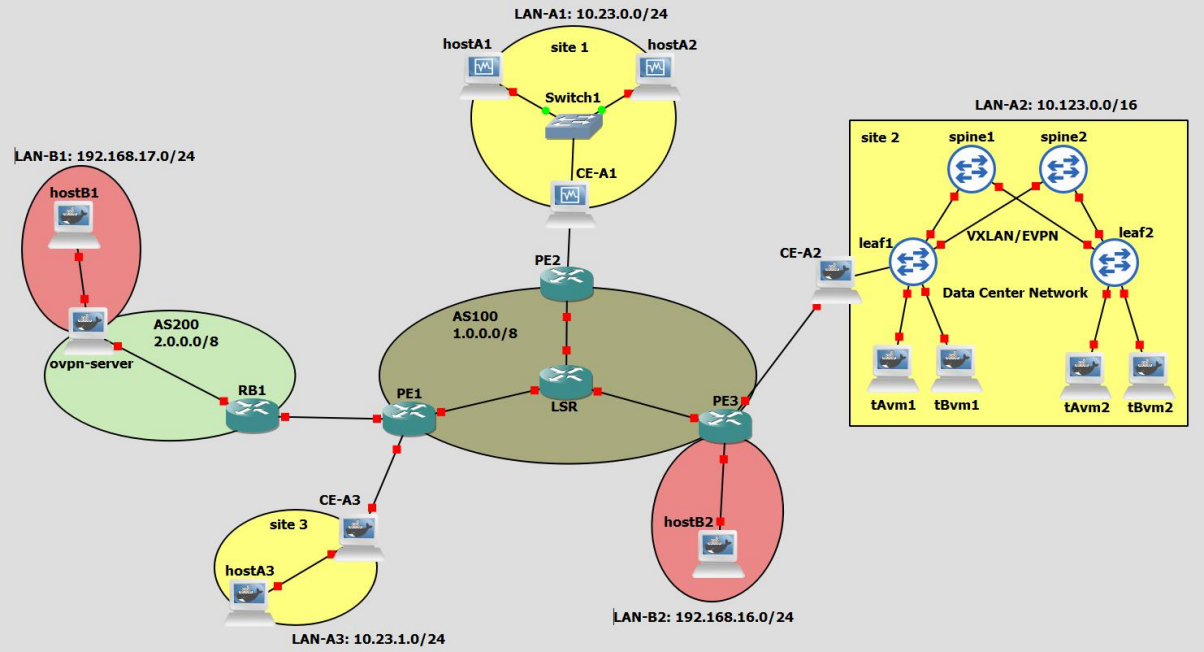
Network and System Defence
Final Projects AY 2022/2023

Project #1



In this project, there are 2 Autonomous Systems that provide network connectivity to five private networks. AS100 provides a BGP/MPLS VPN service for the three sites of VPN A. AS200 is a customer of AS100 and hosts an OpenVPN server with a public IP address, used to provide an overlay VPN for the VPN client in LAN-B1.

AS100

- Setup the necessary iBGP and eBGP peerings between internal and external routers (AS 200)
- Deploy MPLS with LDP in the AS100 core network
- Setup BGP/MPLS VPN to realize an Intra-AS VPN that connects the three sites of VPNA
  - Site 2 is the HUB, Sites 1 and 3 are the SPOKES
  - Spoke-to-spoke connectivity is enabled through the HUB

AS200

- Setup eBGP peering with AS100
- No need to setup OSPF between *ovpn-server* and RB1; static configuration is enough.

LAN-A1

- Setup MACsec in the LAN with MACsec Key Agreement protocol for all the devices in the LAN
- Realize a Firewall (with iptables/NETFILTER) in CE-A1 with the following security policies:
    - **Permit** traffic between LAN and external network only if initiated from the LAN, with dynamic source address translation
    - **Deny** all traffic to GW except ssh and ICMP only if initiated from the LAN
    - **Permit** traffic from GW to anywhere (and related response packets)
    - **Permit** port forwarding with DNAT to hostA1 and hostA2 from the external network only for the HTTP service

LAN-A2

LAN A2 is a leaf-spine Datacenter network with two leaves and two spines. There are 2 tenants in the cloud network, each hosting two machines connected, one to leaf1 and the other to leaf2. The tenants are assigned with ONE broadcast domain each; choose the broadcast domain network from the /16 private network provided in the Figure.

