McSOC:

A scripted 'SOC in a BOX' network deployment

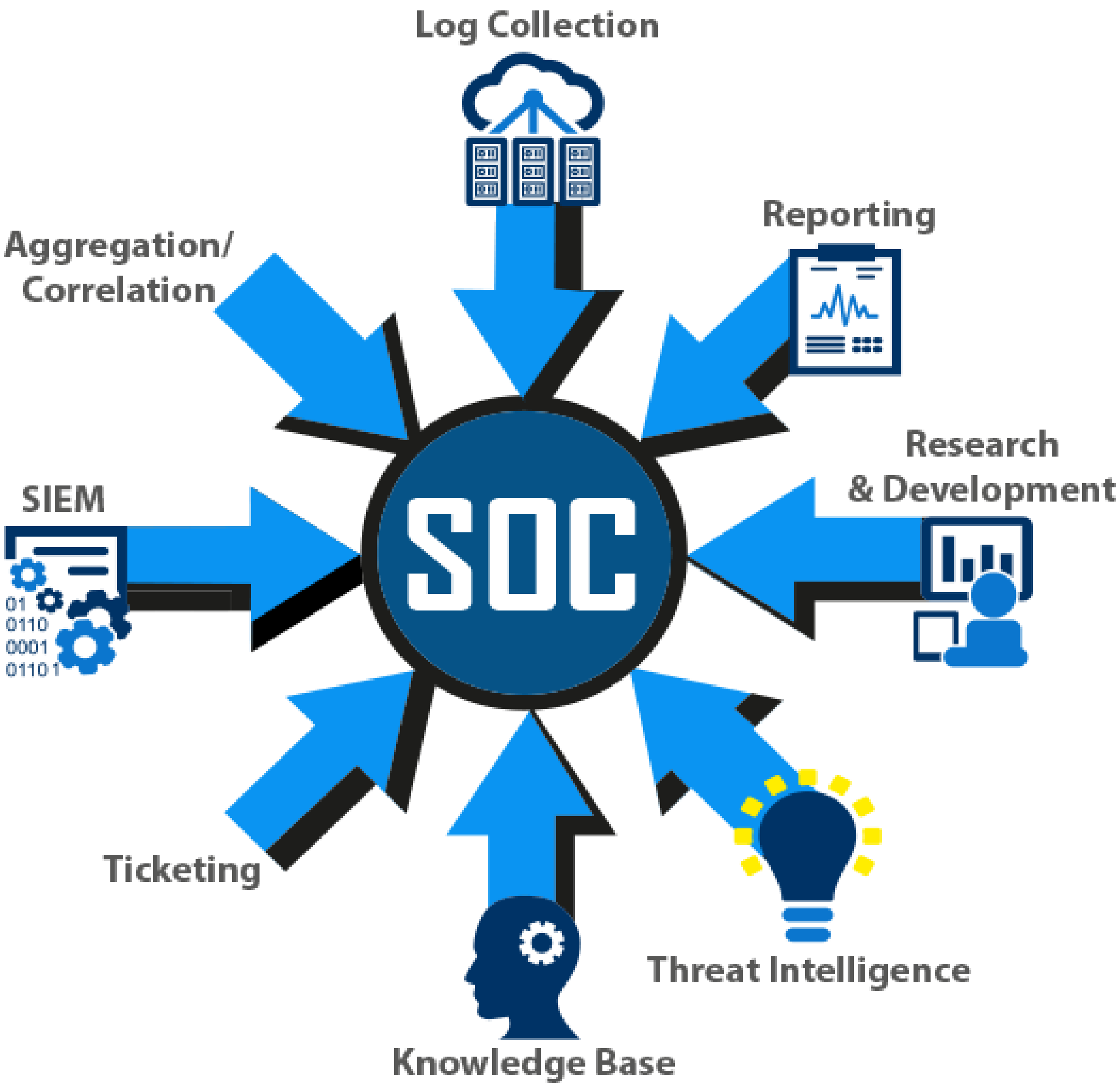
Ronald Broberg
December 2016

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

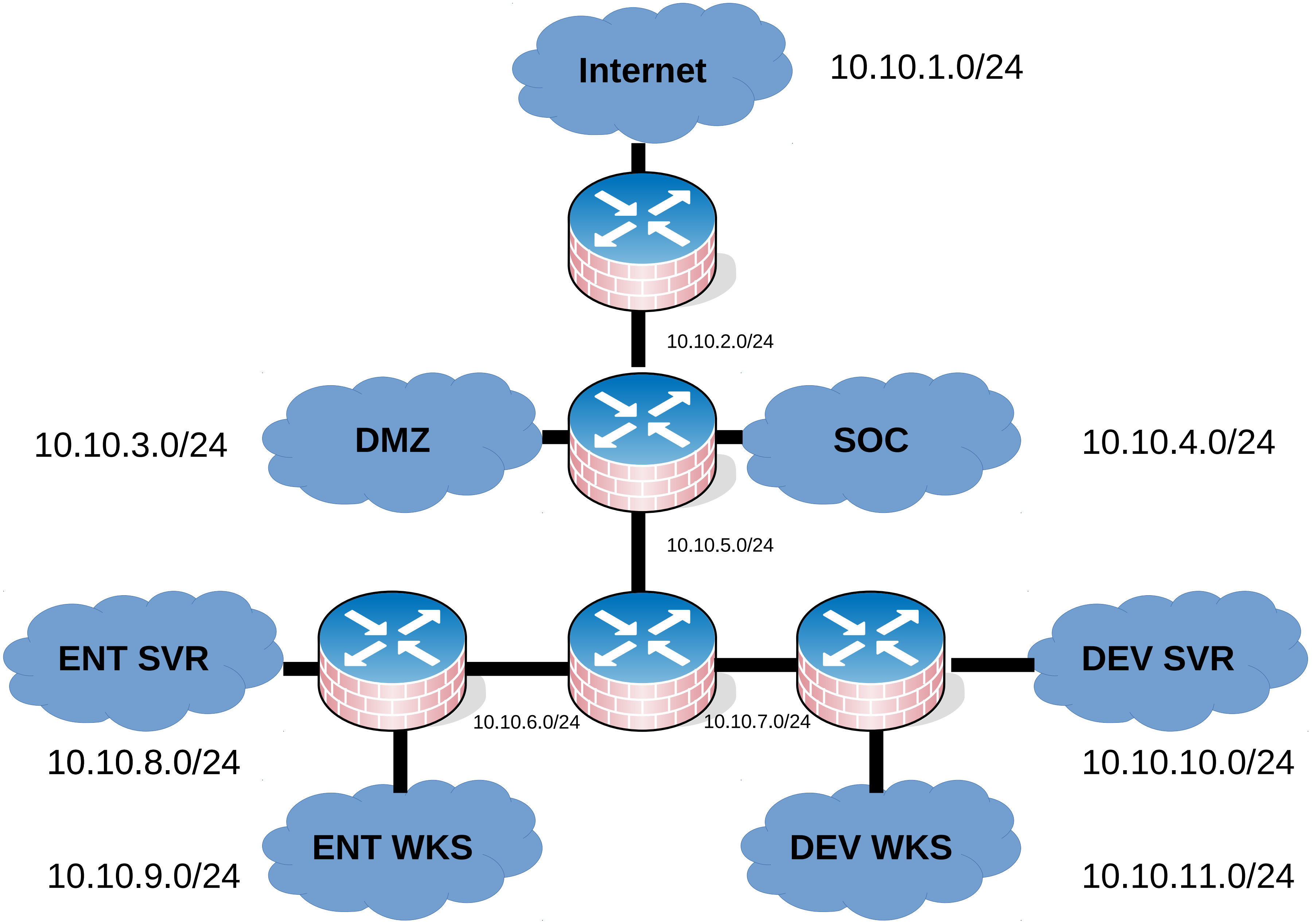
- **Resource Constraints**
  - Not a scalable architecture

