

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



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

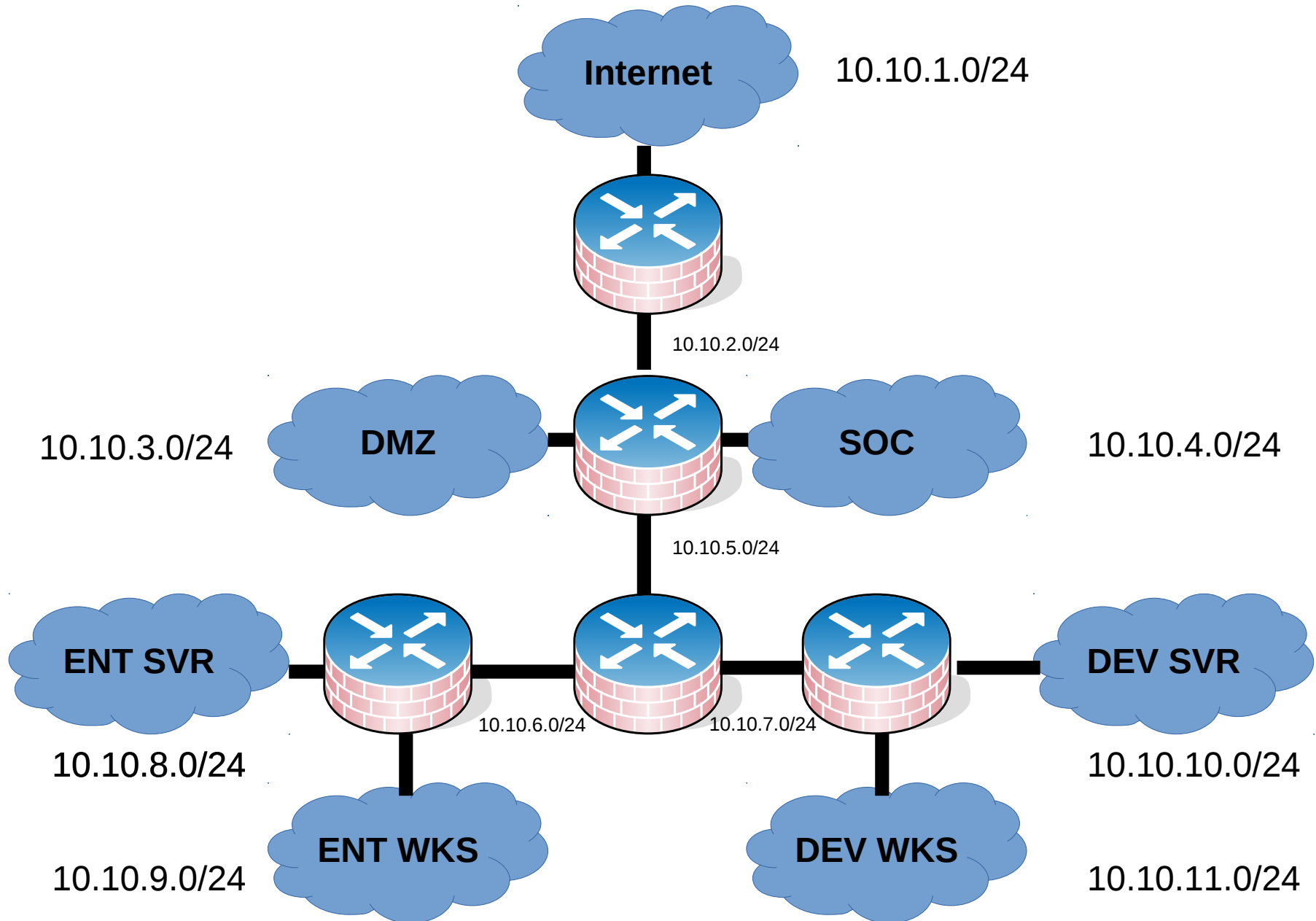
- **Open Source Components**
 - Minimize License Issues
 - Maximize Re-usability
- **Deployable to Multiple Visualization Hosts**
 - Develop on single server (Oracle VirtualBox)
 - Deploy to Amazon AWS or Vmware Fusion
- **Automated Testing**
 - Deployed Project should be able to self-validate

