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 Security Systems

- Firewall
- Intrusion Prevention System (IPS)
  - Performs deep-packet inspection
- Intrusion Detection Systems (IDS)
  - Performs deep-packet (DPI) and shallow-packet inspection (SPI)
- Security Appliance
  - Unified communications security
  - Firewall services
  - Real-time threat defense
  - Secure remote access
  - Secure communications services
  - Content security

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

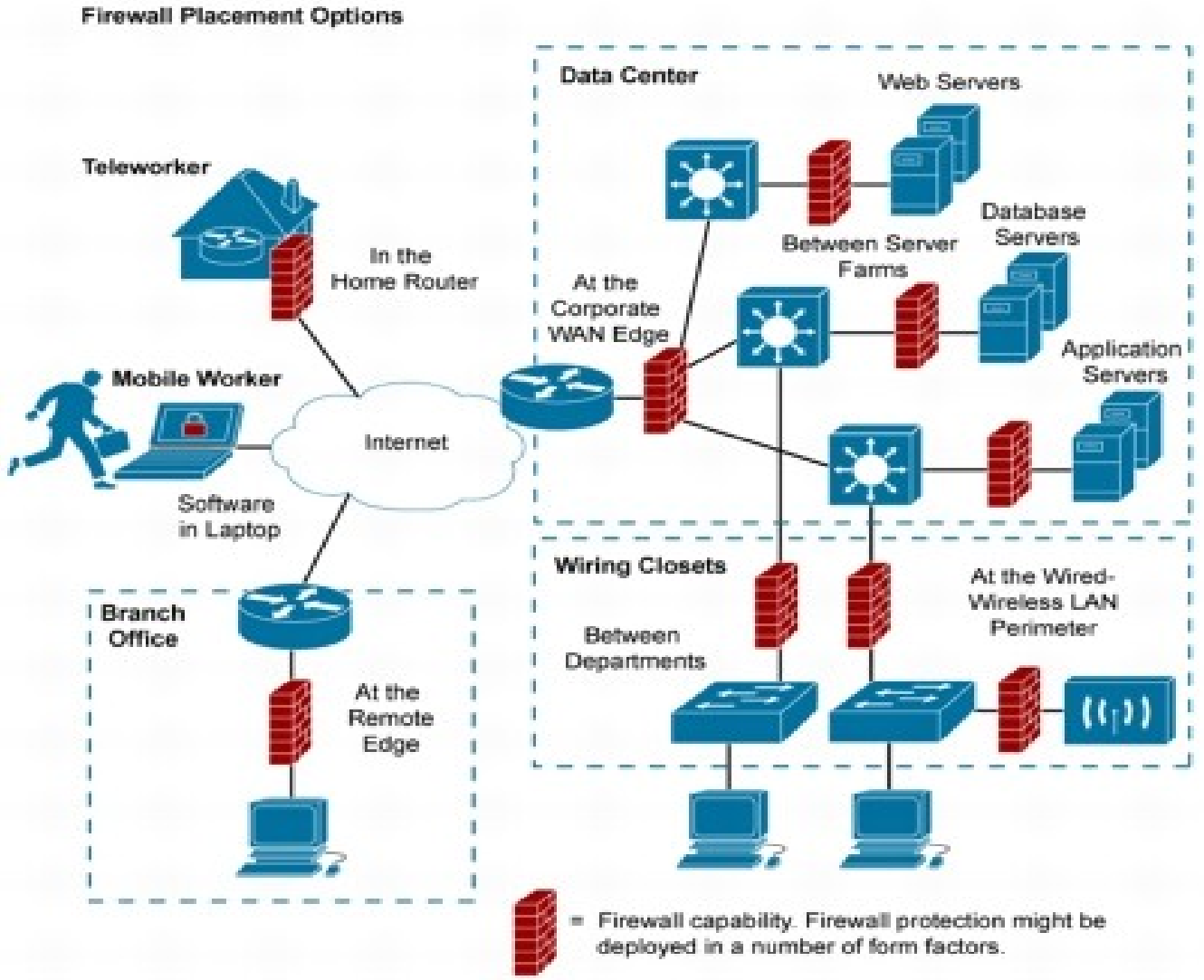
- NAT (Network Address Translation).
- Authorization
  - Flows (packet filtering).
  - Users (application and circuit level).
- Redirecting.
  - To specif machines.
  - Proxing.
- Content analysis.
- Secure communication.
  - Site-to-site VPN.
    - IPsec.
  - Remote-access VPN.
- DoS and DDoS detection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

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

Deploying Firewalls

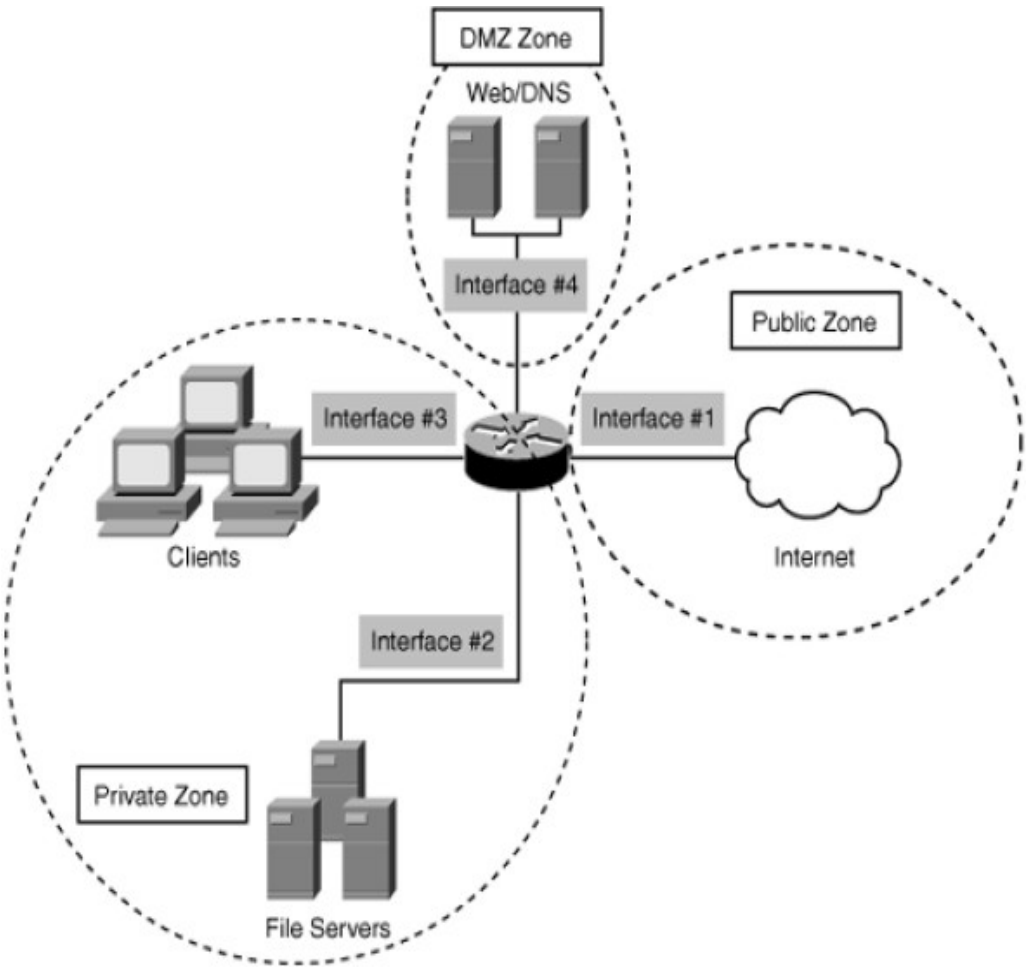
- Network must be protected at multiple levels and locations



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).