- **The NAT interface links nodes undesirably**
  - Limits use a CyberRange model

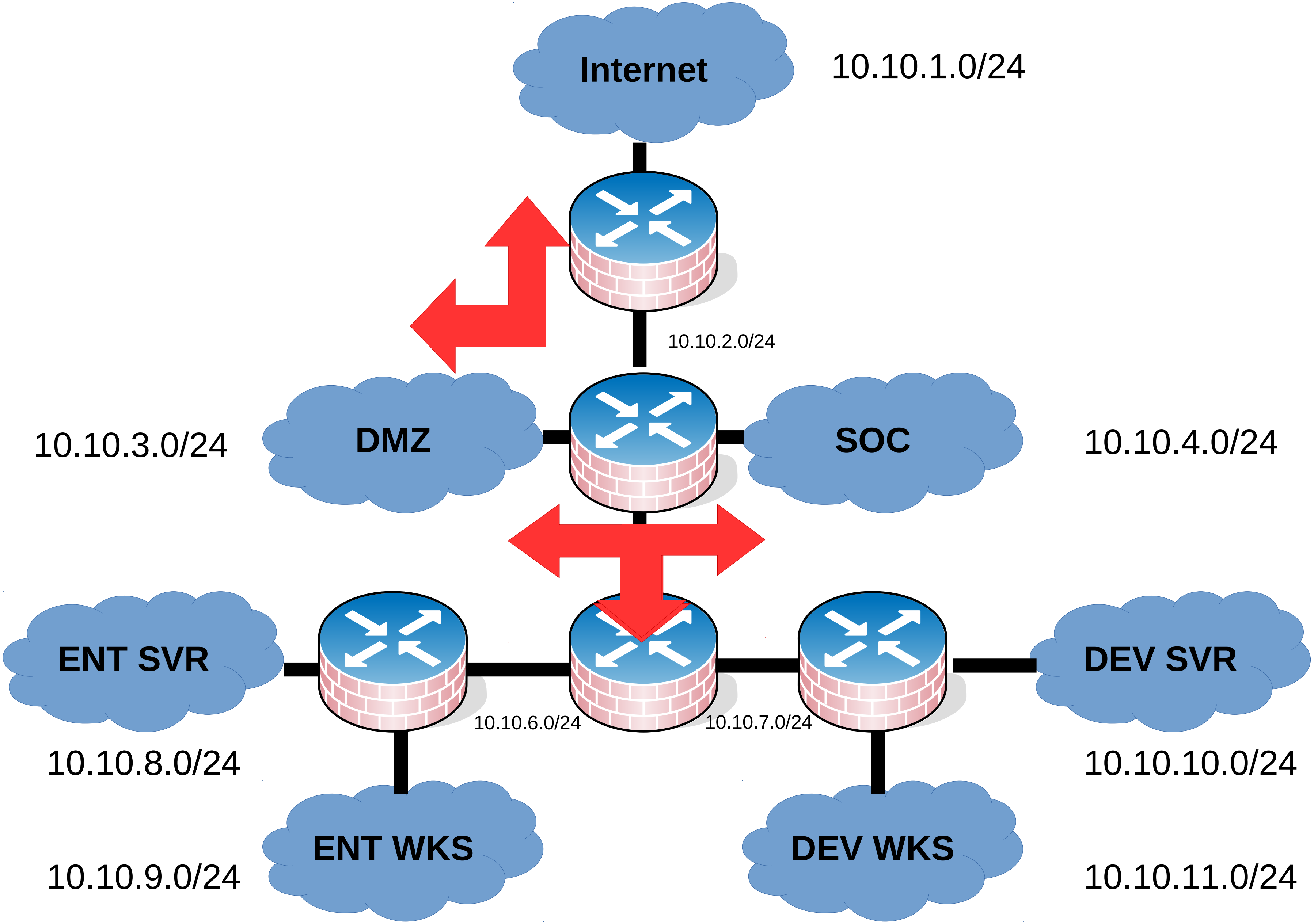
- **Lack of Microsoft Components**
  - Enterprise Servers Lack Key Microsoft Services
    - Active Directory
    - Exchange
  - Enterprise Workstation Are Not Microsoft
    - Unrealistic reflection of Enterprise

