

# **Secure Network Design and Implementation**

Son Dang, Prakiti Dhungel, Ashwini Gondhi

University of North Texas

CSCE 5585 Advanced Network Security

Dr. Ali Zarafshani

11/25/2025

# Abstract

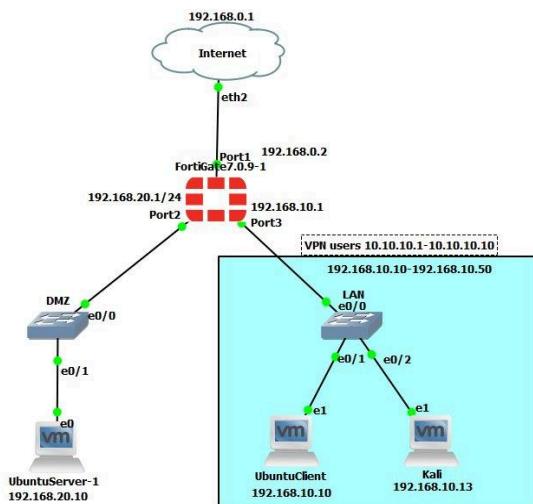
This project aims to design a secure network environment using GNS3 and Fortigate firewalls. It involves network topology with complete segmentation for the DMZ and LAN network, VPN services for remote connections, and IDS/IPS integrated functions utilizing Wireshark and Suricata software as well as the integrated IDS/IPS capabilities on FortiGate firewalls. The research also shows how Wireshark and Suricata can work together to protect a network by simulating a SYN flooding attacks. Additionally, by conducting a vulnerability assessment using Nexus, we can identify potential weaknesses and propose mitigation strategies to enhance the security defense of the system.

## 1. Introduction

This project focuses on designing and implementing a secure network environment using GNS3 and FortiGate firewall. We configured the network to demonstrate secure segmentation between the DMZ and LAN, VPN functionality, and IDS/IPS, showcasing threat detection and prevention using Wireshark and Suricata. We also performed a security assessment to identify vulnerabilities and propose mitigation strategies.

## 2. Network Environment (GNS3)

- FortiGate firewall (v7.0.9)
- DMZ, LAN switch
- Ubuntu server, Ubuntu/Kali clients
- Suricata & Wireshark



## 3. FortiGate Firewall Policies:

For our network firewall policies, we are allowing all traffic except from the DMZ to the LAN, since DMZ is a public-facing server, we do not want it to interact with our private local network. Firewall policy rules:

Allowed: LAN→DMZ, LAN→Internet, DMZ→Internet, VPN Remote→:LAN

Blocked: DMZ→LAN

Name	Source	Destination	Schedule	Action	NAT	Security Profiles	Log	Bytes
Block DMZ to LAN	all	all	always	ALL DENY			Disabled	0 B
DMZ to Internet	all	all	always	ALL ACCEPT	Enabled	IPS all_default SSL certificate-inspection	UTM	0 B
LAN to DMZ	all	all	always	ALL ACCEPT	Enabled	IPS all_default SSL certificate-inspection	UTM	1.42 MB
LAN to Internet	all	all	always	ALL ACCEPT	Enabled	IPS default SSL certificate-inspection	UTM	612.25 kB
vpn_VPN_remote_0	VPN_range	lan	always	ALL ACCEPT	Enabled	IPS high_security SSL certificate-inspection	UTM	0 B
Implicit								

## 4. VPN Remote Access

We have configured remote access for external users to access the private LAN network. New users will be assigned an IP address from 10.10.10.1 to 10.10.10.10, demonstrating how IPSec and tunneling work.

Tunnel Template



Convert To Custom Tunnel

Dialup - FortiClient (Windows, Mac OS, Android)