McSOC: Constraints and Limitations

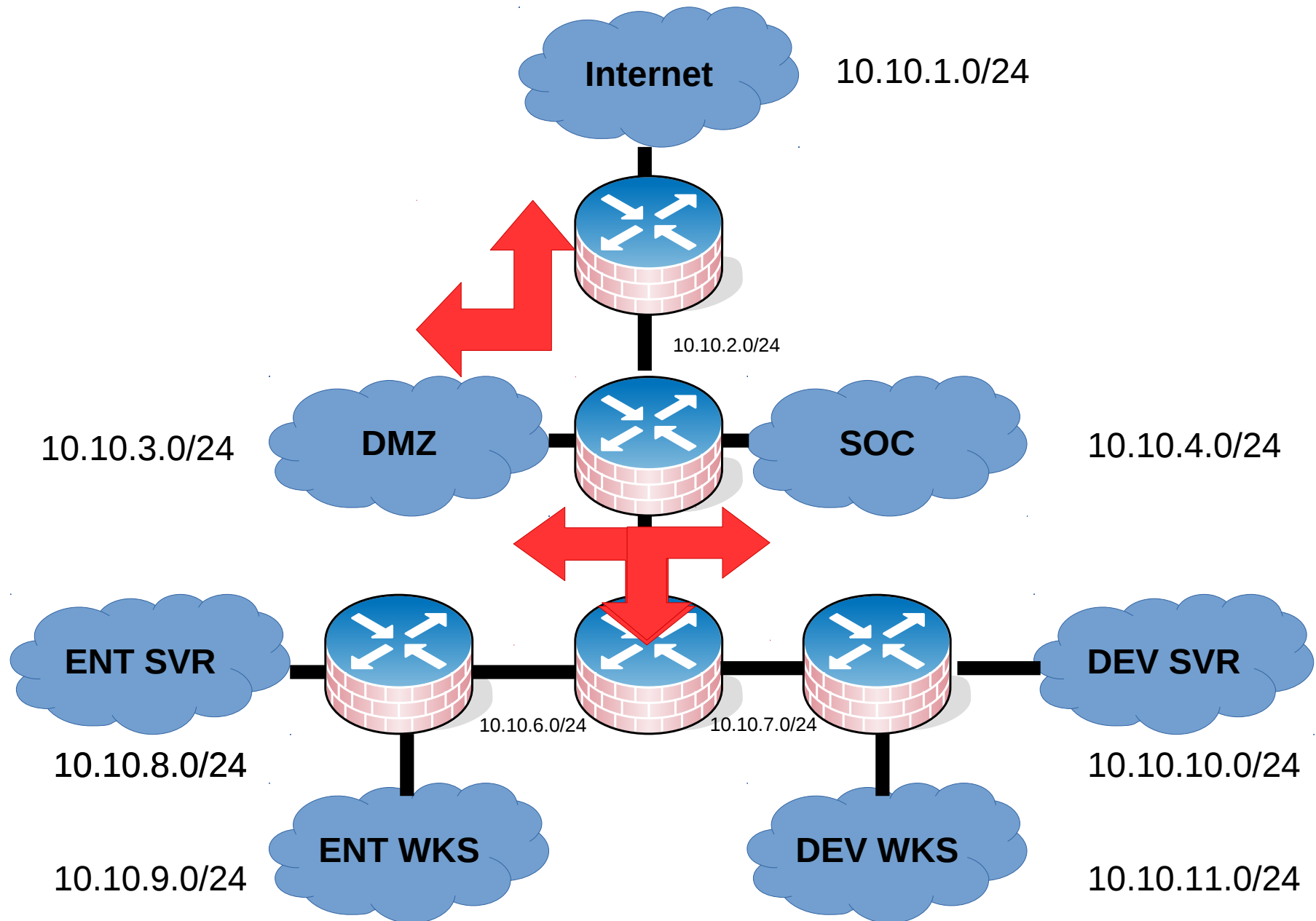
- **Resource Constraints**
 - Not a scalable architecture
- **The NAT interface links nodes undesirably**
 - Limits use a CyberRange model
- **Lack of Microsoft Components**
 - Enterprise Servers Lack Key Microsoft Services
 - Active Directory
 - Exchange
 - Enterprise Workstation Are Not Microsoft
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