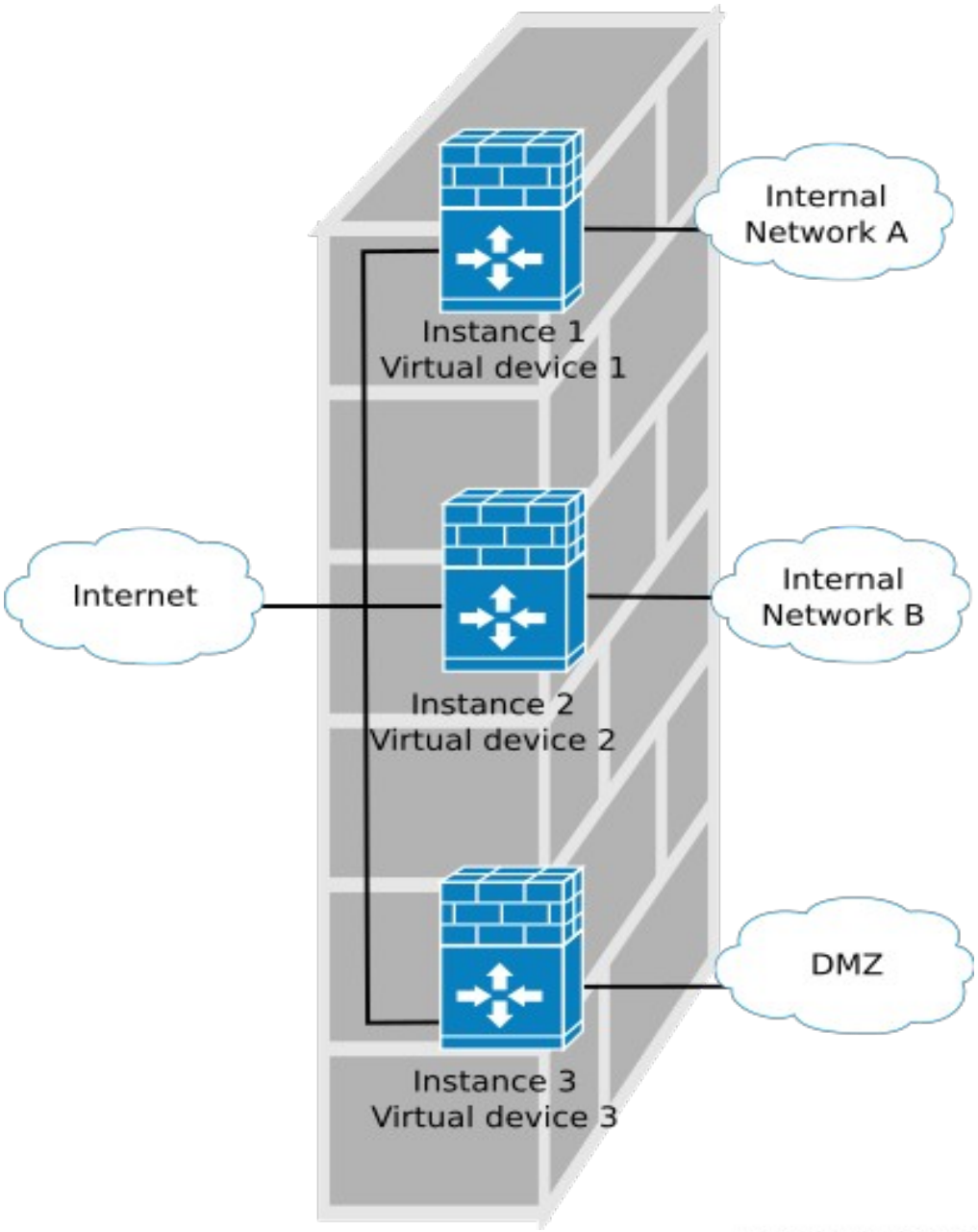
Firewall Zones/Group



- A network can be divided in multiple zones/groups with different security levels.
  - Collections of IP addresses, networks, or ports.
- 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.

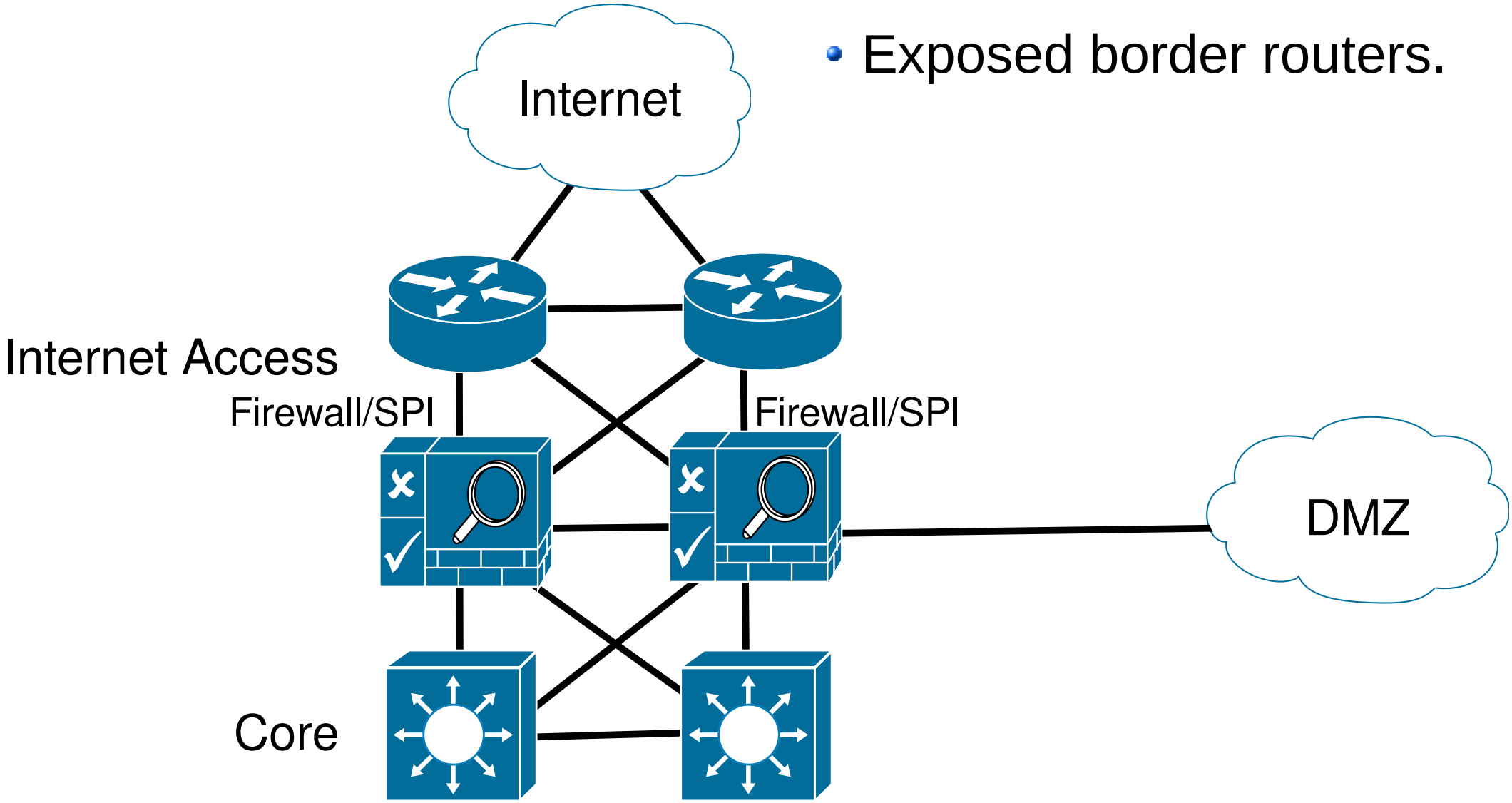
Firewall Virtual Instances

- 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.



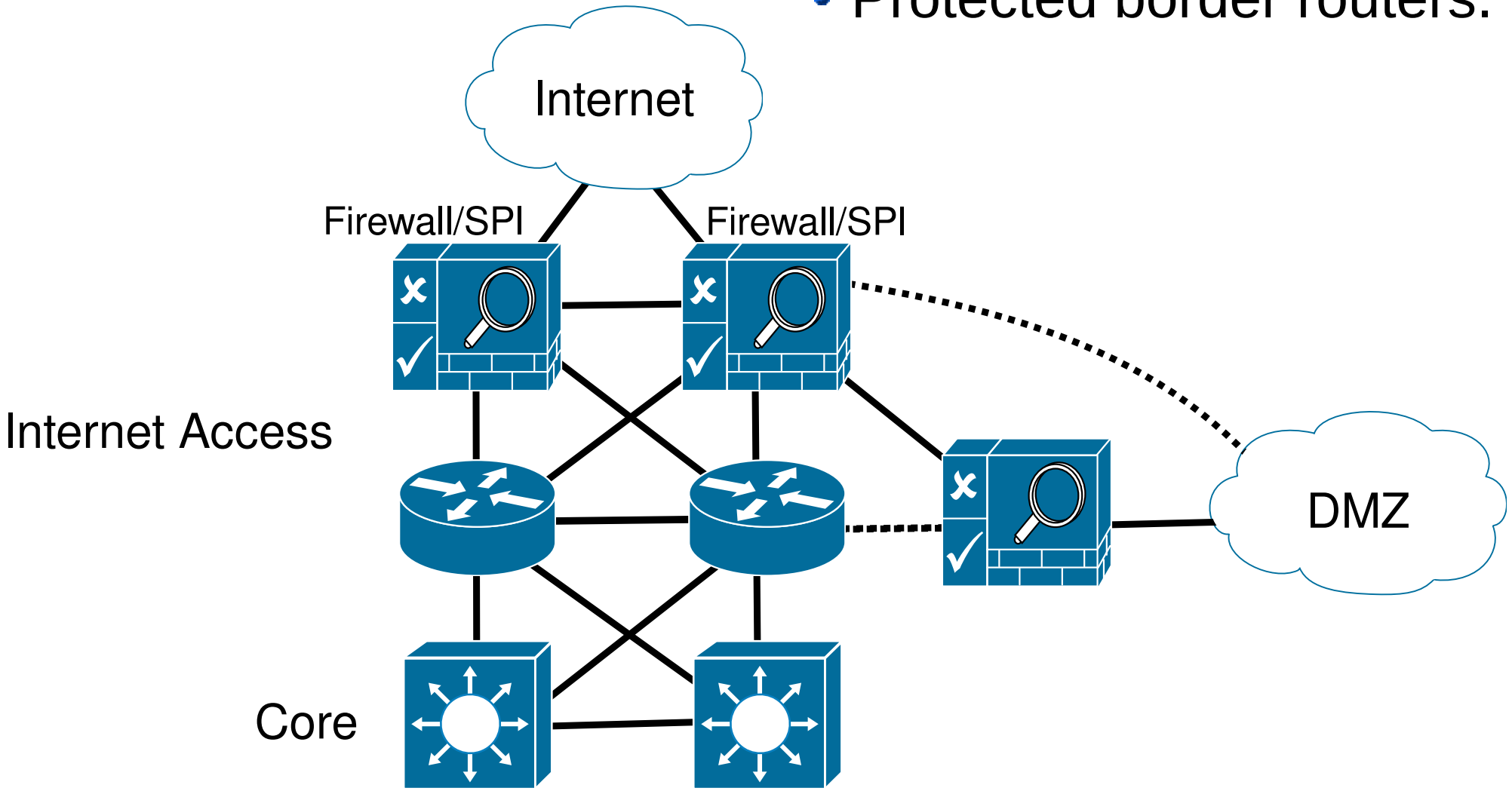
Firewall placement (with Redundancy)

