McSOC:

A scripted 'SOC in a BOX' network deployment

Ronald Broberg
December 2016

McSOC: Executive Summary

Create a redeployable network architecture that can

- ***demonstrate SOC capabilities***
- ***provide a platform to develop SOC solutions***
- ***Be delivered as a training environment***

McSOC: Capabilities

https://www.nuspire.com/technologies/soc/

McSOC: High Level Features

- **Infrastructure as Code**
  - Network Deployment and Configuration is Scripted
- **Self-Validation**
  - Continuous Monitoring
  - Automated Testing
- **Capabilities Definition**
  - Capabilities Documentation bundle
- **Use Case Development**
  - Use Cases bundled

McSOC: Technology Guide

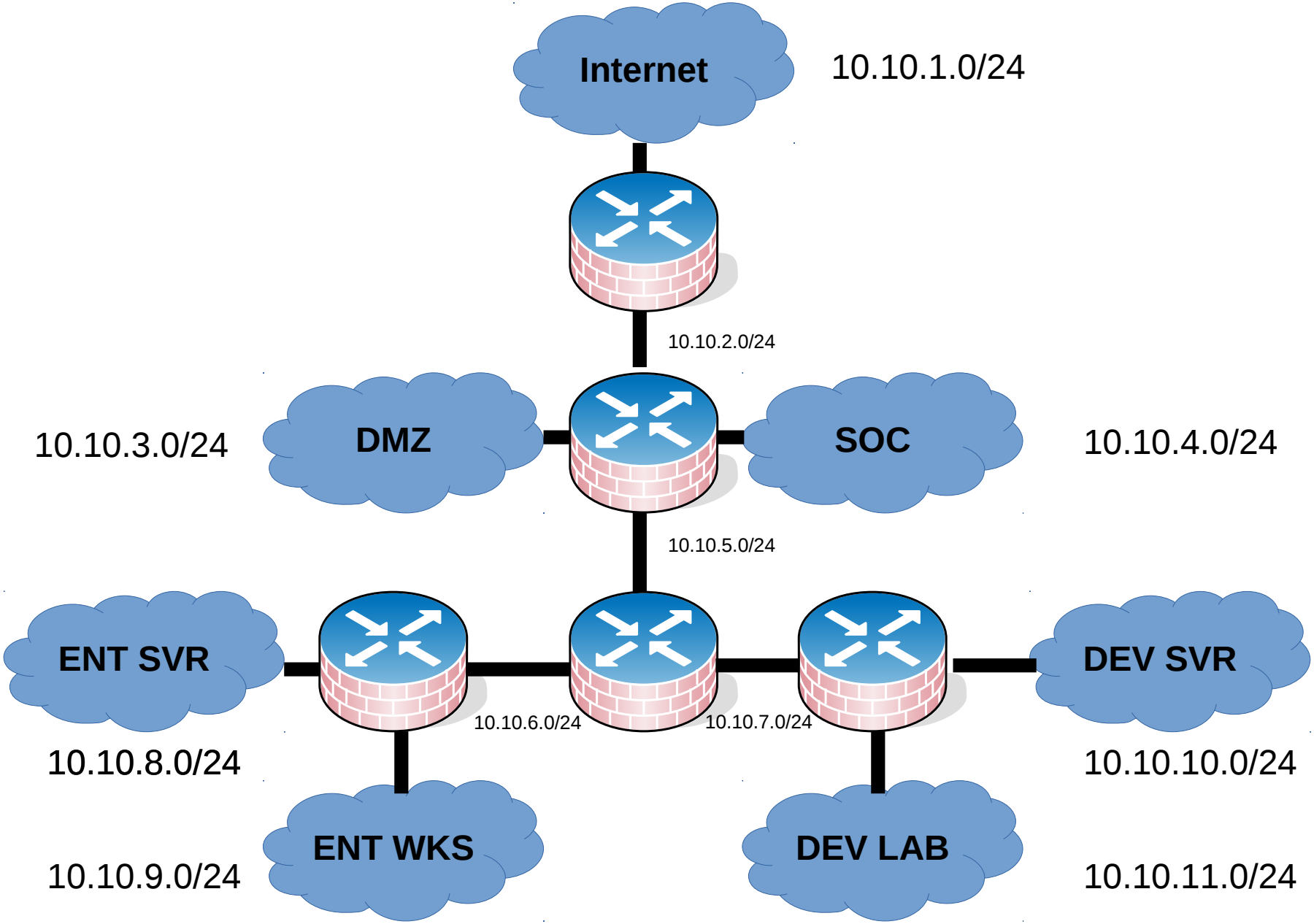
- **Open Source Components**
  - Minimize License Issues
  - Maximize Re-usability
- **Deployable to Multiple Visualization Hosts**
  - Develop on single server (Oracle VirtualBox)
  - Deploy to Amazon AWS or Vmware Fusion
- **Automated Testing**
  - Deployed Project should be able to self-validate

