorHouses.com, The History of Castles: Fortifications Around the World by Christopher Gravett
DOOMSDAY CASTLE
#DOOMSDAYCASTLE
TUESDAYS 10P
NATIONAL GEOGRAPHIC CHANNEL

Your Castle's Defense System
Prevention
First Line of Defense
Social Distancing
(Walls & Moat)
Handwashing
("Rain of Arrows")
Mask
(Gate/Drawbridge)
Internal Defense
(Walls are Breached!)
Healthy Weight,
Diet & Exercise
(Inner Wall &
Courtyard)
Stress Management &
Restorative Sleep
(Towers and Residence)
Strong Immune
System
(Knights and Archers)

Infrastructure Security

- Secure Failure
  - In the event of a failure on a component, that infrastructure component should go to a safe state
  - All components might fail
  - If a router is compromised, it is better to turn it off that to have an open path to the interior of our infrastructure
  - And if a system or process is compromised, turn it off is again preferable
  - The point here is how to detect a failure on any component that is essential to the normal functioning of the infrastructure

Infrastructure Security

- Minimal Privilege
  - Only the minimum permissions required to carry out an operation should be assigned for the minimum possible time
  - When we assign any type of permissions to a component, we always incur some risk
    - In a Bank, does everyone have the combination of the main safe?
  - If a particular application is just going to do query operations, why assign it write permissions?
  - Laziness often works against this principle
    - "But the X application does not work if it does not run as admin ..."
    - Which group(s) does the user who uses the computer belong to?

Infrastructure Security

- Compartmentation
  - Split the infrastructure into different units, to isolate components with access privileges
  - It allows the principle of least privilege to be applied more effectively
  - How is a modern submarine built? Why?
  - Example
    - Monolithic versus Modular approach

Infrastructure Security

- Simplicity
  - Complexity increases risks, so avoiding complexity is avoiding problems
  - Functionality
    - Include an interesting but insecure functionality?
  - Ease of Use
    - May collide with safety
  - However
    - Building a system without cryptography is simpler than one with…
    - And the principle of defense in depth?
  - *There are two ways to make a system. One is to make it so simple that there are obviously no deficiencies. The other is to make it so complex that there are no obvious deficiencies.* (adapted from C.A.R. Hoare)

Infrastructure Security

- Promote Privacy
  - Privacy is often seen as a security concern
  - Protect information about users very carefully (GDPR)
  - Privacy versus Ease of Use
  - System privacy?
    - What services are working?
    - What information does each of these provide?
    - How the system works?

Infrastructure Security

- Saving Secrets is Hard
  - Try to keep as few secrets as possible as they tend to escape
  - Assume the attacker can know everything we know
    - How the infrastructure is
    - How the application is structured
    - The application code
  - Security should not depend on the secret of the mechanism
  - Security through ignorance typically does not serve as a general principle
    - But can help (examples?)

Infrastructure Security

- Distrust by Default
  - Trust relationships are established between entities that mutually believe that they have certain properties
    - The company employees do not try to subvert the security policies
    - The operating system manages memory in a certain way
    - The corresponding application always sends information correctly
  - Should we trust an application just because it is advertised as using 512-bit encryption?
    - Do not rely on data from outside
  - Confidence misplaced
    - A Web application uses the user's browser to prevent malicious information from being entered

Infrastructure Security

- Use Public Information Sources
    - Public scrutiny is usually very important
    - Cryptography is a good example
        - Which cryptographic algorithm do you prefer?
            - AES or Ultra Secure Encryption, a secret algorithm invented by a company?
    - Use libraries of functions considered secure
        - Not to do with open source, but rather with scrutinized code
    - Rule: Do not invent cryptographic algorithms!

Infrastructure Security

- Specifically to the infrastructure, some more aspects must be kept in mind
  1. Authentication of source data
  2. Authorization of commands
  3. Message Integrity Protection
  4. Message repetition prevention
  5. Confidentiality of data
  6. Distribution of keys
  7. Reliability versus trust

Infrastructure Security

- Authentication of source data
  - Ensure the data may have been issued only by the correct equipment
  - Use encryption, hashes, MACs, etc.
  - Use public key infrastructures
  - Use mixed solutions based on previous
- Authorization of commands
  - Only allow the execution of previously determined commands
  - Ignore all other "commands"
  - Default network mistrust

Infrastructure Security

- Message Integrity Protection
  - Current protection methods include the entire message whereby changing data invalidates the entire packet
- Message Repetition Prevention
  - Prevent a captured legitimate message from being replayed later
  - Use timestamping and clock synchronization
  - Use session testimonials to ensure authenticity of stakeholders

Infrastructure Security

- Confidentiality of data
  - Use encryption on the data to be transmitted
  - Use symmetric ciphers (and even MACs)
  - Use public key systems
  - Use mixed solutions
- Distribution of keys
  - Use public key systems
    - Allows safe distribution of symmetric keys
  - Avoid using default keys
    - Some systems may be induced to an initial state using default keys, which are known to everyone

Infrastructure Security

- Reliability versus trust
  - They are not the same thing!
  - A reliable system is not at risk
  - A trusted system may not be reliable (in the case of a poorly managed PKI system)
  - How do you know if a system is reliable?

