Network Flow Control

Segurança em Redes de Comunicações

Mestrado em Cibersegurança

Mestrado em Engenharia de Computadores e Telemática

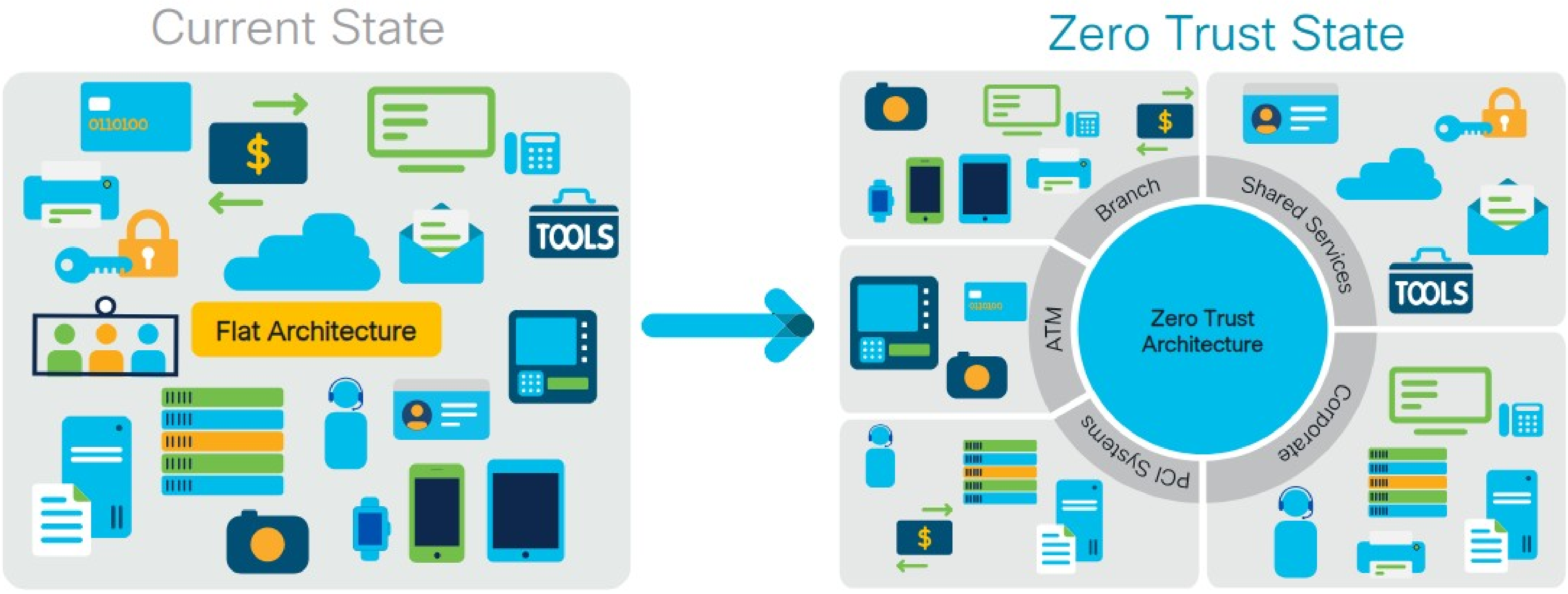
DETI-UA

universidade de aveiro

deti.ua.pt

Network (micro-)segmentation

- One of the concepts to create a Zero Trust Architecture
- Security strategy that divides a network into smaller and isolated segments.
- Can be achieved by creating data flow boundaries and enforcing strict controls between different segments.



As Published by Cisco Press Book: "Zero Trust Architecture"

Firewalls

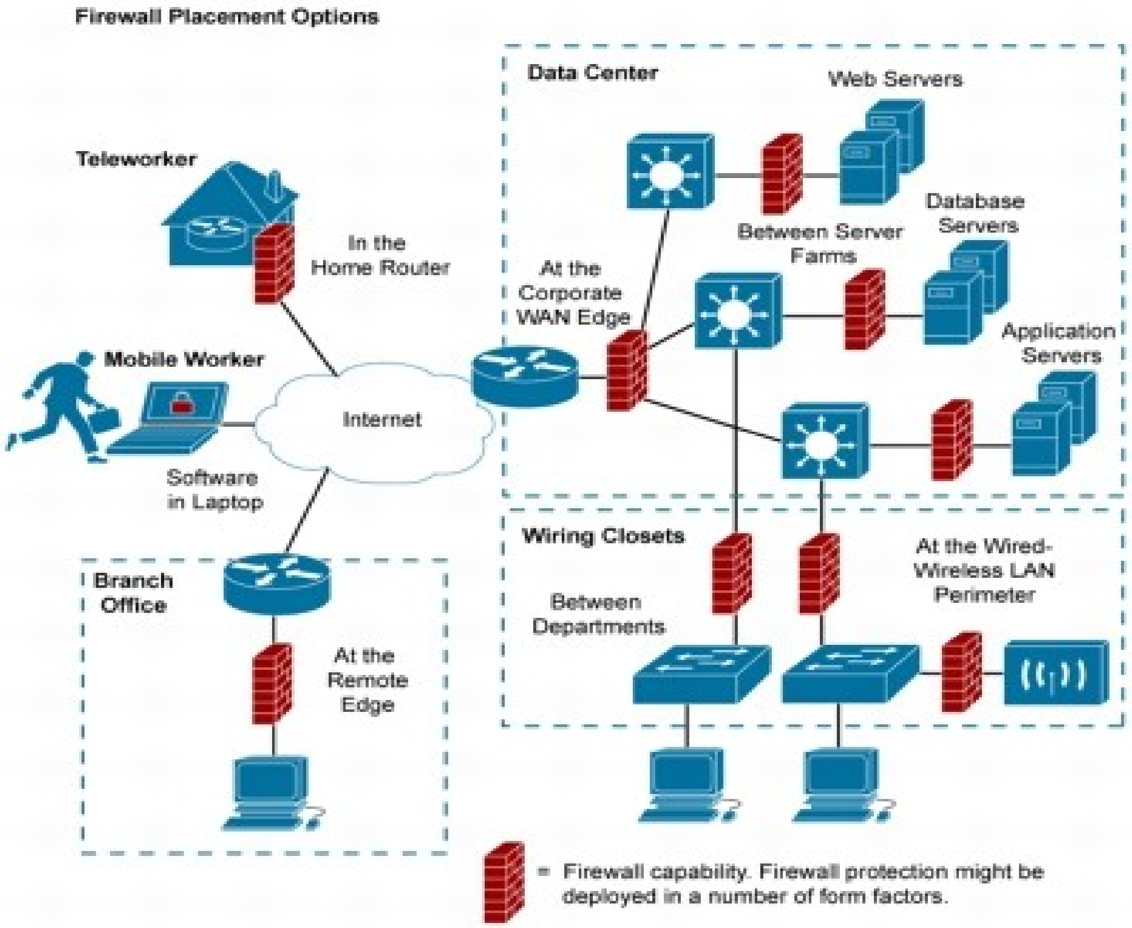
- A firewall provides a single point of defense between networks and protects one network from the others.
- It is a system or group of systems that enforces a control policy between two or more networks (access control, flow control and content control).
- It is a network gateway that enforces the rules of network security.
- Minimizes local vulnerabilities.
- Evaluates each network packet against the policies of network security.
- Can monitor all the network traffic and alert to any attempts to bypass security or to any patterns of inappropriate use.
- Can be hardware or software based.

Firewalls Security/Network Services

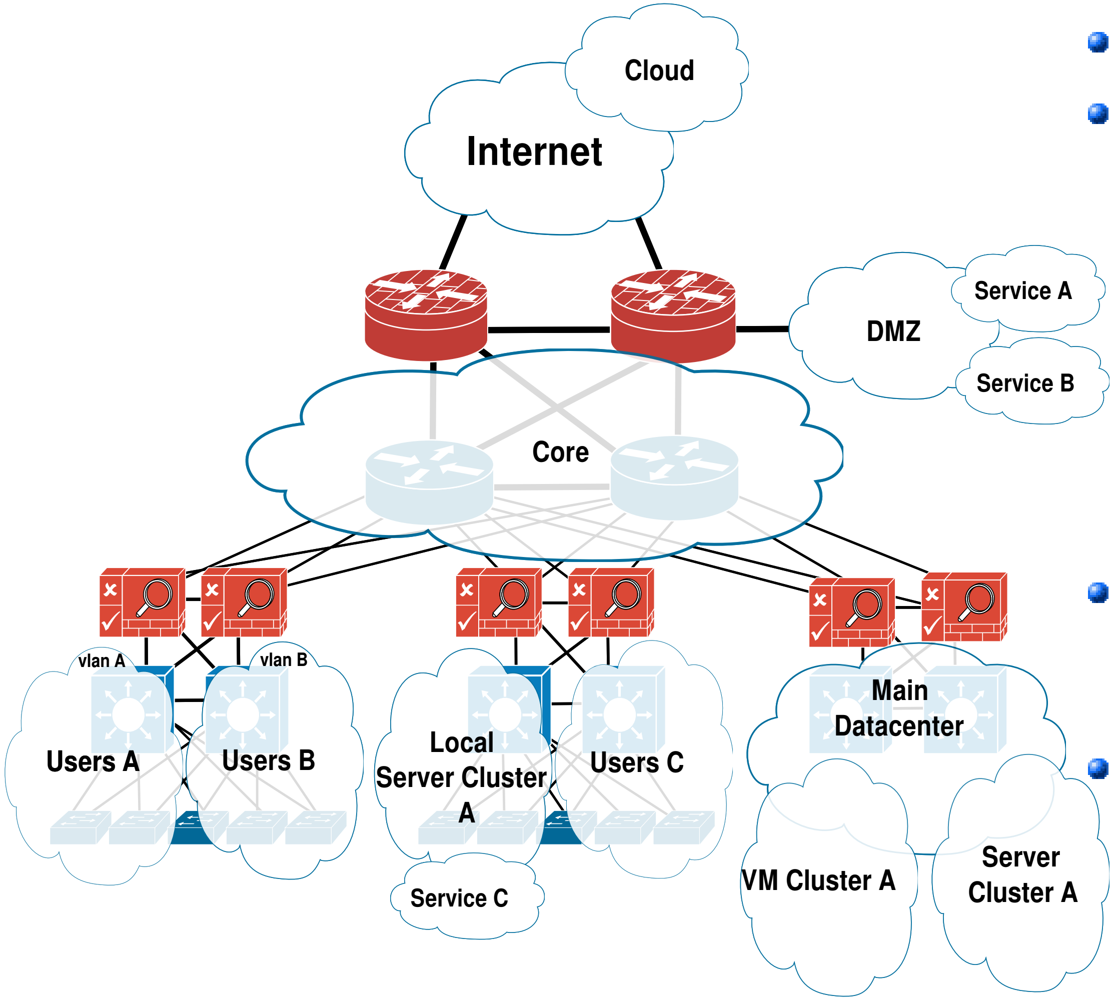
- NAT (Network Address Translation).
- Authorization
  - Flows (packet filtering).
  - Users (application and circuit level).
- Redirecting.
  - To specif machines.
  - Proxing.
- Content analysis.
- Secure communication.
  - Site-to-site VPN.
    - IPsec.
  - Remote-access VPN.
- DoS and DDoS detection and defense.

Deploying Firewalls

- Zero Trust imposes that network must have micro-segmentation.
- Network must be controlled at multiple levels and locations



Firewall Zones/Segments/Groups



- A network must be micro-segmented.
- Must be divided in multiple zones/segments/groups with different security levels.
  - Collections of network ports, IP addresses, IP networks, service ports, Security Group Tags (SGT), other IDs.
  - Some firewalls only allow zones defined by interface name. Other IDs only used to define traffic source/destination.
- Once created, a group can be referenced by firewall rules as either a source or destination.
- Example: a Demilitarized Zone (DMZ) is a perimeter network outside the protected internal/private network
  - Used to place public servers/services.
  - The DMZ is a "semi-protected" Zone.
    - It must be assumed that any machine placed on the DMZ is at risk.