McSOC: Constraints and Limitations

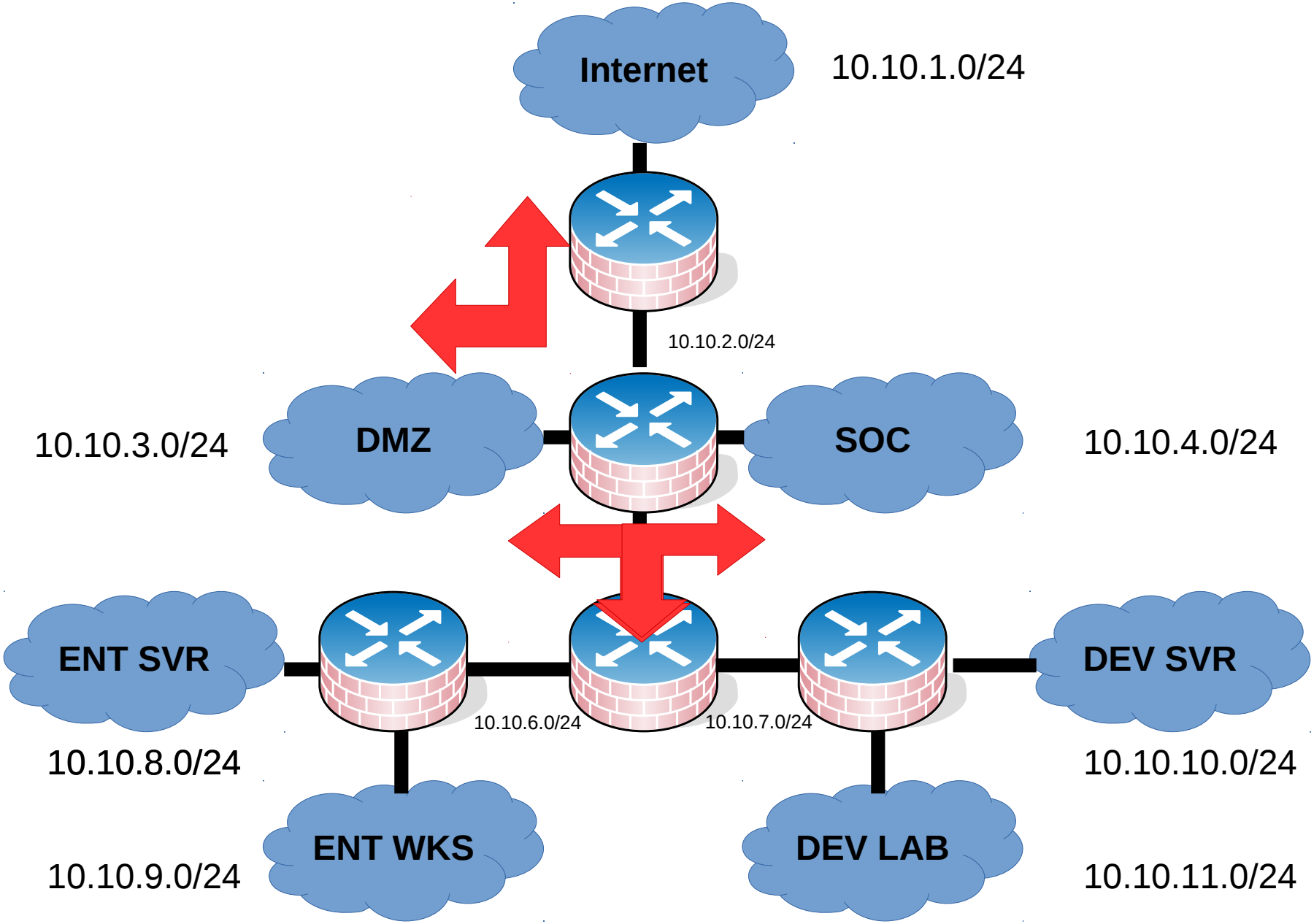
- **Resource Constraints**
  - Not a scalable architecture
- **The NAT interface links nodes undesirably**
  - Limits use a CyberRange model
- **Lack of Microsoft Components**
  - Enterprise Servers Lack Key Microsoft Services
    - Active Directory
    - Exchange
  - Enterprise Workstation Are Not Microsoft
    - Unrealistic reflection of Enterprise