Infrastructure Design

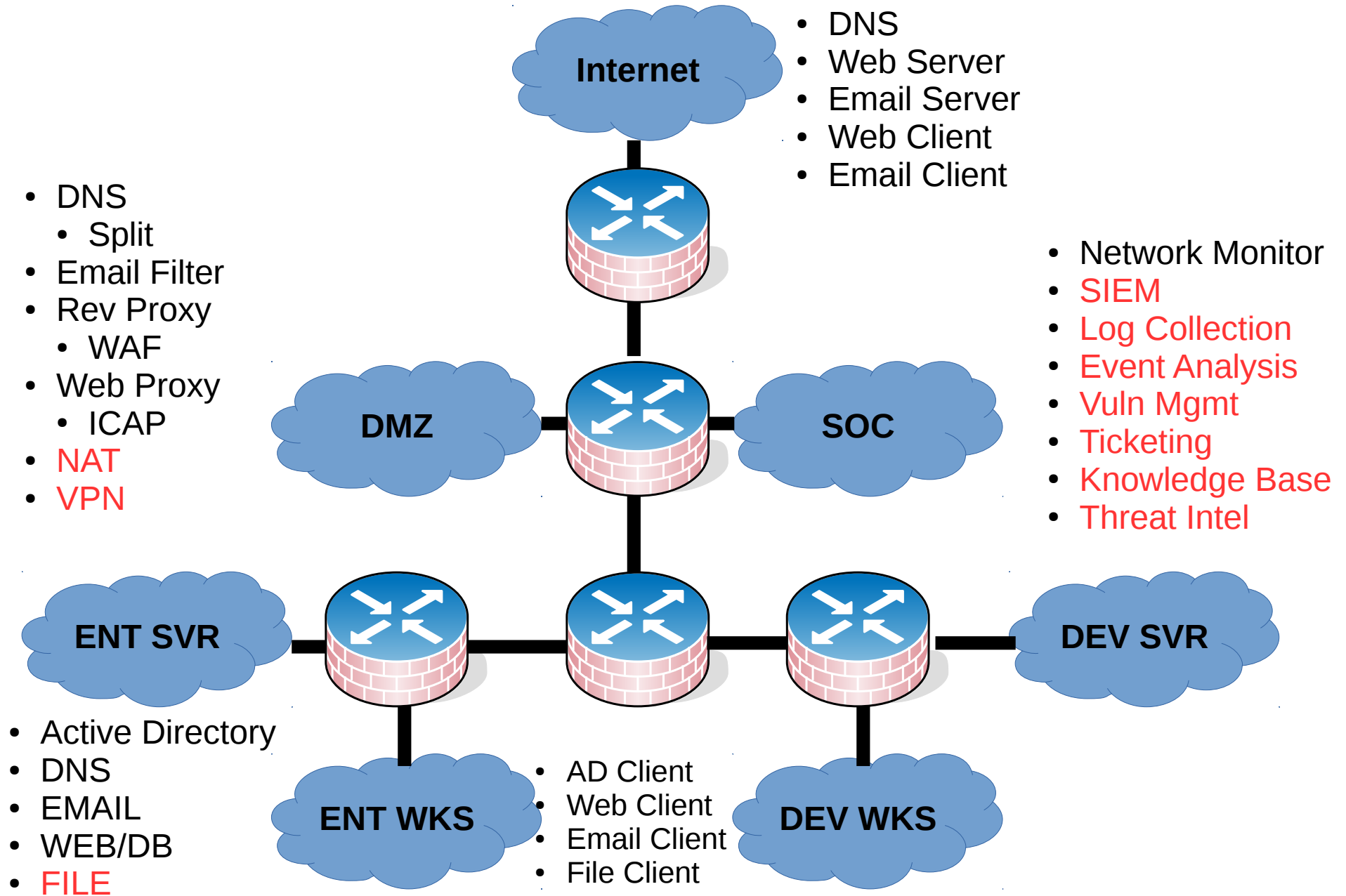
McSOC: Network Layout



McSOC: Network Routing



McSOC: Infrastructure Layout



McSOC : WAN : TESTMAIL




www.shutterstock.com · 141034570

CentOS 7

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


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


[Home](#) | [Login/Register](#) | [Toggle Hints](#) | [Toggle Security](#) | [Reset DB](#) | [View Log](#) | [View Captured Data](#) | [Hide Popup Hints](#) | [Enforce SSL](#)


OWASP Top 10 ▾
Web Services ▾
HTML 5 ▾
Others ▾
Documentation ▾
Resources ▾



Release Announcements



Video Tutorials

Mutillidae: Deliberately Vulnerable Web Pen-Testing Application


 [Like Mutillidae? Check out how to help](#)


 [What Should I Do?](#)


 [Video Tutorials](#)


 [Help Me!](#)


 [Listing of vulnerabilities](#)


 [Bug Tracker](#)

 [Bug Report Email Address](#)

 [What's New? Click Here](#)

 [Release Announcements](#)

 [PHP MvAdmin Console](#)

 [Feature Requests](#)

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

CentOS 7

McSOC: - : ROUTERS

System
Advanced
Cert Manager
Firmware
General Setup
High Avail. Sync
Logout
Packages
Routing
Setup Wizard
User Manager

Interfaces
(assign)
LAN
OPT1
WAN
WLAN

Firewall
Aliases
NAT
Rules
Schedules
Traffic Shaper
Virtual IPs

Services
Captive Portal
DHCP Relay
DHCP Server
DHCPv6 Relay
DHCPv6 Server/RA
DNS Forwarder
Dynamic DNS
IGMP proxy
Load Balancer
NTP
PPPoE Server
SNMP
UPnP & NAT-PMP
Wake on LAN

VPN
IPsec
L2TP
OpenVPN
PPTP

Status
CARP (failover)
Dashboard
DHCP Leases
DHCPv6 Leases
Filter Reload
Gateways
Interfaces
IPsec
Load Balancer
NTP
OpenVPN
Package Logs
Queues
RRD Graphs
Services
System Logs
Traffic Graph
UPnP & NAT-PMP
Wireless

