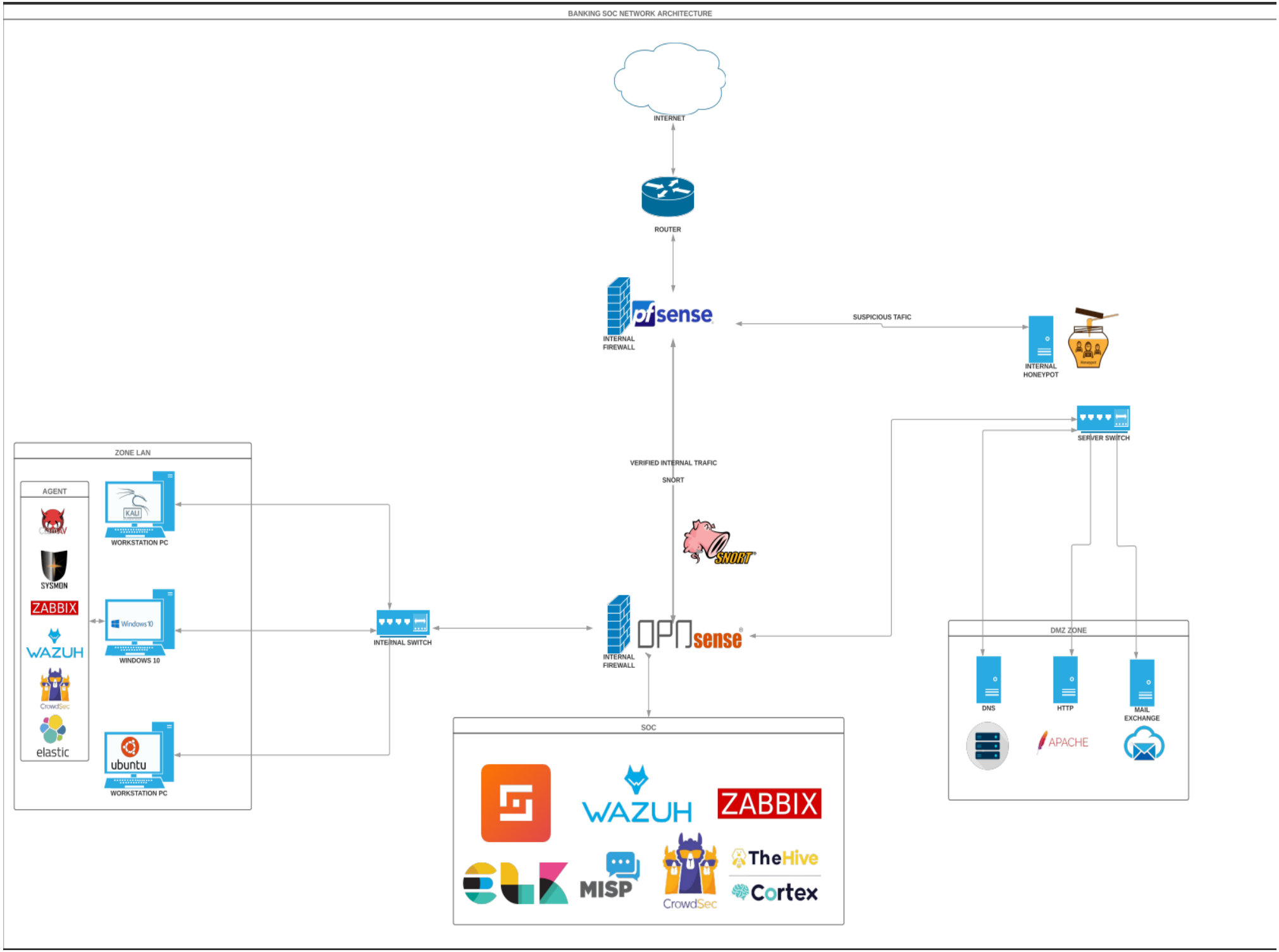
BANKING SOC NETWORK ARCHITECTURE
INTERNET
ROUTER
INTERNAL FIREWALL
pfsense
SUSPICIOUS TAFIC
INTERNAL HONEYPOT
SERVER SWITCH
VERIFIED INTERNAL TRAFIC
SNORT
SNORT
ZONE LAN
AGENT
SYSMON
ZABBIX
WAZUH
CrowdSec
elastic
WORKSTATION PC
WINDOWS 10
WORKSTATION PC
INTERNAL SWITCH
INTERNAL FIREWALL
OPNsense
DMZ ZONE
DNS
HTTP
MAIL EXCHANGE
APACHE
SOC
WAZUH
ZABBIX
MISP
CrowdSec
TheHive
Cortex

the physical architecture referring to a Next Generation Security Operations Center (SOC) designed specifically for banking organizations. The architecture is built using NIST standards and consists of three different zones: LAN, SOC, and DMZ.

The **LAN** zone includes various agents such as Sysmon, ZABBIX, and WAZUH, along with an Elastic search engine, and workstations running Kali, Windows, and Ubuntu operating systems. The LAN is connected via a switch and is protected by a firewall called OpenSense.

The **SOC** zone is connected to the LAN via the same firewall, OpenSense. The SOC includes an Endpoint Detection and Response (EDR) system called WAZUH and a Network Detection and Response (NDR) system. The SOC also includes various security tools such as MISP, ELK, Cortex, and TheHive, which together form a Security Orchestration, Automation, and Response (SOAR) system.

The **DMZ** zone is also connected to the same firewall, OpenSense, and includes various services such as DNS, HTTP, and MAIL. The DMZ is designed to isolate and protect external-facing services from the rest of the network.

Finally, the architecture includes a honeypot, which is connected to another firewall called Pfsense. The Pfsense firewall is connected to a router, which in turn connects to the internet.

Overall, this architecture is designed to provide comprehensive security for banking organizations by combining various security tools and techniques across multiple zones of

the network.

HONEYPOT	**192.168.2.100**