Infrastructure Design

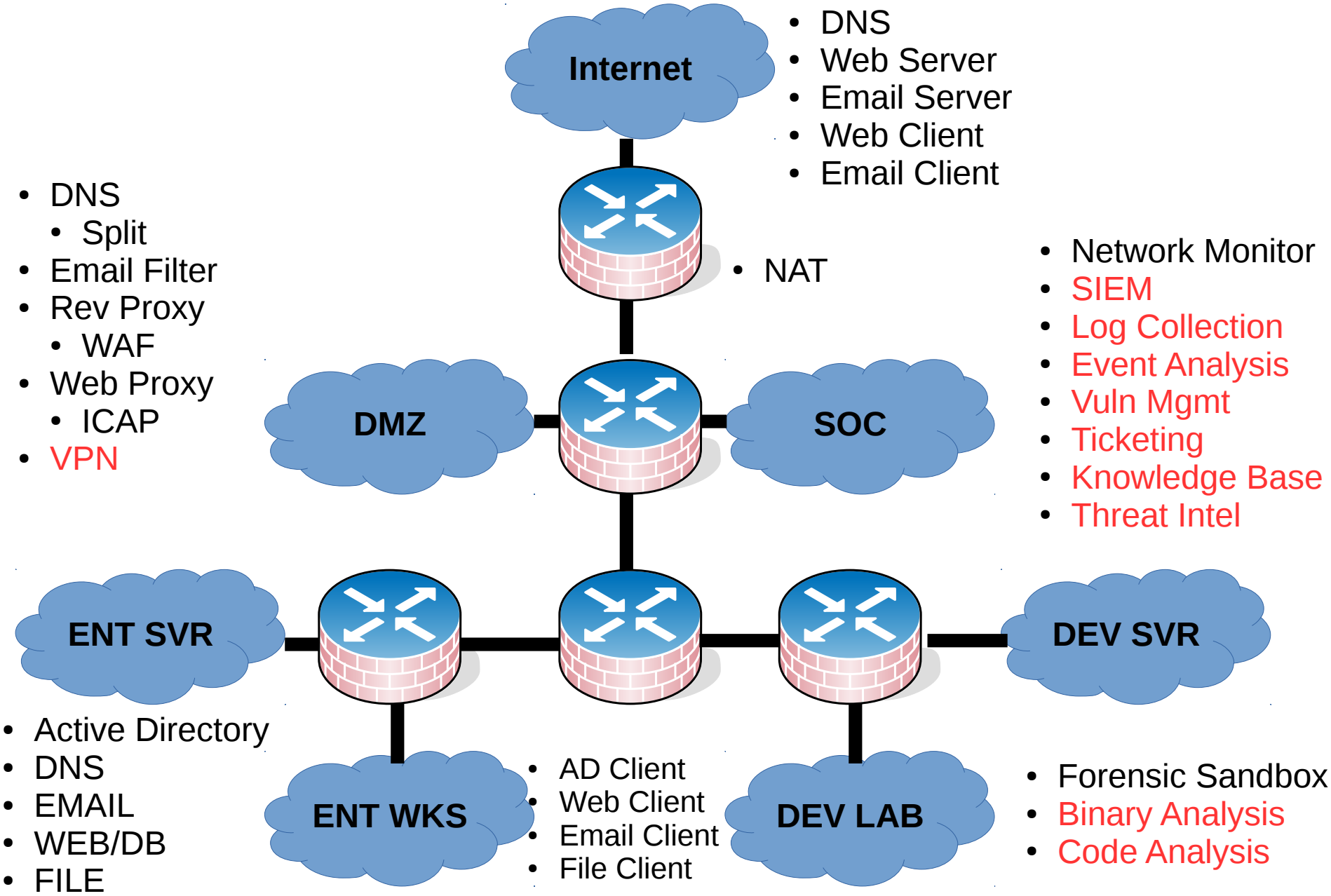
McSOC: Network Layout



McSOC: Network Routing



McSOC: Infrastructure Layout

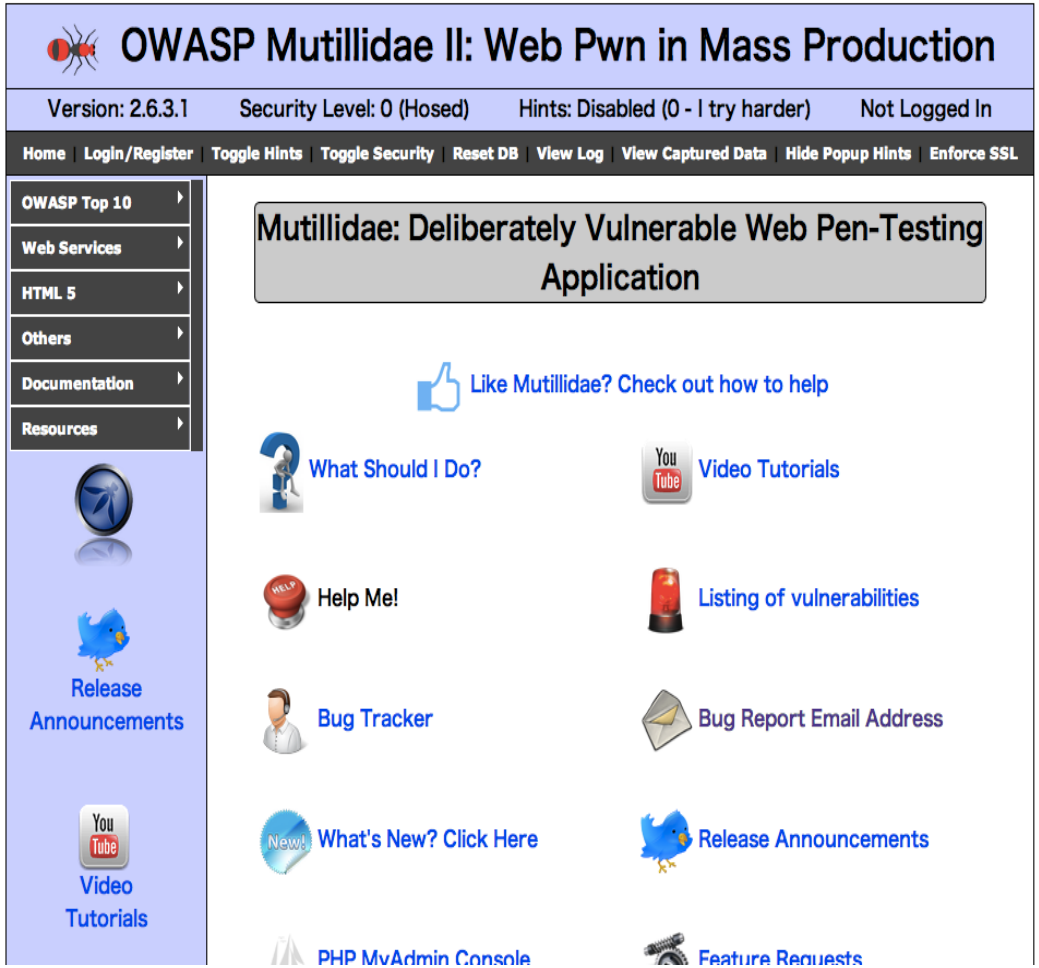


McSOC : WAN : TESTMAIL

- Test Services
  - DNSMASQ
  - NGINX Web Server
  - Email Server
    - MTA
    - MDA
  - Email Client
    - Web Mail