Convert To Custom Tunnel

---

Name

Comments

VPN: VPN (Created by VPN wizard)  
32/255

---

Network

Incoming Interface : port1

IPv4 client address range : 10.10.10.1-10.10.10.10/255.255.255.255

 Edit

---

Authentication

Authentication Method : Pre-shared Key

 Edit

---

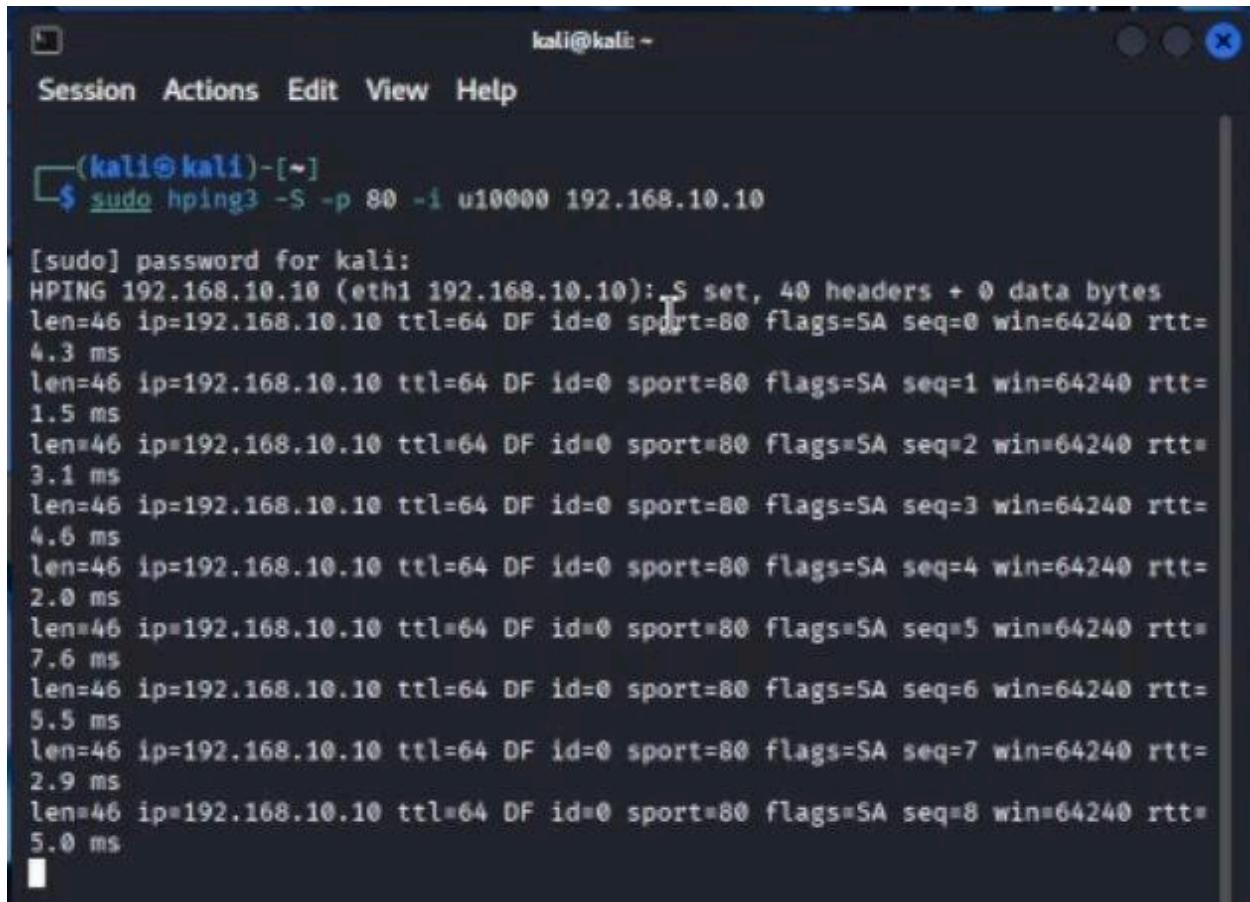
XAUTH

User Group: vpn

 Edit

## 5. IDS/IPS Config/Simulating SYN flood attack

Along with IPS in firewall functionality, we also implement additional IDS and IPS in the Ubuntu Client to demonstrate the effectiveness of both systems. First, we use the hping3 attack to flood the Ubuntu with SYN packets from the Kali client to the Ubuntu Client. From the Ubuntu client, we detected the attacks using Wireshark and prevented them using Suricata.



The screenshot shows a terminal window titled 'kali@kali: ~'. The menu bar includes 'Session', 'Actions', 'Edit', 'View', and 'Help'. The command entered is '\$ sudo hping3 -S -p 80 -i u10000 192.168.10.10'. The output shows the results of the hping3 command, which is sending SYN packets to the specified target. The output is as follows:

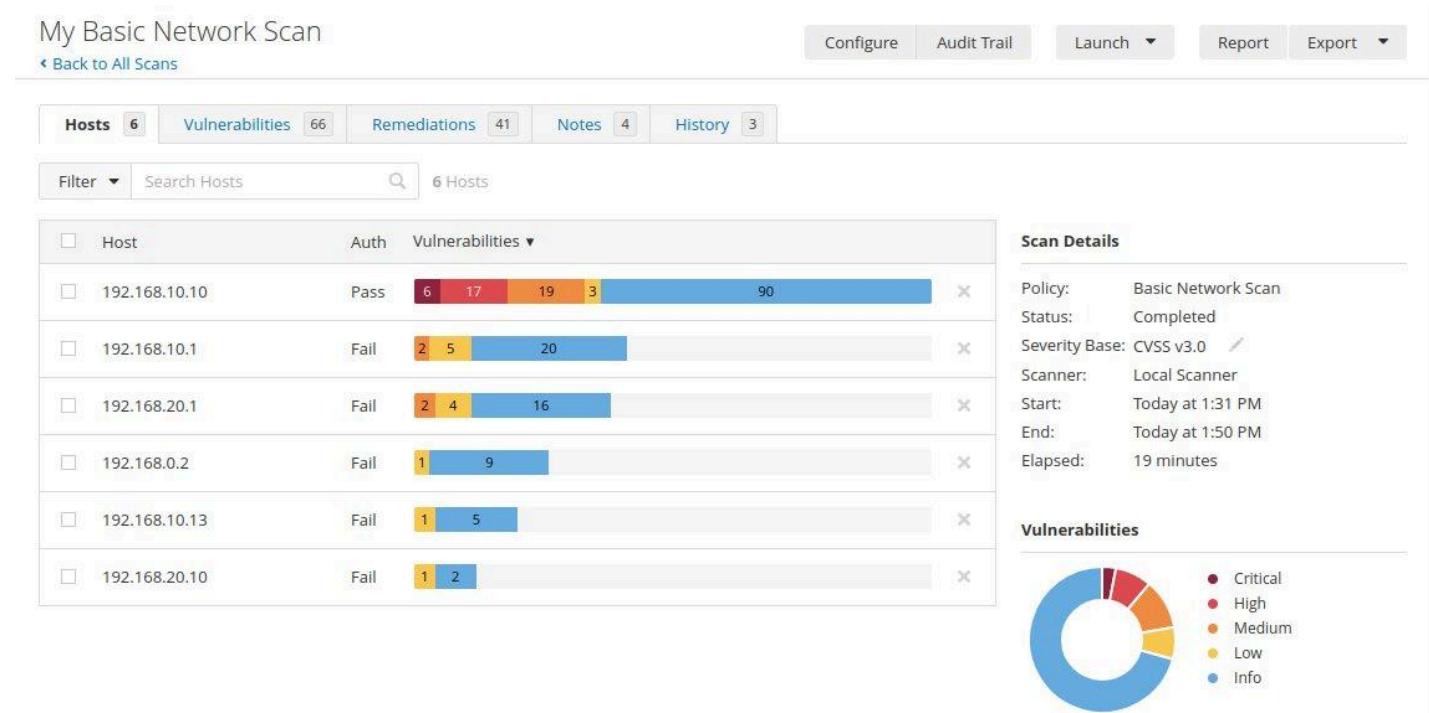
```
[sudo] password for kali:  
HPING 192.168.10.10 (eth1 192.168.10.10): S set, 40 headers + 0 data bytes  
len=46 ip=192.168.10.10 ttl=64 DF id=0 sport=80 flags=SA seq=0 win=64240 rtt=4.3 ms  
len=46 ip=192.168.10.10 ttl=64 DF id=0 sport=80 flags=SA seq=1 win=64240 rtt=1.5 ms  
len=46 ip=192.168.10.10 ttl=64 DF id=0 sport=80 flags=SA seq=2 win=64240 rtt=3.1 ms  
len=46 ip=192.168.10.10 ttl=64 DF id=0 sport=80 flags=SA seq=3 win=64240 rtt=4.6 ms  
len=46 ip=192.168.10.10 ttl=64 DF id=0 sport=80 flags=SA seq=4 win=64240 rtt=2.0 ms  
len=46 ip=192.168.10.10 ttl=64 DF id=0 sport=80 flags=SA seq=5 win=64240 rtt=7.6 ms  
len=46 ip=192.168.10.10 ttl=64 DF id=0 sport=80 flags=SA seq=6 win=64240 rtt=5.5 ms  
len=46 ip=192.168.10.10 ttl=64 DF id=0 sport=80 flags=SA seq=7 win=64240 rtt=2.9 ms  
len=46 ip=192.168.10.10 ttl=64 DF id=0 sport=80 flags=SA seq=8 win=64240 rtt=5.0 ms
```

