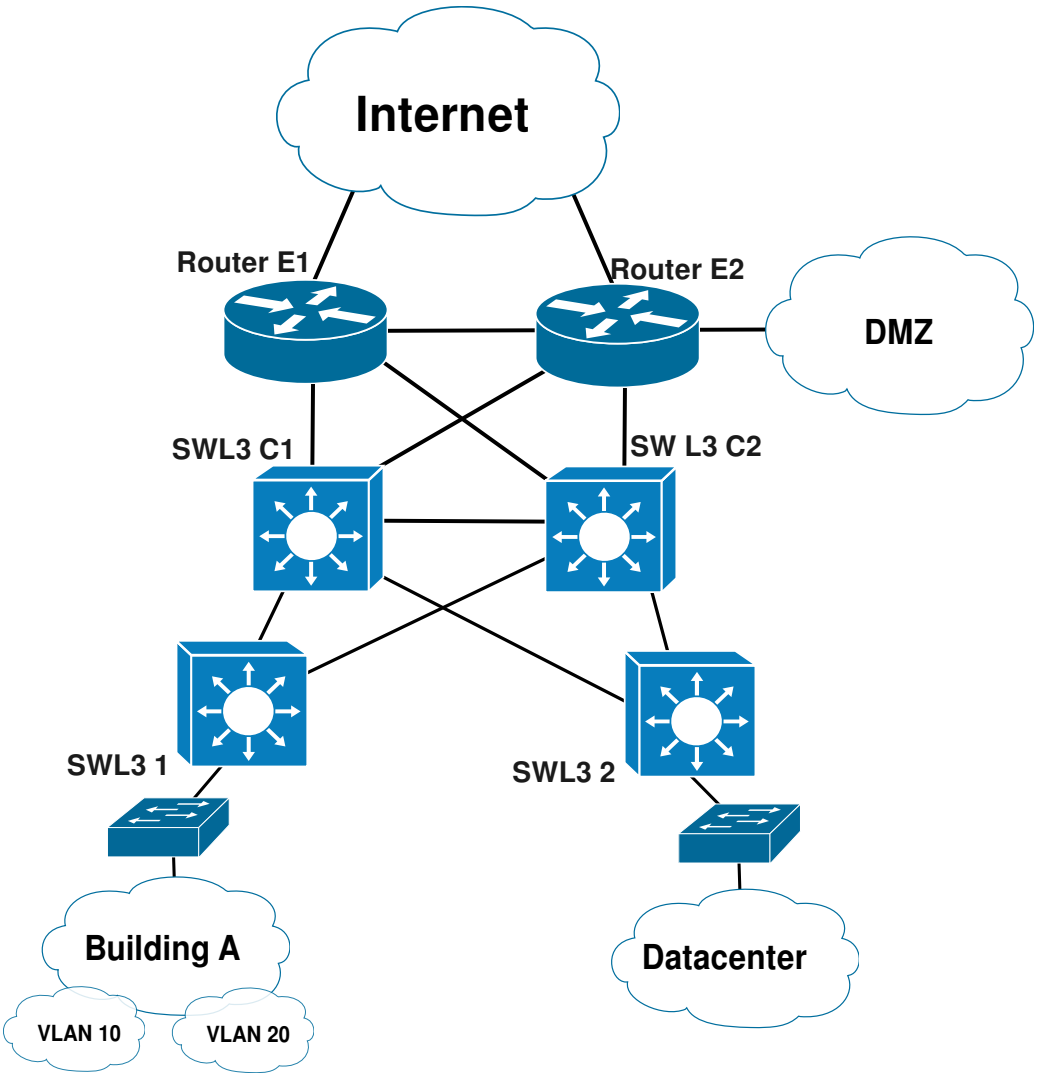
Segurança em Redes de Comunicações
Security in Communications Networks
First Project

Professor:
Paulo Salvador salvador@ua.pt;

Objective: Describe the configuration and operational tests of a network with redundant load-balancers and firewalls.

Description:

- Consider the (simplified) network in appendix.
- Use the network 10.0.0.0/16 to the internal connections, the network 10.10.0.0/24 for VLAN 10, the network 10.20.0.0/24for VLAN 20, 10.100.0.0/16 for the internal Datacenter, and network 200.0.0.0/24 for the DMZ. You may use network 100.0.0.0/24 for testing Internet services.
- Consider that the network have the following services (each one deployed in more than one server):
  - In the DMZ: Web services (HTTPS UDP/TCP 443), E-mail (IMAP TCP 993 and SMTP TCP 25), DNS (UDP 53).
  - In the internal Datacenter: Intranet/Storage (TCP 443), internal DNS (DNS 53), Databases (TCP 3306).
- **Note: You do not need to deploy the servers and you may choose the used IPv4 addresses in all servers/LANs/VLANs.**
- Consider the following security policies
  1. The network should able to handle high-rate DDoS attacks from the Internet.
  2. Internal devices may only access Internet services using ports TCP/UDP 80 and 443;
  3. All DMZ services must be accessible from the Internet and from inside the network;
  4. The intranet/storage and internal DNS may only be accessible by devices on VLAN 10 and 20.
  5. The internal Databases may only be accessible by devices on VLAN 20.
  6. A specific device on VLAN 1 (Building A) can PING and use SSH (port TCP 22) to access the console of all network devices.
  7. VLAN 10 devices may only use VoIP (SIP, port UDP 5060) to communicate directly with VLAN 20 devices, and vice-versa (do not deploy firewalls on the switching network of Building A).
- Define the placement of the firewalls, load-balancers and zones required to implement the security policies.
- Deploy and test the network using GNS3 (without security policies, but including the firewalls with an accept all policy and load balancers).
- Implement and test the security policies on the deployed network.
- Present a report of the configuration and operational tests of the scenario described above.
  Submit via e-learning, in format PDF, until April 29th.
  Should be done by a group of 2 students. Exceptionally, can be done individually.
- Task grading:
  Firewall and load-balancers deployment (2 points).
  Network routing and connectivity (2 points).
  Devices state synchronization (3 points).
  Zones definition [based on a security policies] (3 points).
  Inter-zone rules [based on a security policies] (6 points).
  Report (4 points).


Internet
Router E1
Router E2
DMZ
SWL3 C1
SW L3 C2
SWL3 1
SWL3 2
Building A
VLAN 10
VLAN 20
Datacenter