CentOS 7

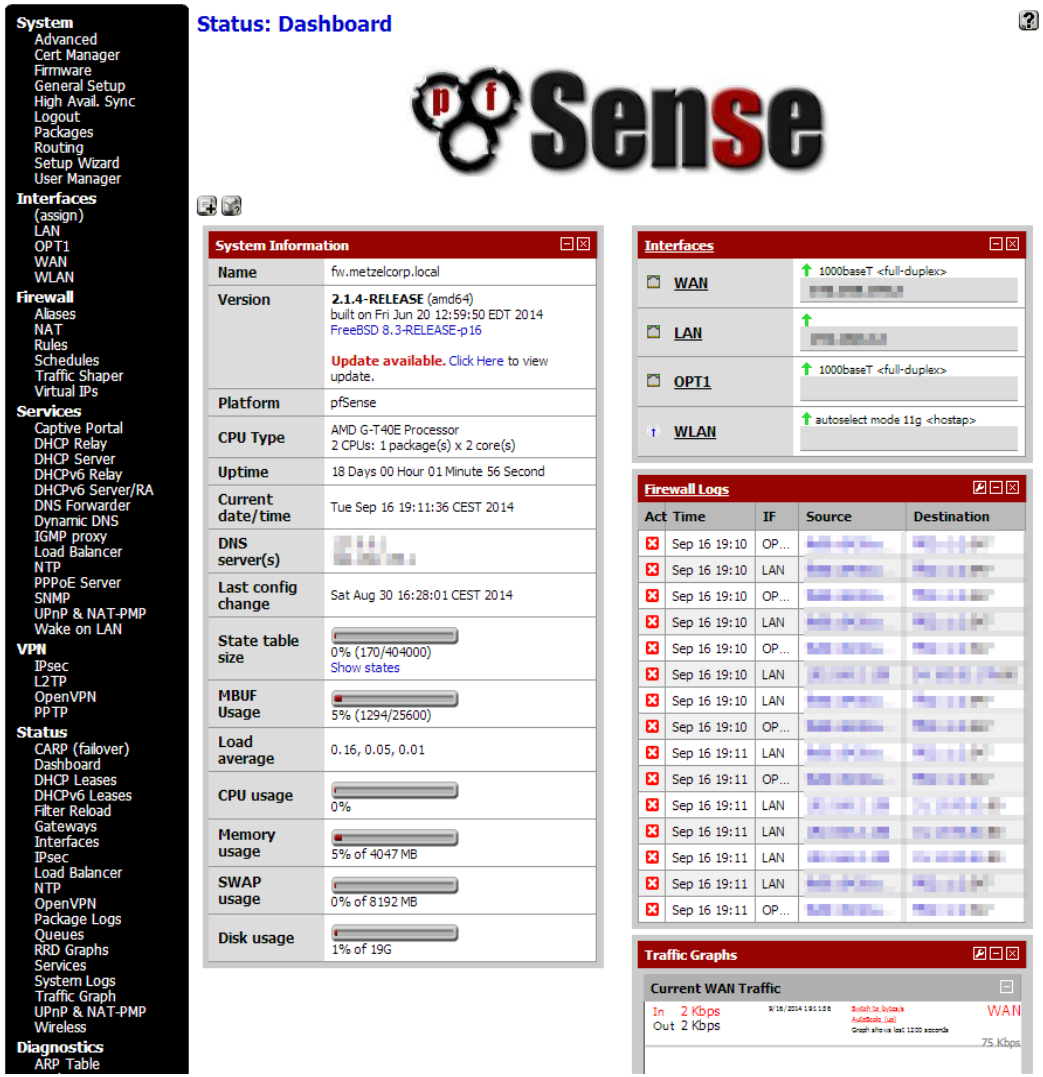
McSOC : WAN : TESTWEB



- **Test Web Services**
  - Mutillidae Web Server
  - LAMP
  - EICAR files

CentOS 7

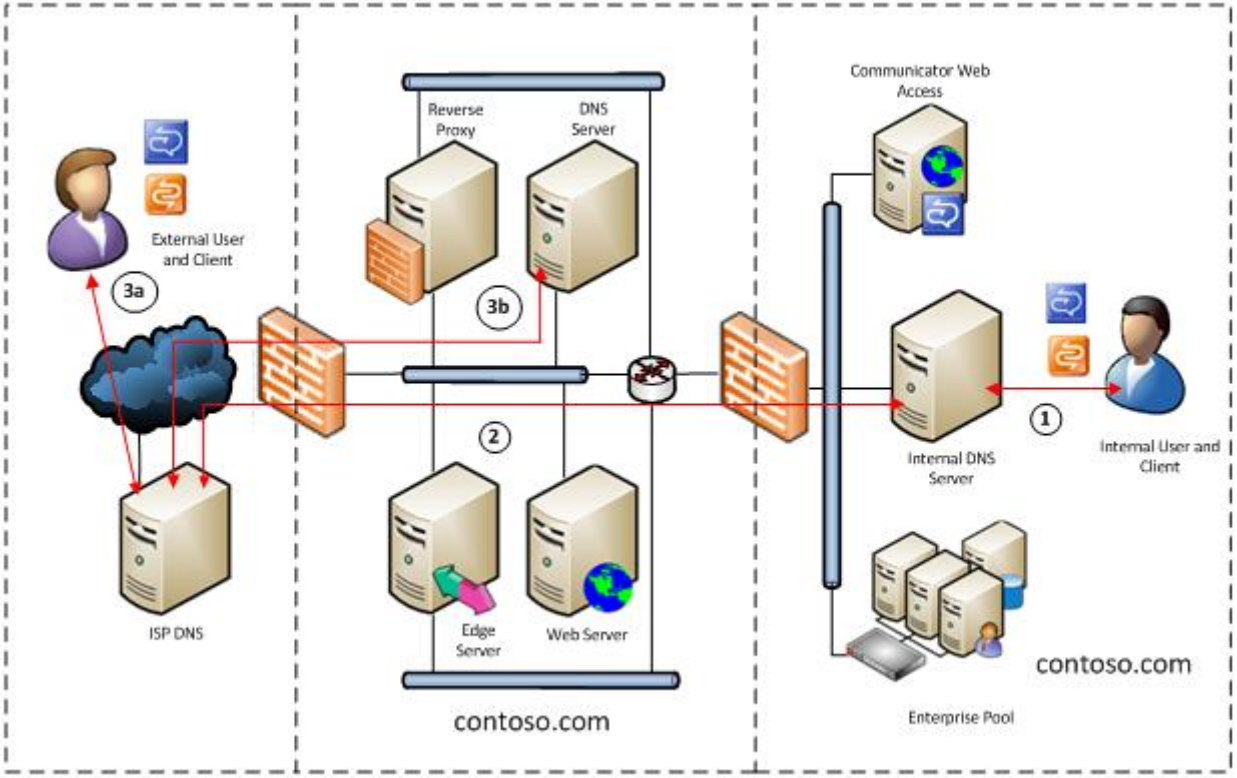
McSOC: - : ROUTERS



- **pfSense**
  - Firewall
  - Routing
  - SNMP

FreeBSD 10

McSOC : DMZ : DNS

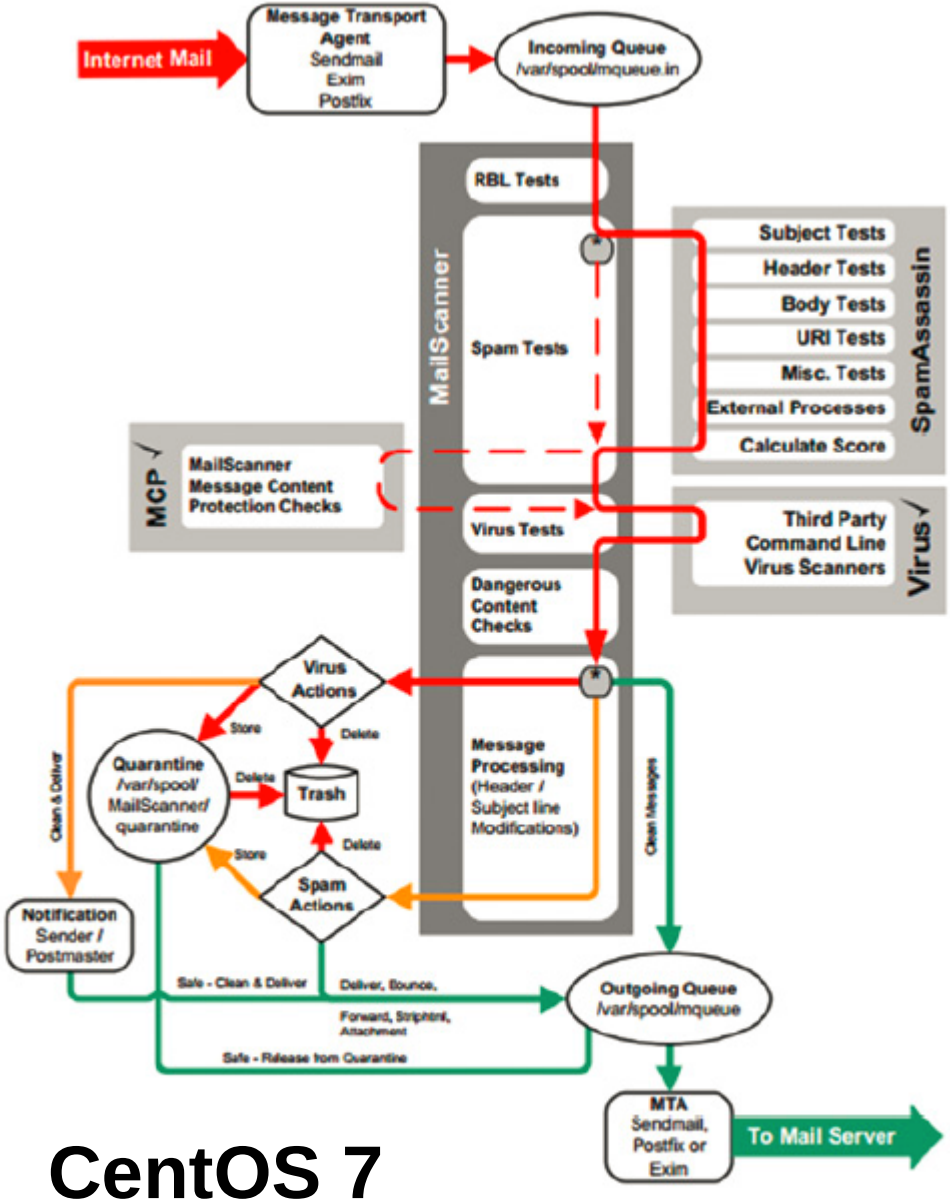


- DMZ DNS
  - Split DNS
  - DNSMASQ

CentOS 7

https://www.ixsystems.com/blog/an-email-gateway-with-freebsd-to-prevent-malware-and-undesirable-messages/

McSOC : DMZ : MAIL



CentOS 7

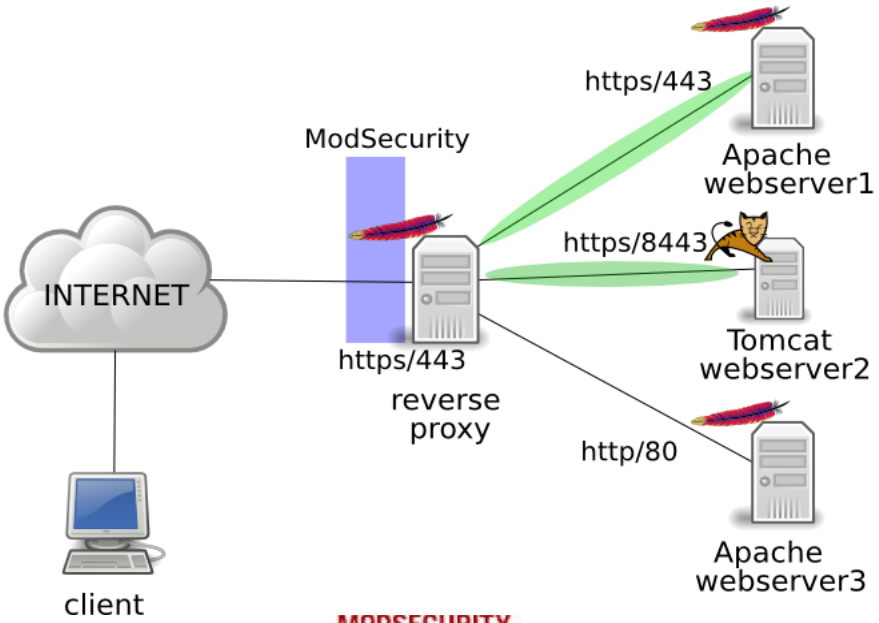
- Mail Gateway
  - Postfix
  - MailScanner
  - SpamAssassin
  - ClamAV

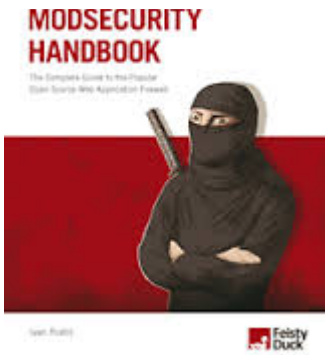
https://www.ixsystems.com/blog/an-email-gateway-with-freebsd-to-prevent-malware-and-undesirable-messages/