Diagnostics
ARP Table

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)	
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>
LAN	↑
OPT1	↑ 1000baseT <full-duplex>
WLAN	↑ autoselect mode 11g <hostap>

Firewall Logs

Act	Time	IF	Source	Destination
×	Sep 16 19:10	OP...		
×	Sep 16 19:10	LAN		
×	Sep 16 19:10	OP...		
×	Sep 16 19:10	LAN		
×	Sep 16 19:10	OP...		
×	Sep 16 19:10	LAN		
×	Sep 16 19:10	OP...		
×	Sep 16 19:10	LAN		
×	Sep 16 19:10	OP...		
×	Sep 16 19:10	LAN		
×	Sep 16 19:11	OP...		
×	Sep 16 19:11	LAN		
×	Sep 16 19:11	LAN		
×	Sep 16 19:11	LAN		
×	Sep 16 19:11	LAN		
×	Sep 16 19:11	OP...		

Traffic Graphs

Current WAN Traffic

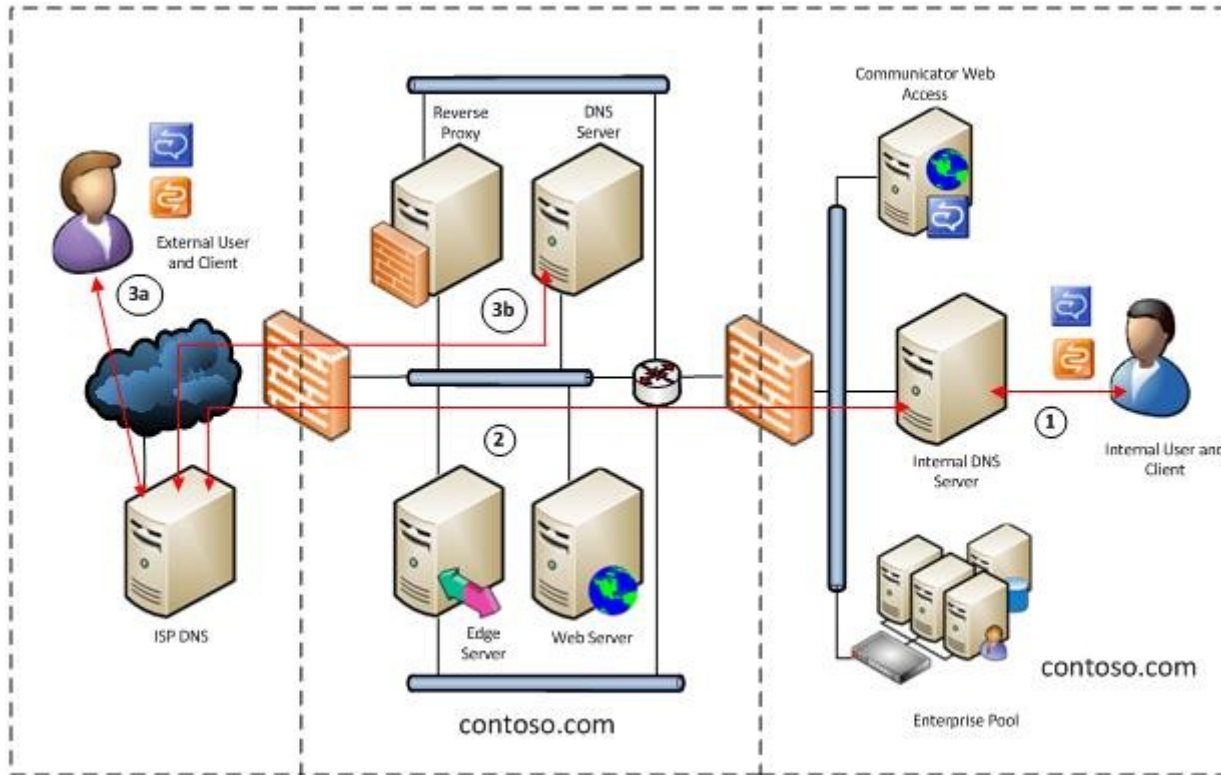
In 2 Kbps
Out 2 Kbps

W/16/2014 19:11:58
Switch to local
Autobahn (Lan)
Graph shows last 1200 seconds
75 Kbps