Types of Firewalls

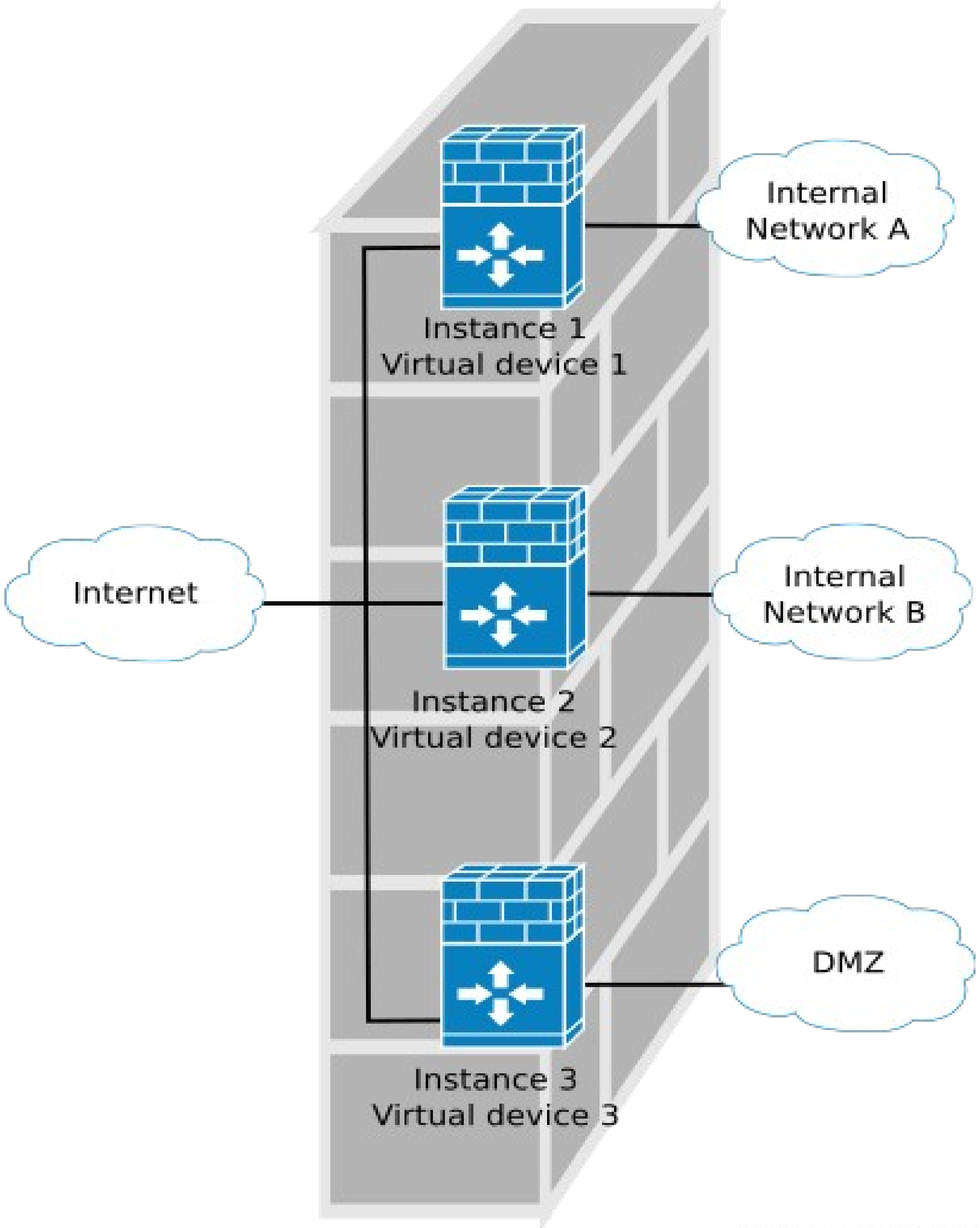
- Network-Level Firewalls (L2/L3)
    - Packet filtering
    - Inspecting packet headers and filtering traffic based on
        - the IP address of the source and the destination, the port and the service (L3)
        - source and the destination MAC addresses (L2)
- Circuit-Level Firewalls (L4)
    - Monitor TCP handshaking between packets to make sure a session is legitimate
    - Traffic is filtered based on specified session rules
- Application-Level Firewalls (L4+)
    - Application-level firewalls are sometimes called proxies
    - Looking more deeply into the application data
    - Consider the context of client requests and application responses
    - Attempt to enforce correct application behavior and block malicious activity
    - Application-level filtering may include protection against Spam and viruses as well, and block undesirable Web sites based on content rather than just their IP address
    - Slow and resources consuming tasks
- Stateful Multi-level Firewalls (L*)
    - Filter packets at the network level and they recognize and process application-level data
    - Since they don't employ proxies, they have reasonably good performance even performing deep packet analysis
- Host Level / Personal Firewalls
    - Act only within a specif host
    - Filter all communication layers
    - Control OS processes/applications

Stateful vs. Stateless Firewalls

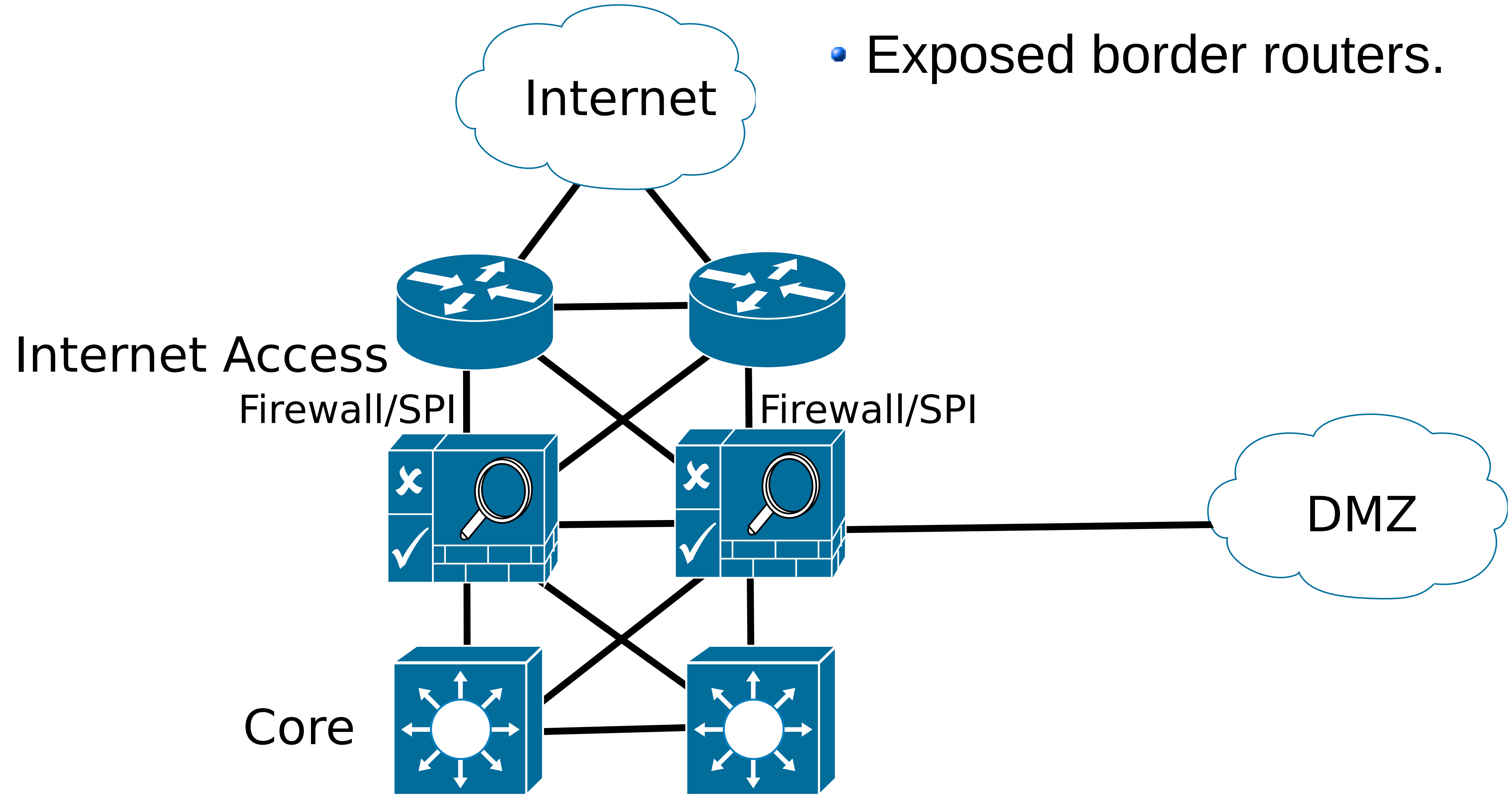
- Stateless firewalls
  - Controls traffic by applying rules to single frames/packets
    - Does not need to track traffic flows/sessions.
  - Rules based on specific values on frames/packet available headers.
    - Set of basic permit/deny actions for input and output based on IP addresses, UDP/TCP ports, etc…
    - Usually called ACL (Access List).
  - They are fast and consume very low computing resources.
    - Perform well under heavy traffic load.
    - Ideal to defense against DDoS attacks in the first line of network defense.
    - Cost-effective compared with stateful firewall types.
- Stateful firewalls
  - Monitor all traffic flows/sessions.
  - Controls traffic based on the connection state of a flow/session.
    - Automatic bidirectional rules (reflexive rules).
  - Connection state is maintained in a state table.
    - State tables must be synchronized with other firewalls when in a redundant scenario (load balancing) or high-availability scenario (backup upon failure).

Firewall Virtual Instances

- Firewalls may have (theoretical) isolated instances to handle different zones/groups.
- Each instance is a virtual device that can perform flow control, switch, and/or routing.


Internal Network A
Instance 1 Virtual device 1
Internet
Internal Network B
Instance 2 Virtual device 2
DMZ
Instance 3 Virtual device 3

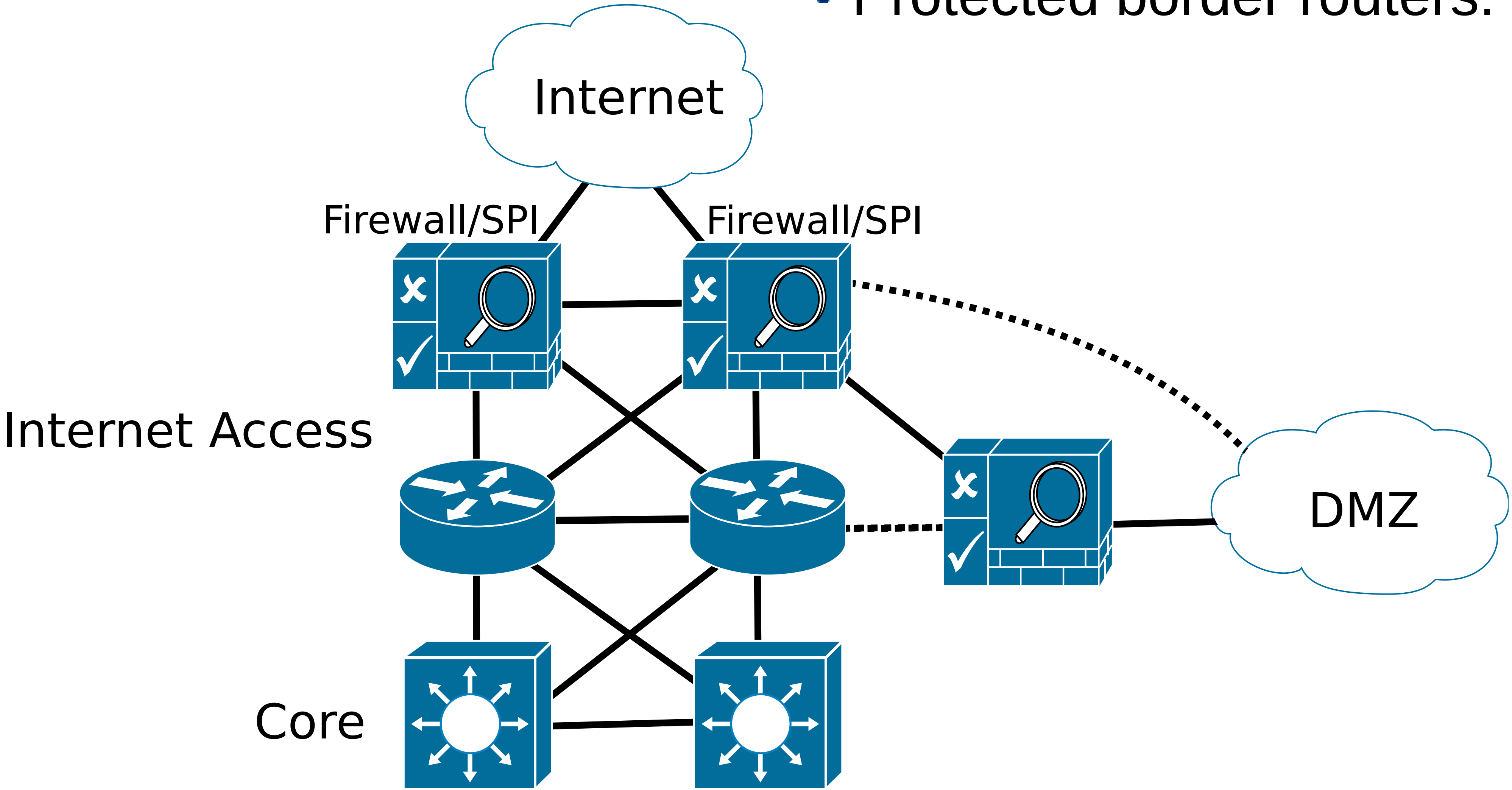
Firewall placement (with Redundancy)



- Exposed border routers.