Capturing from ens35							
...	Time	Source	Destination	Protocol	Length	Info	
591	7.407640973	192.168.10.13	192.168.10.10	TCP	60	2761 → 80 [SYN] Seq=0 Win=512 Len=0	
592	7.417966311	192.168.10.13	192.168.10.10	TCP	60	2762 → 80 [SYN] Seq=0 Win=512 Len=0	
593	7.428135395	192.168.10.13	192.168.10.10	TCP	60	2763 → 80 [SYN] Seq=0 Win=512 Len=0	
594	7.438654039	192.168.10.13	192.168.10.10	TCP	60	2764 → 80 [SYN] Seq=0 Win=512 Len=0	
595	7.449140730	192.168.10.13	192.168.10.10	TCP	60	2765 → 80 [SYN] Seq=0 Win=512 Len=0	
596	7.459613041	192.168.10.13	192.168.10.10	TCP	60	2766 → 80 [SYN] Seq=0 Win=512 Len=0	
597	7.470464821	192.168.10.13	192.168.10.10	TCP	60	2767 → 80 [SYN] Seq=0 Win=512 Len=0	
598	7.480602514	192.168.10.13	192.168.10.10	TCP	60	2768 → 80 [SYN] Seq=0 Win=512 Len=0	
599	7.490821251	192.168.10.13	192.168.10.10	TCP	60	2769 → 80 [SYN] Seq=0 Win=512 Len=0	
600	7.501535813	192.168.10.13	192.168.10.10	TCP	60	2770 → 80 [SYN] Seq=0 Win=512 Len=0	
601	7.511342970	192.168.10.13	192.168.10.10	TCP	60	2771 → 80 [SYN] Seq=0 Win=512 Len=0	
602	7.521441861	192.168.10.13	192.168.10.10	TCP	60	2772 → 80 [SYN] Seq=0 Win=512 Len=0	

```
sec-lab@unt-sec:~$ sudo tail -f /var/log/suricata/fast.log
[sudo] password for sec-lab:
11/18/2025-11:40:30.516904 [Drop] [**] [1:1000001:0] BLOCK ALL from Kali [**] [Classification: (null) [Priority: 3] {TCP} 192.168.10.13:16744 -> 192.168.10.10:80
11/18/2025-11:40:30.527062 [Drop] [**] [1:1000001:0] BLOCK ALL from Kali [**] [Classification: (null) [Priority: 3] {TCP} 192.168.10.13:16745 -> 192.168.10.10:80
11/18/2025-11:40:30.537433 [Drop] [**] [1:1000001:0] BLOCK ALL from Kali [**] [Classification: (null) [Priority: 3] {TCP} 192.168.10.13:16746 -> 192.168.10.10:80
11/18/2025-11:40:30.547789 [Drop] [**] [1:1000001:0] BLOCK ALL from Kali [**] [Classification: (null) [Priority: 3] {TCP} 192.168.10.13:16747 -> 192.168.10.10:80
11/18/2025-11:40:30.558144 [Drop] [**] [1:1000001:0] BLOCK ALL from Kali [**] [Classification: (null) [Priority: 3] {TCP} 192.168.10.13:16748 -> 192.168.10.10:80
11/18/2025-11:40:30.568422 [Drop] [**] [1:1000001:0] BLOCK ALL from Kali [**] [Classification: (null) [Priority: 3] {TCP} 192.168.10.13:16749 -> 192.168.10.10:80
11/18/2025-11:40:30.578525 [Drop] [**] [1:1000001:0] BLOCK ALL from Kali [**] [Classification: (null) [Priority: 3] {TCP} 192.168.10.13:16750 -> 192.168.10.10:80
11/18/2025-11:40:30.588960 [Drop] [**] [1:1000001:0] BLOCK ALL from Kali [**] [Classification: (null) [Priority: 3] {TCP} 192.168.10.13:16751 -> 192.168.10.10:80
11/18/2025-11:40:30.599434 [Drop] [**] [1:1000001:0] BLOCK ALL from Kali [**]
```

## 6. Security Assessment Host-Level Findings

For our network security assessment, we utilize Nessus, a vulnerability assessment tool. After performing a host scan and a vulnerability assessment, we found several critical vulnerabilities only within the Host level and two minor vulnerabilities within the network level. The goal of the vulnerability assessment is to find weaknesses within the system and to propose mitigation strategies to enhance the network security..



## 9. Conclusion

In conclusion, the project showcases a secure network design by evaluating the functionality as well as the effectiveness of the IDS/IPS, Firewall policies, and remote access VPN. By using a simulated SYN flood attack using hping, we can see how the system works as intended by detecting and preventing the malicious traffic. FortiGate firewall filtering of traffic was also demonstrated with complete segmentation from the DMZ to the LAN switch using a firewall policy. In addition, the vulnerability assessment highlights the importance of keeping a system up to date and under constant observation. These practices combined will greatly reduce the number of vulnerabilities, demonstrating strengths in network security.

## References

*CVE-1999-0524 Detail.* NVD. (2004, January 1). <https://nvd.nist.gov/vuln/detail/CVE-1999-0524>

*CVE-2019-0053 Detail.* NVD. (2019, July 24). <https://nvd.nist.gov/vuln/detail/CVE-2019-0053>