- pfSense
 - Firewall
 - Routing
 - SNMP

FreeBSD 10

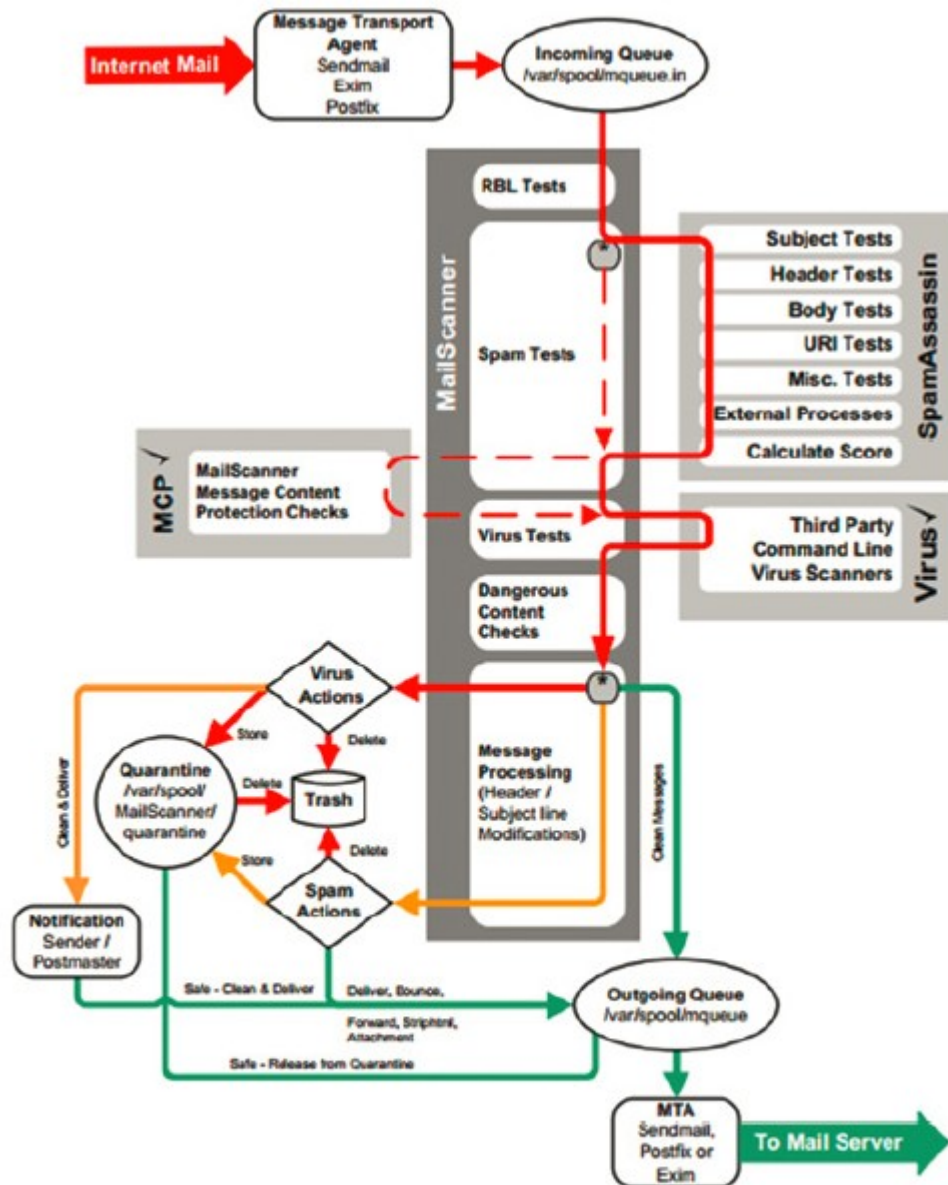
McSOC : DMZ : DNS



- DMZ DNS
 - DNSMASQ

CentOS 7

McSOC : DMZ : MAIL

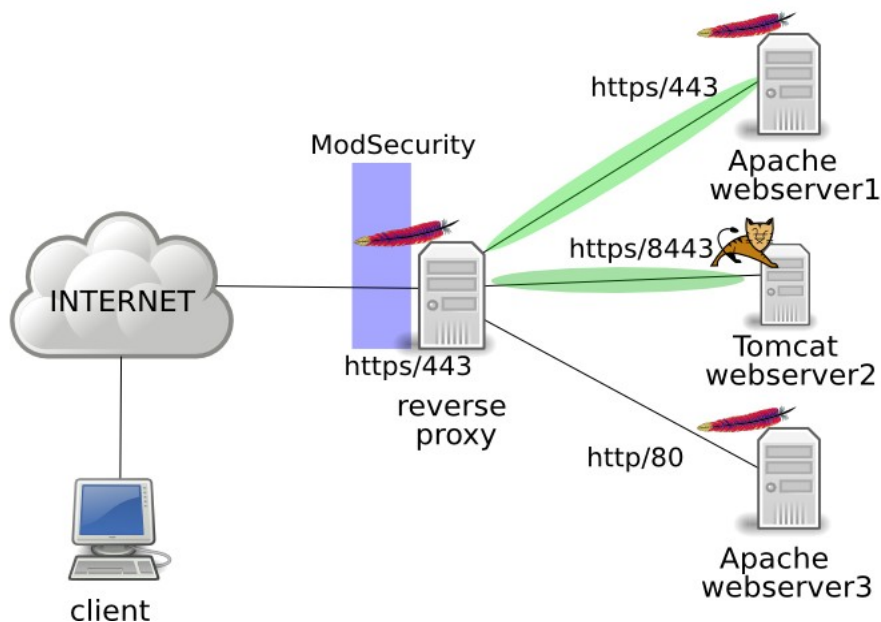


- Mail Gateway
 - Postfix
 - MailScanner
 - SpamAssassin
 - ClamAV

CentOS 7

McSOC : DMZ : WEB

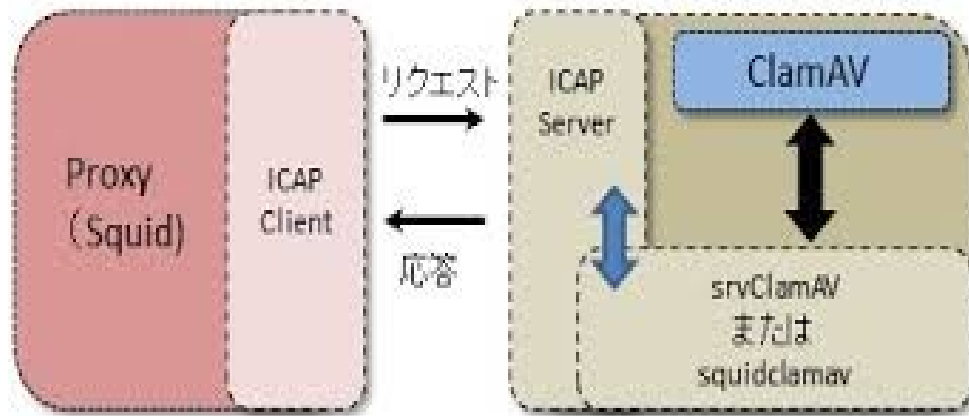