Infrastructure Security

- With all these principles, a definition of the trust perimeters of our infrastructure can be made
  - Frontiers with other networks
    - Internet access
    - Remote access
    - Related organizations
    - Other organizations
  - Boundaries within our infrastructure
    - Servers / Workstations
    - Demilitarized zones
- Whatever zone is considered, trust is never complete (100%)

Infrastructure Security

- A subverted system can compromise other systems on same network
- If it is contained on a single segment, the damage is lower and more controllable
- As a consequence, there is a need to create zones of trust even inside the internal infrastructure
- And define rigid security policies for the entire infrastructure and specifically for each zone

Infrastructure Security

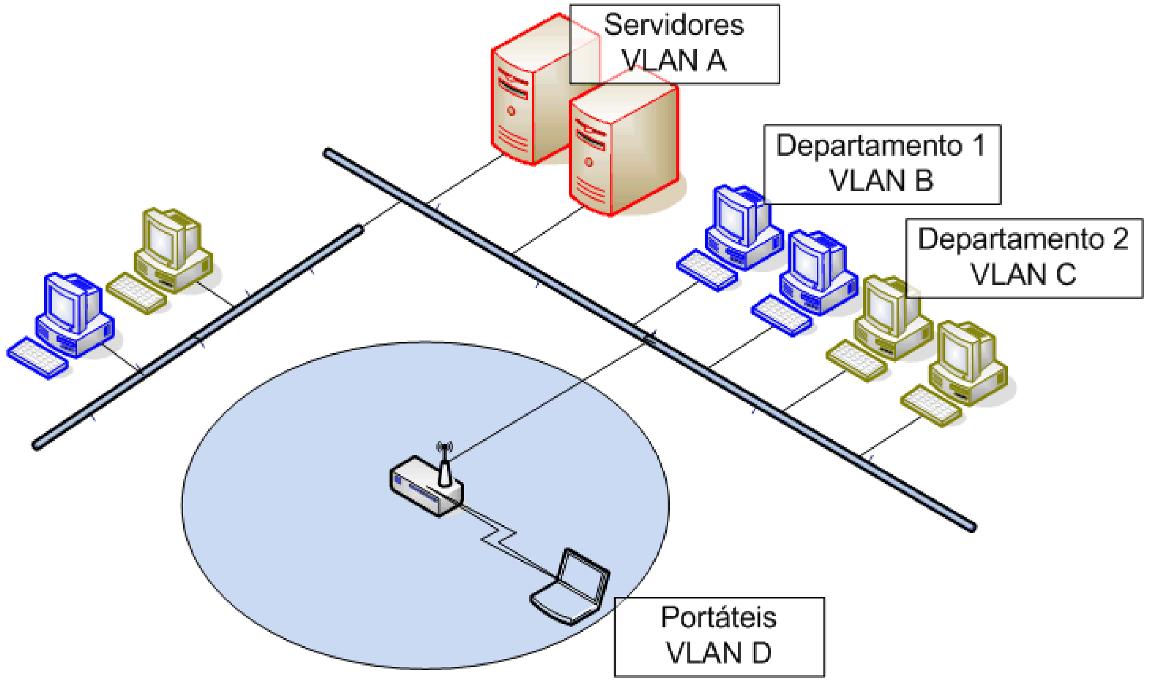
- The regular use of a perimeter defense can and should be used
  - For Internet access
  - For other companies / branches
- It is crucial to safeguard the defense of the perimeter
  - External networks can be attacked and used without the knowledge of their administrators
  - The administrators of other networks make mistakes
  - Users of other networks can subvert the security of these networks.