Infrastructure Design

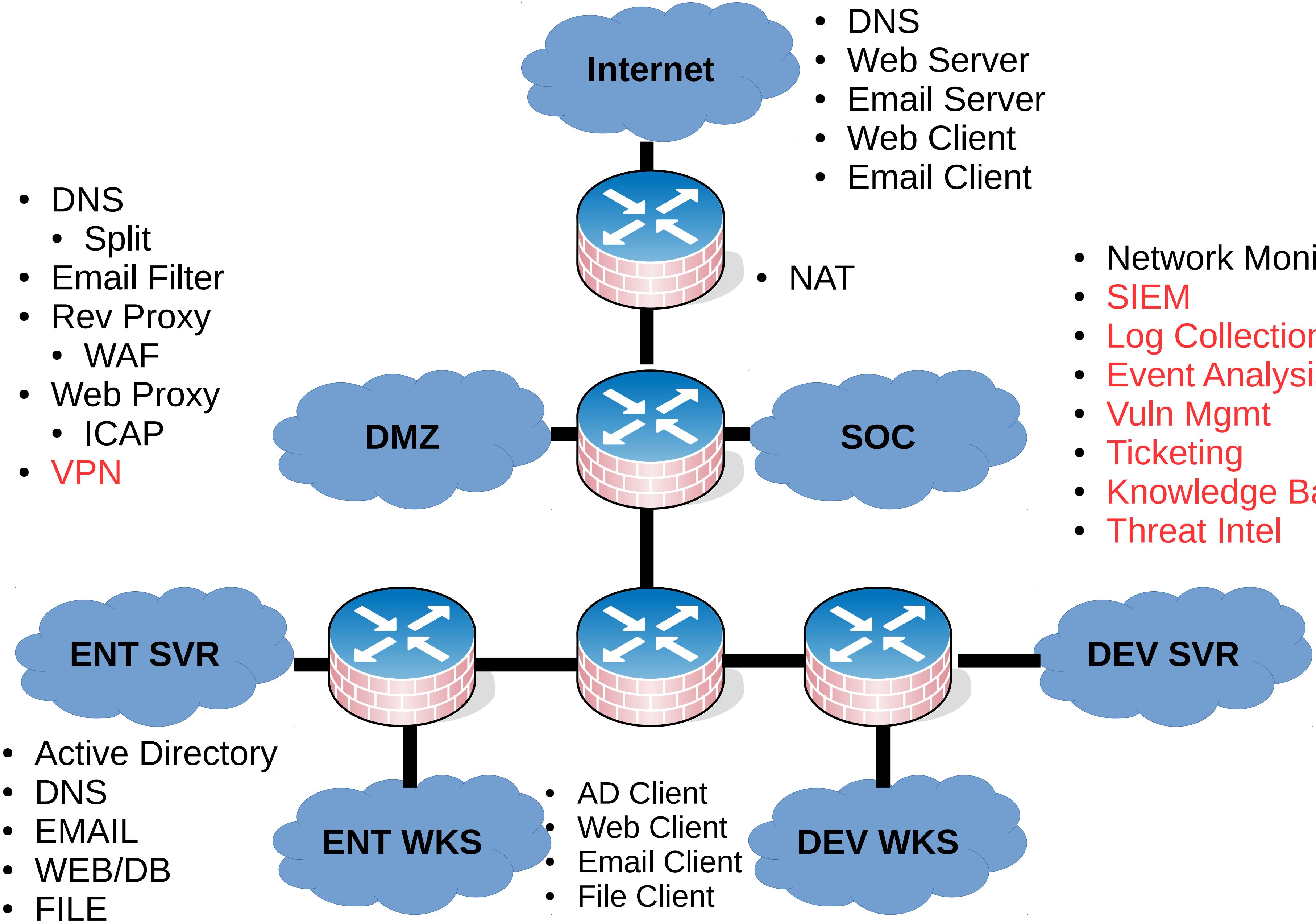
McSOC: Network Layout



McSOC: Network Routing



McSOC: Infrastructure Layout



- DNS
- Web Server
- Email Server
- Web Client
- Email Client

- DNS
  - Split
- Email Filter
- Rev Proxy
  - WAF
- Web Proxy
  - ICAP
- VPN

- NAT

- Network Monitor
- SIEM
- Log Collection
- Event Analysis
- Vuln Mgmt
- Ticketing
- Knowledge Base
- Threat Intel