Apache + ModSecurity: Reverse Proxy. • NGINX Reverse Proxy



- 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

CentOS 7

McSOC : DMZ : PROXY

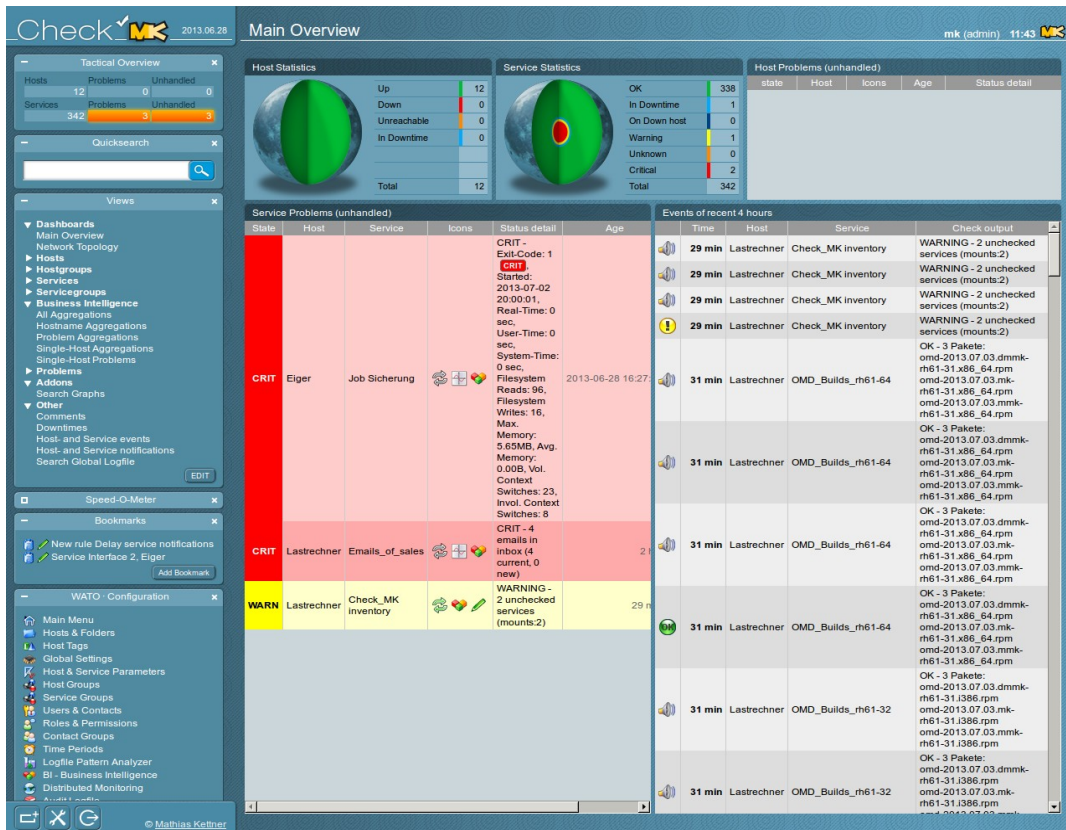


- SQUID Web Proxy
 - Squid
 - ClamAV
 - SquidClamAV
 - C-ICAP
 - Web antivirus service
 - basic URL filtering service