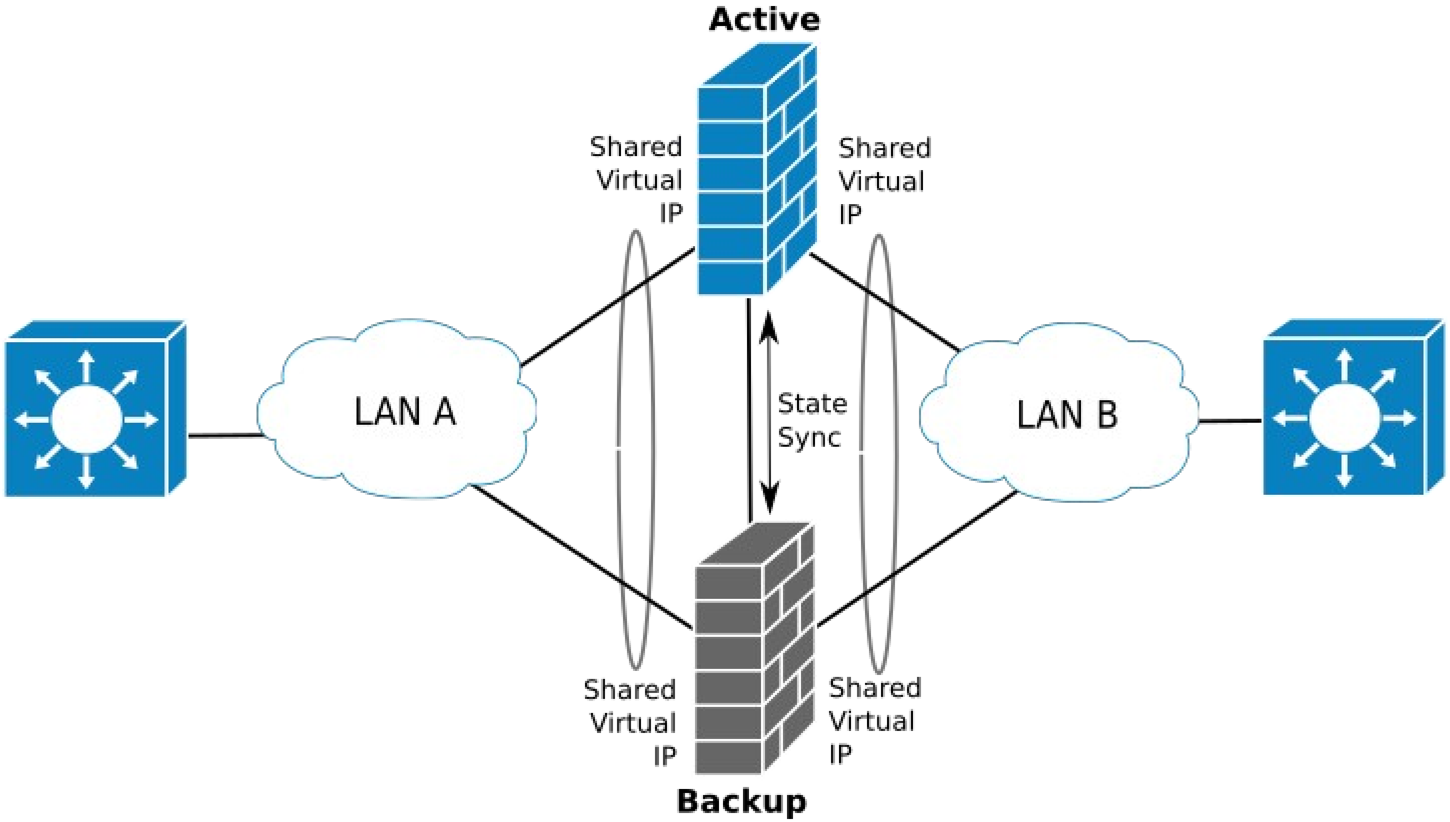
Firewall placement (with Redundancy)

- Protected border routers.



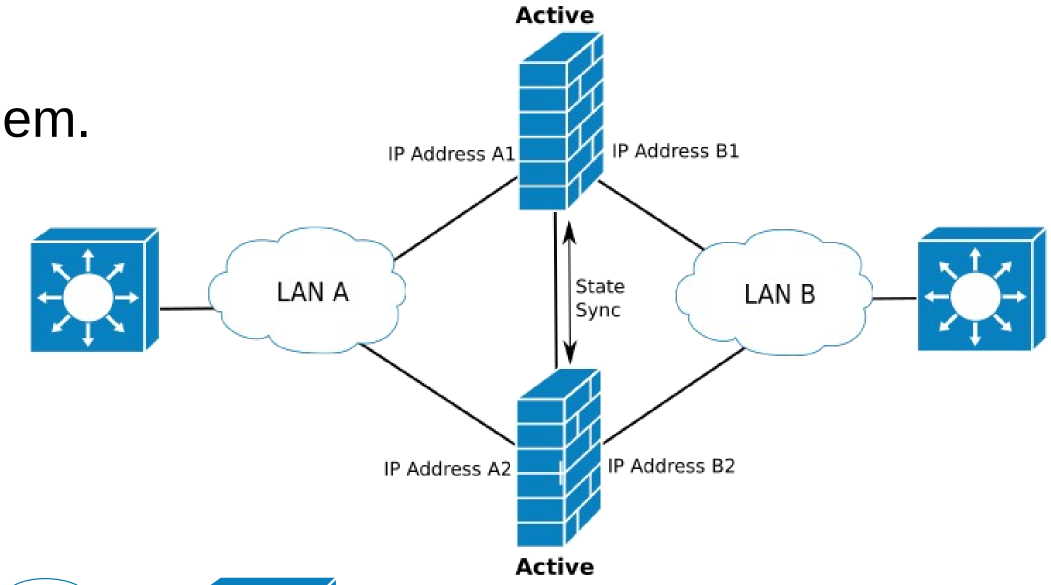
High-Availability (1)

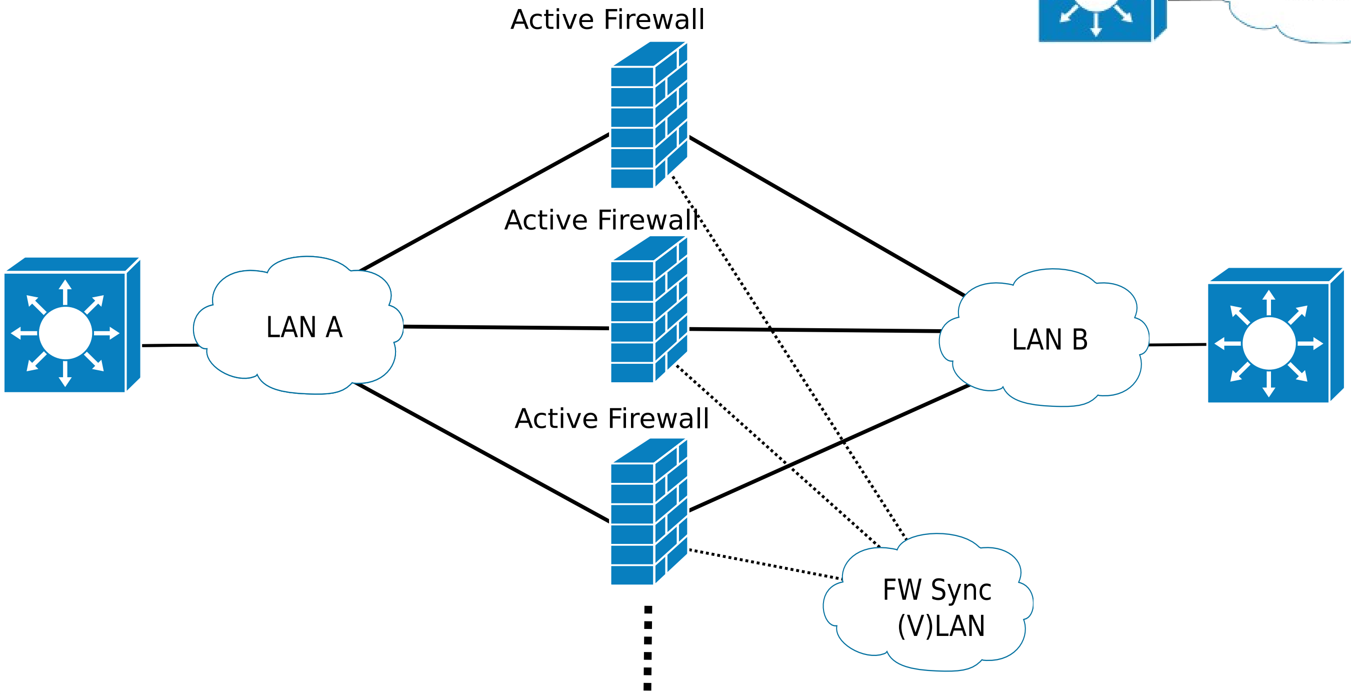
- Active-Backup Scenario
  - Firewalls share state via a dedicated connection
  - Firewalls share LAN (Virtual) IP addresses.
  - Backup firewall assumes IP and Services upon failure of Active firewall.
  - Usually implemented with Virtual Router Redundancy Protocol (VRRP)
    - FWs use the same MAC and IP addresses
    - The backup FW assumes addresses and functions upon detection of the active FW failure.



High-Availability / Cluster (2)

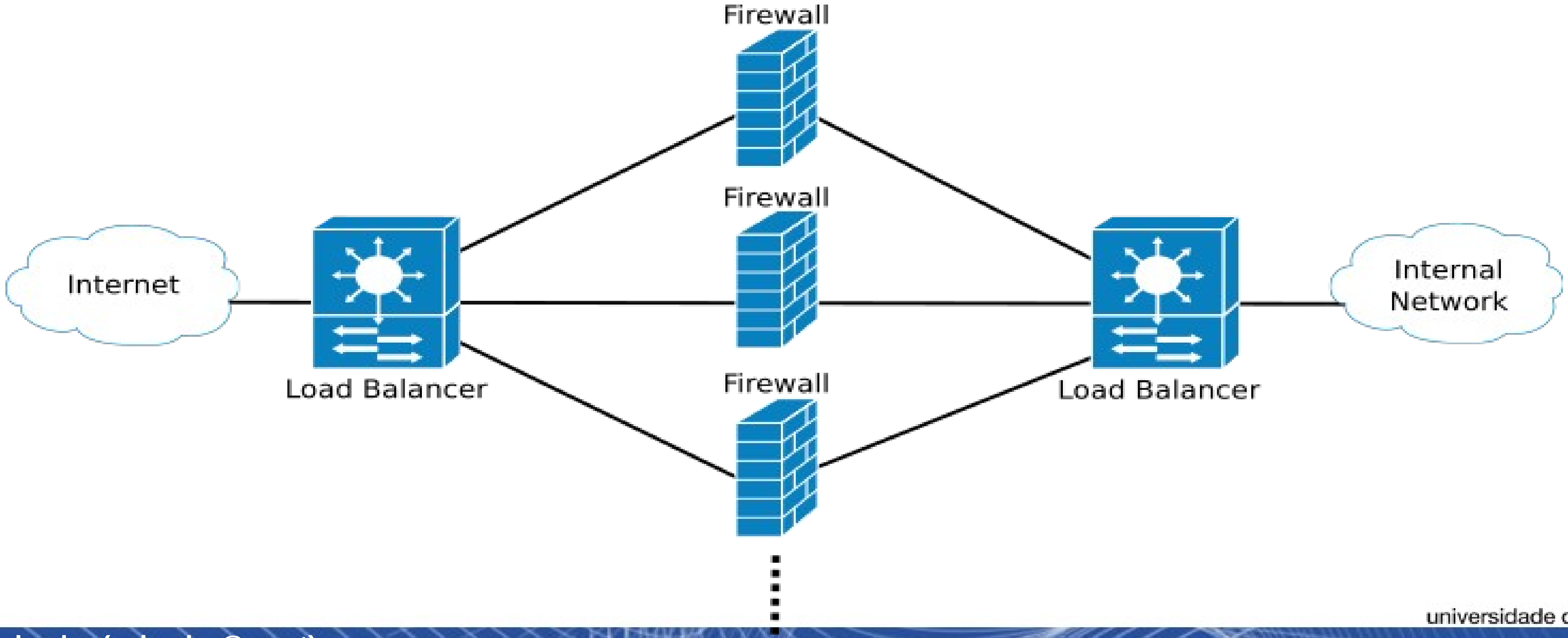
- Active-Active Scenario
  - Multiple firewalls (cluster) share state via a dedicated connection/(V)LAN
  - Firewalls have their on IP addresses.
  - Both work simultaneously.
    - Share load.
    - Solve asymmetric routing problem.
    - Work with load-balancers.