- Exposed border routers.



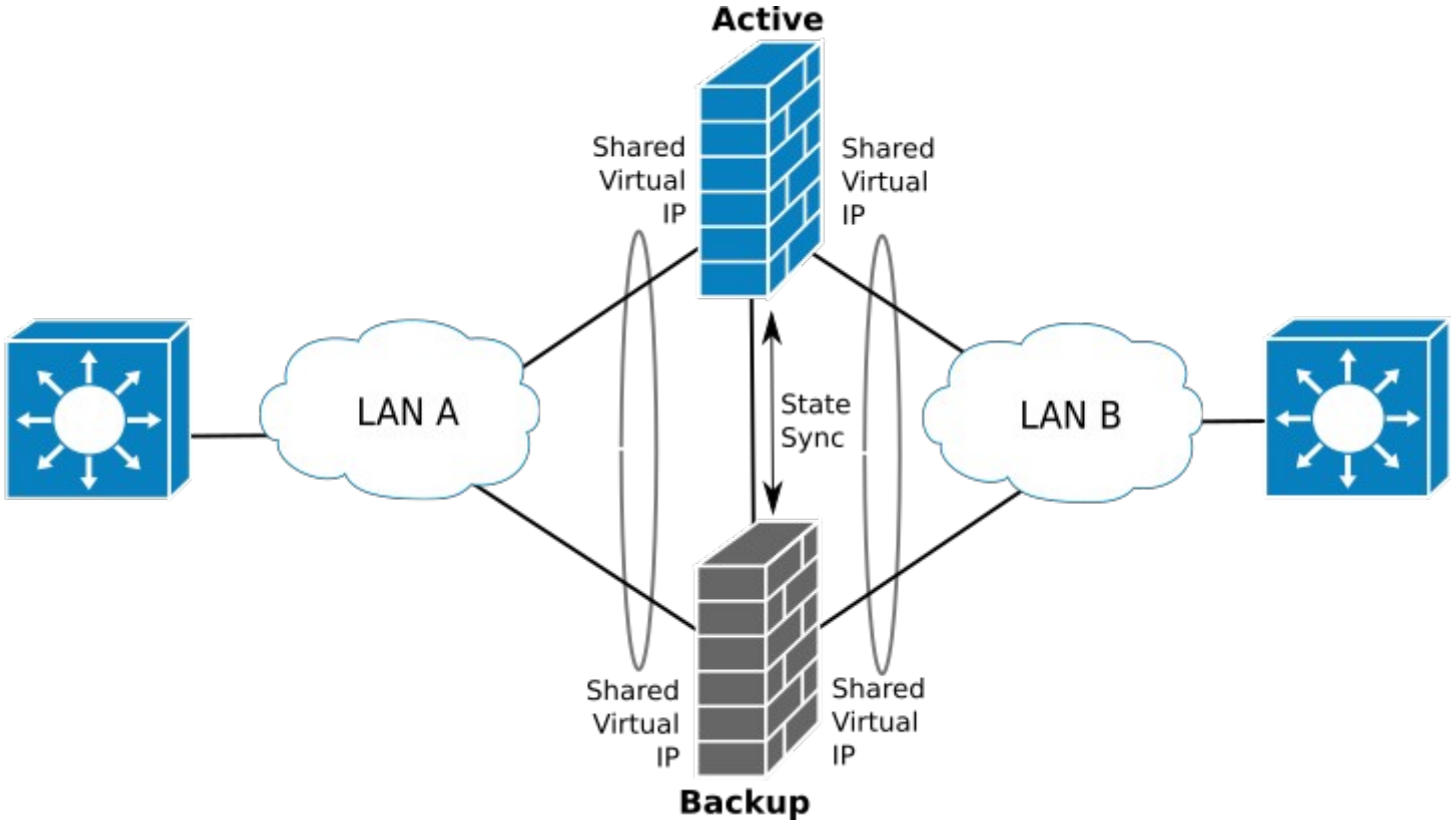
Firewall placement (with Redundancy)

- Protected border routers.



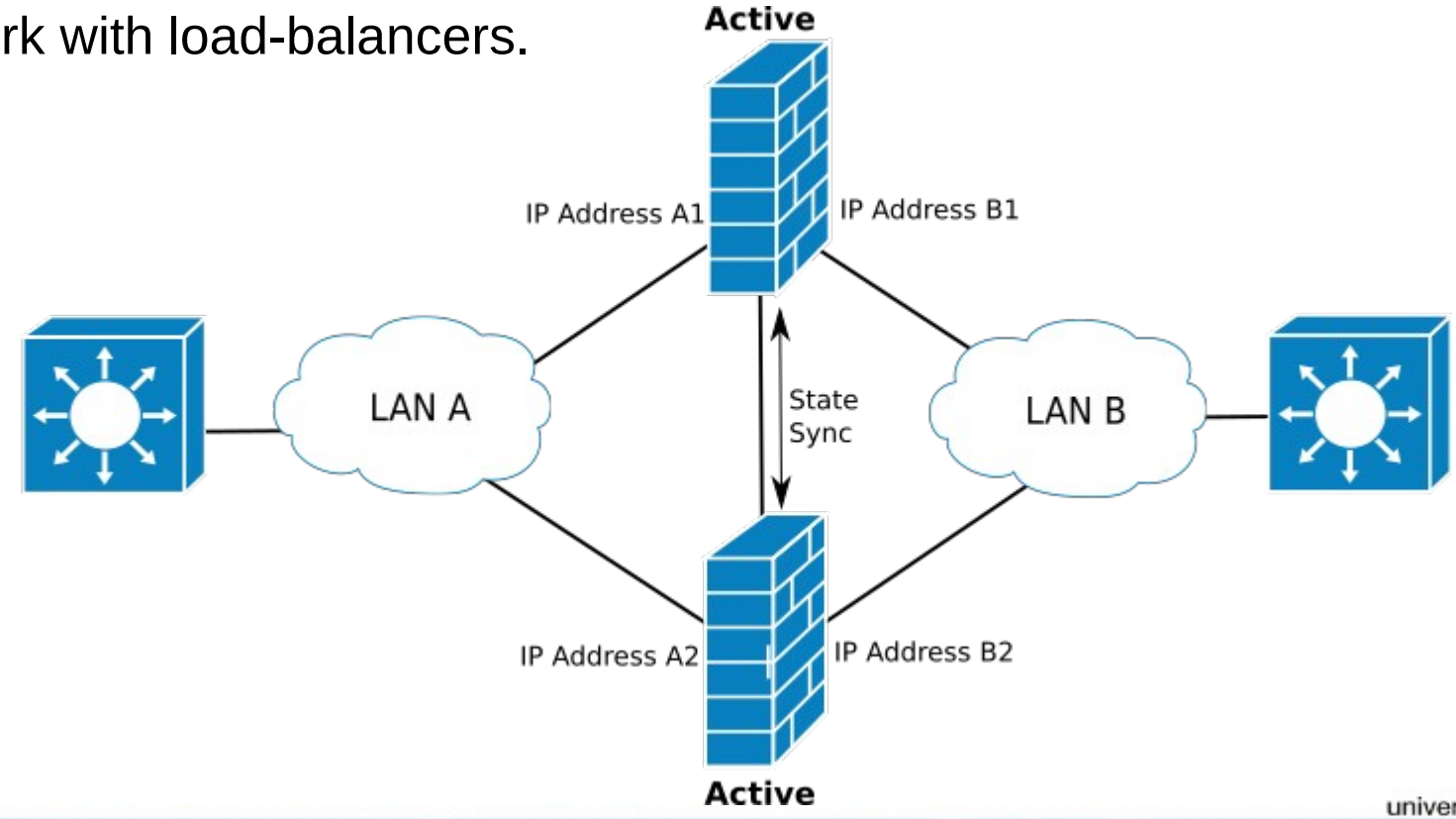
High-Availability (1)

- 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.