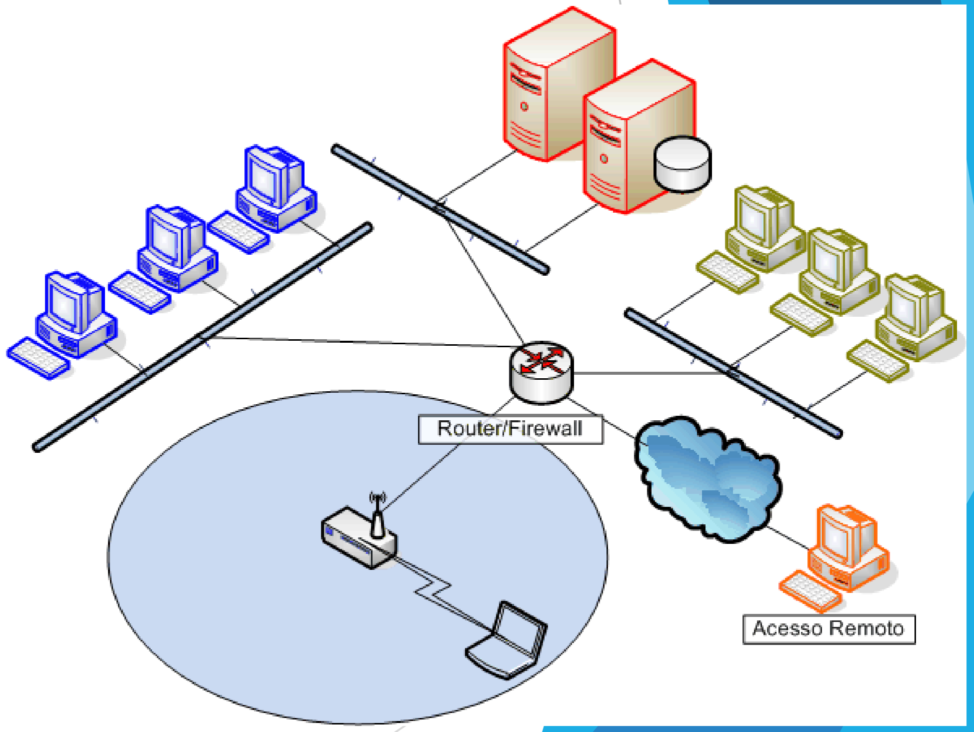
Infrastructure Security

- Cares to be taken
  - Network design
    - Separate properly in safety zones
    - Carefully pondering the use of wireless networks
  - Use of firewalls
    - Set permitted traffic and deny everything else
    - Mainly monitor the services allowed
  - Monitoring the firewall
    - VPNs not provided
    - Tunnels of protocols not foreseen
  - Use of intrusion detection systems (IDS) or intrusion prevention systems (IPS)
  - Periodic execution of external audits
    - Penetration tests (with prior legal consent)

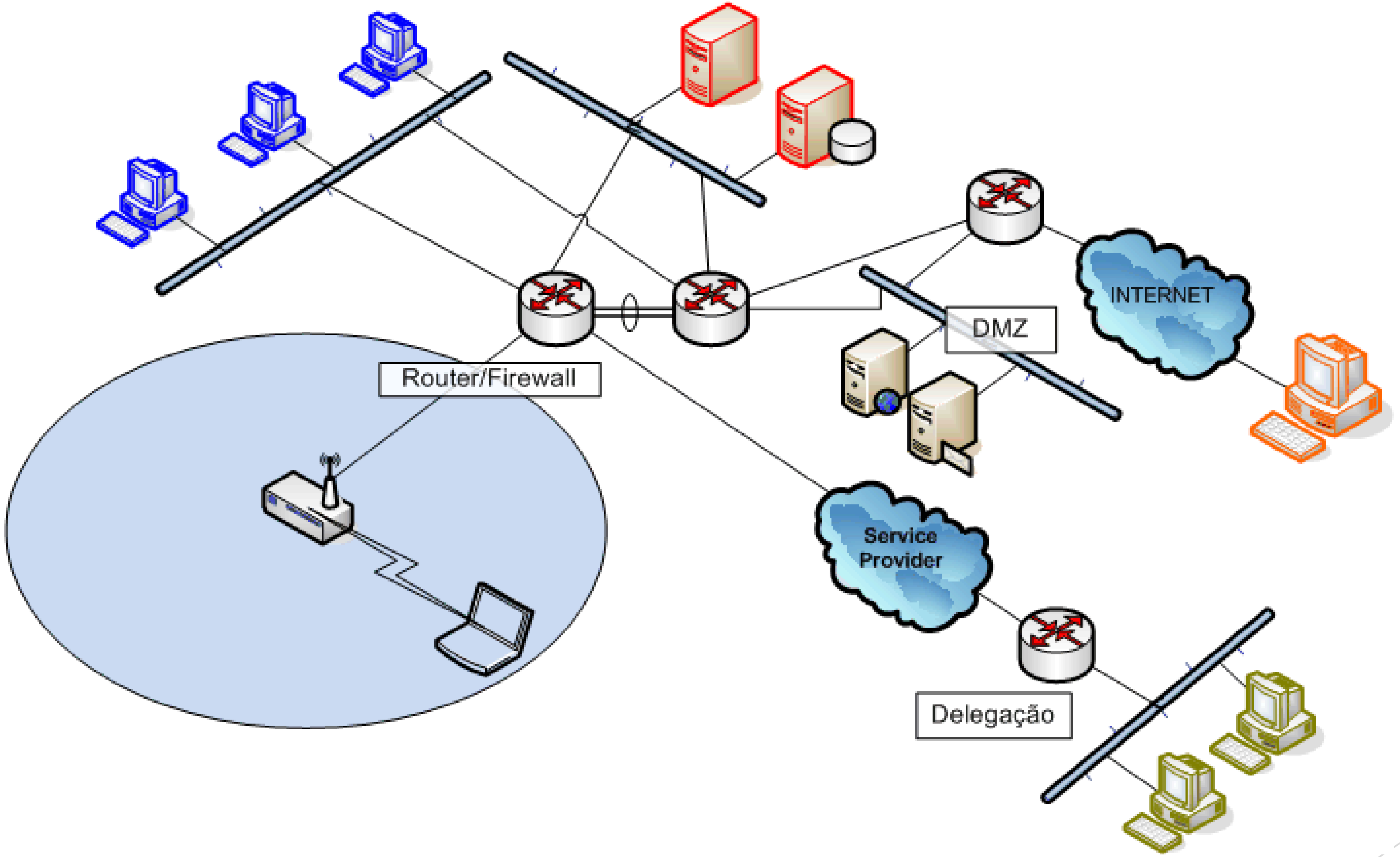
Infrastructure Security

- *Compartmentation* refers having a frontier between each defined trust zone





Infrastructure Security



Infrastructure Security

- What about wireless networks?
  - Where is the perimeter?
  - Enhance security
    - Put the wireless network on a separate IP subnet through a restrictive firewall
    - Reduce signal power to minimum
    - Use only the latest protocols available and tested
    - IEEE 802.1x (network access control)
    - Use VPN-like solution