- Active Directory
- DNS
- EMAIL
- WEB/DB
- FILE

- AD Client
- Web Client
- Email Client
- File Client

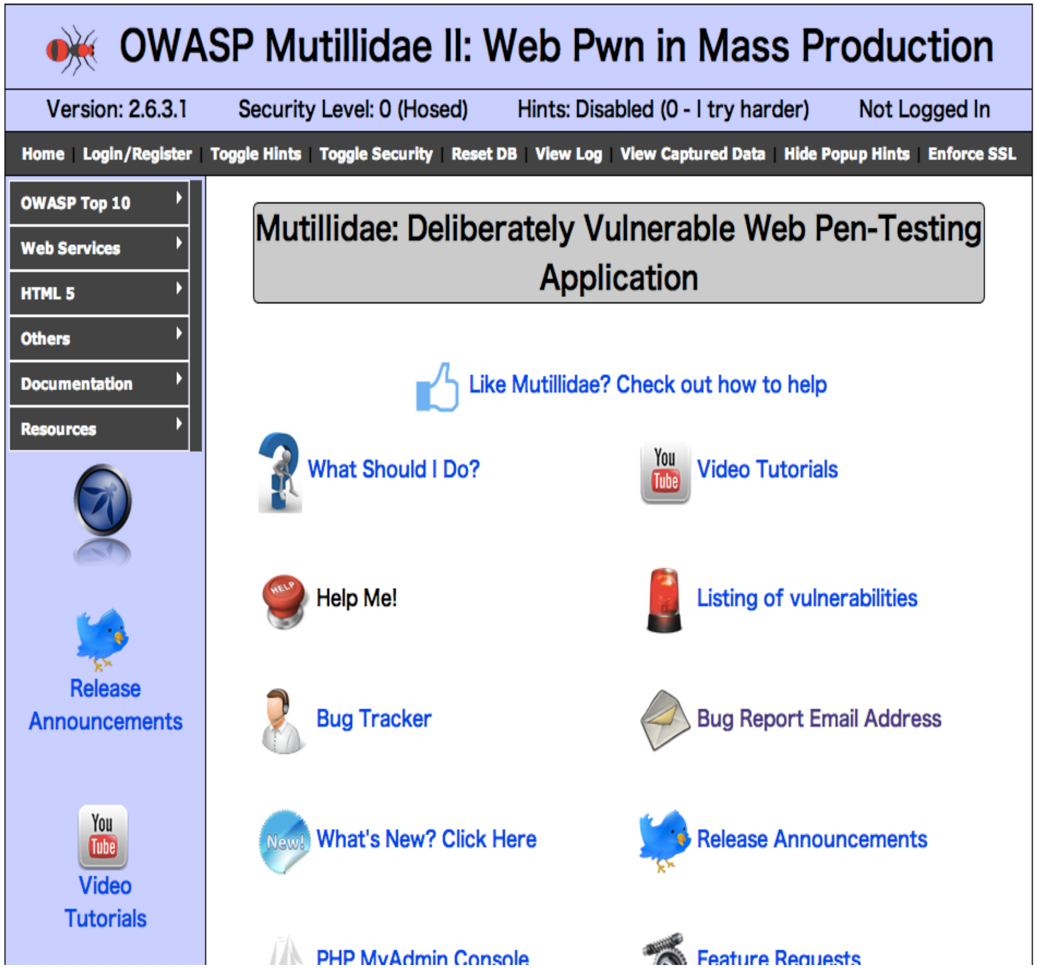
McSOC : WAN : TESTMAIL

www.shutterstock.com · 141034570

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

CentOS 7

McSOC : WAN : TESTWEB



OWASP Mutillidae II: Web Pwn in Mass Production

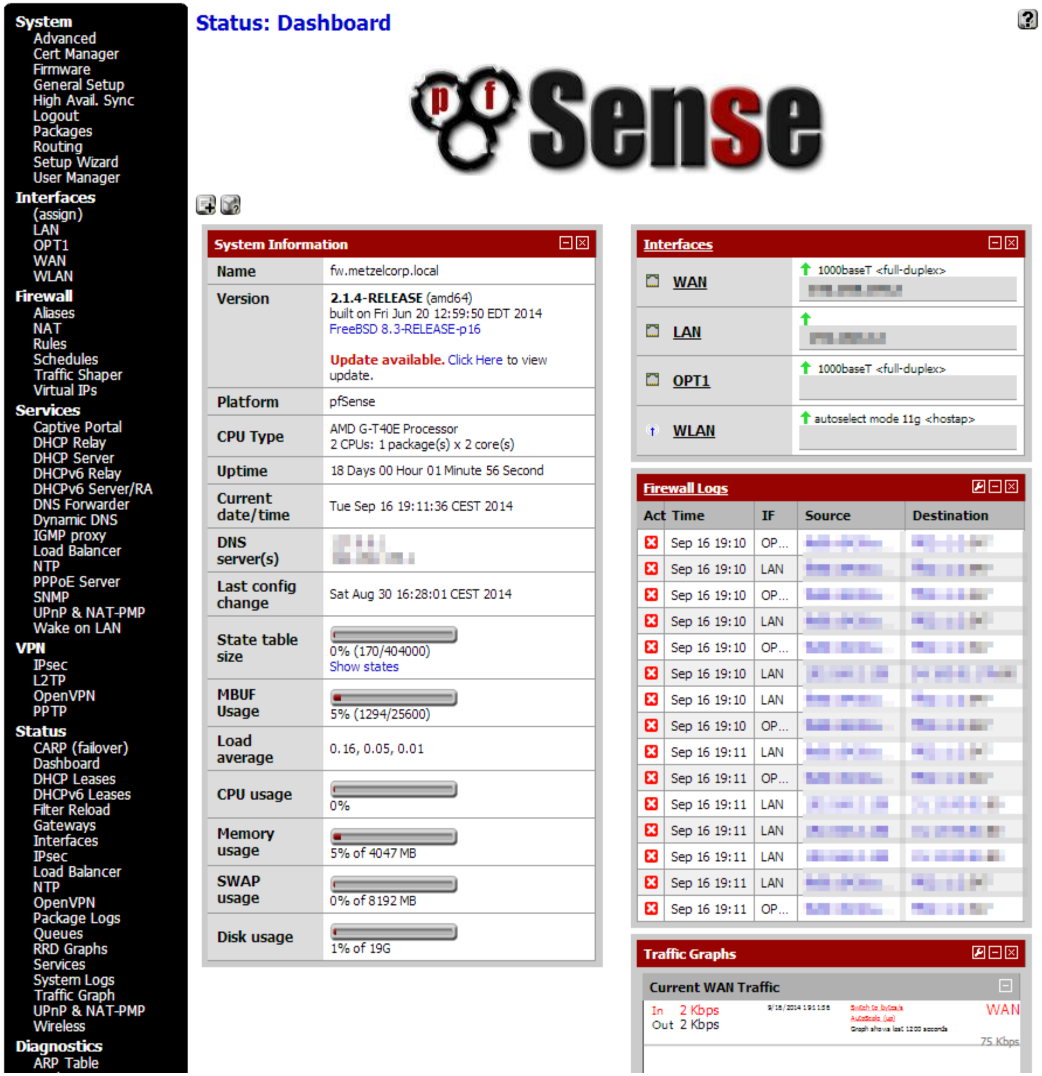
Version: 2.6.3.1 Security Level: 0 (Hosed) Hints: Disabled (0 - I try harder) Not Logged In

Mutillidae: Deliberately Vulnerable Web Pen-Testing Application

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

CentOS 7

McSOC: - : ROUTERS



Status: Dashboard

System Information

Name	fw.metzelcorp.local
Version	**2.1.4-RELEASE** (amd64) built on Fri Jun 20 12:59:50 EDT 2014 FreeBSD 8.3-RELEASE-p16 **Update available.** Click Here to view update.
Platform	pfSense
CPU Type	AMD G-T40E Processor 2 CPUs: 1 package(s) x 2 core(s)
Uptime	18 Days 00 Hour 01 Minute 56 Second
Current date/time	Tue Sep 16 19:11:36 CEST 2014
DNS server(s)	[redacted]
Last config change	Sat Aug 30 16:28:01 CEST 2014
State table size	0% (170/404000) Show states
MBUF Usage	5% (1294/25600)
Load average	0.16, 0.05, 0.01
CPU usage	0%
Memory usage	5% of 4047 MB
SWAP usage	0% of 8192 MB
Disk usage	1% of 19G

Interfaces

WAN	1000baseT <full-duplex> [redacted]
LAN	[redacted]
OPT1	1000baseT <full-duplex>
WLAN	autoselect mode 11g <hostap>

Firewall Logs

Act	Time	IF	Source	Destination
☒	Sep 16 19:10	OP...	[redacted]	[redacted]
☒	Sep 16 19:10	LAN	[redacted]	[redacted]
☒	Sep 16 19:10	OP...	[redacted]	[redacted]
☒	Sep 16 19:10	LAN	[redacted]	[redacted]
☒	Sep 16 19:10	OP...	[redacted]	[redacted]
☒	Sep 16 19:10	LAN	[redacted]	[redacted]
☒	Sep 16 19:10	LAN	[redacted]	[redacted]
☒	Sep 16 19:10	OP...	[redacted]	[redacted]
☒	Sep 16 19:11	LAN	[redacted]	[redacted]
☒	Sep 16 19:11	OP...	[redacted]	[redacted]
☒	Sep 16 19:11	LAN	[redacted]	[redacted]
☒	Sep 16 19:11	LAN	[redacted]	[redacted]
☒	Sep 16 19:11	LAN	[redacted]	[redacted]
☒	Sep 16 19:11	LAN	[redacted]	[redacted]
☒	Sep 16 19:11	OP...	[redacted]	[redacted]