Figure 2. *MailScanner process flow*

McSOC : DMZ : WEB

Apache + ModSecurity: Reverse Proxy.



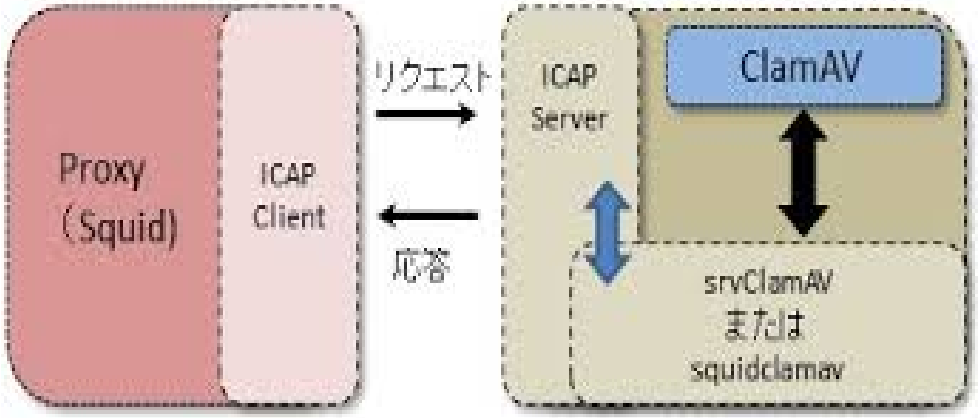


CentOS 7

- NGINX Reverse Proxy
  - Load Balancing
  - SSL Termination
  - HTTP Sanitizing
  - ModSecurity WAF
    - OWASP CRS
      - SQL Injection (SQLi)
      - Cross Site Scripting (XSS)
      - Local File Inclusion (LFI)
      - Remote File Inclusion (RFI)
      - Remote Code Execution (RCE)
      - PHP Code Injection
      - HTTP Protocol Violations
      - Shellshock
      - Session Fixation
      - Scanner Detection
      - Metadata/Error Leakages
      - Project Honey Pot Blacklist
      - GeoIP Country Blocking

https://adolfomaltez.files.wordpress.com/2011/05/apache-reverse-proxy-modsecurity.png