Infrastructure Security

- As a more complete separator of trust zones, a firewall is usually used (and perhaps the best component)
- In terms of operation mode firewalls might be:
  - Stateless (or packet-filtering)
  - Circuit-level
  - Stateful
  - Proxy (or application-level)
  - Next- generation

Infrastructure Security

- Stateless
  - Pros
    - Do not maintain state of the connections
    - Filtering is static and based on packet headers
    - Low resource consumption
    - Minimal impact on network
  - Cons
    - No analysis of packets payload (the *real* data)
    - Vulnerable to Denial of Service (DoS)

Infrastructure Security

- Circuit-level
  - Pros
    - Operates at layer 5 (session) of OSI model
    - Monitors TCP handshakes between local and remote hosts
    - Only process requested transactions and reject all other traffic
    - Minimum impact on end-user experience
  - Cons
    - Should not be the only firewall as it does not filters content
    - Often requires tweaks on software and network protocol

Infrastructure Security

- Stateful
  - Pros
    - Maintain state of the connections, thus considers previously inspected packets
    - Allows stopping majority of attacks to protocol flaws
    - Detailed logging capabilities
  - Cons
    - More expensive
    - High knowledge needed to configure
    - Heavy processing, with impact on performance
    - No authentication support
    - Vulnerable to TCP flood attacks that take advantage of pre-established connections

Infrastructure Security

- Proxy (or application-level)
  - Pros
    - Allows Deep Packet Inspection (DPI) that checks both packet headers and payloads
    - Add an extra layer of separation between clients and network
    - Fine-grained security controls over network traffic
    - Conceal internal IP addresses from potential threat actors
  - Cons
    - Increased latency due to thorough packet checks and extra communication steps
    - Not as cost-effective as other types of firewalls due to high processing overhead
    - Difficult to configure and manage
    - Not compatible with every network protocols

Infrastructure Security

- Next-generation
  - Pros
    - Deep packet inspection that analyzes the traffic's content
    - TCP handshake checks
    - Surface-level packet inspection
    - Includes Intrusion Detection System (IDS) and / or Intrusion Prevention System (IPS)
    - Includes malware detection
    - Advanced threat intelligence (reputation-based detection, anomaly-based detection, etc.)
  - Cons
    - A massive single point of failure
    - Slow deployment time
    - Require a high degree of expertise to set up and run
    - Hindered network performance

Infrastructure Security

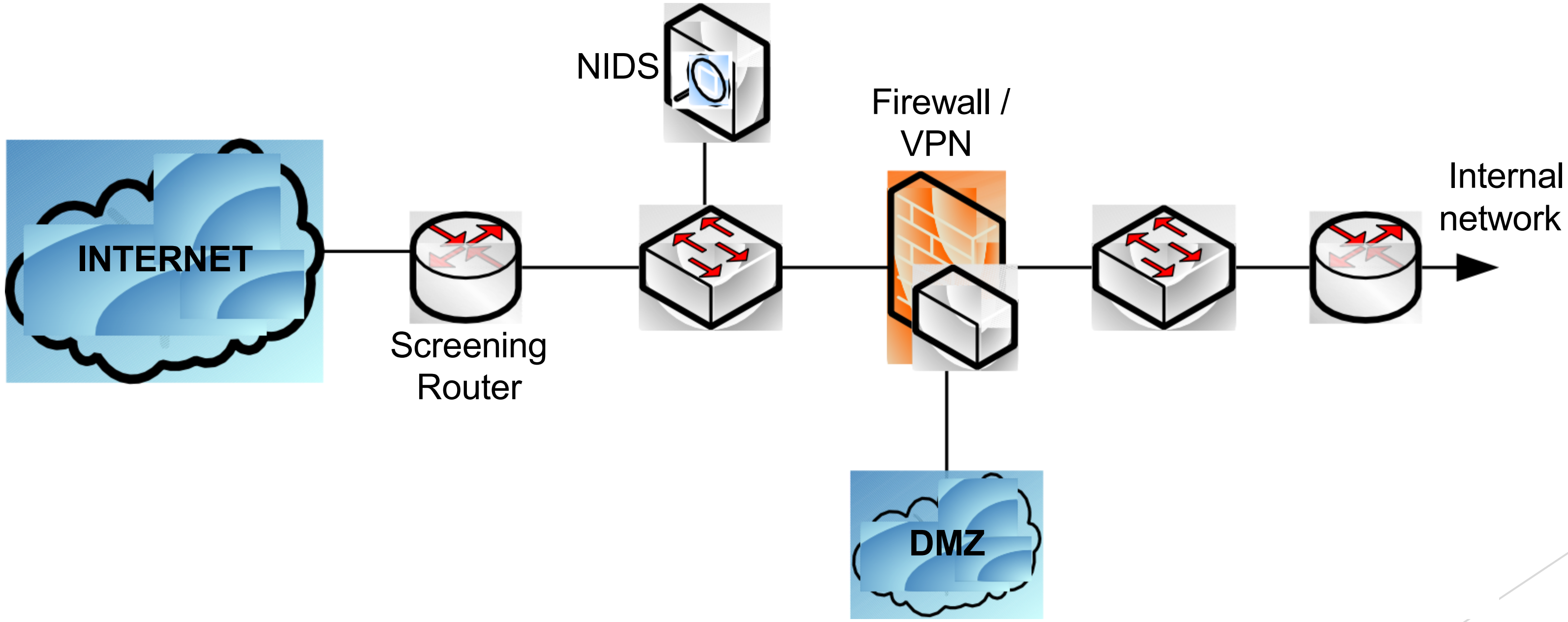
- Intrusion Detection System (IDS)
  - An IDS is a system that monitors traffic in order to detect recognized patterns or signatures of malware
  - When detecting that sort of traffic they generate an alert
  - In a Security Operations Center (SOC) it is expected that the alert is seen and will be investigated by an analyst
- Intrusion Prevention System (IPS)
  - Same mode of operation of the IDS plus blocking the suspected packet
- A tradeoff between system availability and usability should be considered
  - An IDS leaves a window for an attacker to cause damage to a target system
  - An IPS when misjudging a packet will impact negatively the system usability