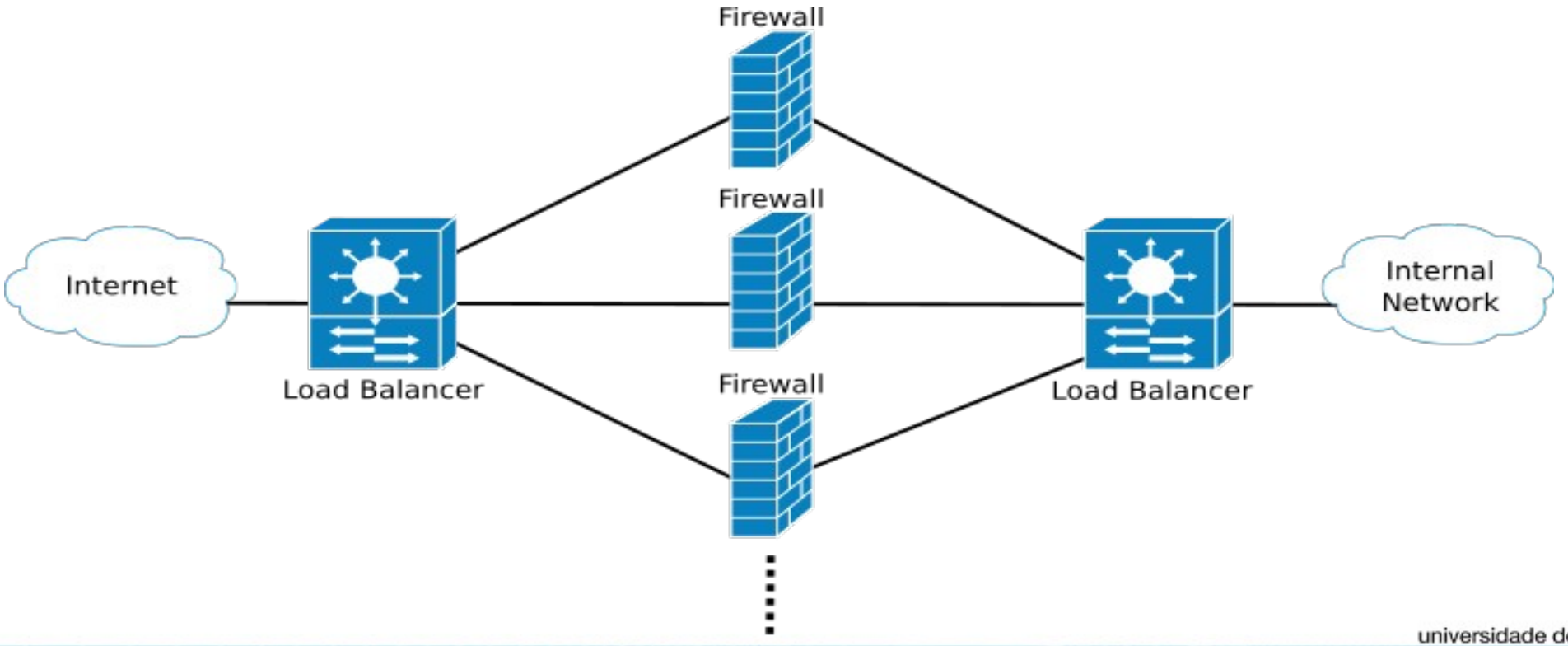
High-Availability (2)

- Active-Active Scenario
  - Firewalls share state via a dedicated connection
  - 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.
- 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.

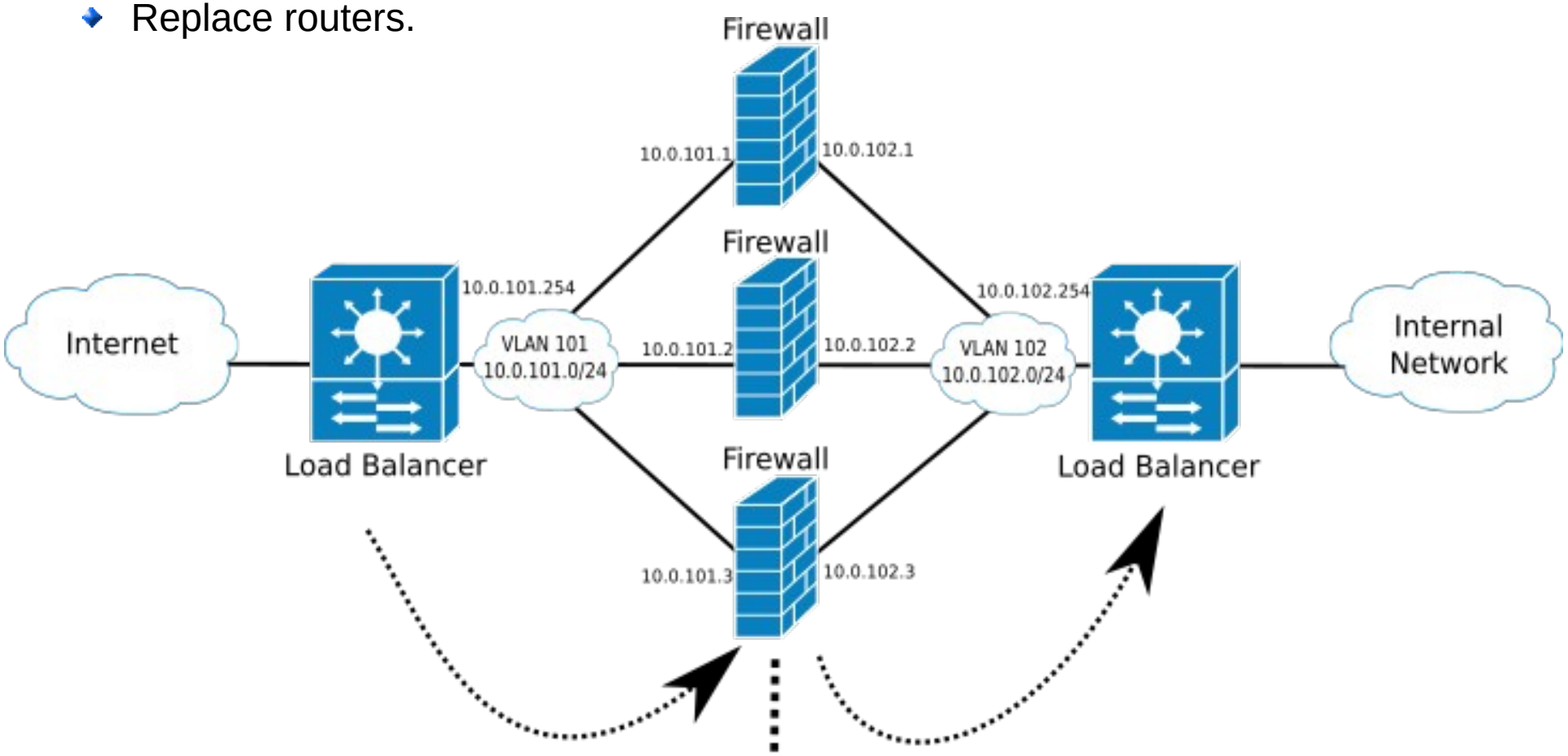


Load Balancing Algorithms

- 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 syncronization (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.
- “Smart”
  - Based on an external source of information.