- Realize VXLAN/EVPN forwarding in the DC network to provide L2VPNs between the tenants' machines
- In leaf1, realize an outbound connection to reach the external network and the other sites of the configured Intra-AS VPN.
- Security policy (default DROP):
    - **Permit** traffic between LAN-A2 and the external network (including LAN-A1 and LAN-A3) only if initiated from LAN-A2
    - **Permit** forwarding between the spokes

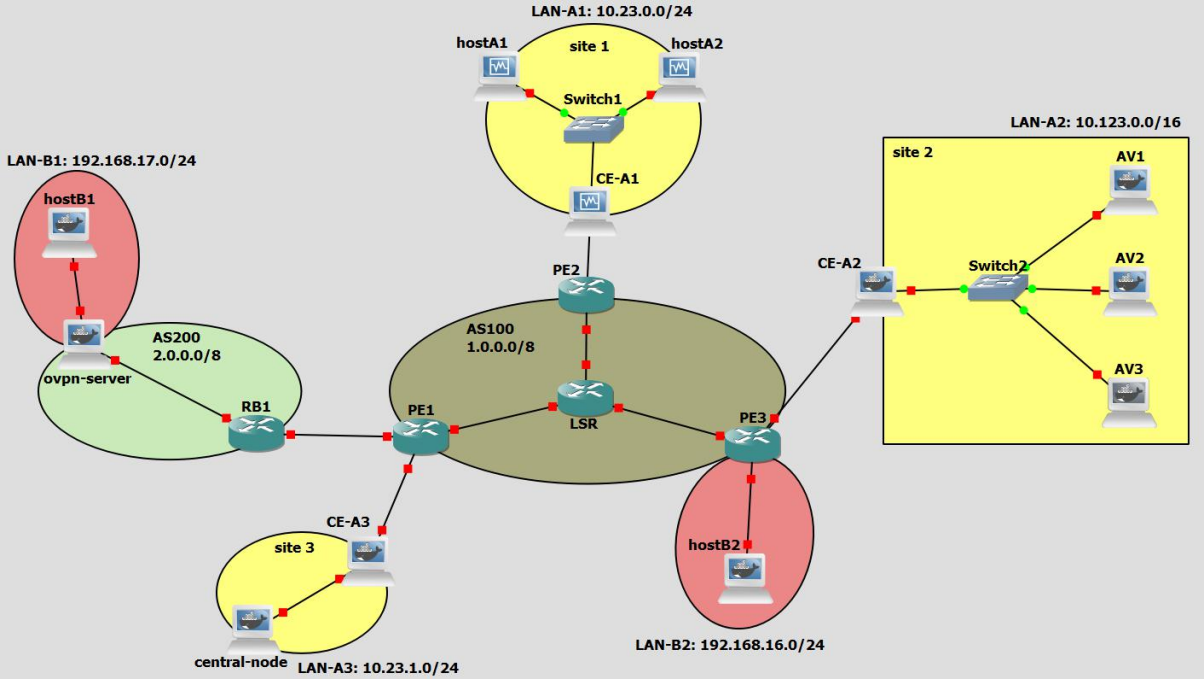
LAN-A3

LAN-A3 is Site 3 of the BGP/MPLS VPN in which there is just a Customer Edge, facing AS200, and one device in the private network. The device is sensitive, so it must be configured to use Mandatory Access Control.

OPENVPN

Setup OpenVPN with one server and one client. The server is in AS200, with a public IP taken from the 2.0.0.0/8 network. The client is host-B2, behind the private network in LAN-B2. The OpenVPN server provides access to LAN-B1 to which it serves as the gateway.

Project #2



In this project, you are expected to create a virtualized environment to test binaries for the presence of malware.
In particular, you have to setup multiple virtual machines or containers in Site 2, each hosting a different AV of your choice.
A central node (in Site 3) will allow dropping an executable and distributing it to the various testing nodes. The testing nodes will scan/run the executables and deliver results to the central node, which will build a report to the user, showing what threats (if any) were discovered in the binary.
Given the criticality of this infrastructure, certain precautions must be taken:
1. Runner nodes must be subject to snapshots so that they can be restarted in a 'clean' state each time a new scan has to be started.
2. To prevent the exfiltration of threats on the network, nodes must be protected by a firewall implemented in CE-A2. The firewall must permit the bidirectional end-to-end communication between the central node and the AVs, and deny all the rest.
In the central node, setup an external internet connection through a VirtualBox NAT interface.

Except for LAN-A2, the rest of the network configuration is the same as in Project 1, including the hub-and-spoke BGP/MPLS VPN connecting the three customer sites.