McSOC : DMZ : PROXY

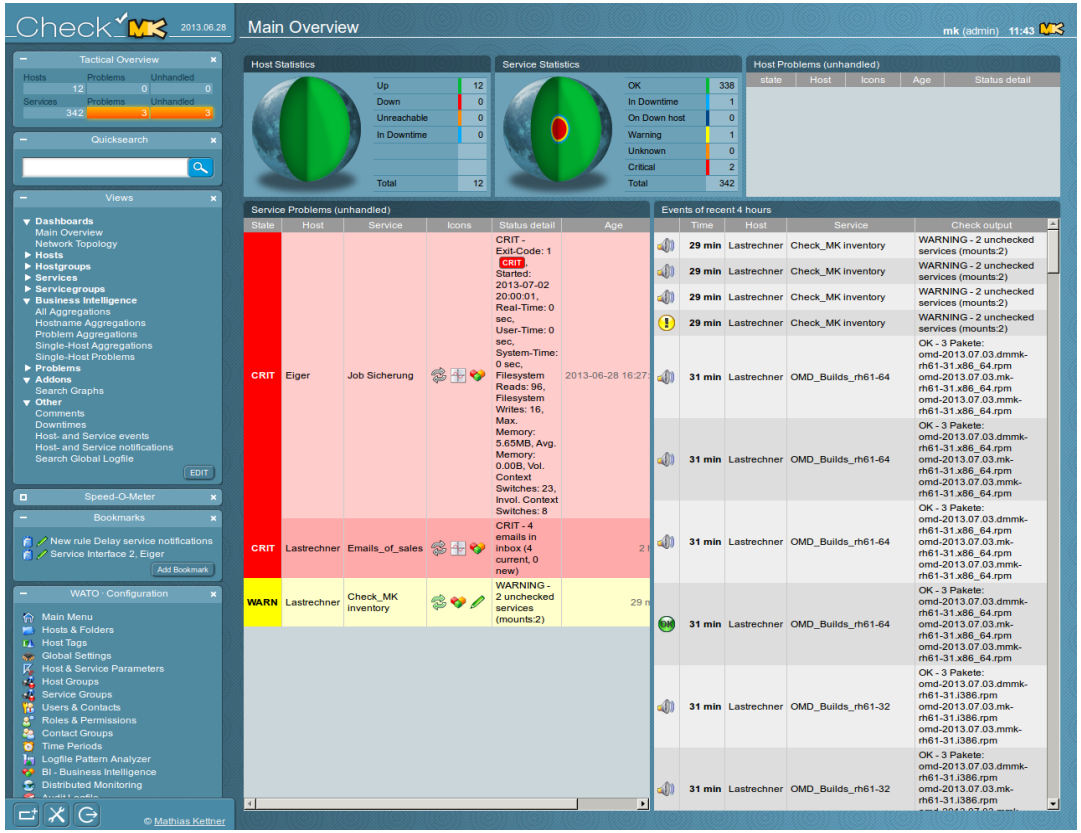


- SQUID Web Proxy
  - Squid
  - ClamAV
  - SquidClamAV
  - C-ICAP
    - Web antivirus service
    - basic URL filtering service