Load Balancing Firewall Load

- Load-balancing equipment can distribute traffic by multiple firewalls (cluster).
- When the load balancer routes the traffic from the same flow ALWAYS to the same firewall (depends on the LB algorithm):
  - Firewalls do not have to share connections states!
  - Decrease processing and memory requirements of each firewall.
  - Allow for a scalable growth of traffic.
  - Makes the network less vulnerable to DoS attacks.
  - When its also responsible to distribute policies/rules is called an Orchestrator.

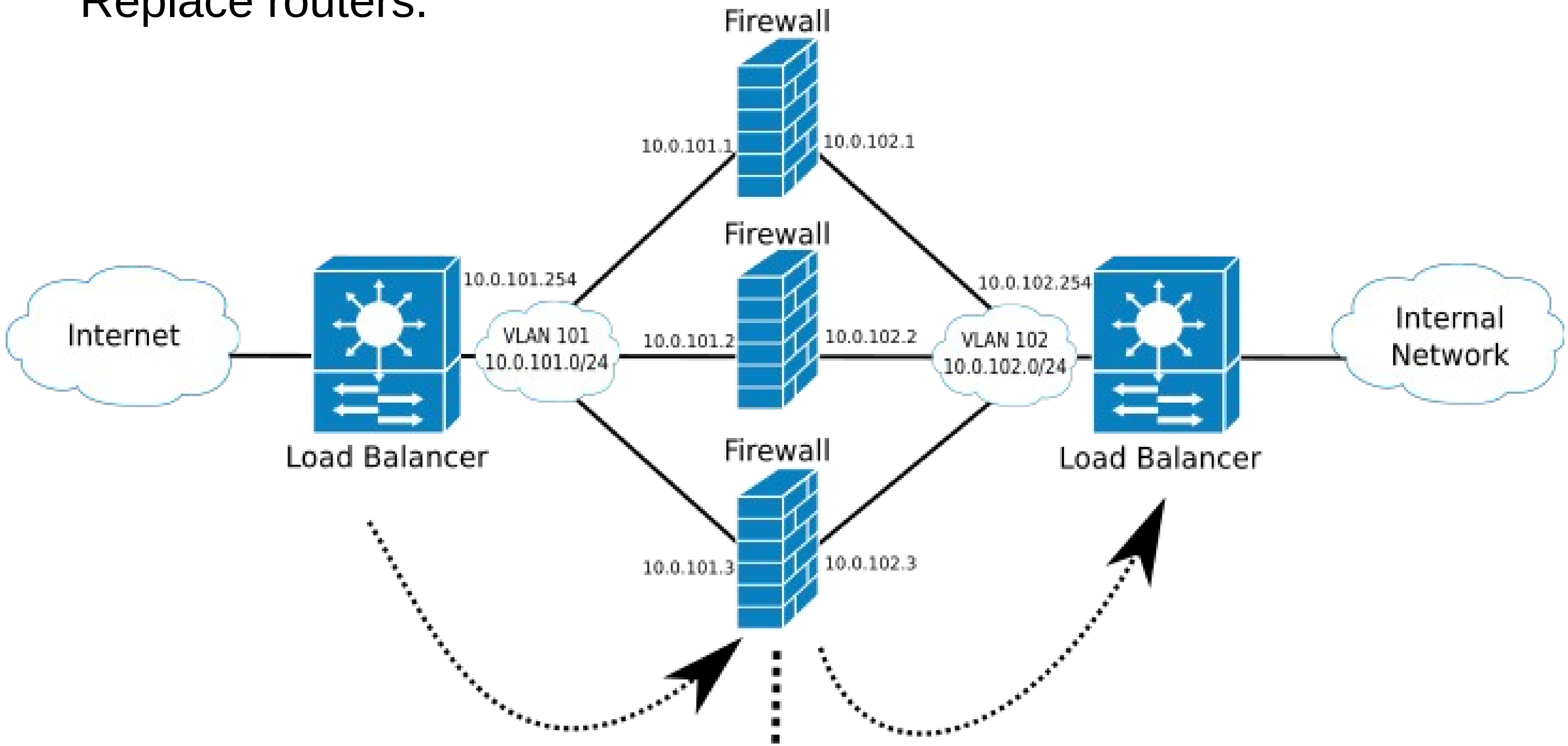


Load Balancing Algorithms

- IP Hash
  - The IP address (or a set of flow identifiers) of the client is used to determine which server/firewall receives the flow or request.
  - Does not require state synchronization (FW or LB). Hash function output determines target.
- Round Robin or Random
  - Requests are distributed across the group of devices sequentially.
  - If firewalls do not share state, load-balancers must “memorize” the interface by witch they received the traffic from firewalls, and use the same interface to route the response traffic.
- Least Connections
  - A new request is sent to the server/firewall with the fewest current connections.
  - The relative computing capacity of each server/firewall is factored into determining which one has the least connections.
  - If firewalls do not share state, load-balancers must “memorize” the interface by witch they received the traffic from firewalls, and use the same interface to route the response traffic.
- Centralized/“Smart”
  - Based on an external source of information.

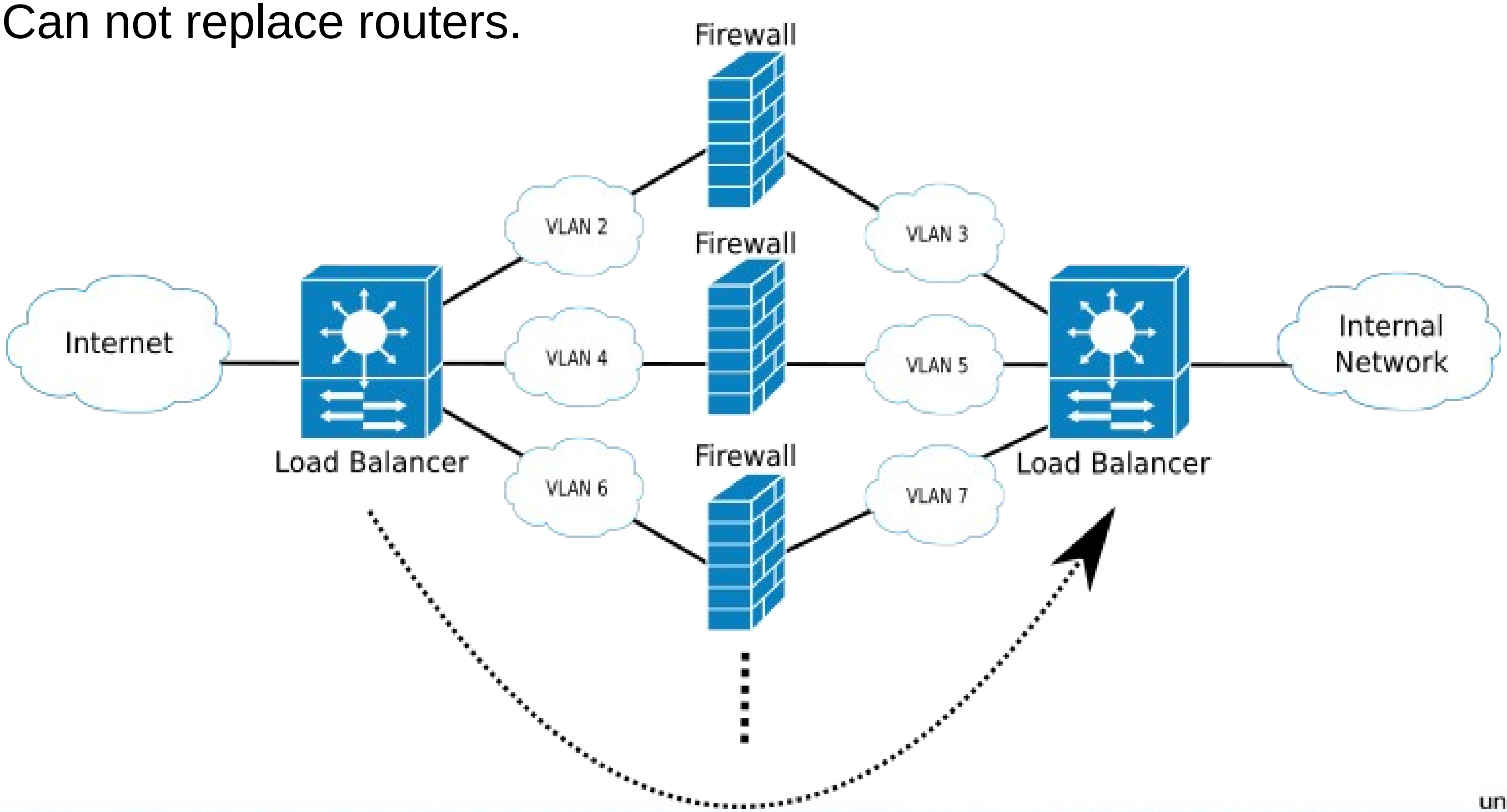
Addressed Firewalls

- Interfaces have IP addresses.
- Load balancers (or routers) route traffic as an IP next-hop.
- Can provide routing services.
  - Replace routers.



