

The diagram illustrates a network topology for a security lab. At the center is a Firewall (FW) with interfaces e0, e1, e2, e3, e4, and e5. Interface e0 is connected to the Internet (192.168.114.2) via a DHCP server (19.168.114.0). Interface e1 is connected to a LAN switch (LAN-SW) via a link with IP 192.168.1.0. Interface e2 is connected to a SeOnion device (192.168.114.50) via a link with IP 192.168.114.0. Interface e3 is connected to a Kali machine (192.168.3.0) via a link with IP 192.168.3.0. Interface e4 is connected to a SeOnion device (192.168.4.x) via a link with IP 192.168.4.x. Interface e5 is connected to a Spunk machine (192.168.5.x) via a link with IP 192.168.5.0. The LAN switch (LAN-SW) has interfaces e0/0, e0/1, e0/2, and e0/3. Interface e0/0 is connected to the FW via a link with IP 192.168.1.0. Interface e0/1 is connected to a VSRV machine (192.168.1.x). Interface e0/2 is connected to an ADC machine (192.168.1.100). Interface e0/3 is connected to a PC machine (192.168.1.10). A SeOnion device (192.168.114.50) is connected to a MGMT machine (192.168.114.1) via a link with IP 192.168.114.0. A 'SPAN' configuration is shown on the FW, indicating traffic monitoring on interface e1.

| | |
|--------------------------------|------------------|
| External Subnet | 192.168.114.0/24 |
| Internal LAN Subnet | 192.168.1.0/24 |
| SPAN Port IP Address | No IP Address |
| Attacker Subnet | 192.168.3.0/24 |
| Security Onion Logs Subnet | 192.168.4.0/24 |
| Splunk Log Collector Subnet | 192.168.5.0/24 |
| Metasploitable IP Address | Through DHCP |
| ADC IP Address | 192.168.1.100 |
| PC1 IP Address | 192.168.1.10 |
| Attacker IP Address | Through DHCP |
| Splunk IP Address | Through DHCP |
| Security Onion IP Address | 192.168.114.50 |
| Security Onion MGMT IP Address | 192.168.114.1 |
| DNS | 8.8.8.8, 4.4.4.4 |

| VMware Adopter | Network Connection | Role | PfSense Interfaces |
|-------------------|--------------------|----------|--------------------|
| Network Adopter | NAT | WAN | EM0 |
| Network Adopter 2 | VMNet2 | LAN | EM1 |
| Network Adopter 3 | VMNet3 | SPAN | EM2 |
| Network Adopter 4 | VMNet4 | KALI | EM3 |
| Network Adopter 5 | VMNet5 | SECONION | EM4 |
| Network Adopter 6 | VMNet6 | SPLUNK | EM5 |

| IP Subnet | Network Connection | Role | PfSense Interfaces | VMware Adopter |
|------------------|--------------------|----------|--------------------|-------------------|
| 192.168.114.0/24 | NAT | WAN | EM0 | Network Adopter |
| 192.168.1.0/24 | VMNet2 | LAN | EM1 | Network Adopter 2 |
| No IP Address | VMNet3 | SPAN | EM2 | Network Adopter 3 |
| 192.168.3.0/24 | VMNet4 | KALI | EM3 | Network Adopter 4 |
| 192.168.4.0/24 | VMNet5 | SECONION | EM4 | Network Adopter 5 |
| 192.168.5.0/24 | VMNet6 | SPLUNK | EM5 | Network Adopter 6 |

Hardware Options

| Device | Summary |
|-------------------|--------------------------------|
| Memory | 2 GB |
| Processors | 1 |
| Hard Disk (SCSI) | 20 GB |
| CD/DVD (IDE) | Using file C:\Users\USER\Do... |
| Network Adapter | NAT |
| Network Adapter 2 | Custom (VMnet2) |
| Network Adapter 3 | Custom (VMnet3) |
| Network Adapter 4 | Custom (VMnet4) |
| Network Adapter 5 | Custom (VMnet5) |
| Network Adapter 6 | Custom (VMnet6) |

Memory

Specify the amount of memory allocated to this virtual machine. The memory size must be a multiple of 4 MB.

Memory for this virtual machine: 2048 MB

128 GB -
64 GB -
32 GB -
16 GB -
8 GB -

Maximum recommended memory (Memory swapping may)

Interfaces / Interface Assignments

Interface Assignments

Interface Groups Wireless VLANs QinQs PPPs GREs GIFs Bridges LAGGs

| Interface | Network port |
|-----------|---|
| WAN | em0 (00:0c:29:f4:a9:b6) |
| LAN | em1 (00:0c:29:f4:a9:c0) Delete |
| SPAN | em2 (00:0c:29:f4:a9:ca) Delete |
| KALI | em3 (00:0c:29:f4:a9:d4) Delete |
| SecOnion | em4 (00:0c:29:f4:a9:de) Delete |
| Splunk | em5 (00:0c:29:f4:a9:e8) Delete |