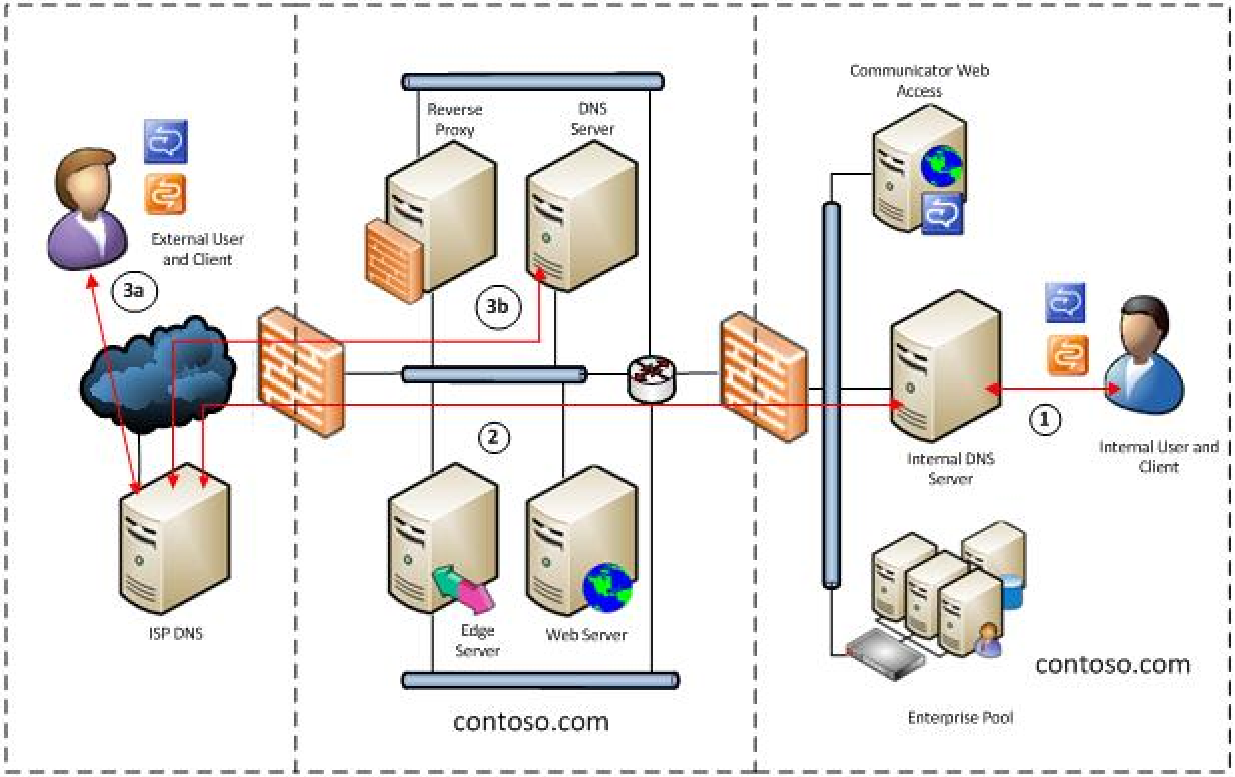
Traffic Graphs

Current WAN Traffic

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

FreeBSD 10

McSOC : DMZ : DNS

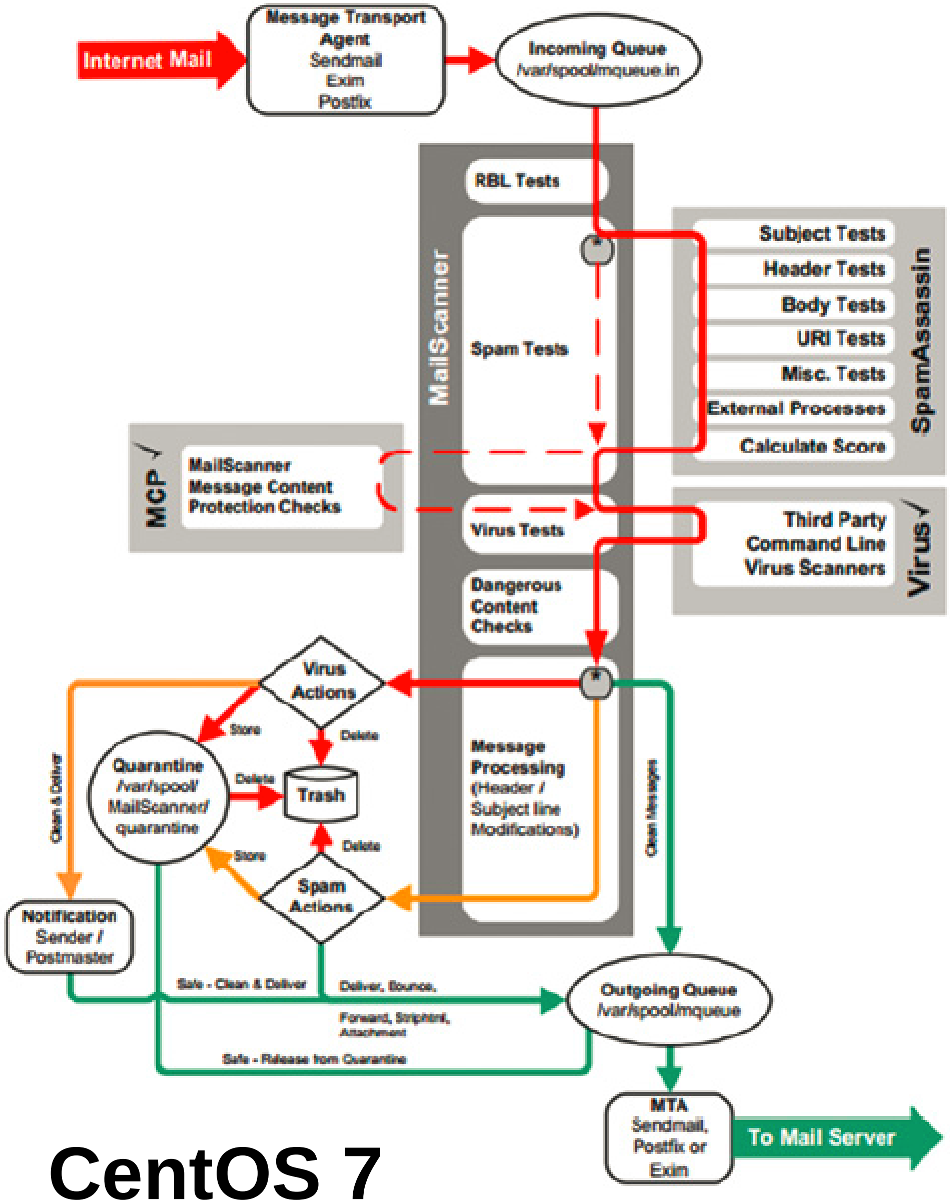


- DMZ DNS
  - Split DNS
  - DNSMASQ

CentOS 7

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

McSOC : DMZ : MAIL


Internet Mail
Message Transport Agent Sendmail Exim Postfix
Incoming Queue /var/spool/mqueue.in
MailScanner
RBL Tests
Spam Tests
Subject Tests
Header Tests
Body Tests
URI Tests
Misc. Tests
External Processes
Calculate Score
SpamAssassin
MCP
MailScanner Message Content Protection Checks
Virus Tests
Third Party Command Line Virus Scanners
Virus
Dangerous Content Checks
Virus Actions
Store
Delete
Quarantine /var/spool/ MailScanner/ quarantine
Trash
Clean & Deliver
Clean Messages
Message Processing (Header / Subject line Modifications)
Spam Actions
Notification Sender / Postmaster
Safe - Clean & Deliver
Deliver, Bounce, Forward, Striphtml, Attachment
Safe - Release from Quarantine
Outgoing Queue /var/spool/mqueue
MTA Sendmail, Postfix or Exim
To Mail Server

