**Network Security Project**

**CSCE 5585**

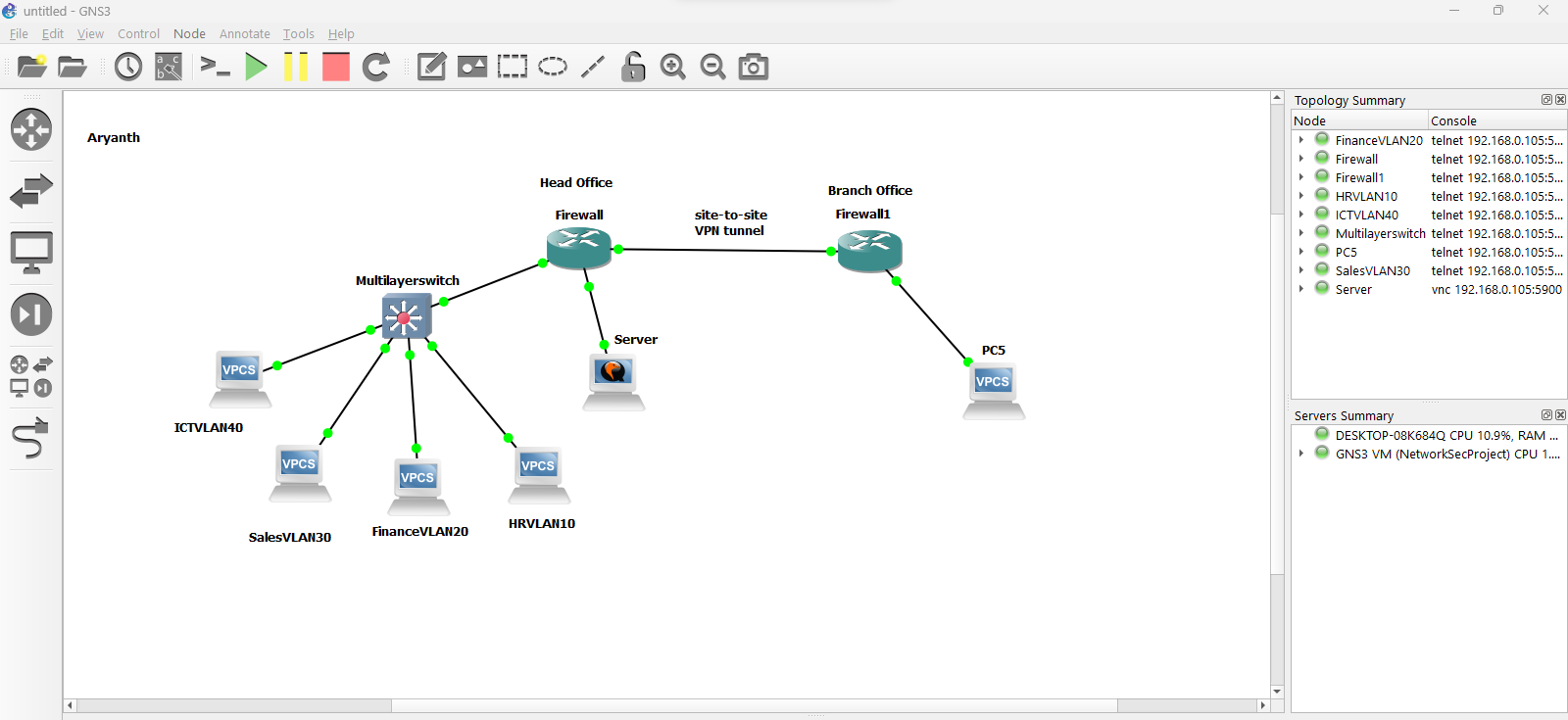
**Set Up**

GNS3 was the mainly used virtual network simulation platform established in the GNS3 VM for better virtual resource utilization. These covered a multilayer switch, virtual PCs (VPCS), a server, and FortiGate firewalls for both head office and branch office protection. It notes that perimeter security and access policies of the two facilities were to be governed by FortiGate firewalls also used to create a secure site-to-site VPN connection.