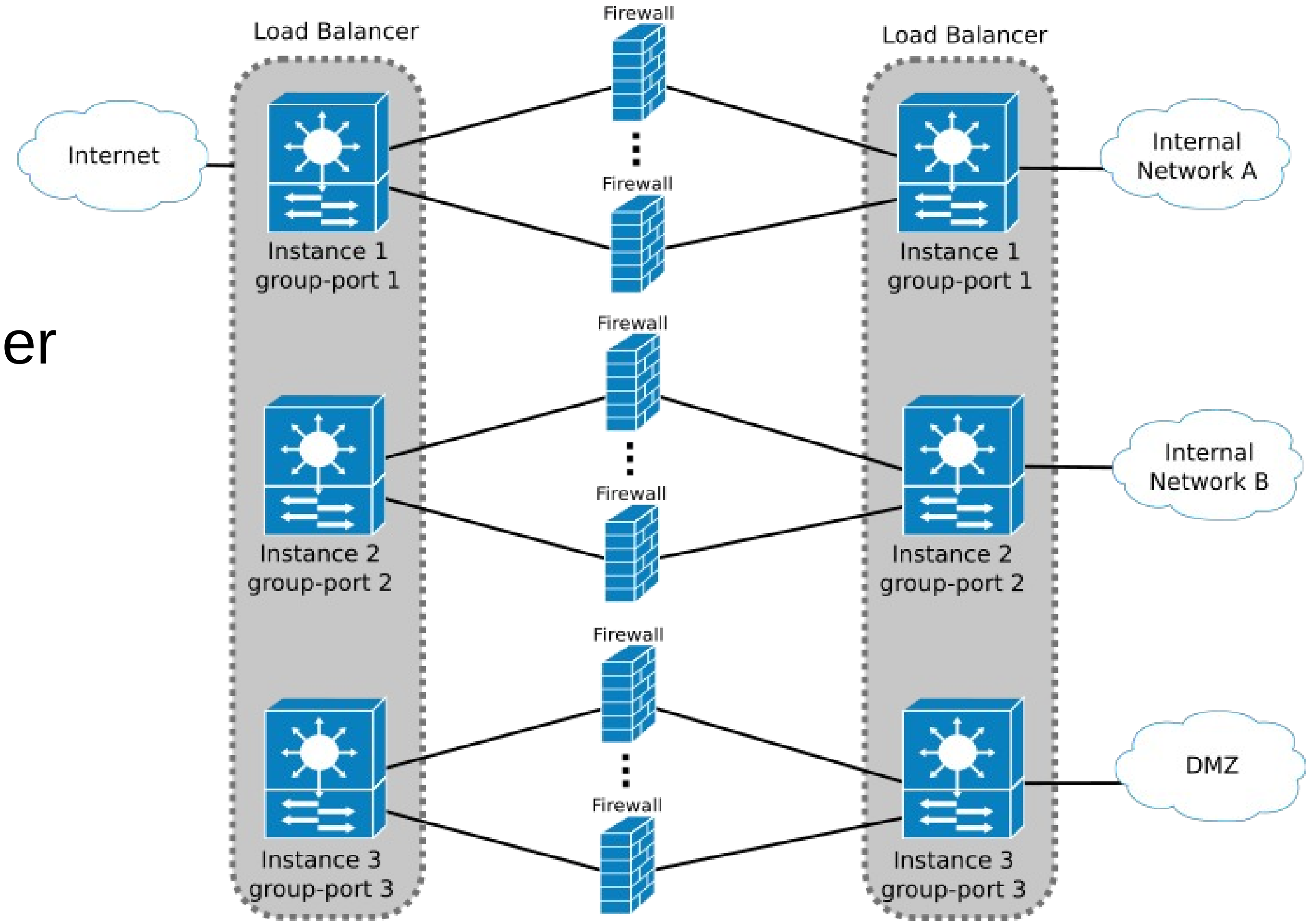
Stealth Firewalls

- Interfaces do not have IP addresses.
  - May have multiple layer rules.
- Load balancers (or swicthes) route traffic on a per interface/VLAN basis.
- Can not provide routing or NAT/PAT services.
  - Can not replace routers.



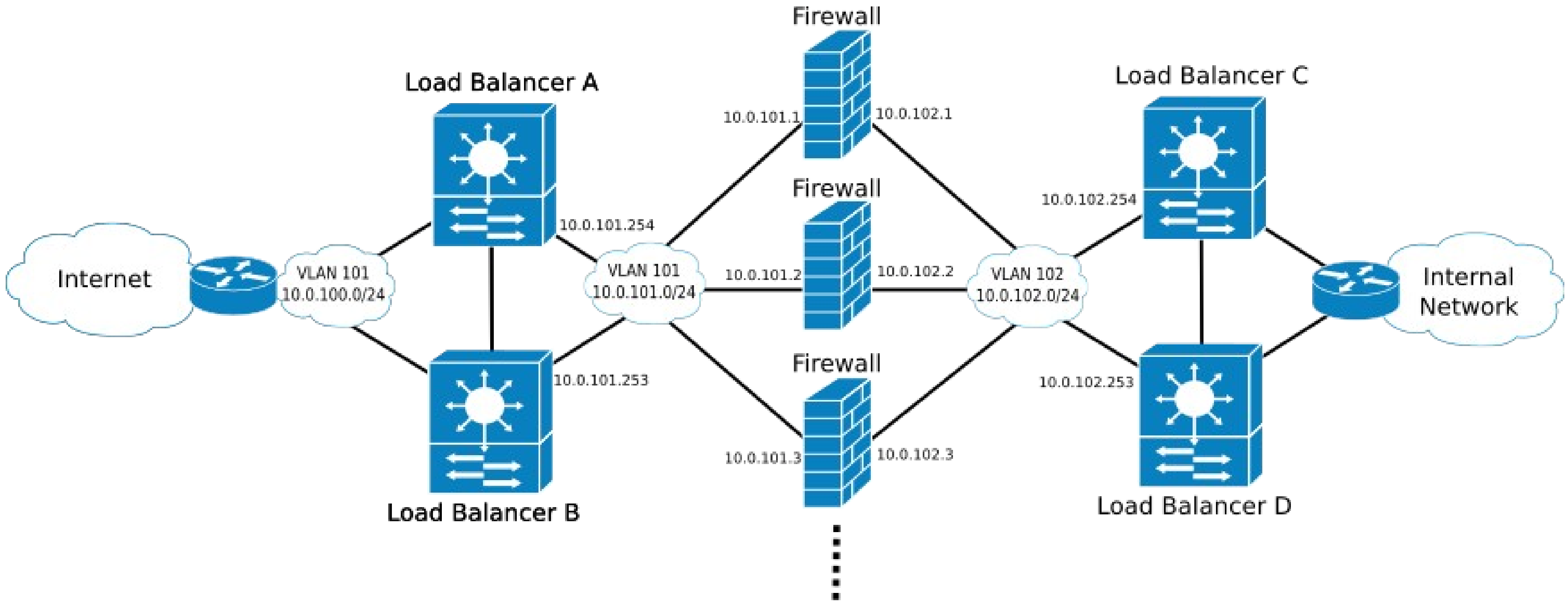
Load-Balancers Instances

- Load balancers may have (theoretical) isolated instances to handle different zones/groups.
  - With a set of firewalls per zone/group.
- Physical or virtual partitions.
- Some vendor call it group-ports.



Redundant Load Balancers

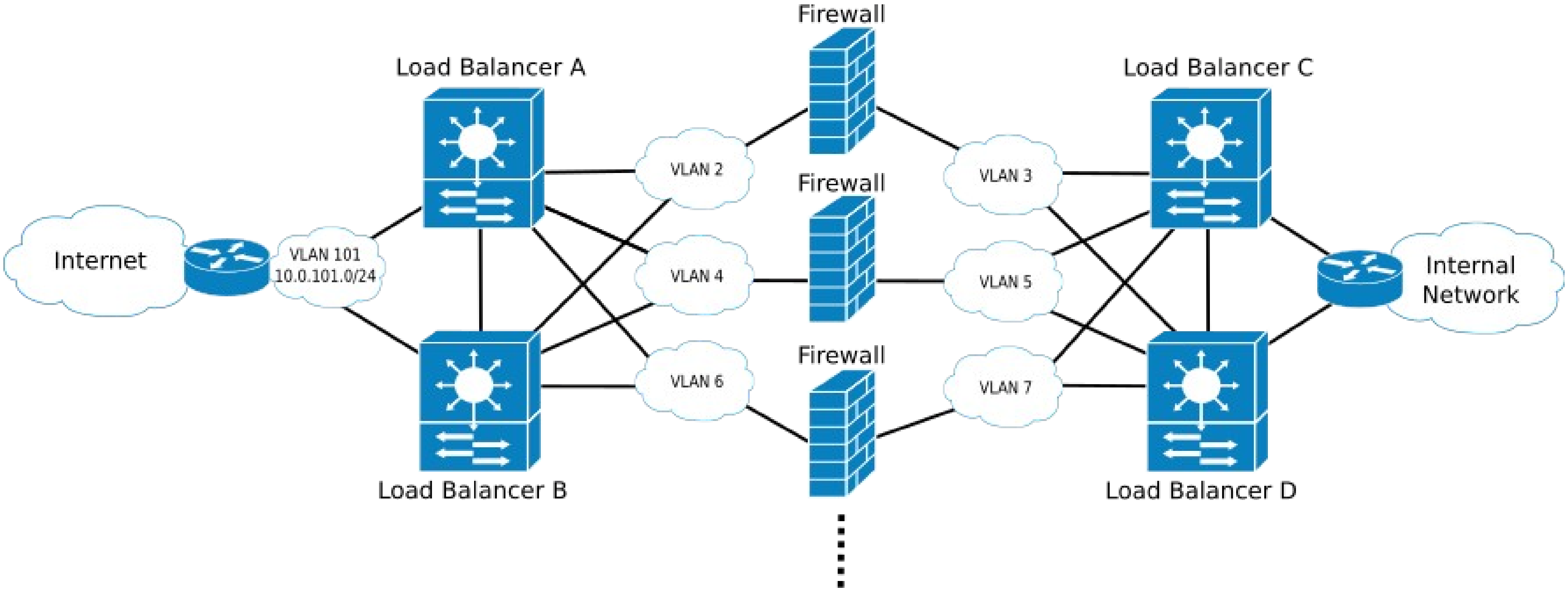
Addressed Firewalls



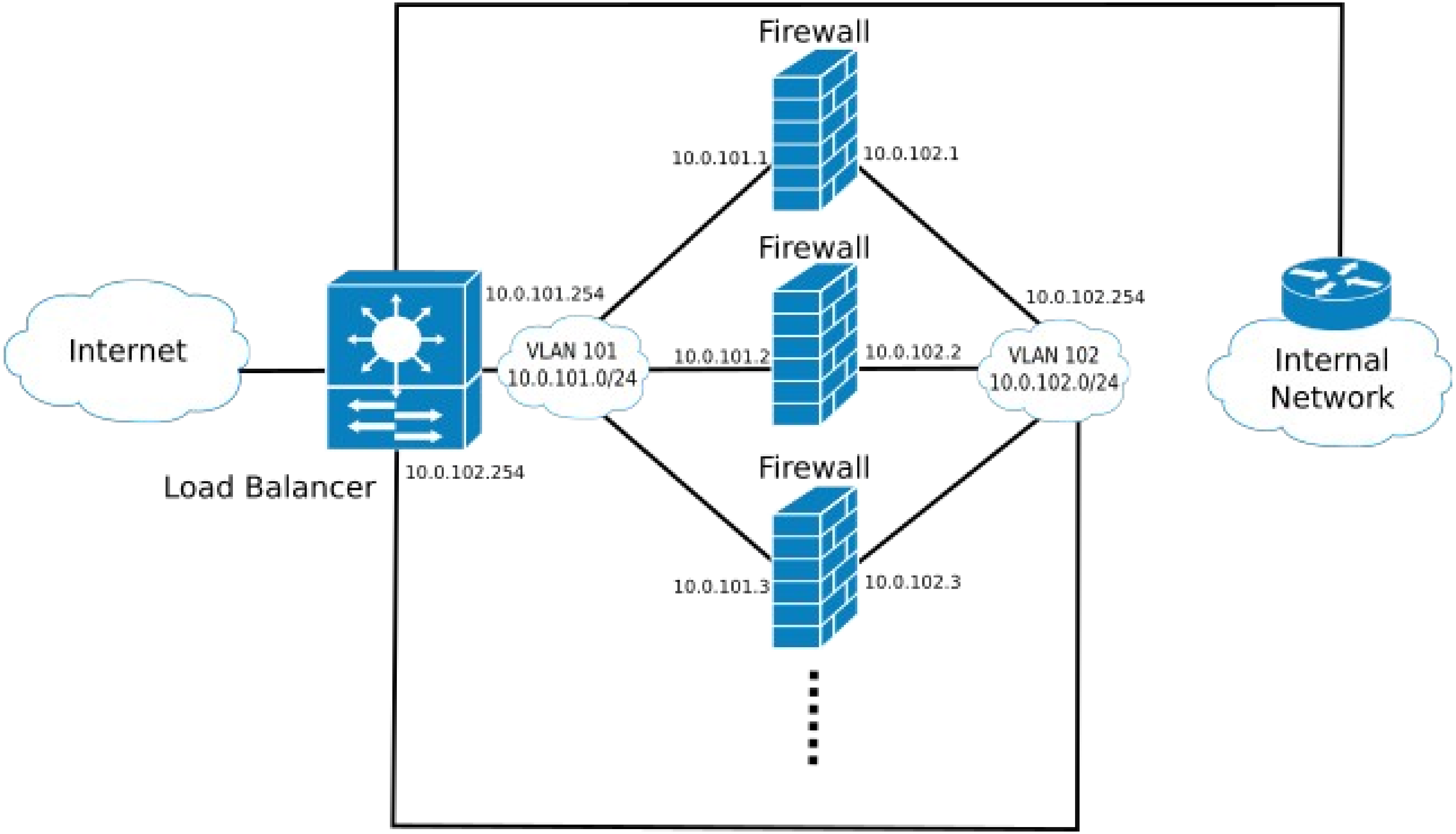
- To avoid FW state synchronizaion Load-Balancers should Sent packets of the same flow always to same firewall.
  - Must lower FW memory overload chance.
- Load-Balancers using IP Hash LB algorithms do nor require routing history synchronization (between LB).
  - Using other LB algorithms, they must share routing history.