CentOS 7

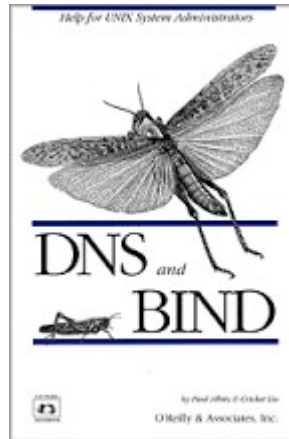
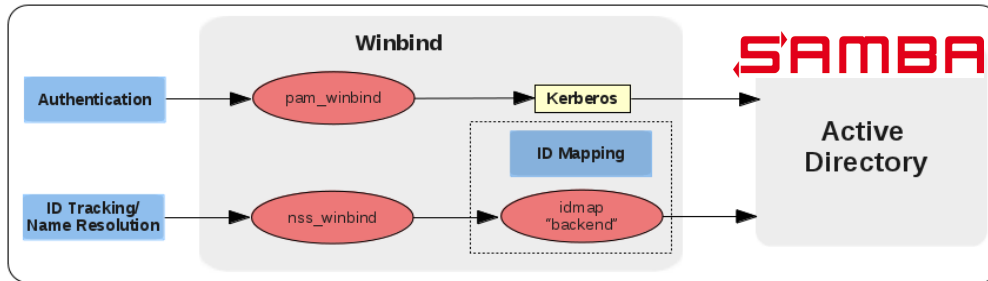
McSOC: SOC : NAGIOS