This multilayer switch was implemented to address VLAN segmentation, trunking, and inter-VLAN routing with SVIs. Client computers were then joined to the corresponding VLAN to mimic endpoint devices of the ICT, HR, finance and sale divisions. Configuration templates for the devices including VLAN tagging and IP addressing were accomplished through a GUI in GNS3. To check connectivity and validate, device login was done through Telnet, whereas the server was checked with VNC viewer. This configuration was made in GNS3 made it possible for one to emulate, test and ensure that the whole network was fit to be implemented.

**Network Design and Segmentation**Our network design incorporates a multilayer switch at the core, configured to manage traffic across four distinct VLANs: The access layer includes ICT (VLAN 40), Human Resource (VLAN 10), Finance (VLAN 20) and Sales (VLAN 30). Every VLAN has allocated concrete numbers of virtual PCs to avoid mixing of departmental traffics and their interconnection. Routing between VLANs has also been implemented in the multilayer switch so that communication between VLANs could be permitted only where appropriate. The switch and the server are connected through a single cable, and it means that the server is the central point of a network as long as services are concerned. Firewall has been implemented at head office network perimeter with an aim of protecting access and egress traffic.

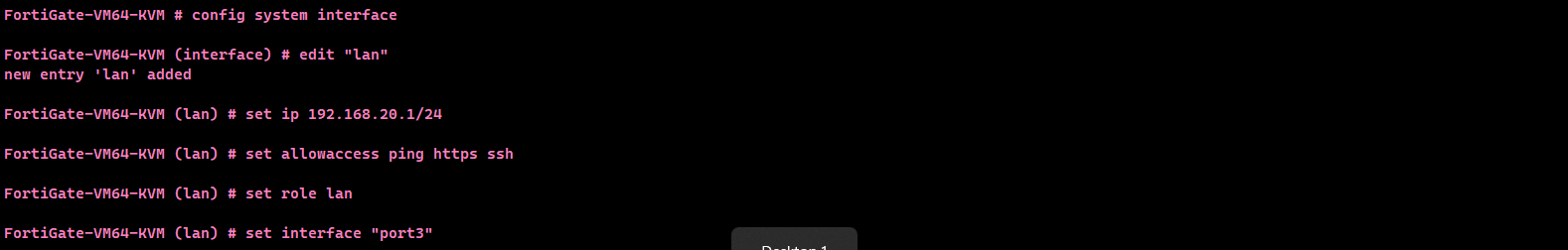
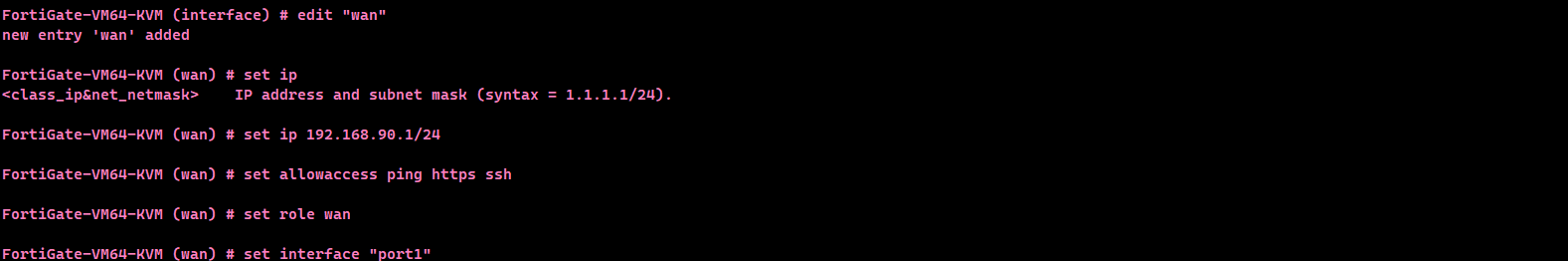
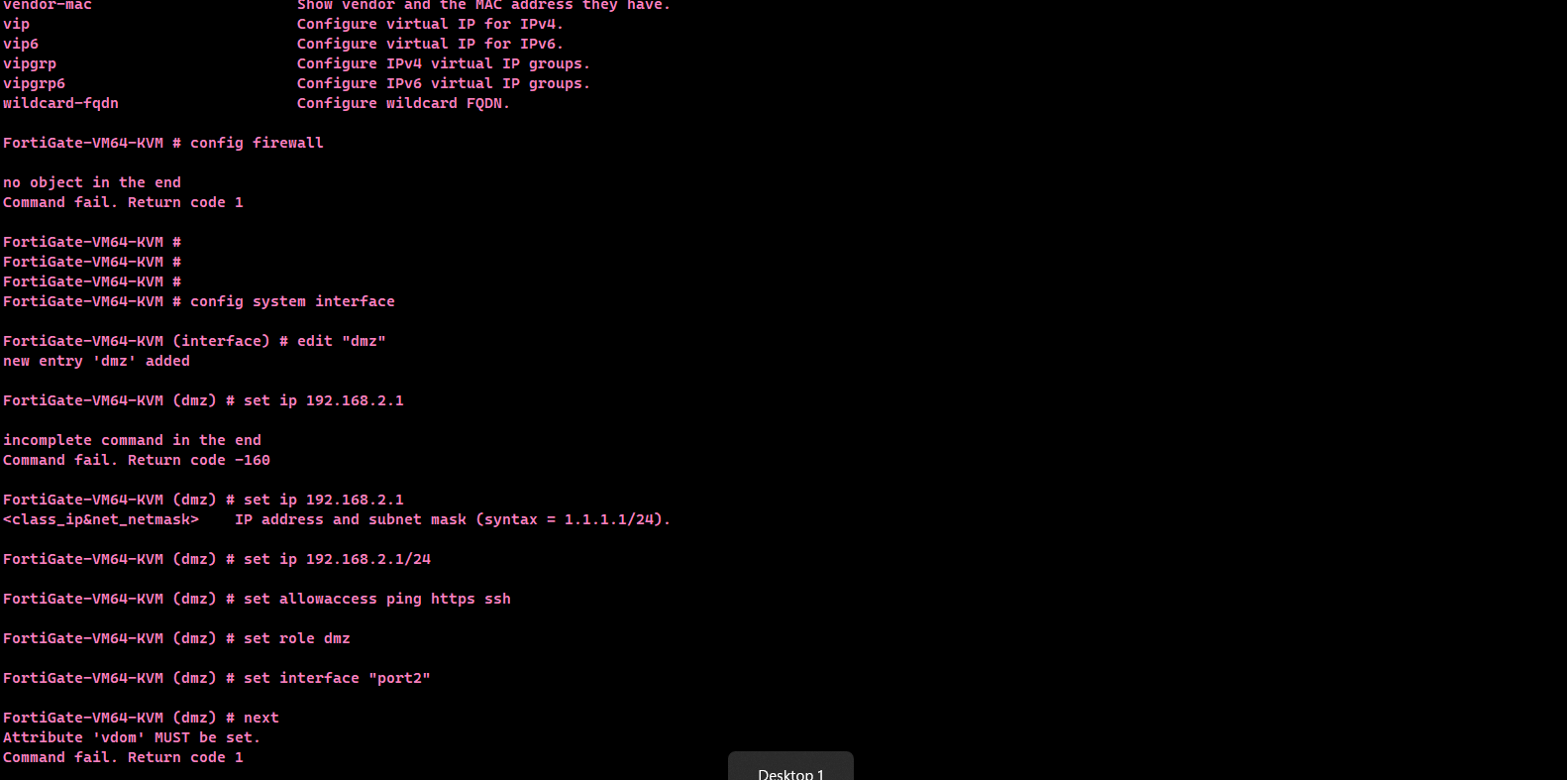
We set up a site to site VPN connection between the head office and the branch office which is a way of creating an encrypted link between the two sites. The branch office is protected by a firewall to access the office local resources and has also an accessible PC to work with. Through the use of VLANs to segment the network and use firewalls for the outer layer security we have enhanced the network for scalability, efficiency together with security and also provide secure transmission of data amongst the different offices through the VPN.