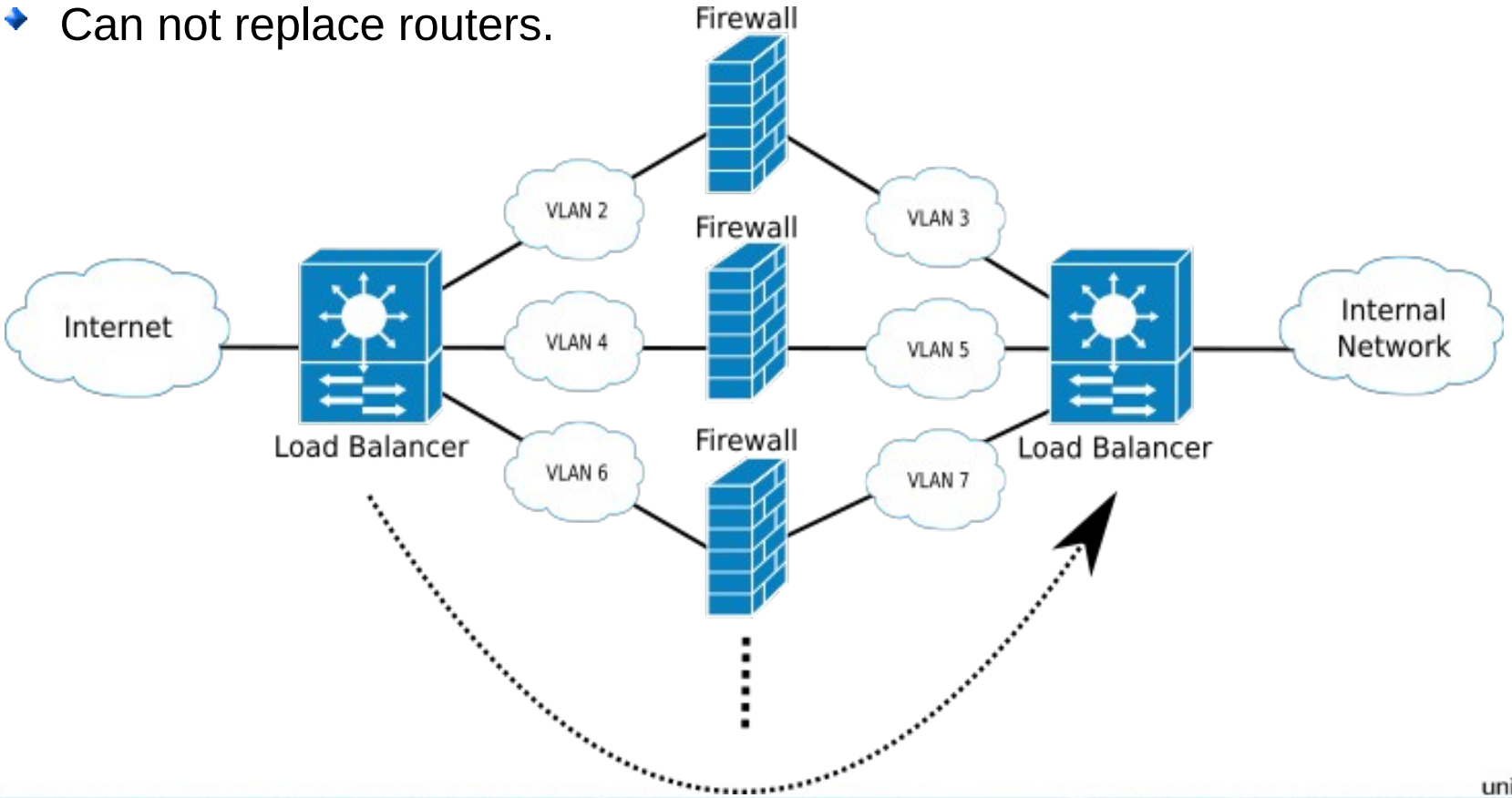
Addressed Firewalls

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



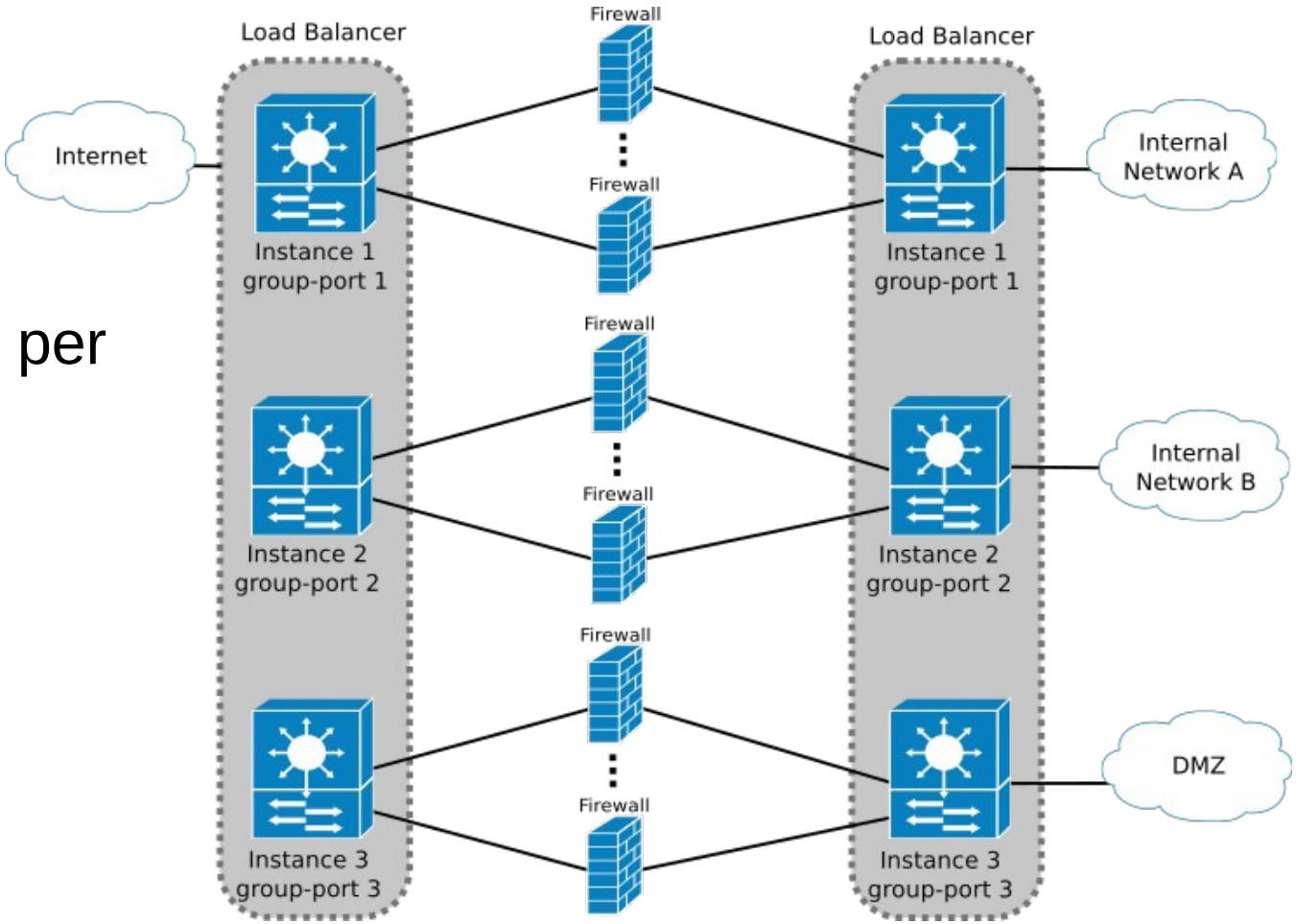
Stealth Firewalls

- 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.