Infrastructure Security

- Intrusion Detection System (IDS)
  - An IDS is a system that monitors traffic in order to detect recognized patterns or signatures of malware
  - When detecting that sort of traffic they generate an alert
  - In a Security Operations Center (SOC) it is expected that the alert is seen and will be investigated by an analyst
- Intrusion Prevention System (IPS)
  - Same mode of operation of the IDS plus blocking the suspected packet
- Both systems might be system-based or network-based
- In this last option, is usually called Network IDS (NIDS) or Network IPS (NIPS)
  - Examples: Snort or Suricata, among others

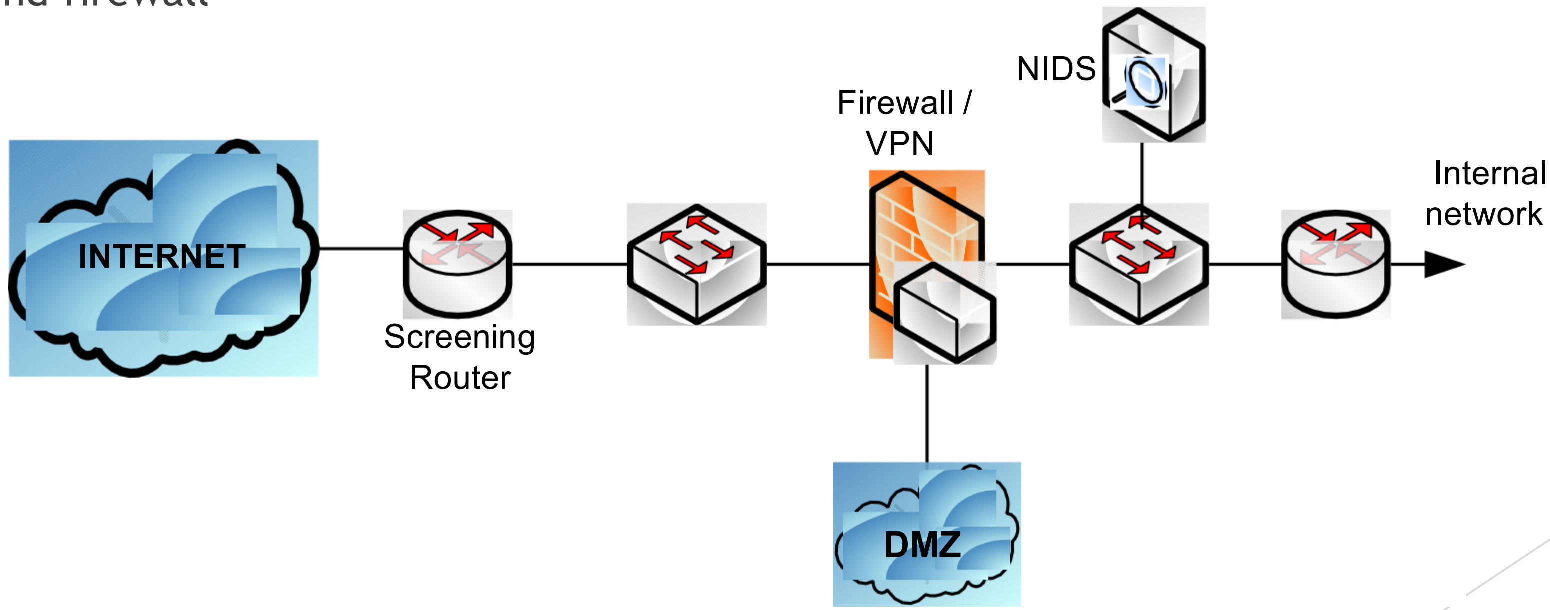
Infrastructure Security

- Assuming always a NIDS type, its position can vary according to what is expected
  - In front of firewall