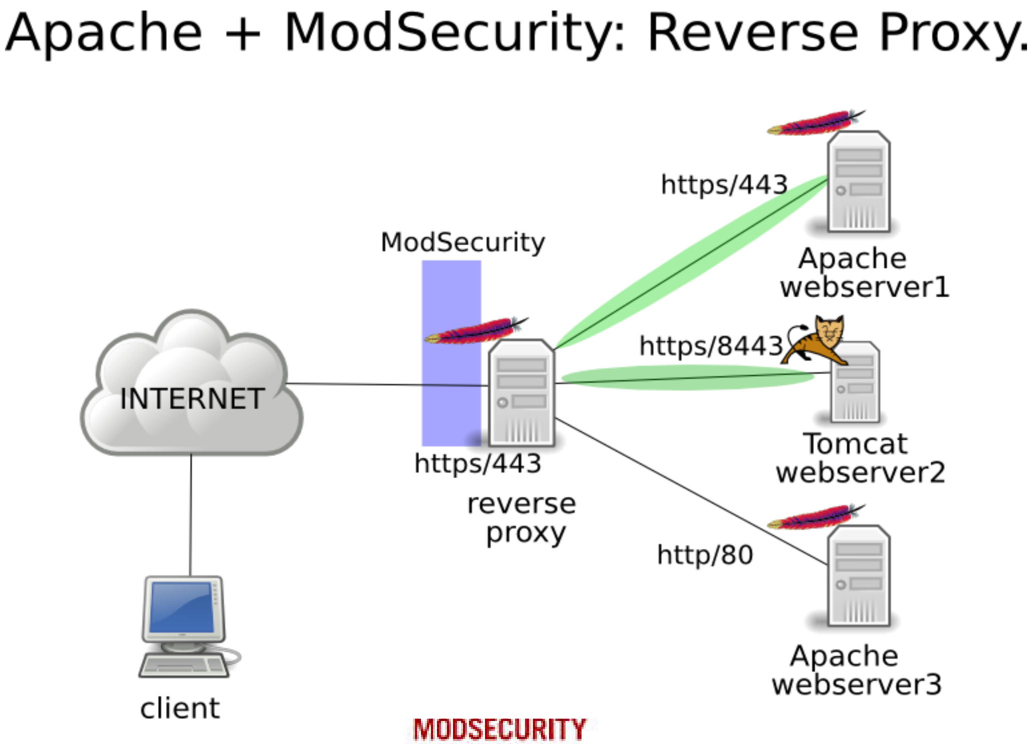
- Mail Gateway
  - Postfix
  - MailScanner
  - SpamAssassin
  - ClamAV

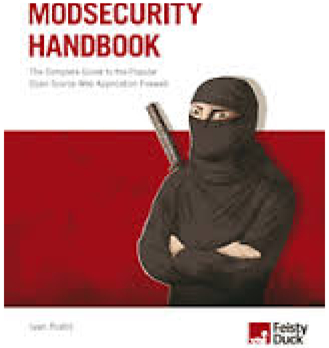
CentOS 7

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

Figure 2. *MailScanner process flow*

McSOC : DMZ : WEB



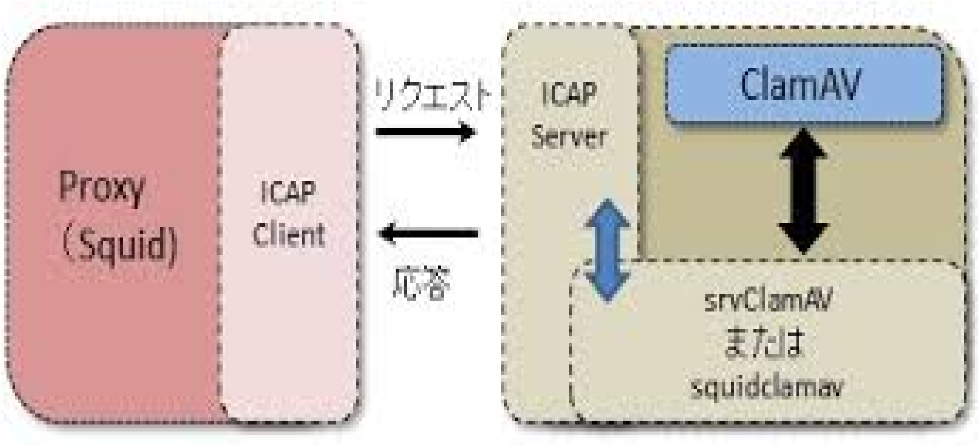


CentOS 7

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

- 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

McSOC : DMZ : PROXY

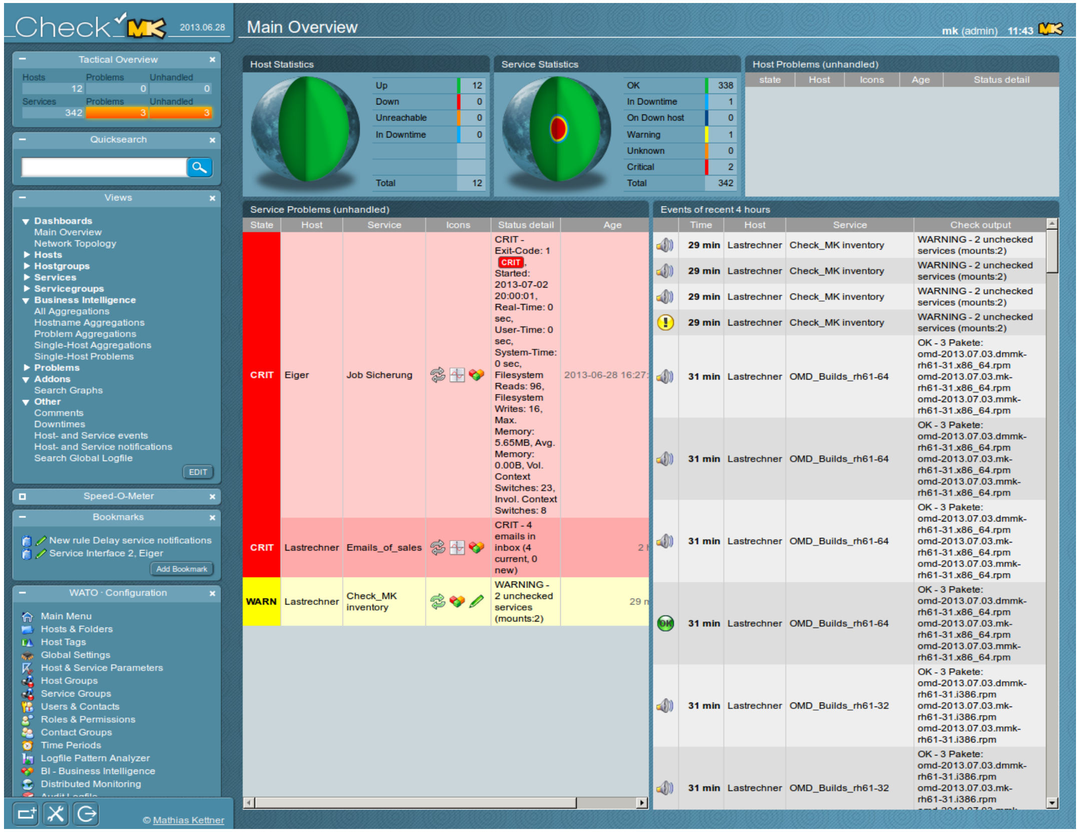


- SQUID Web Proxy
  - Squid
  - ClamAV
  - SquidClamAV
  - C-ICAP
    - Web antivirus service
    - basic URL filtering service

CentOS 7

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

McSOC: SOC : NAGIOS



Tactical Overview

Hosts	Problems	Unhandled
12	0	0
Services	**Problems**	**Unhandled**
342	3	3

Host Statistics

Up	12
Down	0
Unreachable	0
In Downtime	0
Total	12

Service Statistics

OK	338
In Downtime	1
On Down host	0
Warning	1
Unknown	0
Critical	2
Total	342

Host Problems (unhandled)

state	Host	Icons	Age	Status detail

Service Problems (unhandled)