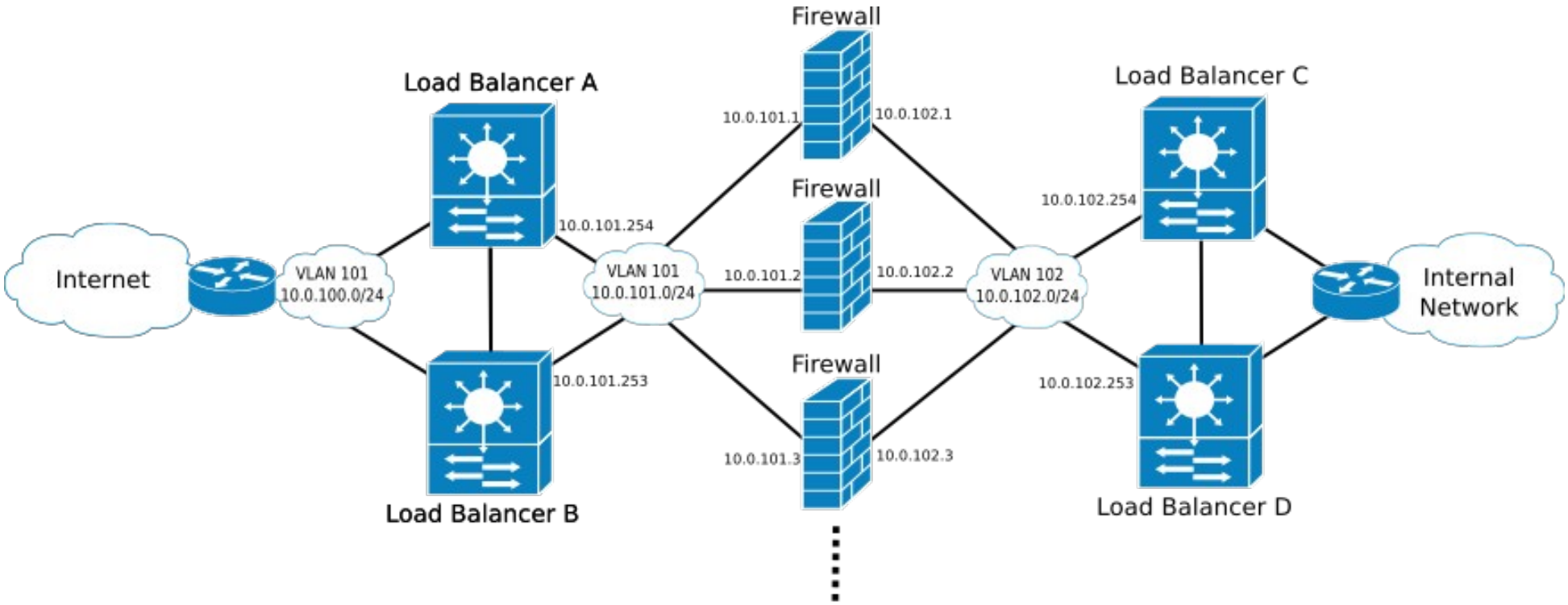
Load-Balancers Instances

- 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

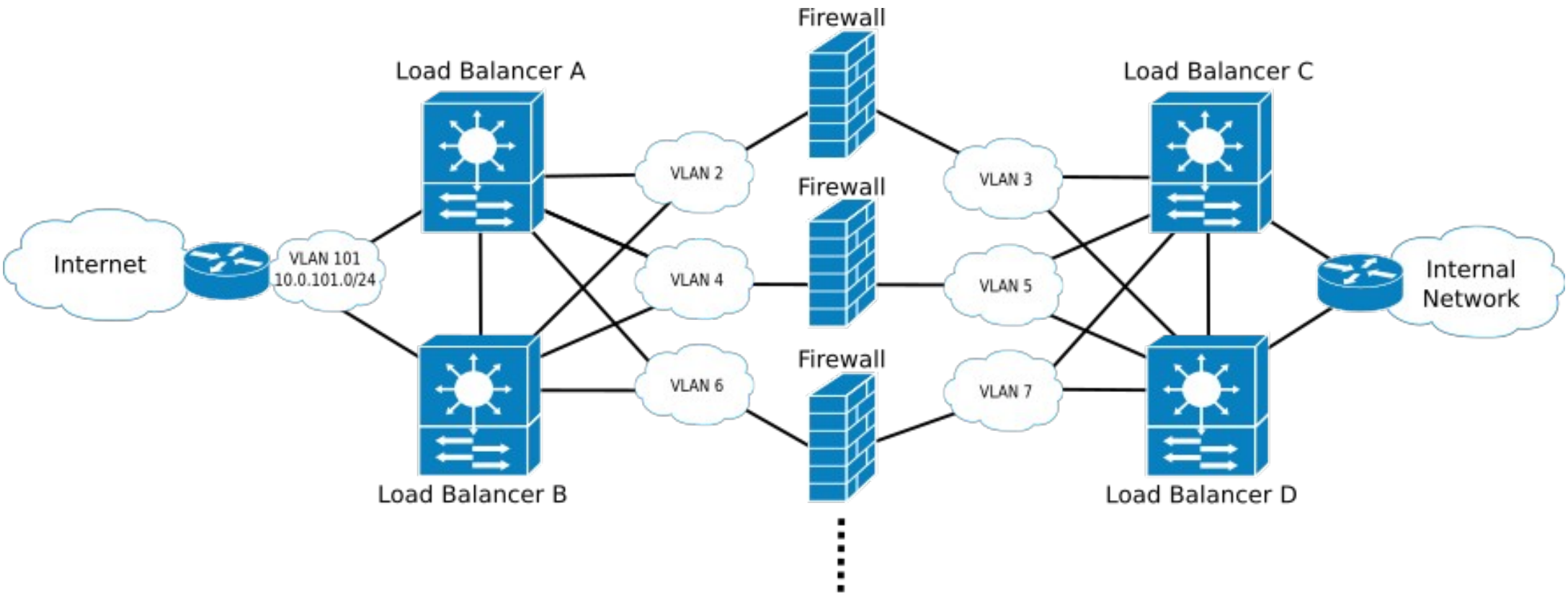
Addressed Firewalls



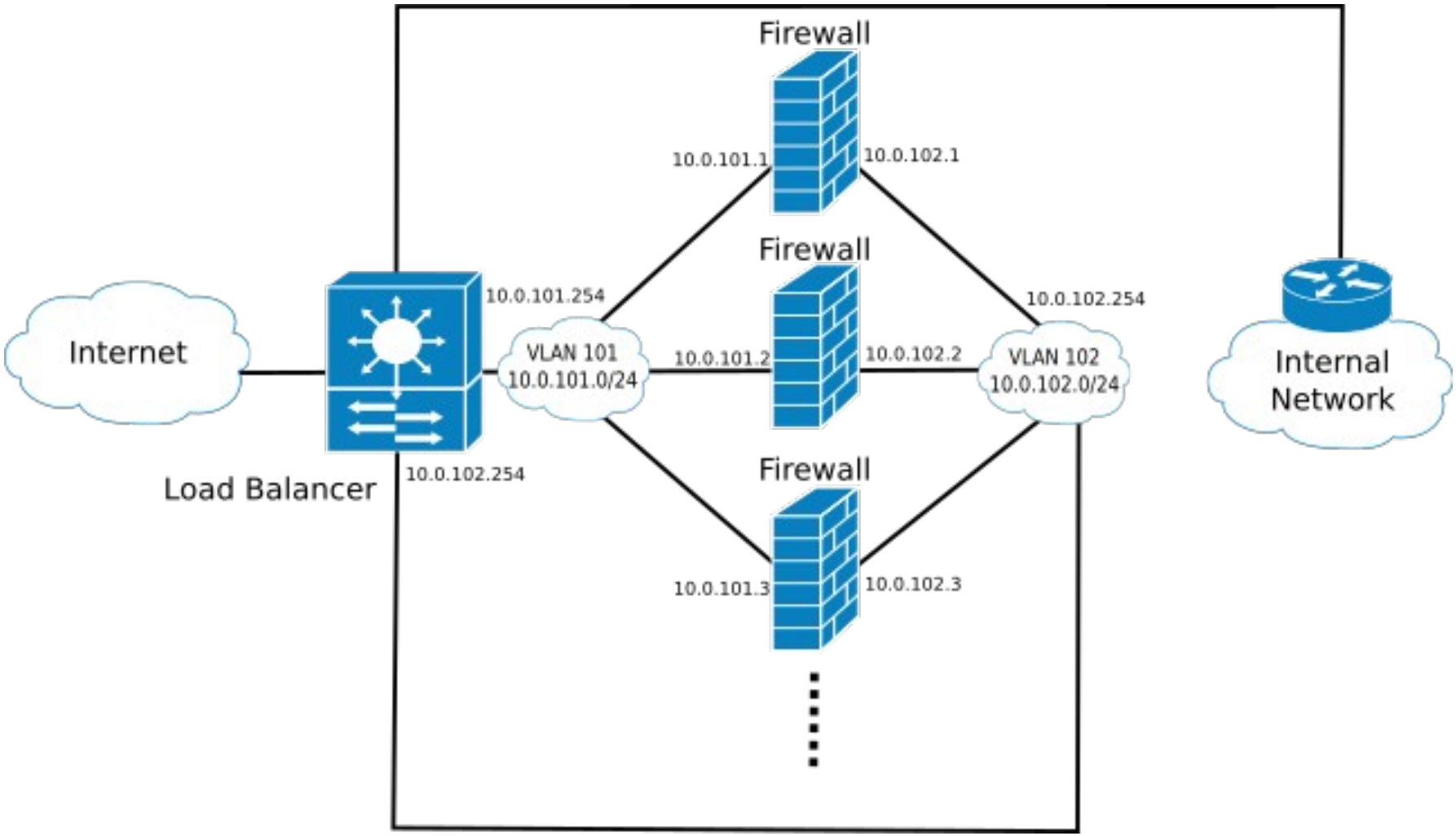
- To avoid FW state synchronizaion Load-Balancers should Sent packets of the same flow always to same firewall.
  - Must lower FW memory overload chance.
- Load-Balancers using IP Hash LB algorithms do nor require routing history synchronization (between LB).
  - Using other LB algorithms, they must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