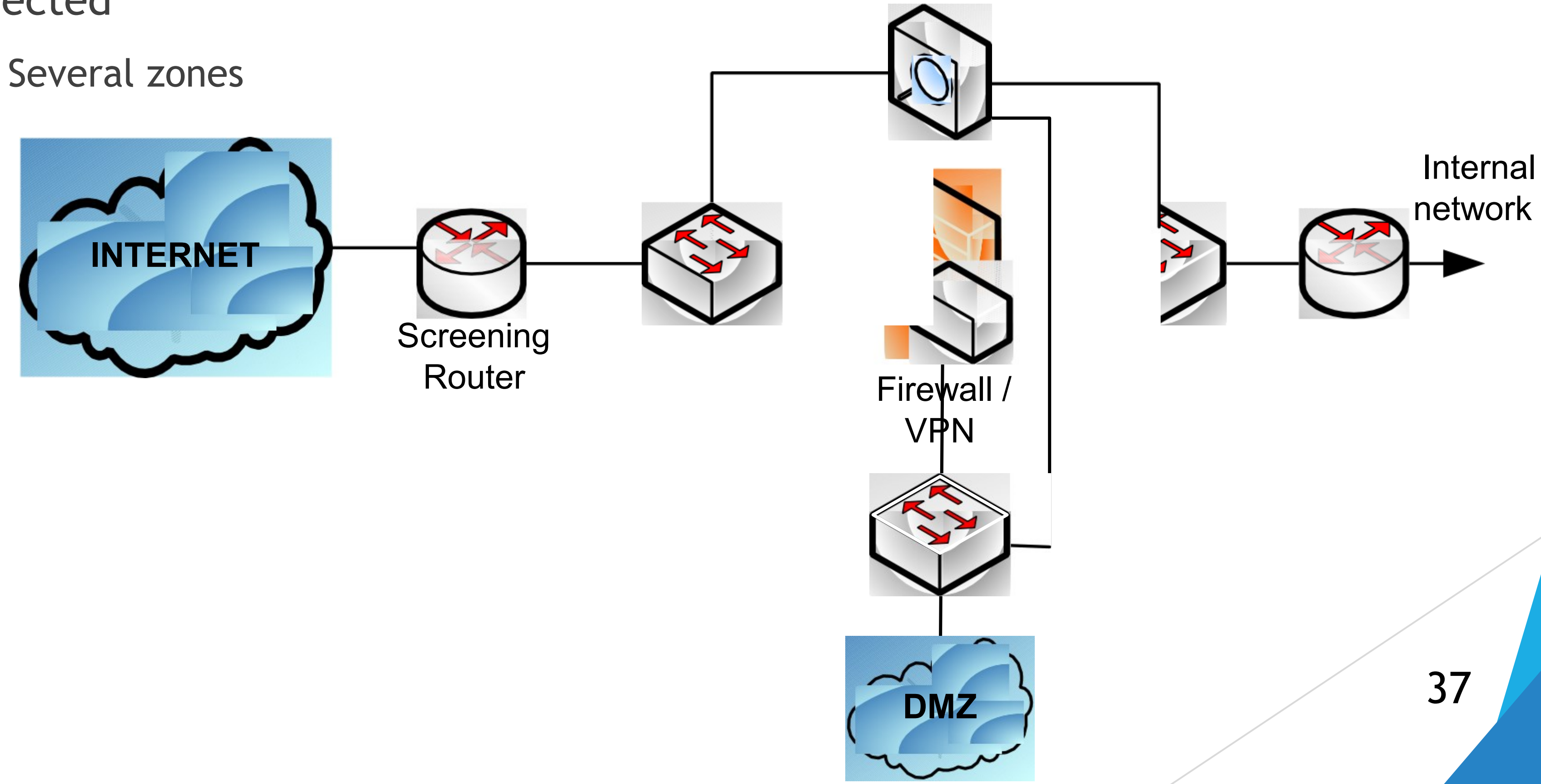
Infrastructure Security

- Assuming always a NIDS type, its position can vary according to what is expected
  - Behind firewall



Infrastructure Security

- Assuming always a NIDS type, its position can vary according to what is expected
  - Several zones