State	Host	Service	Icons	Status detail	Age
CRIT	Eiger	Job Sicherung		CRIT - Exit-Code: 1 CRIT, Started: 2013-07-02 20:00:01, Real-Time: 0 sec, User-Time: 0 sec, System-Time: 0 sec, Filesystem Reads: 96, Filesystem Writes: 16, Max. Memory: 5.65MB, Avg. Memory: 0.00B, Vol. Context Switches: 23, Invol. Context Switches: 8	2013-06-28 16:27:
CRIT	Lastrechner	Emails_of_sales		CRIT - 4 emails in inbox (4 current, 0 new)	2 h
WARN	Lastrechner	Check_MK inventory		WARNING - 2 unchecked services (mounts:2)	29 m

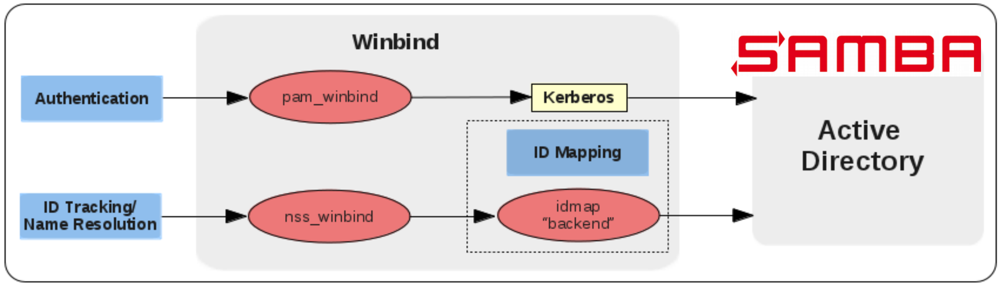
Events of recent 4 hours

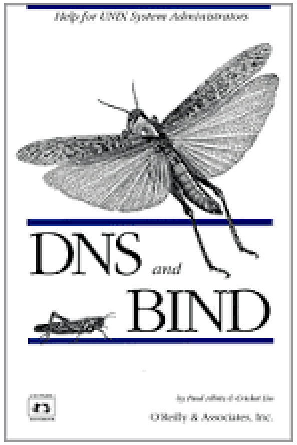
	Time	Host	Service	Check output
🔊	**29 min**	Lastrechner	Check_MK inventory	WARNING - 2 unchecked services (mounts:2)
🔊	**29 min**	Lastrechner	Check_MK inventory	WARNING - 2 unchecked services (mounts:2)
🔊	**29 min**	Lastrechner	Check_MK inventory	WARNING - 2 unchecked services (mounts:2)
!	**29 min**	Lastrechner	Check_MK inventory	WARNING - 2 unchecked services (mounts:2)
🔊	**31 min**	Lastrechner	OMD_Builds_rh61-64	OK - 3 Pakete: omd-2013.07.03.dmmk-rh61-31.x86_64.rpm omd-2013.07.03.mk-rh61-31.x86_64.rpm omd-2013.07.03.mmk-rh61-31.x86_64.rpm
🔊	**31 min**	Lastrechner	OMD_Builds_rh61-64	OK - 3 Pakete: omd-2013.07.03.dmmk-rh61-31.x86_64.rpm omd-2013.07.03.mk-rh61-31.x86_64.rpm omd-2013.07.03.mmk-rh61-31.x86_64.rpm
🔊	**31 min**	Lastrechner	OMD_Builds_rh61-64	OK - 3 Pakete: omd-2013.07.03.dmmk-rh61-31.x86_64.rpm omd-2013.07.03.mk-rh61-31.x86_64.rpm omd-2013.07.03.mmk-rh61-31.x86_64.rpm
OK	**31 min**	Lastrechner	OMD_Builds_rh61-64	OK - 3 Pakete: omd-2013.07.03.dmmk-rh61-31.x86_64.rpm omd-2013.07.03.mk-rh61-31.x86_64.rpm omd-2013.07.03.mmk-rh61-31.x86_64.rpm
🔊	**31 min**	Lastrechner	OMD_Builds_rh61-32	OK - 3 Pakete: omd-2013.07.03.dmmk-rh61-31.i386.rpm omd-2013.07.03.mk-rh61-31.i386.rpm omd-2013.07.03.mmk-rh61-31.i386.rpm
🔊	**31 min**	Lastrechner	OMD_Builds_rh61-32	OK - 3 Pakete: omd-2013.07.03.dmmk-rh61-31.i386.rpm omd-2013.07.03.mk-rh61-31.i386.rpm

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

Ubuntu 16 Xenial

McSOC: ENTSVR : DC1/DNS

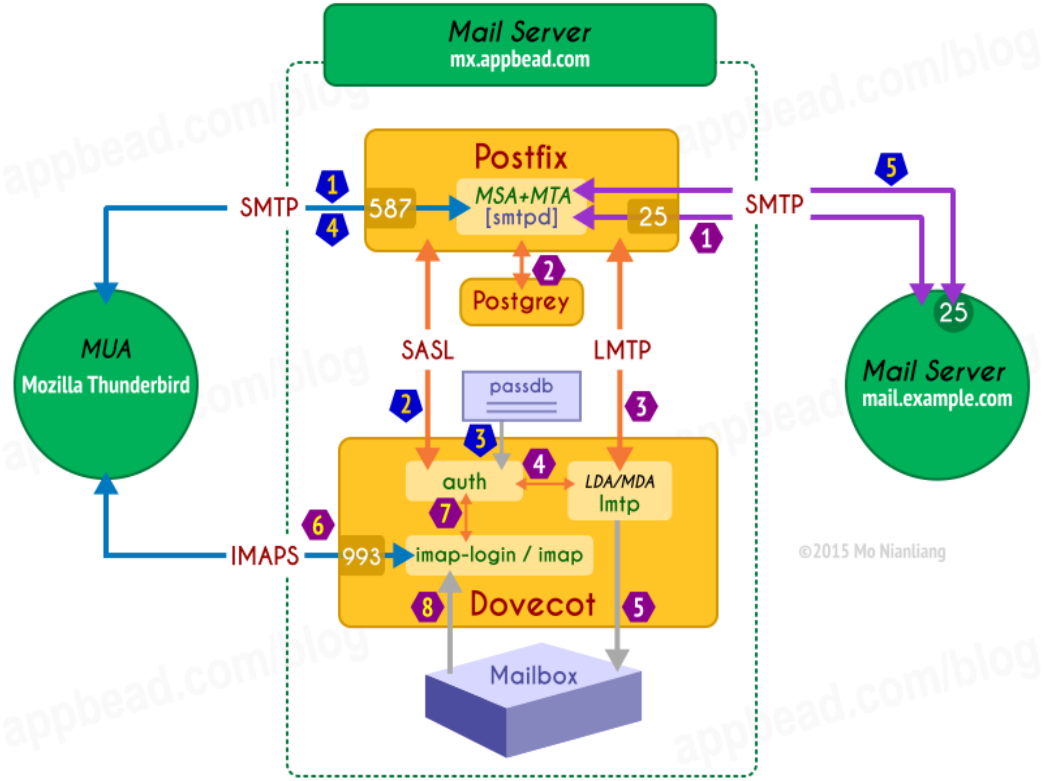



Help for UNIX System Administrators
DNS and BIND
by Paul Albitz & Cricket Liu
O'Reilly & Associates, Inc.