Redundant Load Balancers

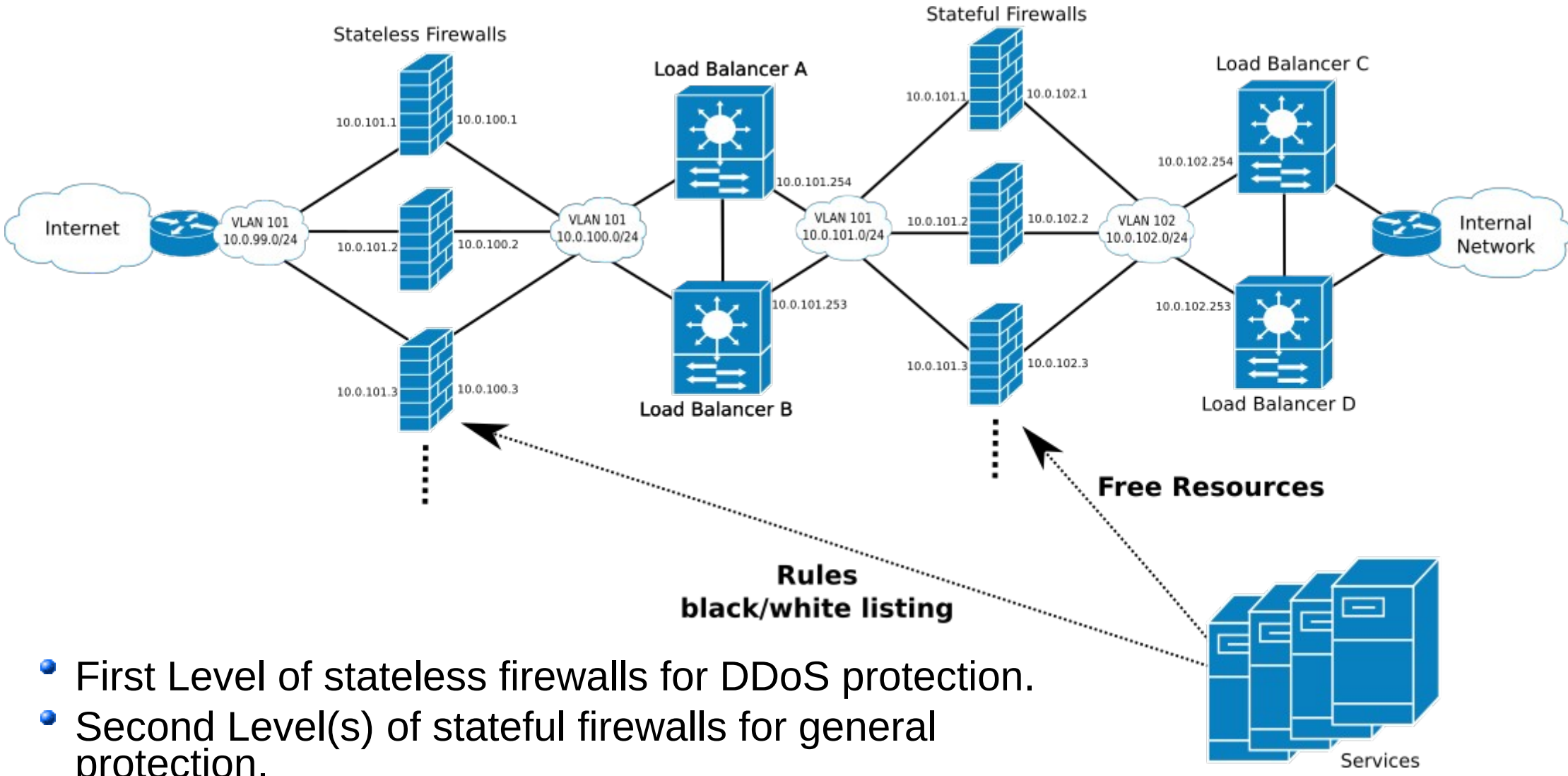
Stealth Firewalls



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

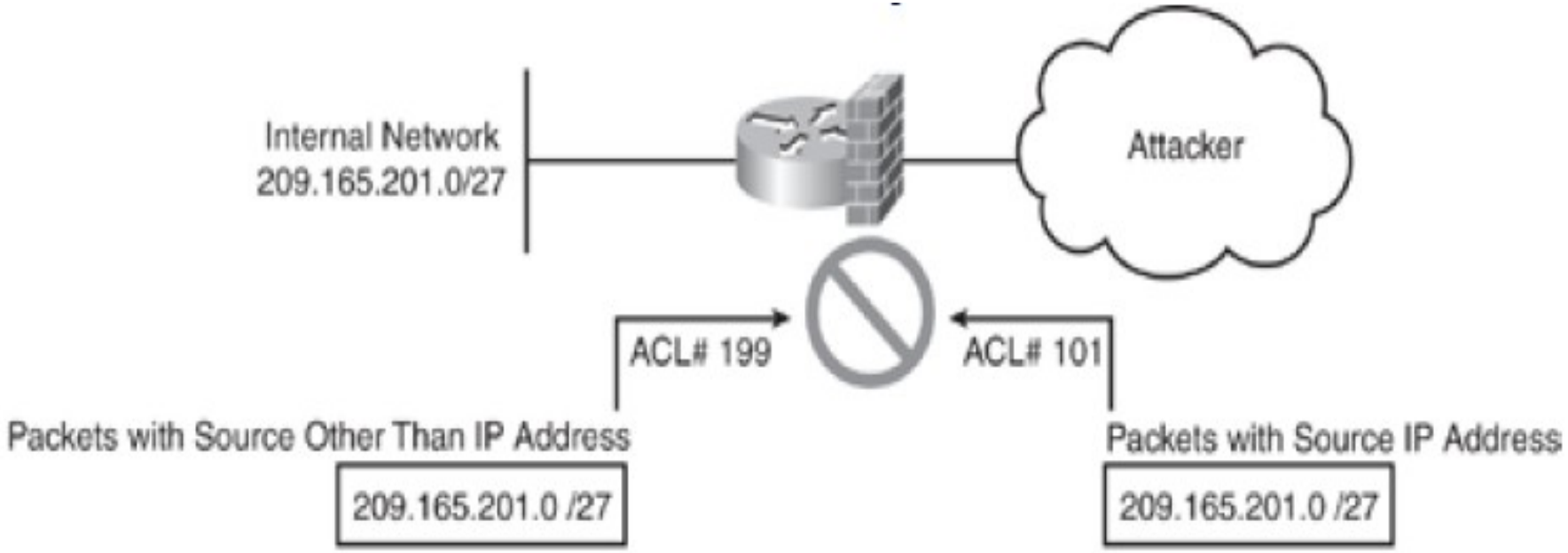
- Firewall rules must be specified based on traffic source, destination and type.
  - Source and destination may be IP addresses, Ports, Zones, etc…
  - Type may be defined in terms of protocol or protocol specifics.
- The first match determines whether the Firewall accepts/rejects the packet.
  - The **order of the conditions is critical**.
- 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)

Best Practices and Recommendations

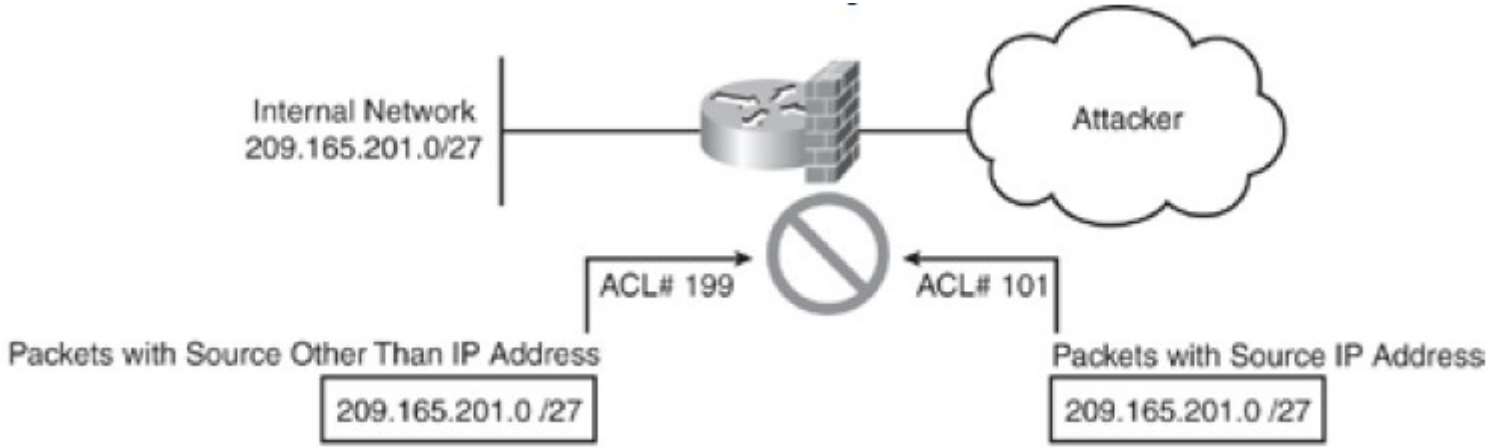
- Standardize your security policies.
  - Includes firewalls, network zones relations, devices and users profiles, active services, etc..
- Blocking all traffic by default.
  - Remove “Accept All” Rules.
- Add “Accept” exceptions.
  - Usually Clients to Service direction.
    - E.g., Internal to Internet, 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.