Infrastructure Security

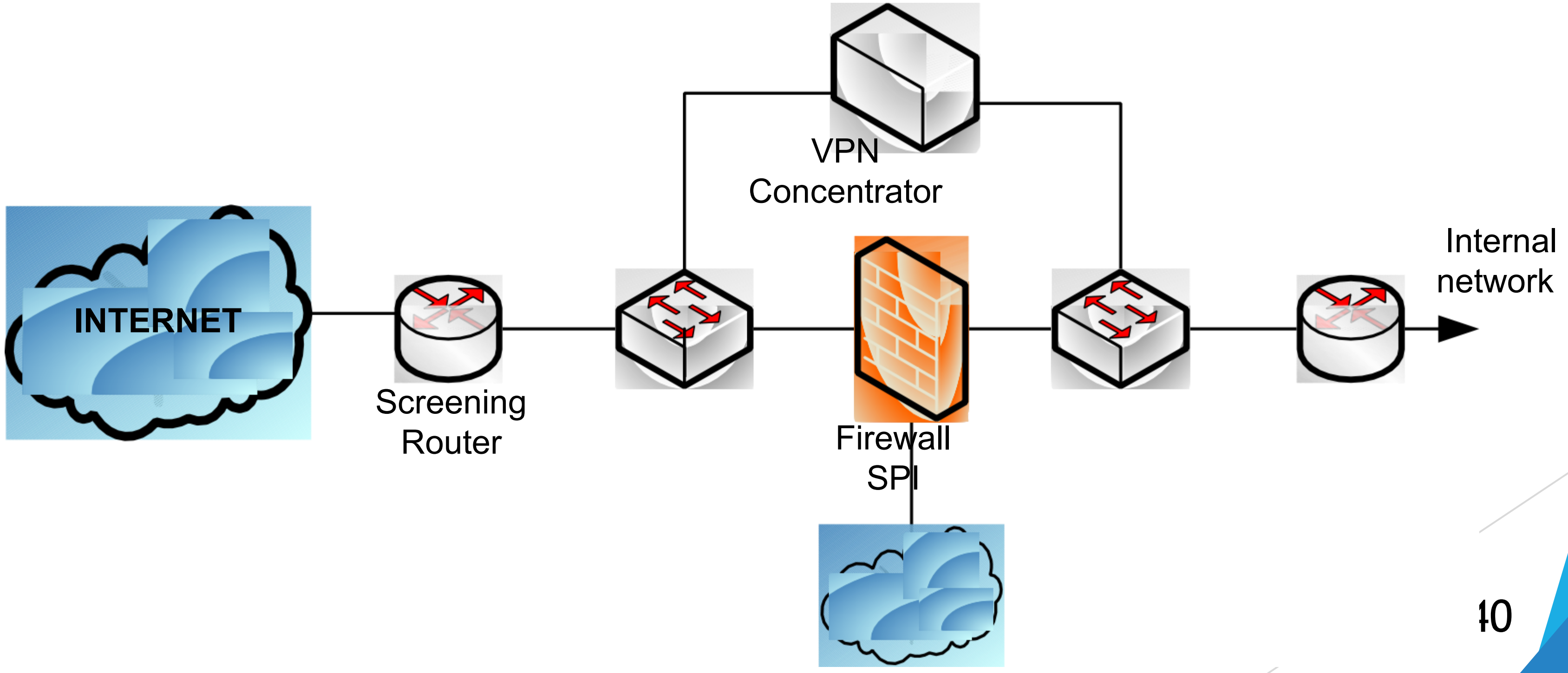
- When there is a need to protect traffic between end points, a Virtual Private Network (VPN) is mandatory
- When should one use a VPN?
  - By common sense, when exchanging sensitive (confidential, private, etc.) data remotely
  - Also, when exchanging sensitive data inside the network
    - It cannot be assumed that no one by accident or proposedly will capture the data
- It is not in this class scope to analyze and describe the actual VPN methods

Infrastructure Security

- Mention only that in abstract terms VPN might be divided into
  - The ones that do not require an app client to be installed on the client system
  - The ones that require an app client to be installed on the client system
- There is obviously an impact of VPN usage on the overall infrastructure
- Yet, for the ones that requires an app client to be installed on the client system there is also an impact on the client system performance
- Is this a potential flaw?