**Firewall configuration and deployment**

The FortiGate firewall was configured with three primary interfaces: DMZ, WAN, and LAN. For clarity and security purposes, each interface was provided with an IP address and a specific function. The WAN interface for connecting the switch to the internet was assigned a Public IP which allowed internet connection and also defined as the default gateway for outgoing and incoming traffic. LAN interface was also given an inside IP address to ensure it only communicates with other nodes in the inside network. At the same time, the DMZ interface was set up to contain services that should not be accessed from the outside, for example, web servers had limited external access but were allowed email pinging https and ssh for administrative reasons only.

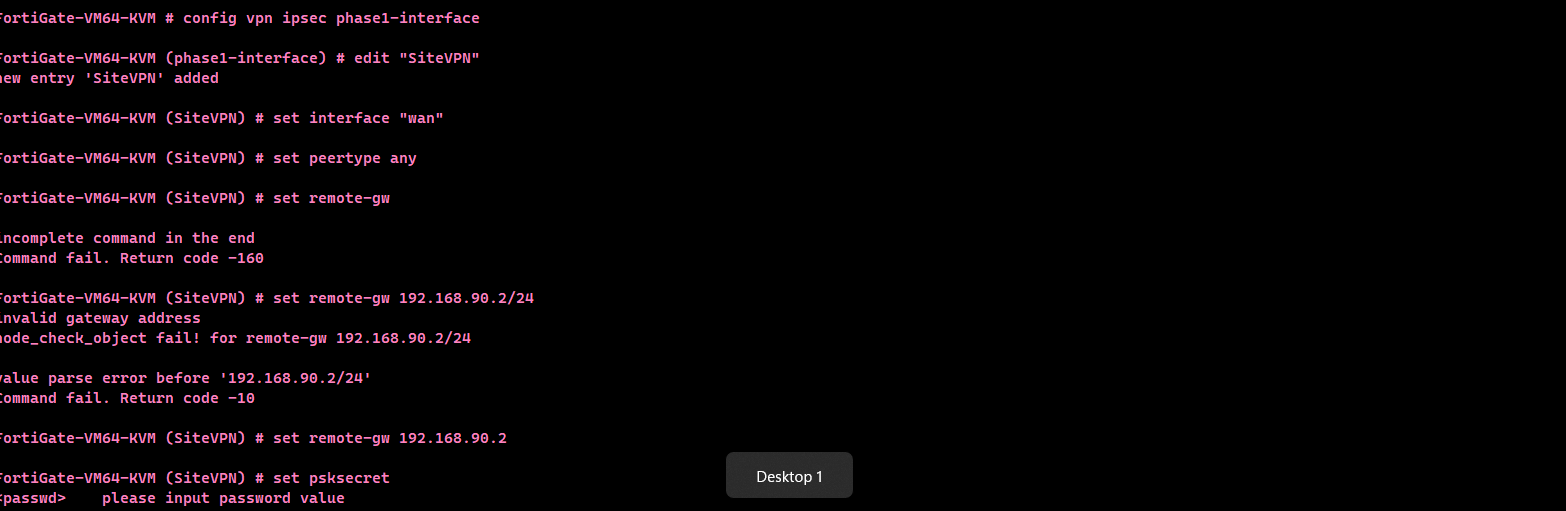
These interfaces were linked up to the right physical ports of a firewall, in relation to the overall architecture of the network. Roles for each interface were established in accordance with their use – LAN for internal communication, WAN for connections to the Internet, and DMZ for semi-closed limited access resources. This segmentation does not only enhance the network security but also makes policy development as well as traffic easy for management. To the configurations I made sure that all interfaces they are intact and ready for further enhancements of the security mechanisms.