Redundant Load Balancers

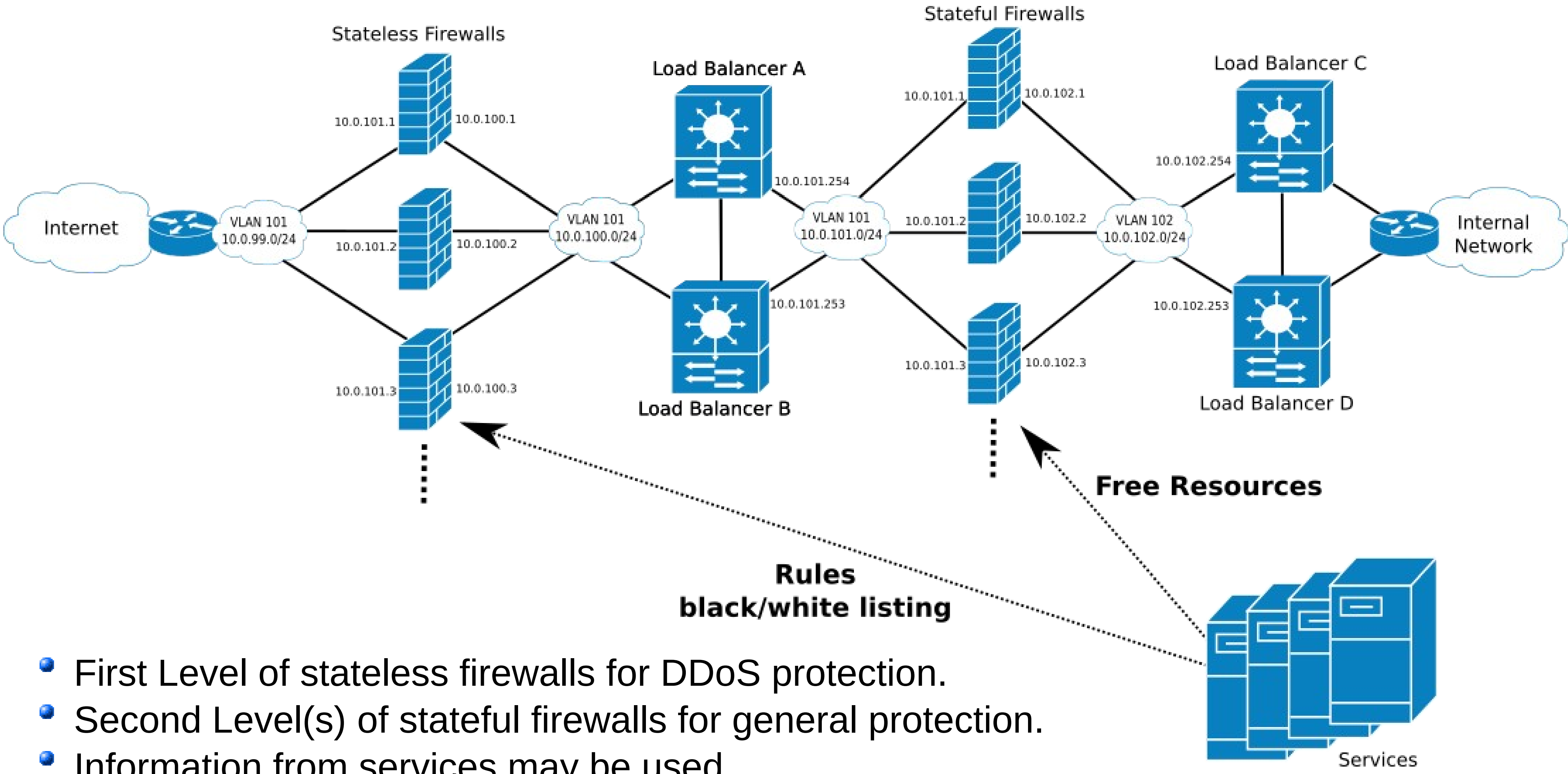
Stealth Firewalls



Single Load Balancer



Multi-Levels of Defense



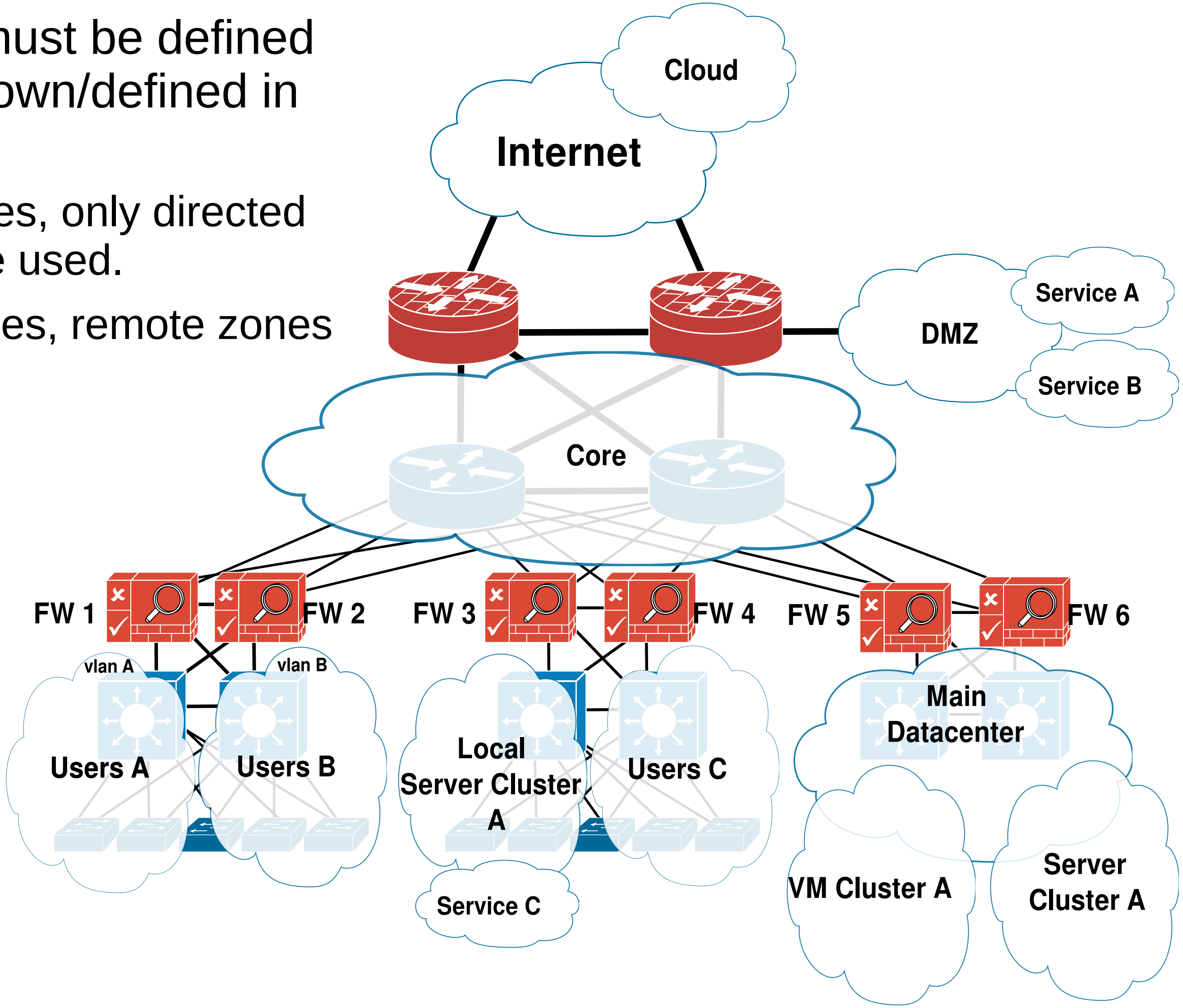
- First Level of stateless firewalls for DDoS protection.
- Second Level(s) of stateful firewalls for general protection.
- Information from services may be used
  - To free resources in the stateful firewalls.
  - To configure black/white lists rules at the stateless firewalls.

Rules (1)

- A Firewall rule (or set of rules, aka as chains) are assigned to the input (or output) of a network interface (or set/group/zone of interfaces).
    - Will be evaluated in respect to all traffic ingressing (or egressing) an interface.
- Firewall rules must specify to which traffic they should match
    - Source and destination may be IP addresses, TCP/UDP ports, set/groups of addresses/ports, etc…
    - Type may be defined in terms of protocol or protocol specifics.
    - Rules may be specified based on the state of a connection (requires a stateful firewall) upon the observation of a packet:
        - NEW - The observed packet packet is starting a new connection, or it is associated with a connection which has not generated packets in both directions.
        - ESTABLISHED - The observed packet is associated with a connection which has generated packets in both directions.
            - Usually a specif rule only allows traffic from one direction, an ESTABLISHED rule must be defined to dynamically allow the response from the other direction.
        - RELATED - The observed packet is starting a new connection, but is associated with an existing connection, such as an ICMP error (e.g., port unreachable related to an UDP connection)
- A match to a rule determines the action to execute to flow, connection or packet.
    - Some firewalls call the actions targets.
    - Possible actions are accept, drop/reject, test with another set of rules/chain, modify packet, etc...
    - The first match determines the action.
    - **The order of the rules is critical.**
    - Some firewall allow probabilistic actions based on weights.

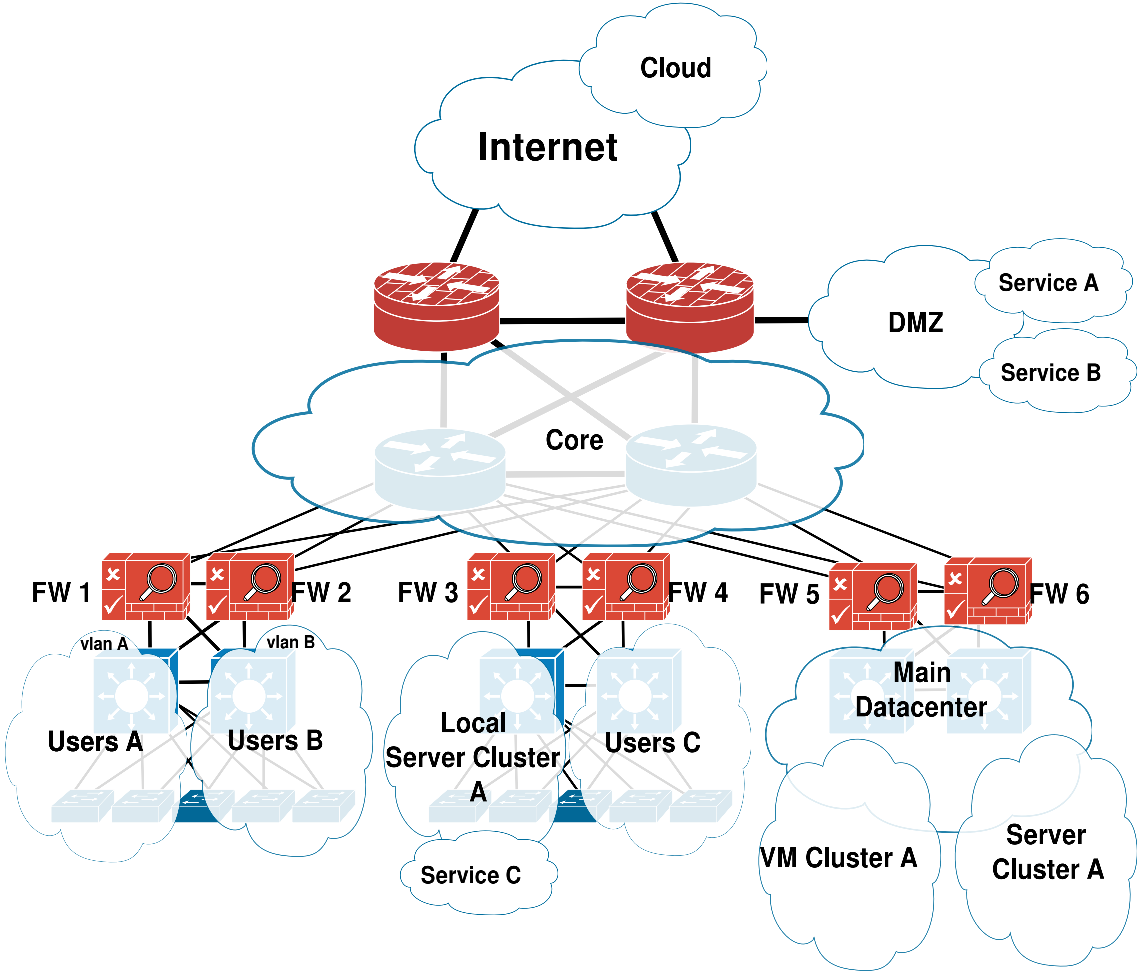
Rules (2)

- Multi zones scenarios
  - Rules in a specific FW must be defined based only on zones known/defined in that firewall.
    - For interface based zones, only directed connected zones can be used.
    - For other IDs based zones, remote zones can be used.