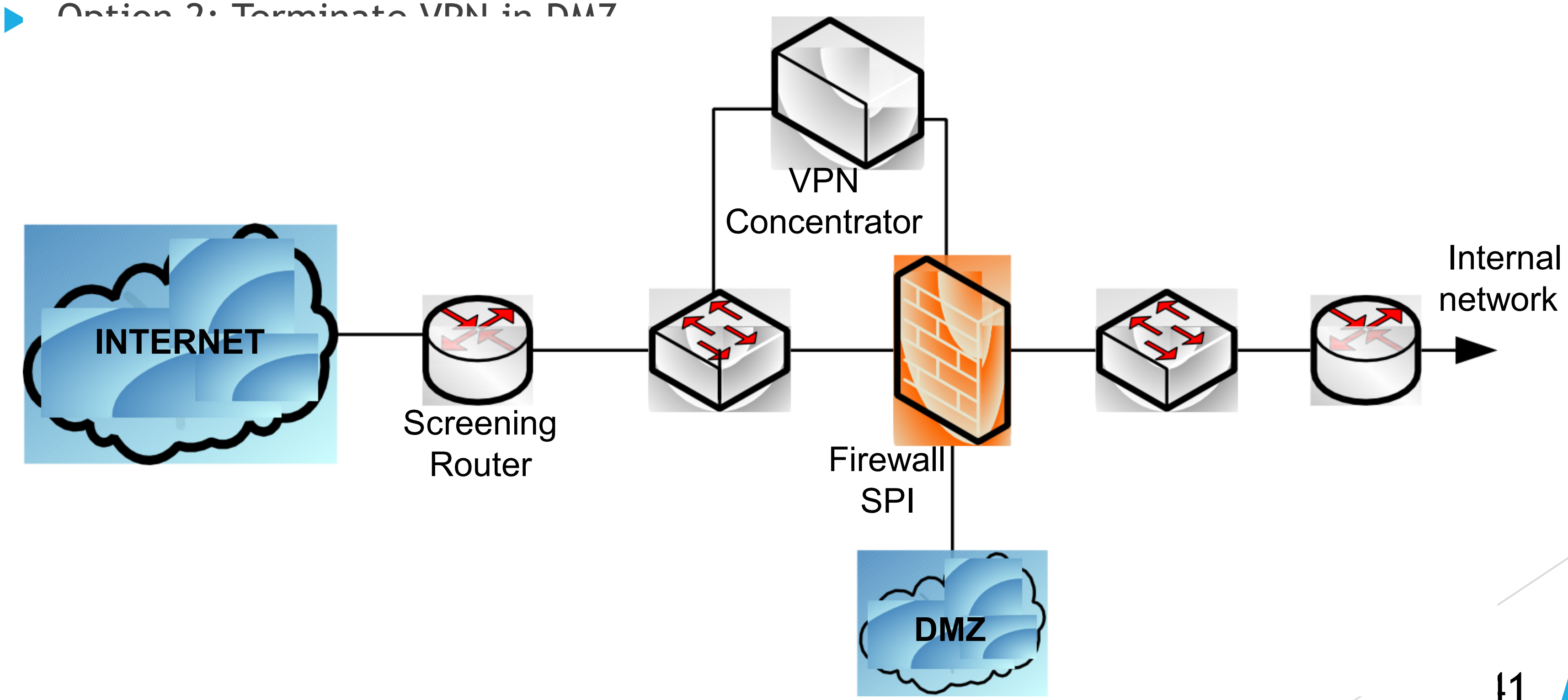
Infrastructure Security

- Considering how the VPN traffic circulates, more than one option is possible
  - Option 1: VPN in parallel with the firewall



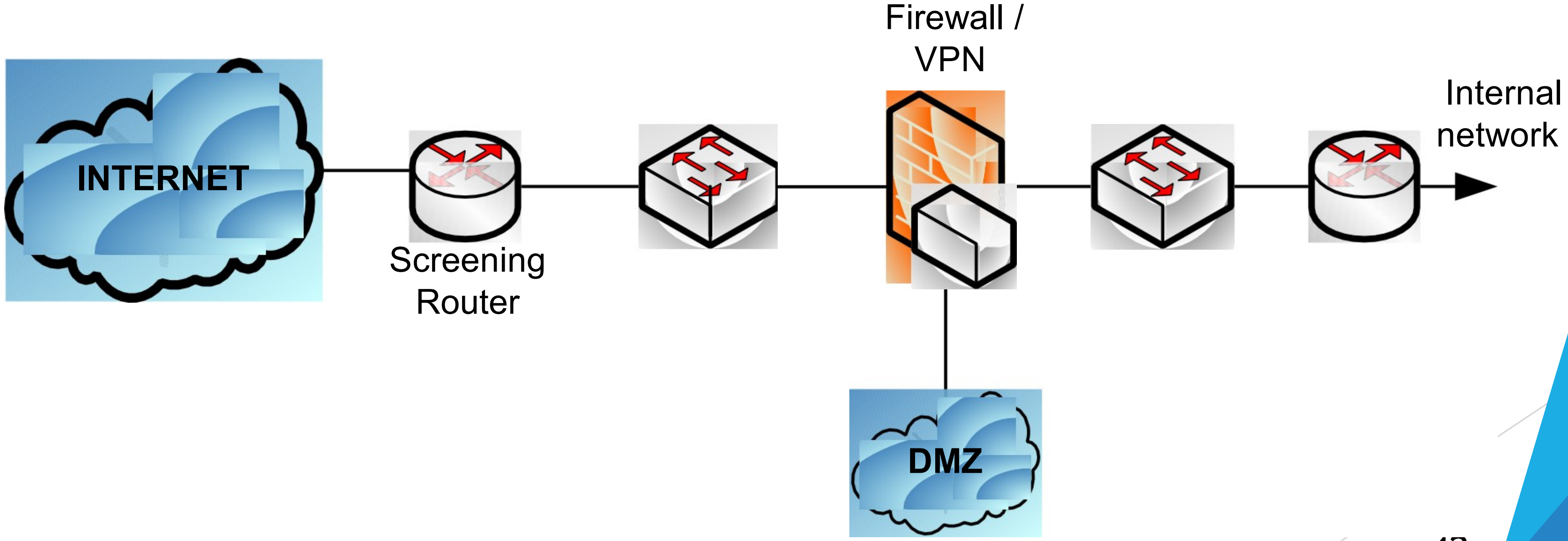
Infrastructure Security

- Considering how the VPN traffic circulates, more than one option is possible
  - Option 2: Terminate VPN in DMZ



Infrastructure Security

- Considering how the VPN traffic circulates, more than one option is possible
  - Option 3: Firewall / I[DP]S integrated with VPN DMZ


Firewall / VPN
INTERNET
Internal network
Screening Router
DMZ