Universidade de Aveiro

Theoretical Exam – Security in Communication Networks
July 6th, 2022

Duration: 2h00m. Carefully justify all your answers.

Considering the corporate network depicted in annex:

1. In the context of the phases of an attack intended to steal data from a corporate network, explain why detecting and mitigating the attack is much more difficult during the infiltration phase than during the propagation and exfiltration phases. (3.0 points)

2. Propose a set of architectural changes to the enterprise network in order to protect it from DDoS attacks and allow the implementation of multiple traffic flow controls. Draw a new network diagram with the changes/additions, indicating the type, functionality and/or operating mode of each equipment. (4.0 points)

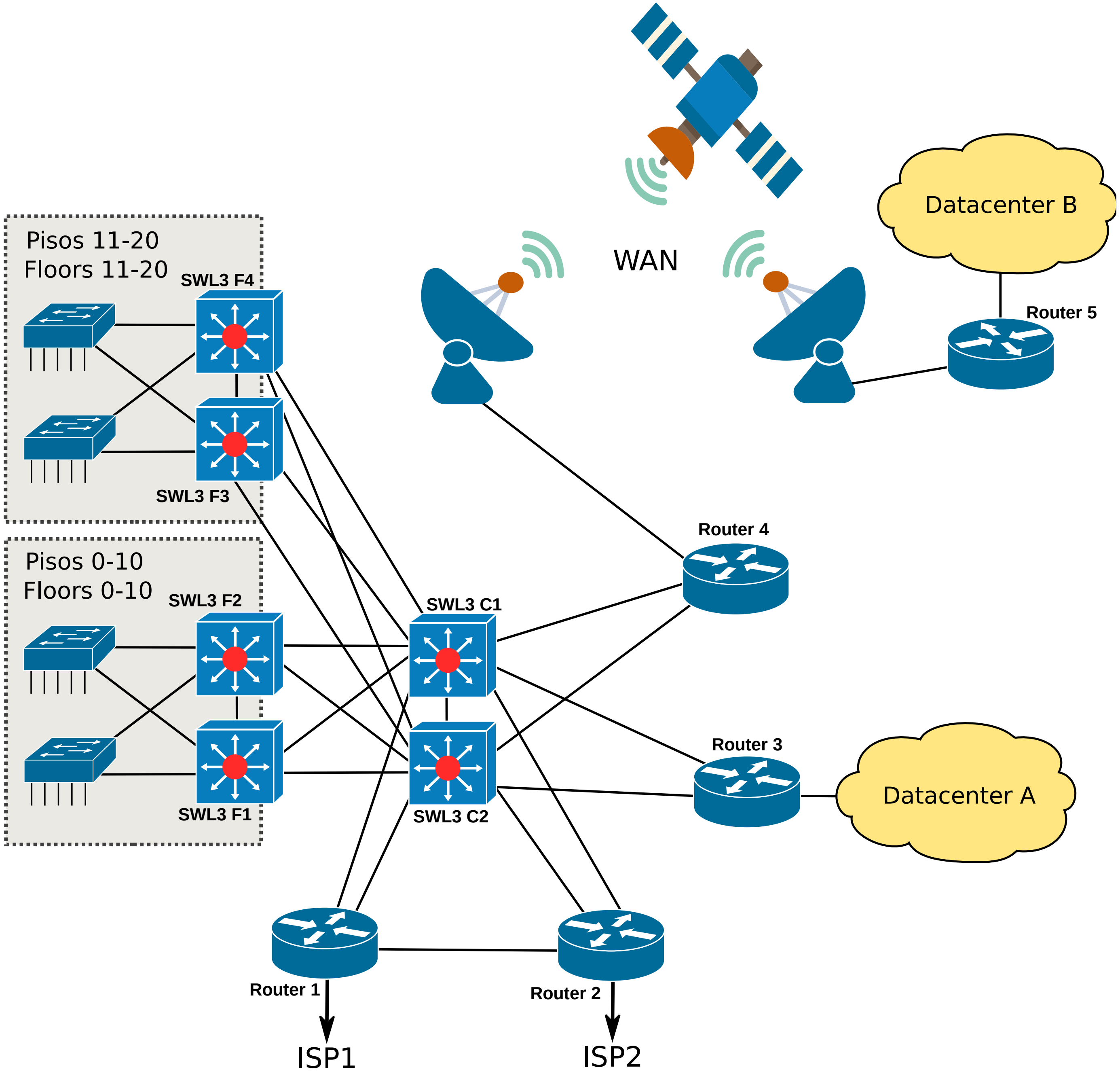
3. Assuming that the company wants to allow internal endpoints (not servers) to only access HTTPS services on the Internet (TCP port 443). And in parallel, implement a set of servers to provide services to the public (Internet), the new services include (i) an HTTPS Web server with several sites/domains (TCP port 443) and (ii) an email server (TCP port 465 for secure SMTP communication between servers and TCP port 993 for client access via IMAPS) . Propose the necessary network architecture changes and present a list of firewall/traffic flow control (high-level) rules at the various sites. (4.0 points)

4. Propose an interconnection solution using the company's WAN connection, between a set of database servers in Datacenter A and Datacenter B, capable of providing network-level confidentiality for data synchronization traffic from the servers (and only this traffic). Also introduce the necessary changes to the traffic flow control policies on the firewalls to allow secure connection establishment and data transmission. (3.0 points)

5. Assuming that the company wants to implement telework where remote users will have privileged access to two HTTPS servers (TCP 443 port) in Datacenter A. Propose an integrated solution that allows remote users access and control access to services. You must include in your proposal the necessary changes to the traffic flow control policies in the firewalls. (3.0 points)

6. Propose a SIEM system, including the data collection process and the definition of alert rules, capable of alerting to:
   a) Illegitimate access attempts (with failed logins) to servers in Datacenter B originating from internal endpoints. (1.5 points)
   b) Possible C&C (command and control) communication via HTTPS between an external attacker and internal machines compromised by agents of a Botnet. (1.5 points)

- On Layer 2 switches in buildings 1 and 2, access ports are configured for VLANs 1,2,3,4,5,6;
- The links between Layer2 switches and Layer3 are made using trunk/inter-switch links with transport permission for all VLAN;
- Interfaces between Layer 3 switches are Layer 3 ports (IP routing) and interfaces between Layer 3 switches and routers are Layer 3 ports (IP routing);
- The company has two internal Datacenters for internal services (Datacenters A e B);
- There is a satellite WAN connection that supports IPv4 connections between the company's network and a remote datacenter (Datacenter B);
- Layer3 switches and routers have OSPFv2 and OSPFv3 protocols active on all IP networks;
- Internet access routers (Routers 1 and 2) are both advertising (by OSPF) default routes;
- All interfaces have an OSPF cost of 1.


WAN
Datacenter B
Router 5
Pisos 11-20
Floors 11-20
SWL3 F4
SWL3 F3
Router 4
Pisos 0-10
Floors 0-10
SWL3 F2
SWL3 C1
Router 3
Datacenter A
SWL3 F1
SWL3 C2
Router 1
Router 2
ISP1
ISP2