- Network Monitor
 - Check_MK
 - Nagios Variant
 - Liveevent Service



Ubuntu 16 Xenial

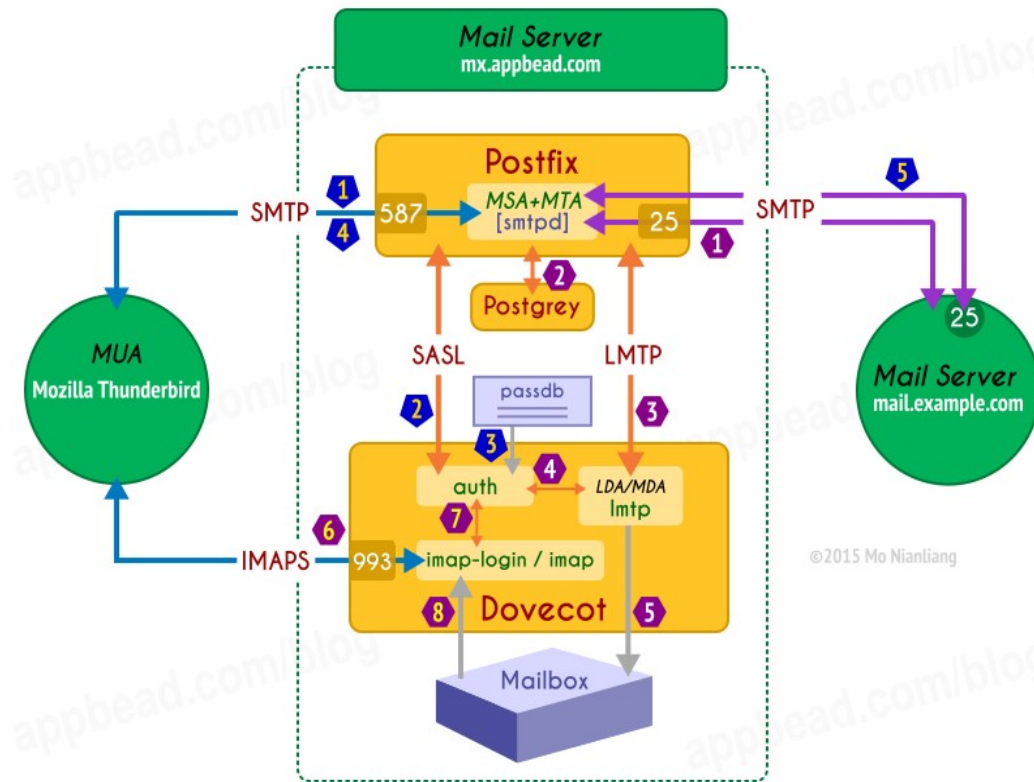
McSOC: ENTSVR : DC1/DNS



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

CentOS 7

McSOC: ENTSVR : MAIL

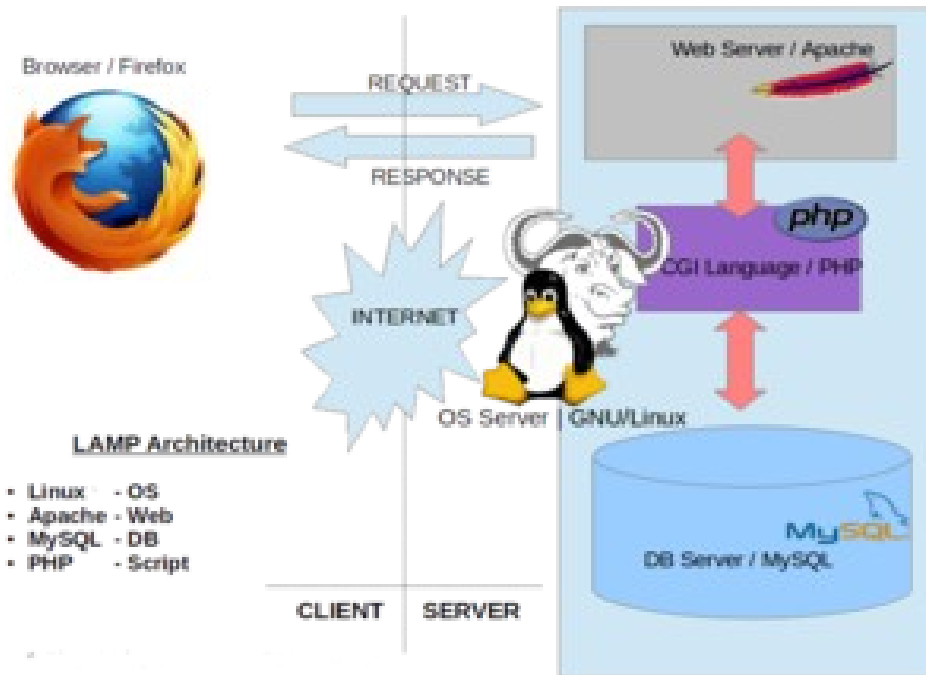


- **Mail Server**

- MTA: PostFix
- MDA: Dovecot
- AD/LDAP Authentication

CentOS 7

McSOC: ENTSVR : WEB/DB



- **Web Server**

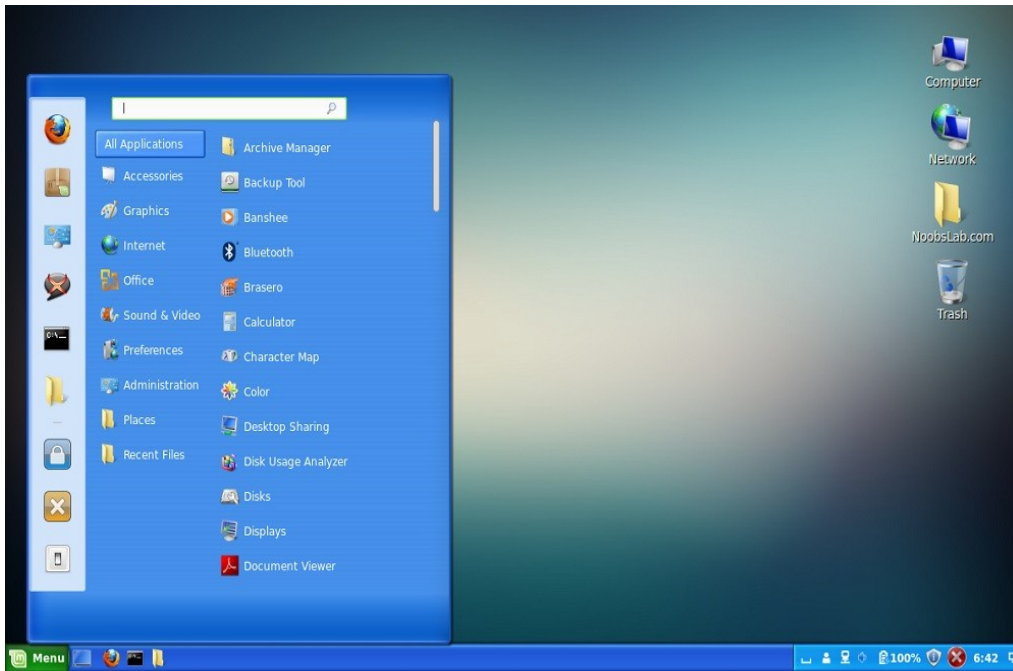
- Apache2
- PHP 5
- Wordpress

- **DB Server**

- MariaDB
 - Fork of MySQL

CentOS 7

McSOC: ENTWKS : WKS101



**Mint Linux 14
Win 7 Look and Feel**

- **Domain Client**
 - Samba4 Authentication
- **Mail Client**
 - Mozilla Thunderbird
- **Web Browser**
 - Mozilla Firefox

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 SSD \$300
- External Storage \$?
- Power Req: 80W chassis (+ ext storage)

McSOC: Intel NUC



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