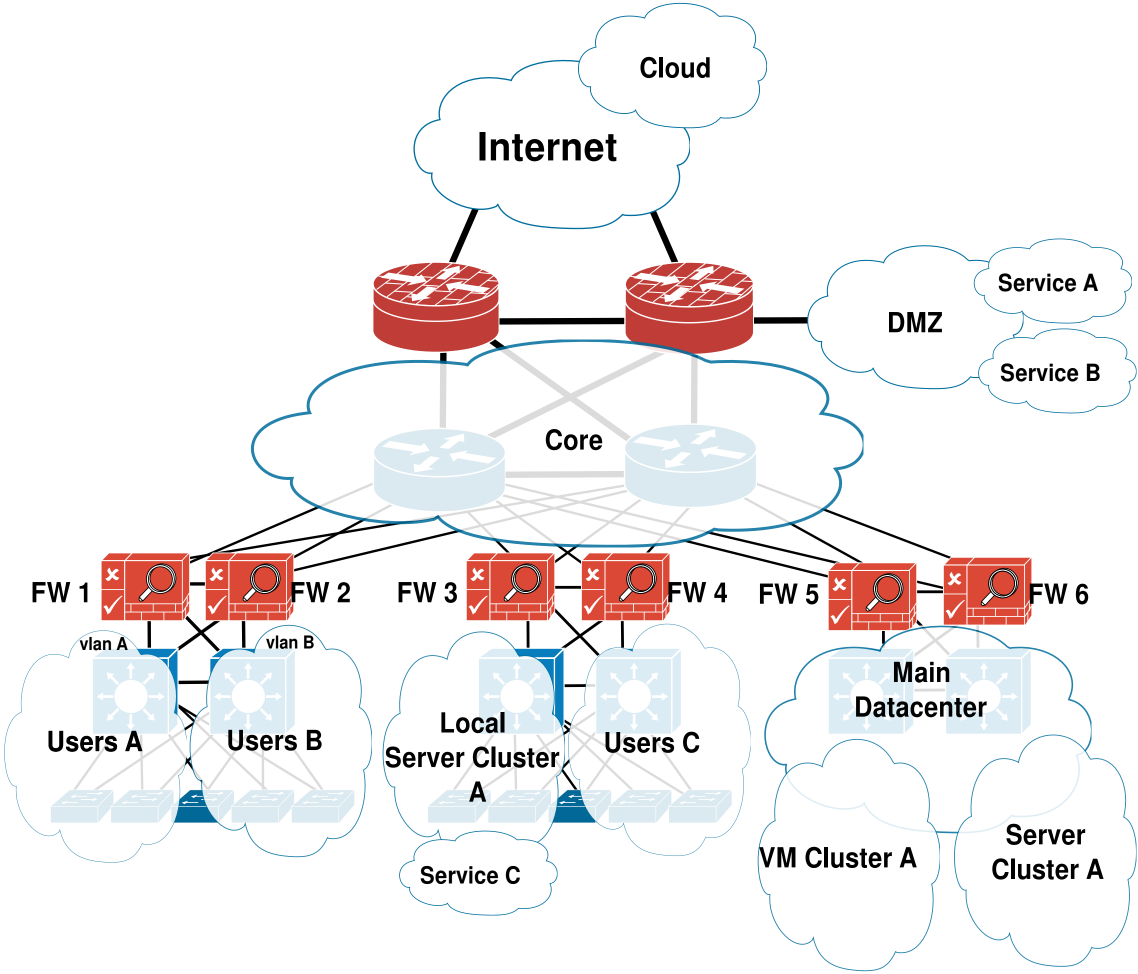
Rules (3)

- Example 1
  - Users A can access Google HTTPS services (defined by IP addresses, and TCP/UDP port 443)
    - FW1/FW2
      - Has a zone assigned to interface vlanA called **UsersA** and another zone called **Core** assigned to all core interfaces.
      - Assign a rule to the INPUT of all interfaces in zone **UsersA** and OUTPUT to any interfaces of zone **Core.**
      - Destiny of flow should be IP addresses/ports of Google Services. May specify source as IP address of specific users of vlan A.
      - Reversed rule applied from zone **Core** to zone **UsersA** allow all response traffic from established flows allowed by previous rules.
    - Main Fws
      - Has a zone assigned to all internet interfaces called **Internet** and another zone called **Core** assigned to all core interfaces.
      - Assign a rule to the INPUT of all interfaces of zone **Core** and OUTPUT to any interfaces of zone **Internet**.
      - Destiny of flow should be IP addresses/ports of Google Services. May specify source as IP address of specific users of vlan A.
      - Reversed rule applied from zone **Internet** to zone **Core** allow all response traffic from established flows allowed by previous rules.



Rules (4)

- Example 2
  - Users B may access VM Cluster A (defined by IP addresses/ports)
  - FW1/FW2
    - Has a zone assigned to interface vlanA called **UsersA** and another zone called **Core** assigned to all core interfaces.
    - Assign a rule to the INPUT of all interfaces in zone **UsersA** and OUTPUT to any interfaces of zone **Core**.
    - Destiny of flow should be IP addresses/ports VM Cluster A. May specify source as IP address of specific users of vlan A.
    - Reversed rule applied from zone **Core** to zone **UsersA** allow all response traffic from established flows allowed by previous rules.
  - FW5/FW6
    - Has a zone assigned to all interfaces/networks of VM Cluster A called **VM Cluster A** and another zone called **Core** assigned to all core interfaces.
    - Assign a rule to the INPUT of all interfaces of zone **Core** and OUTPUT to any interfaces of zone **VM Cluster A**.
    - Destiny of flow should be IP addresses/ports of IP addresses/ports VM Cluster A. May specify source as IP address of specific users of vlan A.
    - Reversed rule applied from zone **VM Cluster A** to zone **Core** allow all response traffic from established flows allowed by previous rules.

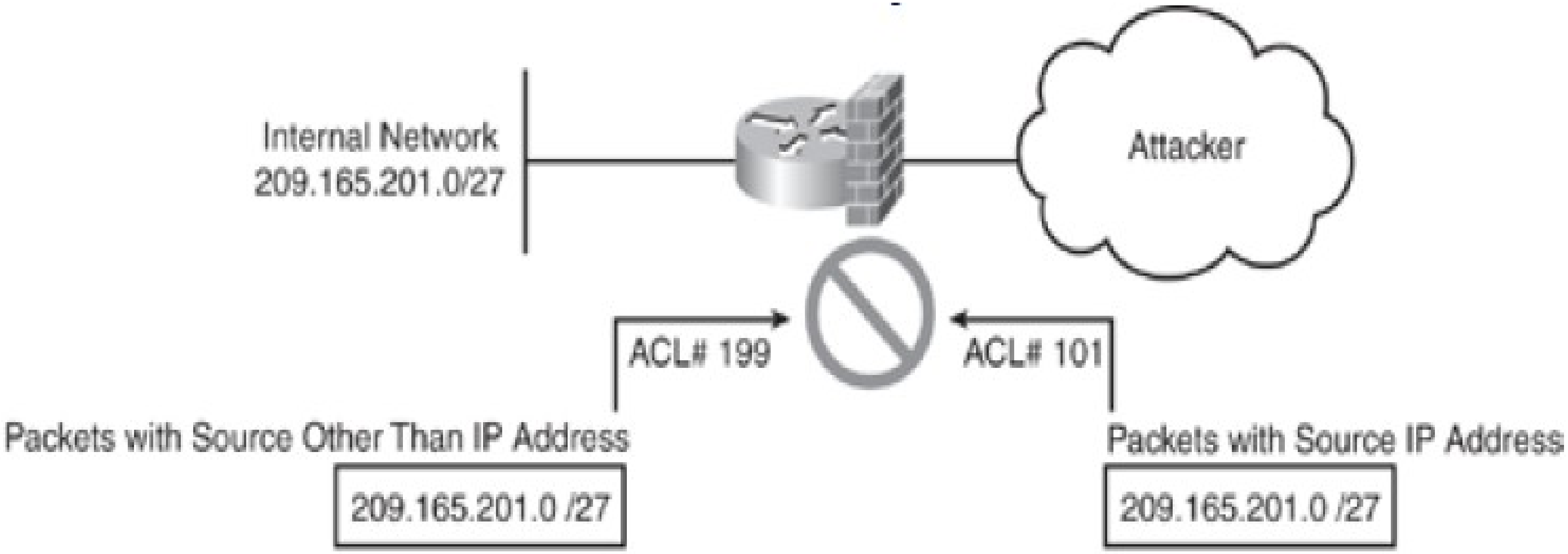


Rules (5)

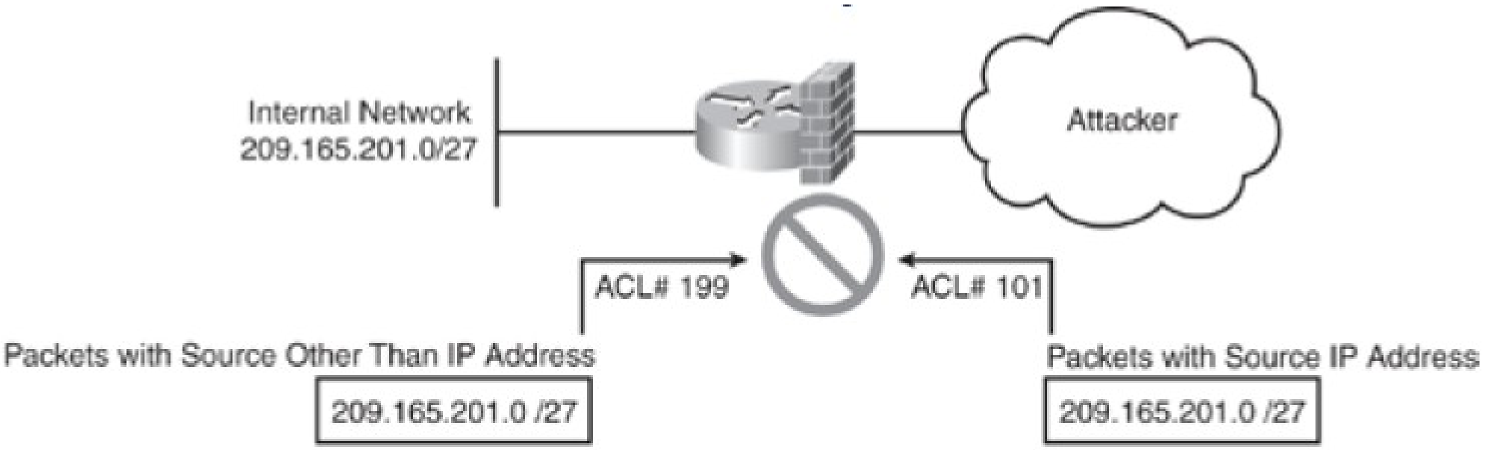
- Best Practices and Recommendations
  - Standardize your security policies.
    - Includes firewalls, network zones relations, devices and users profiles, active services, etc..
  - Define the rules the more specific as possible.
    - Avoid generic rules that may open undesired paths.
  - Blocking all traffic by default.
    - Remove “Accept All” Rules.
  - Add “Accept” exceptions.
    - Usually Clients to Service direction.
      - E.g., Internal to Internet, Internet to DMZ, etc...
      - Add reverse rule base on established /related connections.
  - Maintain documentation of firewall rules:
    - Purpose, relation to security policies, affected devices and users, deployment and expiration dates, identification of the manager.
  - Maintenance and monitoring of rules.
    - Periodically verify validity of rules within current security policies.
    - Analyze usage/match statistics of each rule.
  - Integrate flow control with existing rotting, switching and load balancing policies and services.