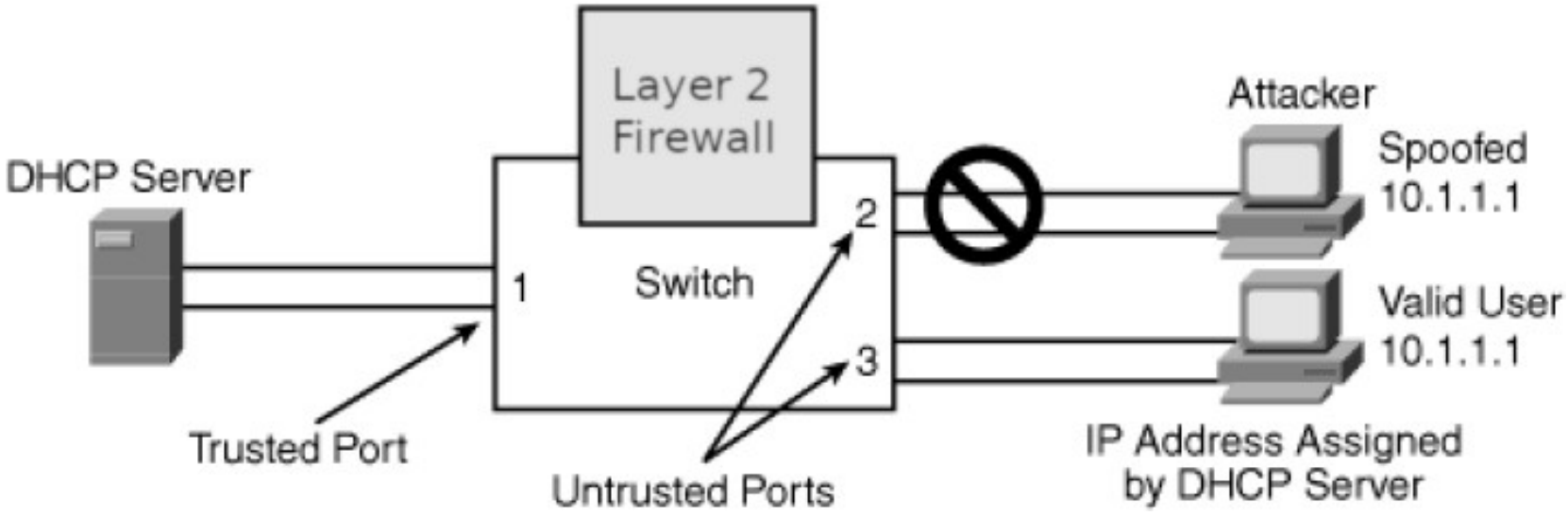
Preventing IP Spoofing at Layer 3



- 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
```

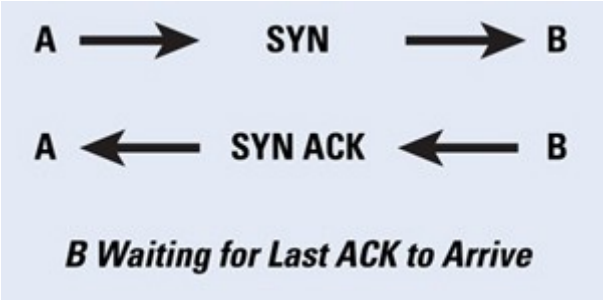
Preventing IP Spoofing at Layer 2



- To prevent IP spoofing attacks by restricting IP traffic on untrusted Layer 2 ports to clients with an assigned IP address.
- Works by filtering IP traffic with a source IP address other than that assigned via Dynamic Host Configuration Protocol (DHCP) or static configuration on the untrusted Layer 2 ports.
- Works in combination with the DHCP and is enabled on untrusted Layer 2 ports.

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.

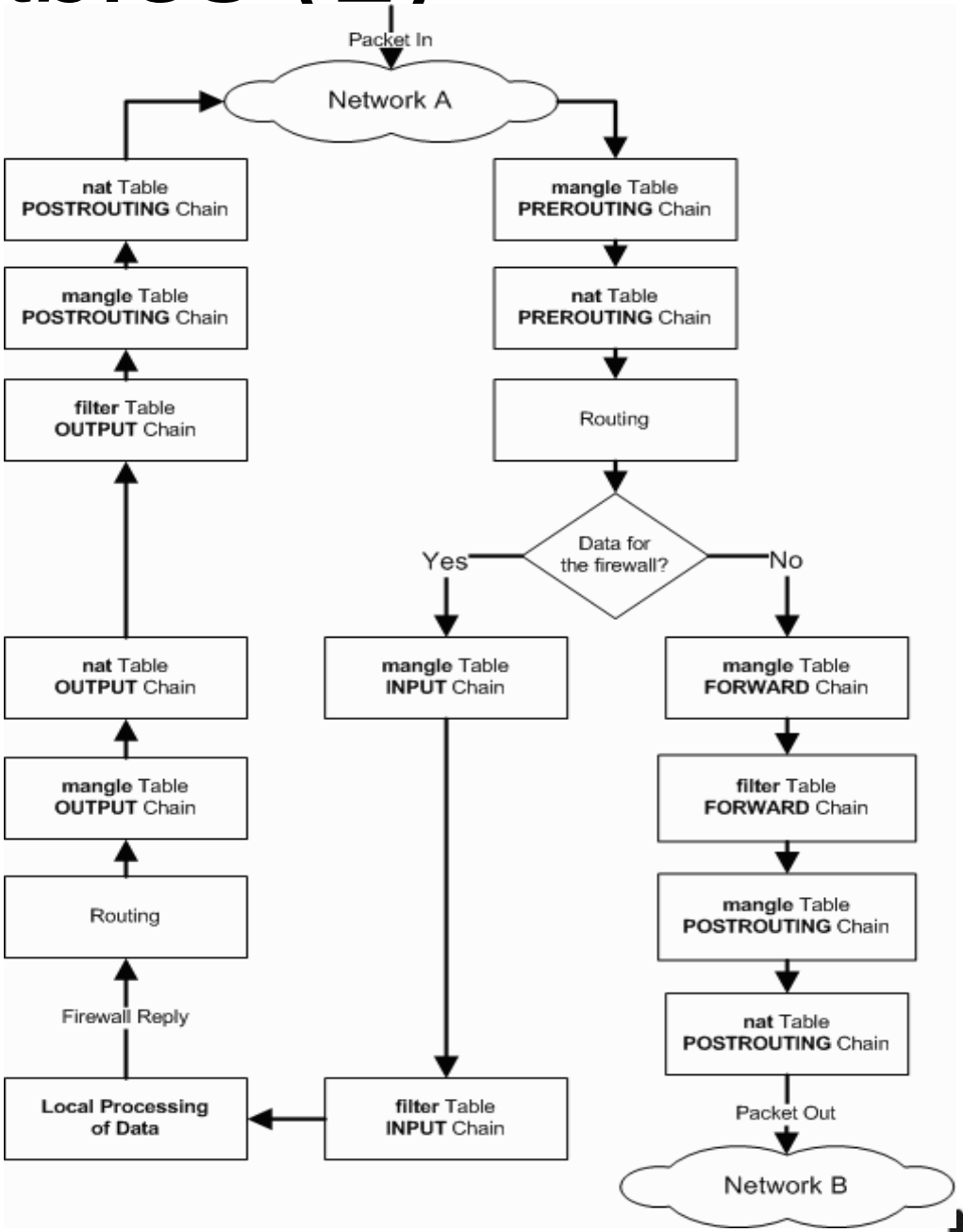


Firewall Performance Evaluation

- 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

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).



universidade de aveiro

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.
- 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.

Cisco's Access Control Lists (ACL)

- An access list is a sequential collection of **permit** and **deny** conditions.
- Software tests packets against the conditions in an access list one by one.
- The first match determines whether the software accepts or rejects the packet.
  - Because the software stops testing conditions after the first match, the order of the conditions is critical.
- If no conditions match, the software rejects the packet.
- Can be applied to inbound or outbound traffic.

ACL Types

- Standard
  - Control traffic by the analysis of the source address of the IP packets.
  - Numbered from 1 to 99
    - Example: access-list 1 permit 10.1.1.0 0.0.0.255
- Extended
  - Control traffic by the analysis of the source and destination addresses and protocol of the IP packets.
  - Numbered from 100 to 199
    - Example: access-list 101 permit ip any 10.1.1.0 0.0.0.255
- Named
  - Allow standard and extended ACLs to be given names instead of numbers Intuitively identify an ACL using an alphanumeric name.
  - Eliminate the number limits that exist on standard and extended ACLs.
  - Named ACLs provide the ability to modify ACLs without deleting and then reconfiguring them.
    - Example: ip access-list {extended | standard} name
- Reflexive
  - Allow IP packets to be filtered based on upper-layer session information.
  - Communication in one direction opens doors in the opposite direction.
  - Generally used to allow outbound traffic and to limit inbound traffic in response to sessions that originate inside the network.
- Context-Based Access Control (CBAC)
  - Inspects traffic to discover and manage state information for TCP and UDP sessions
  - This state information is used to create temporary openings in the firewall access lists