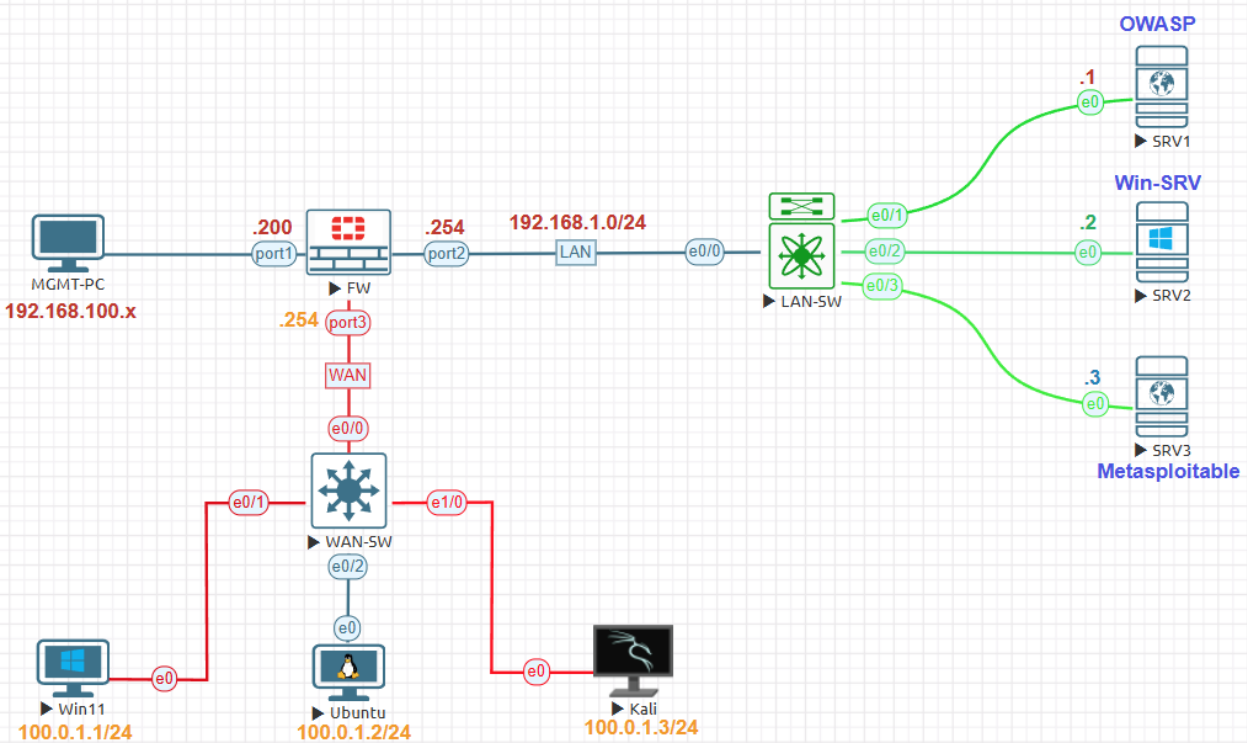
Nessus Lab Setup:

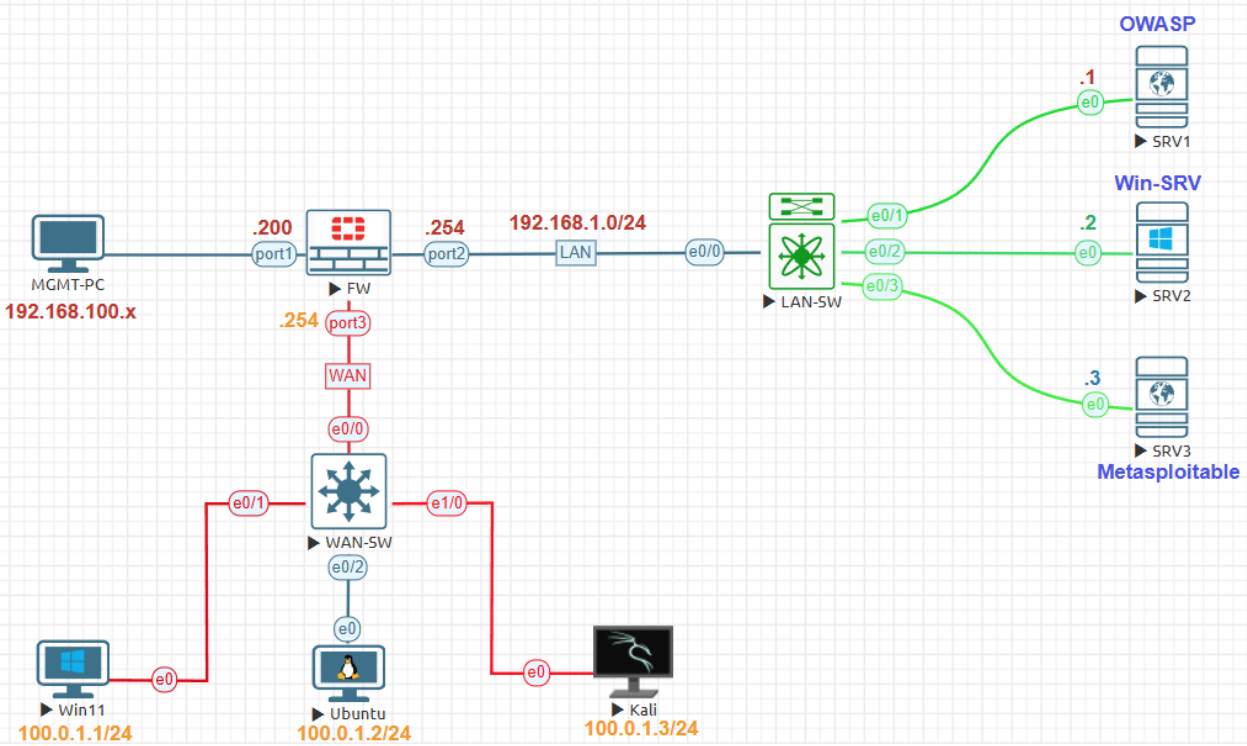


Management Subnet	192.168.100.0/24
FortiGate Management IP	192.168.100.200
Internal Servers Subnet	192.168.1.0/24
FortiGate Firewall External	100.0.1.0/24
FortiGate Firewall LAN IP	192.168.1.254
FortiGate Firewall WAN IP	100.0.1.254
SRV1 IP Address	192.168.1.1
SRV2 IP Address	192.168.1.2
SRV3 IP Address	192.168.1.3
External Win11 IP Address	100.0.1.1
External Ubuntu IP Address	100.0.1.2
External Kali IP Address	100.0.1.3

Images	**Description**
FortiGate Firewall	fortinet-FGT-v7.0.9-build0444
Cisco Switches	i86bi_linux_l2-ipbasek9-ms.high_iron_aug9_2017b.bin
Servers	linux-metasploitable-2, OWASP, Winserver-S2019-R2-x64
Attacker Kali Linux	linux-Kali-2025.1c
Windows	win-11-x64-SE
Ubuntu	linux-ubuntu-22.04-desktop
Internet Link	Management Cloud

Devices	Username	Password
FortiGate 7.0.9	Admin	No password by default
Linux Kali 2025.1c	kali	kali
Linux Ubuntu 22.04 Desktop	user	Test123
Windows 11 x64 SE	user(Administrator)	Test123
Linux Metasploitable 2.0	msfadmin	msfadmin
Linux-OWASP	root	owaspbwa
Windows Server 2019	Administrator	Test123

Main Topology:



This EVE-NG topology represents a segmented network lab for cybersecurity, penetration testing and scanning training. At the core, a Fortinet firewall (FW) connects three zones: MGMT, LAN, and WAN. The MGMT-PC (192.168.100.x) accesses the firewall's port1 (192.168.100.200), while port2 (192.168.1.254) serves the LAN segment. The LAN switch (LAN-SW) connects three vulnerable web servers: SRV1 (OWASP) at 192.168.1.1, SRV2 (Win Server) at 192.168.1.2, and SRV3 (Metasploitable) at 192.168.1.3 — ideal for simulating real-world attacks and testing defenses.

On the WAN side, port3 of the firewall connects to a WAN switch (WAN-SW), which links three attacker machines: Windows 11 (100.0.1.1/24), Ubuntu (100.0.1.2/24), and Kali Linux (100.0.1.3/24). These machines simulate various external threat actors or clients.