IP Spoofing

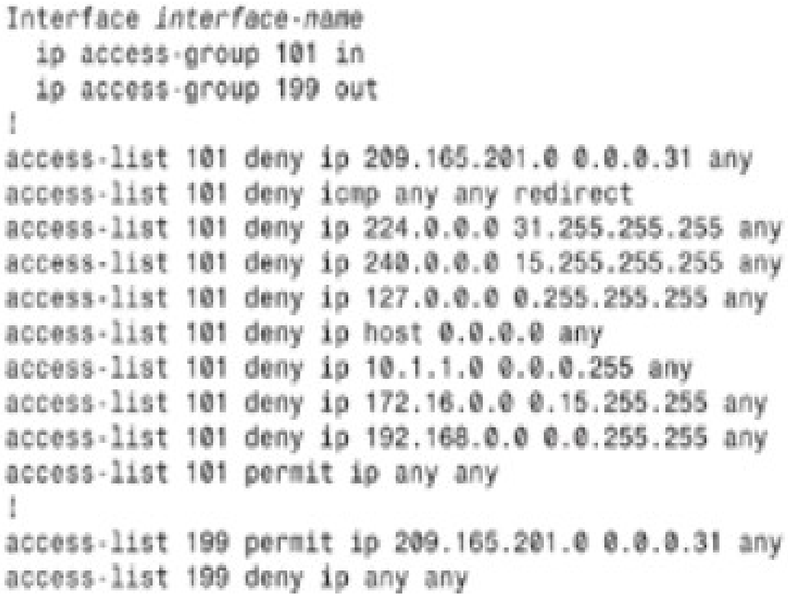
- IP spoofing refers to the creation of IP packets with a forged source IP address.
  - To hide the identity of the sender or impersonate another network system.
  - Spoofing IP datagrams is a well-known problem.
  - Most spoofing is done for illegitimate purposes.



Preventing IP Spoofing at Layer 3



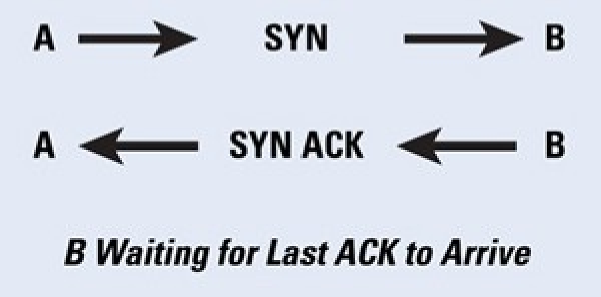
- Deny external traffic with
  - IP source equal to protected network IP ranges.
  - IP source equal to private addresses.
  - Multicast destinations.
- Reverse Path Verification
  - Deny traffic where the source IP network is not reachable using the interface where the packet arrived.



```
Interface interface-name
  ip access-group 101 in
  ip access-group 199 out
!
access-list 101 deny ip 209.165.201.0 0.0.0.31 any
access-list 101 deny icmp any any redirect
access-list 101 deny ip 224.0.0.0 31.255.255.255 any
access-list 101 deny ip 240.0.0.0 15.255.255.255 any
access-list 101 deny ip 127.0.0.0 0.255.255.255 any
access-list 101 deny ip host 0.0.0.0 any
access-list 101 deny ip 10.1.1.0 0.0.0.255 any
access-list 101 deny ip 172.16.0.0 0.15.255.255 any
access-list 101 deny ip 192.168.0.0 0.0.255.255 any
access-list 101 permit ip any any
!
access-list 199 permit ip 209.165.201.0 0.0.0.31 any
access-list 199 deny ip any any
```

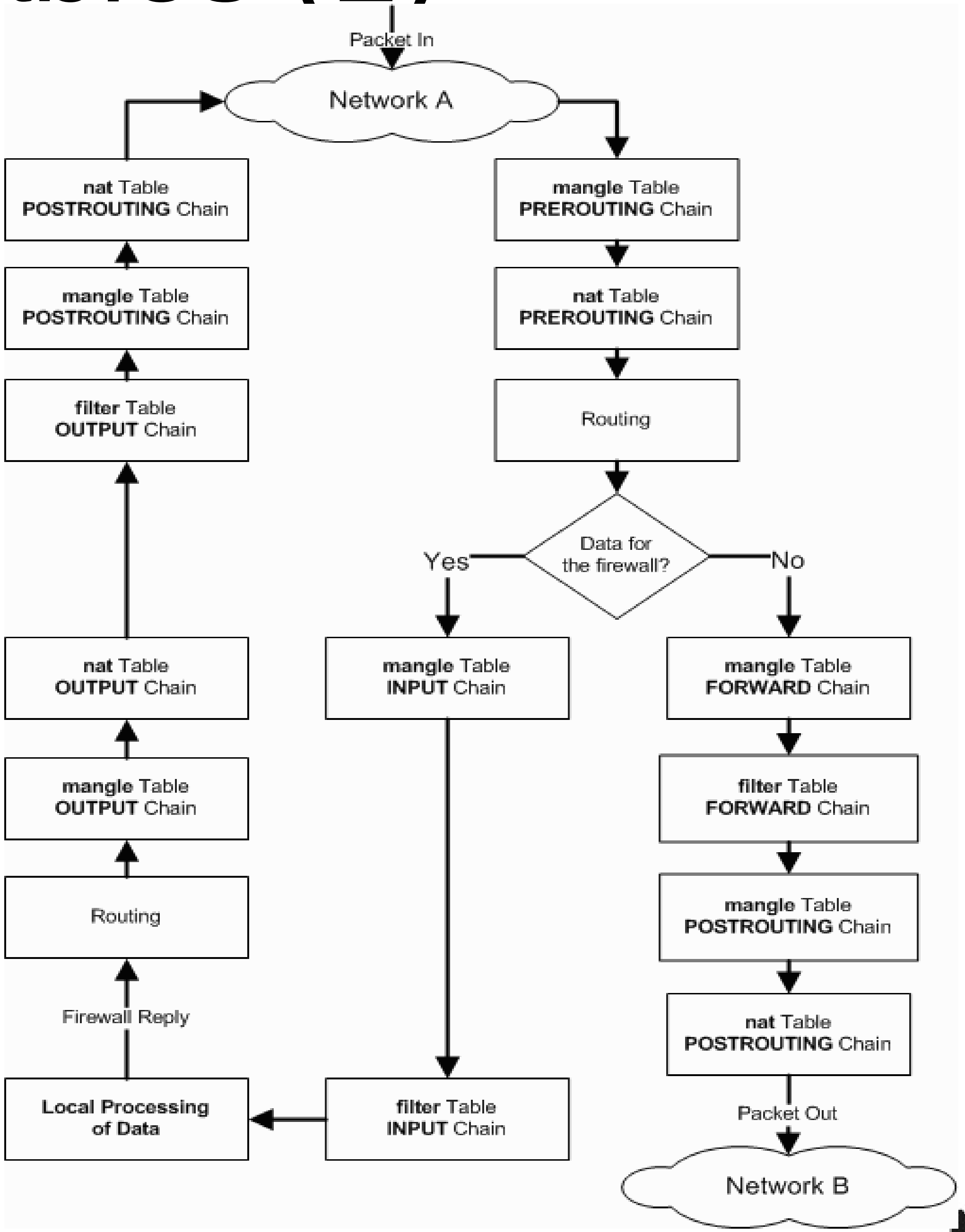
Half-Open TCP Connection Problem

- A DoS attack commonly uses half-open TCP connections.
  - Firewall keeps the state of the TCP session in memory.
  - Multiple half-open TCP connections can overrun firewalls.
    - Define timeout values for half-open TCP sessions:
      - Normal: small/medium values.
      - Under attack (based on traffic thresholds): very small values.
    - May be necessary to use external means to “clean” firewall.
      - Reseting (half-open) connections from the internal servers.



Linux iptables (1)

- Name of the user space tool by which administrators create rules for the packet filtering and NAT modules.
- Used to set up, maintain, and inspect the tables of IP packet filtering rules within the Linux kernel.
- Has 5 default chains:
  - INPUT, OUTPUT, FORWARD
  - PREROUTING
  - POSTROUTING
- Has 3 default tables,
  - Filter, nat and mangle
- Basic decisions
  - ACCEPT, DROP, QUEUE and RETURN
- Extended decisions
  - LOG, MARK, REJECT, TOS, SNAT, DNAT, MASQUERADE, REDIRECT, etc...
- Multiple state machines
  - Conntrack (connection tracker).
-



Packet In
Network A
nat Table POSTROUTING Chain
mangle Table PREROUTING Chain
mangle Table POSTROUTING Chain
nat Table PREROUTING Chain
filter Table OUTPUT Chain
Routing
Yes
Data for the firewall?
No
nat Table OUTPUT Chain
mangle Table INPUT Chain
mangle Table FORWARD Chain
mangle Table OUTPUT Chain
filter Table FORWARD Chain
Routing
mangle Table POSTROUTING Chain
Firewall Reply
nat Table POSTROUTING Chain
Local Processing of Data
filter Table INPUT Chain
Packet Out
Network B

Linux IPTables (2)

- In addition to the built-in chains, the user can create any number of user-defined chains within each table, which allows them to group rules logically.
- Each chain contains a list of rules,
  - When a packet is sent to a chain, it is compared against each rule in the chain in order.
- The rule specifies what properties the packet must have for the rule to match (such as the port number or IP address).
- If the rule does not match, then processing continues with the next rule.
- If, however, the rule does match the packet, then the rule's target instructions are followed (and further processing of the chain is usually aborted).
- Some packet properties can only be examined in certain chains,
  - For example, the outgoing network interface is not valid in the INPUT chain.
- Some targets can only be used in certain chains, and/or certain tables,
  - For example, the SNAT target can only be used in the POSTROUTING chain of the NAT table.
- The target of a rule can be the name of a user-defined chain or one of the built-in targets (ACCEPT, DROP, RETURN, DNAT, SNAT and MASQUERADE).
- You can think of a target in the same way as a subroutine.

Linux nftables

- nftables replaces iptables.
- Provides a new in-kernel packet classification framework that is based on a network-specific Virtual Machine (VM).
- Uses a new nft userspace command line tool.
  - Userspace command line tool, with no need of kernel upgrades.
    - nftables interface and iptables like interface.
- High performance through maps and concatenations.
- Smaller kernel codebase. The intelligence is placed in userspace nft command line tool.
- Unified and consistent syntax for every support protocol family.

Control By Analysis of Higher Layers

- Traffic flow control based on higher layer data/protocols only works with not ciphered traffic.
- Some firewalls provide decryption and inspection of SSL/TLS traffic.
- Traffic deciphering may be achieved using a root certificate on client machines, acting as Certificate Authority for SSL requests.
  - Firewalls must issue certificates to clients on behalf of the web servers they are connecting to.
  - Firewalls intercept SSL/TLS handshake.
  - Requires client device level changes.
- Implementing this technique is processor-intensive.
  - Results in performance degradation.
  - Can be avoided by off-loading SSL/TLS decryption to a dedicated devices.
- May break privacy/confidentiality laws and rights in some countries.

Firewall Performance Evaluation

- Basic Firewall
  - IP Throughput
    - Raw capability of the firewall to pass traffic from interface to interface
  - Latency
    - Time traffic delay in the firewall
    - Should be measured and reported when the firewall is at its operating load
- Traditional Enterprise Firewall
  - Connection Establishment Rate
    - Speed at which firewalls can set up connections
  - Concurrent Connection Capability
    - Total number of open connections through the firewall at any given moment
  - Connection Teardown Rate
    - Speed at which firewalls can teardown connections and free resources
- Next Generation Firewall
  - Application Transaction Rate
    - Capability of the firewall to secure discrete application-layer transactions contained in an open connection
    - May include application-layer gateways, intrusion prevention, or deep-inspection technology
    - Application transaction rate are highly data dependent

Extra References

- Cisco, Zero Trust Architecture (Networking Technology: Security), Pearson, August 2023, ISBN-13:978-0137899739.
- Palo Alto, High Availability Concepts.
- Palo Alto, HA Clustering Overview.
- A. Lindem, A. Dogra, RFC 9568, Virtual Router Redundancy Protocol (VRRP) Version 3 for IPv4 and IPv6, April 2004.