CentOS 7

http://squid.robata.org/setup_clamav.html

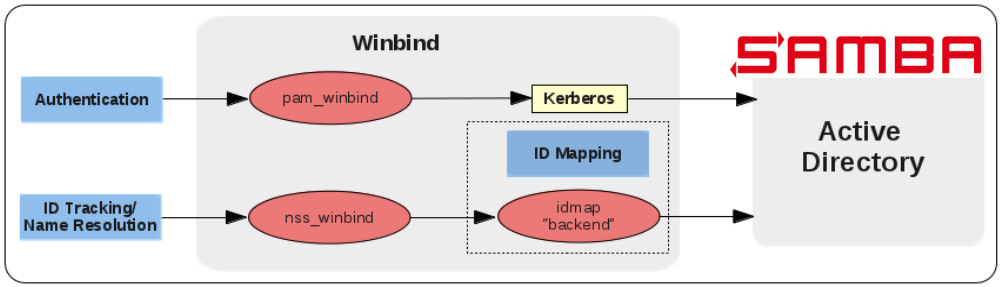
McSOC: SOC : NAGIOS



- **Network Monitor**
  - Check_MK
    - Nagios Variant
    - Liveevent Service

Ubuntu 16 Xenial

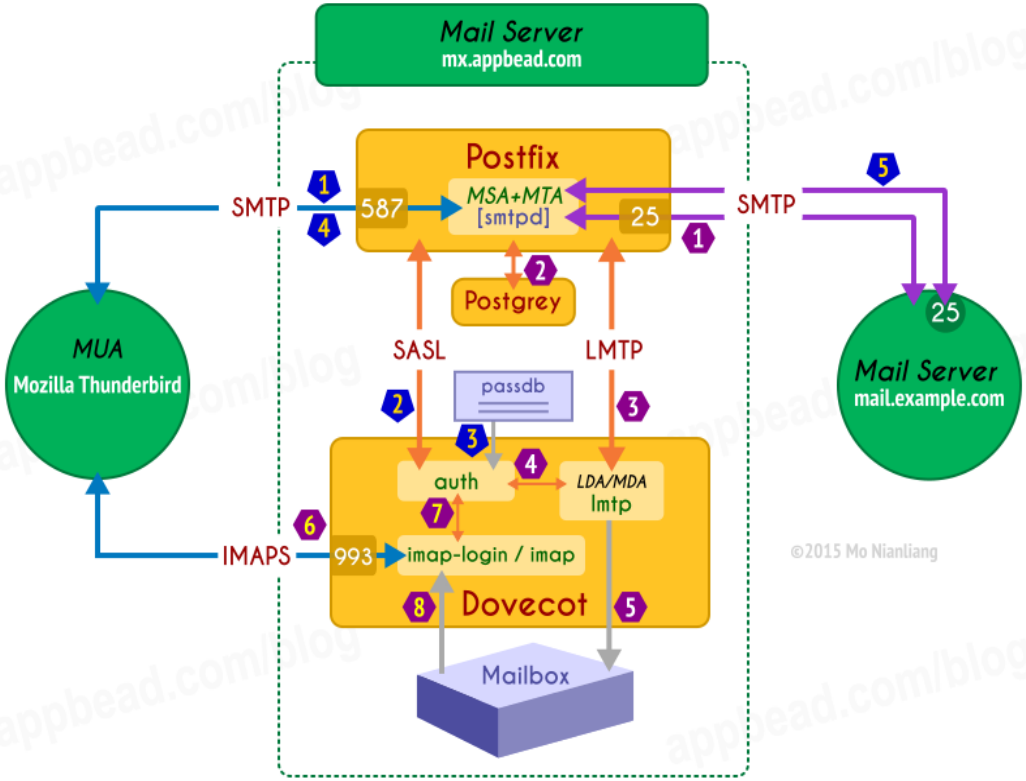
McSOC: ENTSVR : DC1/DNS



- **Domain Controller**
  - Samba4 Authentication
- **DNS Server**
  - Bind9

CentOS 7

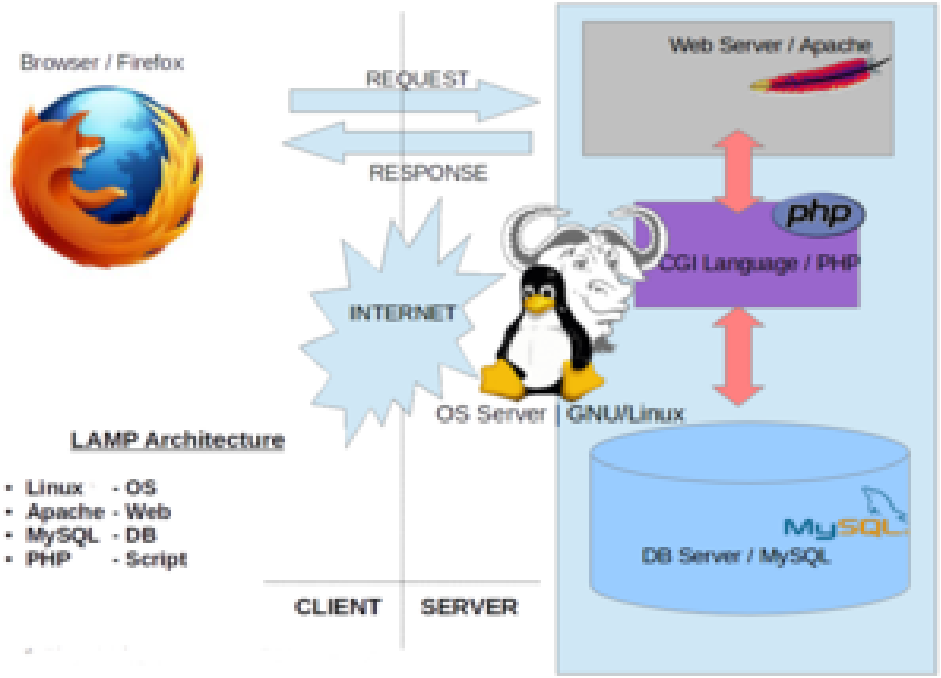
McSOC: ENTSVR : MAIL



- **Mail Server**
  - MTA: PostFix
  - MDA: Dovecot
  - AD/LDAP Authentication

CentOS 7

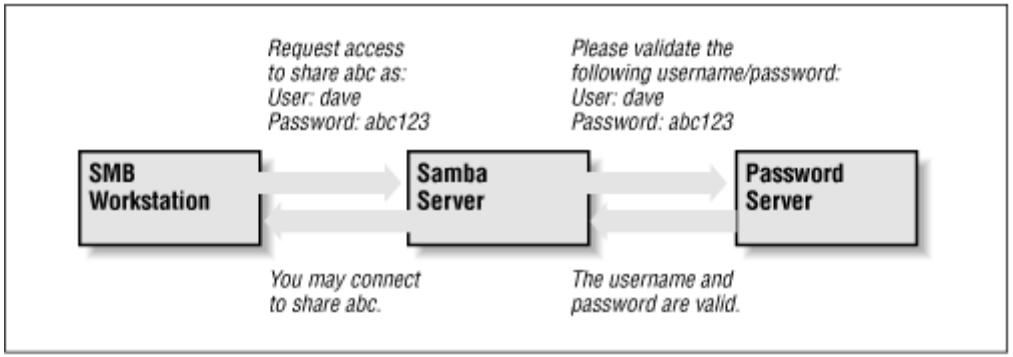
McSOC: ENTSVR : WEB/DB



- **Web Server**
  - Apache2
  - PHP 5
  - Wordpress
- **DB Server**
  - MariaDB
    - Fork of MySQL

CentOS 7

McSOC : DMZ : FILE

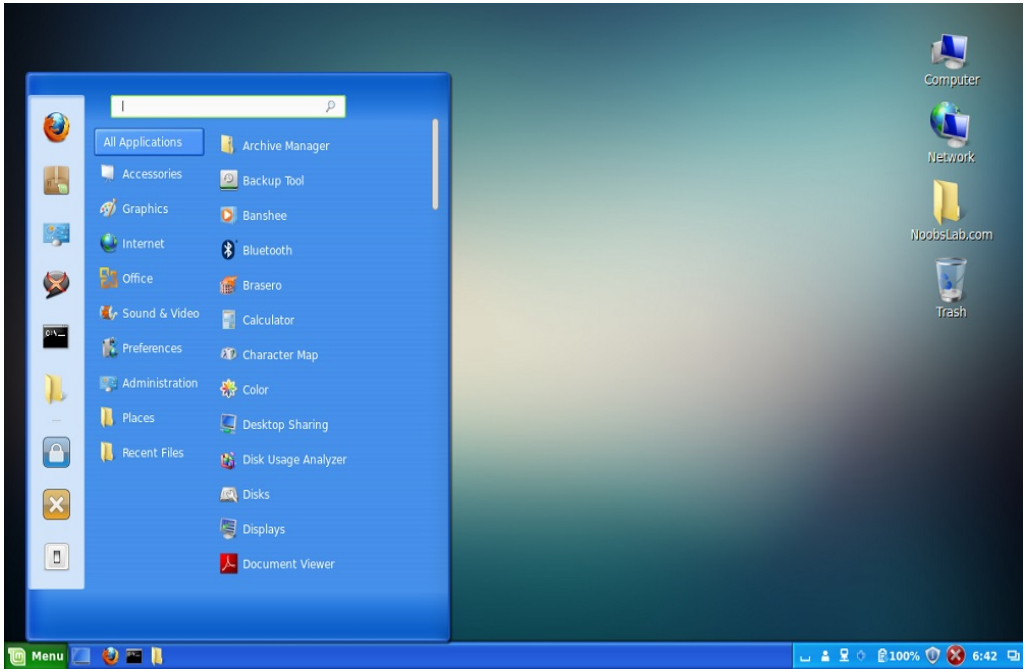


- SMB File Shares
  - Home Directories
    - Automounted on Clients
    - Authenticated against Active Directory
  - Anonymous Public Shares