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

CentOS 7

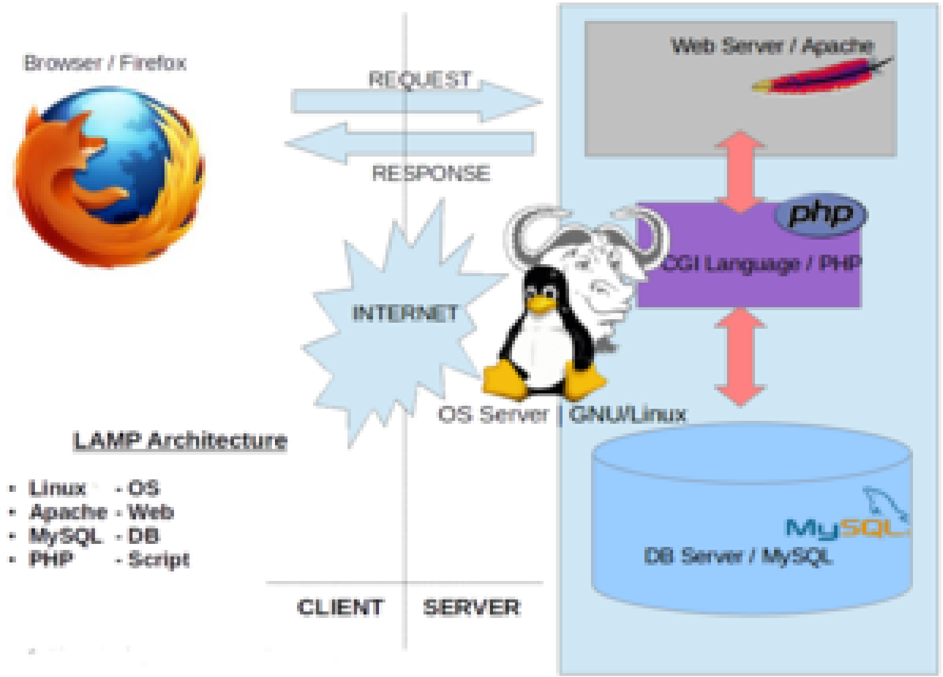
McSOC: ENTSVR : MAIL



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

CentOS 7

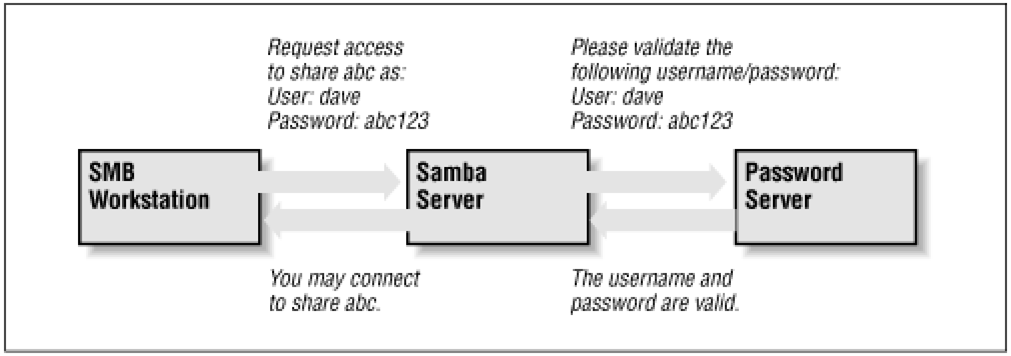
McSOC: ENTSVR : WEB/DB



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

CentOS 7

McSOC : DMZ : FILE

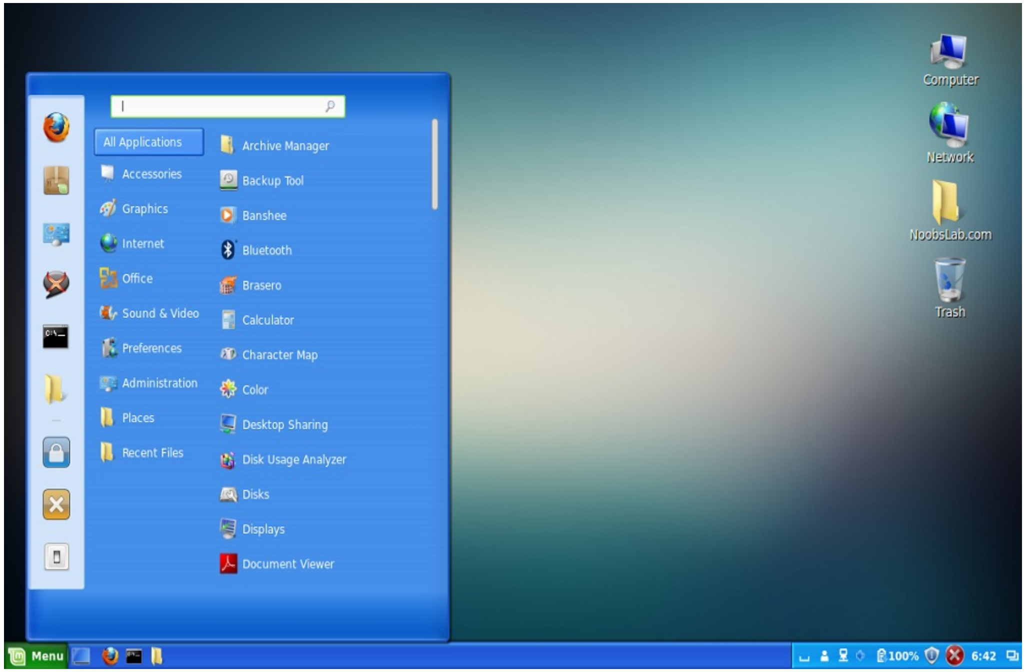


- SMB File Shares
  - Home Directories
    - Automounted on Clients
    - Authenticated against Active Directory
  - Anonymous Public Shares

CentOS 7

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

McSOC: ENTWKS : WKS101



Mint Linux 14

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

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

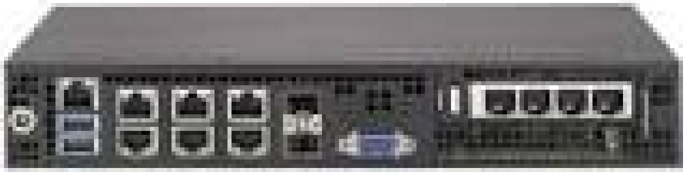
McSOC: HP Proliant DL380

- 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