**VPN Configuration**

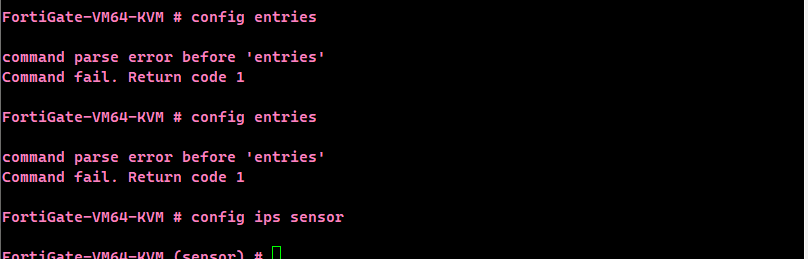
In order to connect the local network with a remote site it was decided to setup a Site-to-Site VPN. For the Phase 1 configuration we had to configure the WAN interface as the local identification, a pre-shared key and the IP address of the remote gateway. Encryption proposals using AES256-SHA256 were chosen to make sure that there is good security for the connection. DPD was configured to monitor the tunnel state and renegotiate the connection, when appropriate.

Phase 2 site settings were done to enable access with the local and remote subnet with traffic routes set for 192.168.1.0/24 for the local subnet and 10.0.0.0/24 for the remote subnet. Policies were implemented to open firewall to let the LAN and the VPN tunnel traffic to pass through in two ways, but with very secure permission. These configurations facilitate interaction with the remote site while at the same time preserving the data integrity and data privacy. Osome simple assessment tools were employed to check on tunnel connectivity and confirm the status of the VPN.



**IDS/IPS**

For strengthening the network security an IPS sensor was set up on the FortiGate firewall. The sensor was placed to monitor the traffic stream and pass the data through known protocols looking for malicious activity and vulnerabilities. Responses were set to “block” for the threats, but logging was turned on for possible incidents identification. Severity levels as well as locations were set to “all” so that coverage ranges from one hundred percent and tackling of numerous threats.The IPS sensor was then used to apply necessary firewall policies for reside in the WAN-DMZ traffic zone where threats are expected to come from. When the IPS was incorporated into the firewall policies, it automatically responds to threats stopping unwanted intrusions instantly. After the configuration is done the diagnostic was run to verify the operations of the sensor and in addition the IPS logs are checked to confirm that it is continually monitoring and defending the network. Such setup offers a strong layer of protection and increases the capability of the firewall in identifying the intrusions.



**Vulnerability Assessment and Penetration testing**

Following the final stages of network configuration, auditing was performed using Metasploit, and Nmap to determine the vulnerability level in the network. With Nmap, we also conducted a more comprehensive network scan of mapping of hosts alive, ports open and services running on the devices in the topology. This let us confirm that only required services were made available externally and also confirmed that FortiGate firewalls properly prevented access by unauthorized traffic. Further, in vulnerability scan, Nmap was employed to determine any open security flaws in the server and connected factors.

Lastly we engaged Metasploit for a number of scenarios with hopes of exploiting the identified vulnerabilities. Different penetration testing modules were conducted on the server and VLAN-segmented devices in order to confirm that the firewall rules, VLAN segmentation, and VPN encryption excluded intruder access and control. The conclusion supported that all the emulated attacks were prevented by the FortiGate firewalls and the VLAN isolation limited the movement within the departments. These tests are useful in as much as they justify the security systems that are in position making sure the network is shielded from external intruders and internal data is protected.