CentOS 7

http://www.oreilly.com/openbook/samba/book/ch06_03.html

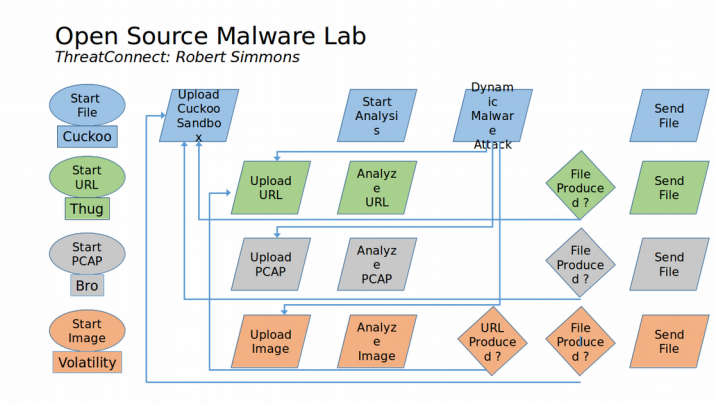
McSOC: ENTWKS : WKS101



- **Domain Client**
  - Samba4 Authentication
  - Networked Home Directory
- **Mail Client**
  - Mozilla Thunderbird
- **Web Browser**
  - Mozilla Firefox
- **Windows Look and Feel**

Mint Linux 14

McSOC: DEVLAB : Forensics



- **Cuckoo Sandbox**
  - Malware execution
- **Thug**
  - URL downloads
- **Bro**
  - Network analysis
- **Volatility**
  - Memory analysis

CentOS 7

Network Data Flow

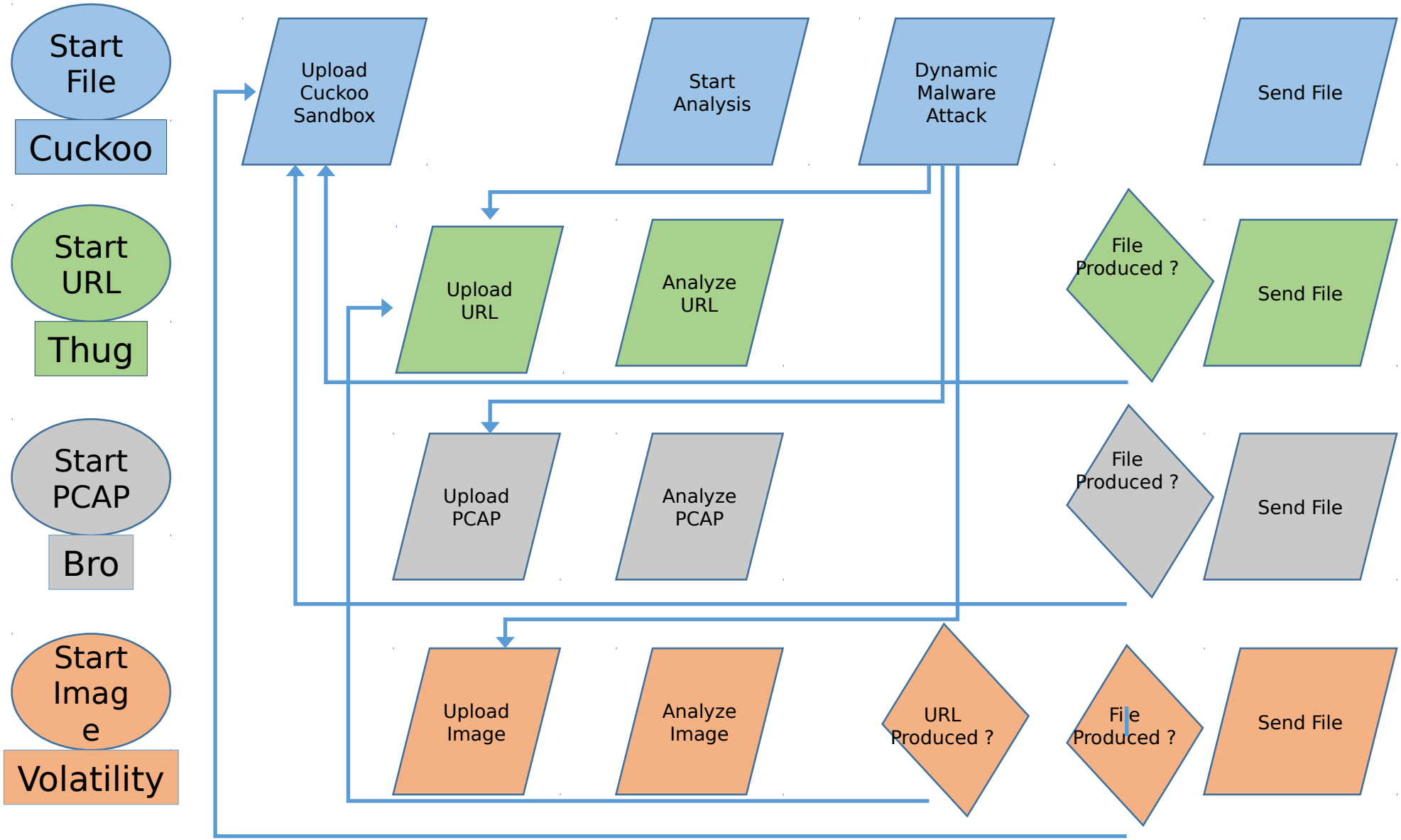
McSOC: Inbound Email Flow

- Postfix holds the mail upon receipt.
- MailScanner scans the email in queue.
  - SpamAssassin
  - ClamAV
- MailScanner re-queues the email and hands it over back to Postfix.
- Postfix processes the email as necessary and delivers the mail to recipient.

Potential Hardware

Open Source Malware Lab

ThreatConnect: Robert Simmons



McSOC: HP Proliant DL380

- Fully loaded $7400
- 64GB RAM
- 2x10TB Storage
- Power Supplies: 2 x 800W

McSOC: Dell R710

- Fully loaded $2600
- 144GB RAM
- 12TB Storage
- Power Supplies: 2 x DELL 870W

McSOC: ServerMicro E300-8D

- Barebones $700
- 128GB RAM $1000
- 512 GB SDD $300
- External Storage $?
- Power Req: 80W chassis (+ ext storage)

McSOC: Intel NUC

- Fully Loaded $1400
- 32GB RAM
- 1 TB SDD
- Power Req: 80W