Gov-X Innovation Challenge 2021

Network Security

Niel van Rooyen

Head: Information Security(CISO)

Niel van Rooyen

Network Security

Background:

With 15 years experience in ICT and Cyber Security space, within the private sector ranging from mining, retail, manufacturing and telecommunication industries, I believe better collaboration between all of these industries and governments specifically around Cyber Security, we will start gaining the required knowledge an have the necessary edge against the ever evolving requirements and threat actors in the "Cyberspace".

Define security

- Confidentiality
- Integrity
- Availability

1.

Threats….

- External

- Hackers & Crackers
- White Hat Hackers
- Scripts Kiddies
- Cyber terrorists
- Black Hat Hackers

- Internal

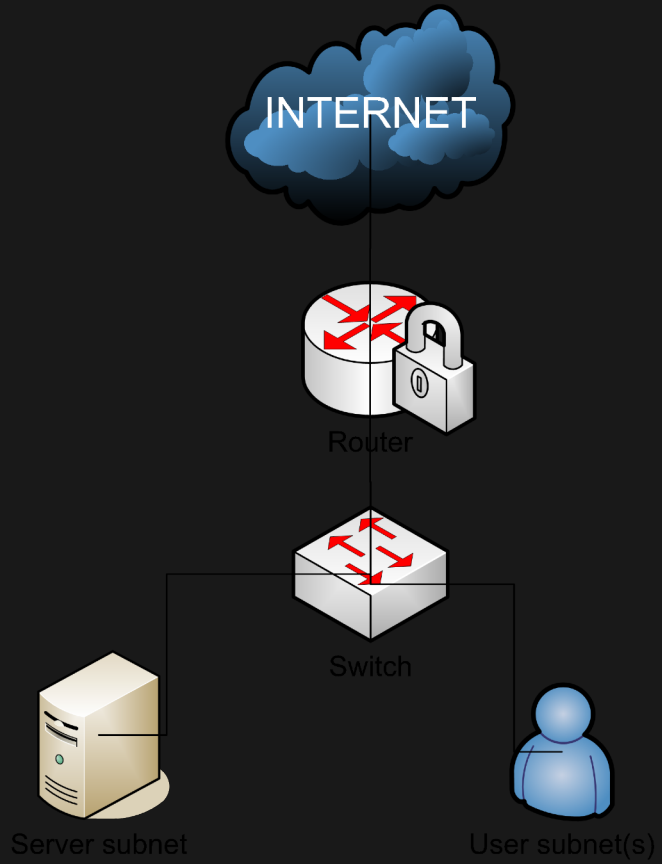
- Employee threats
- Accidents

Threat Types Networking

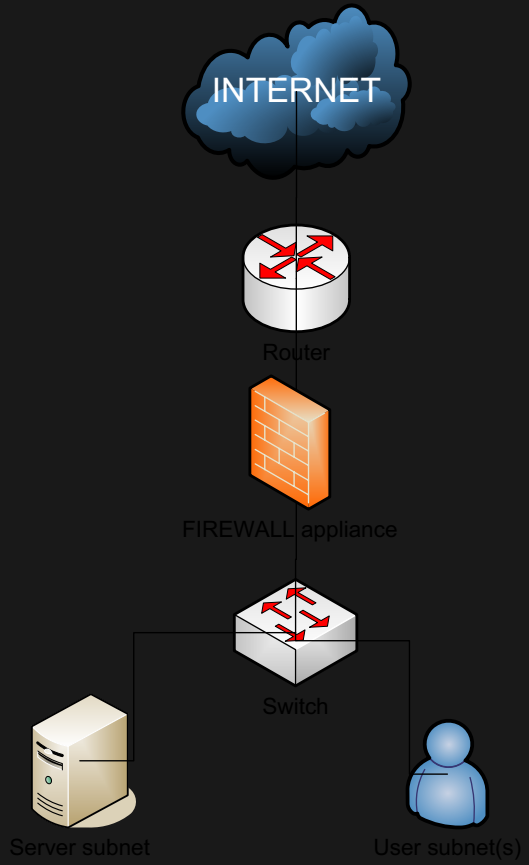
Relevant for any industry

- Denial of Services (DoS)
  - Network flooding
  - Buffer overflows
  - Software error
- Malware
  - Virus, worm, trojan horse
- Social Engineering
- Brute force

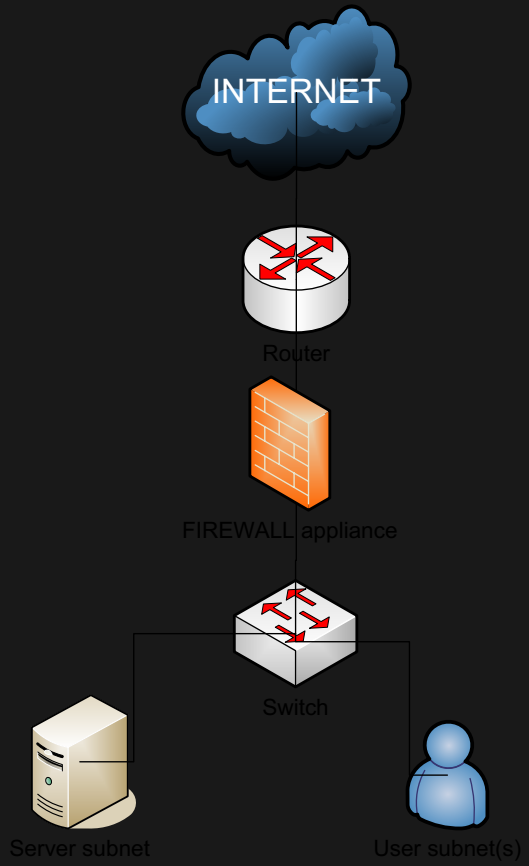
Network Security Layouts



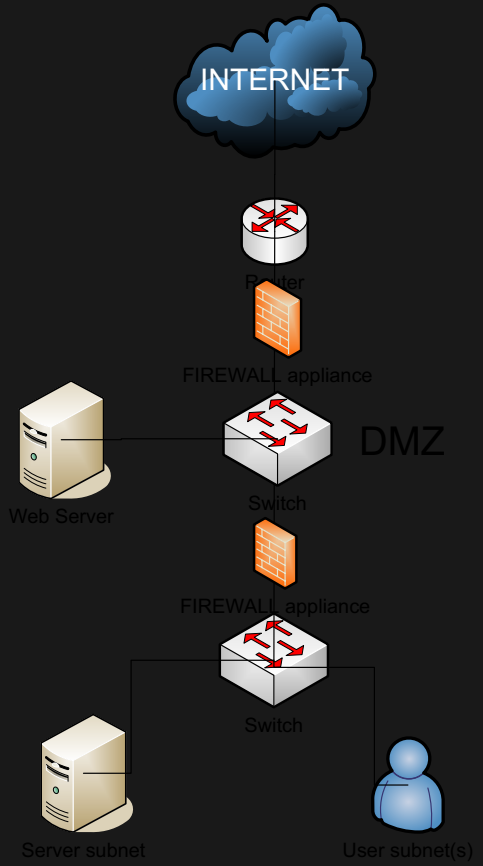
Network Security Layouts 1



Network Security Layouts 2



Network Security Layouts 3



Firewall

- Packet filter
- Stateful
- Application proxy firewalls
- Implementation:
  iptables

Firewall Rules Basics

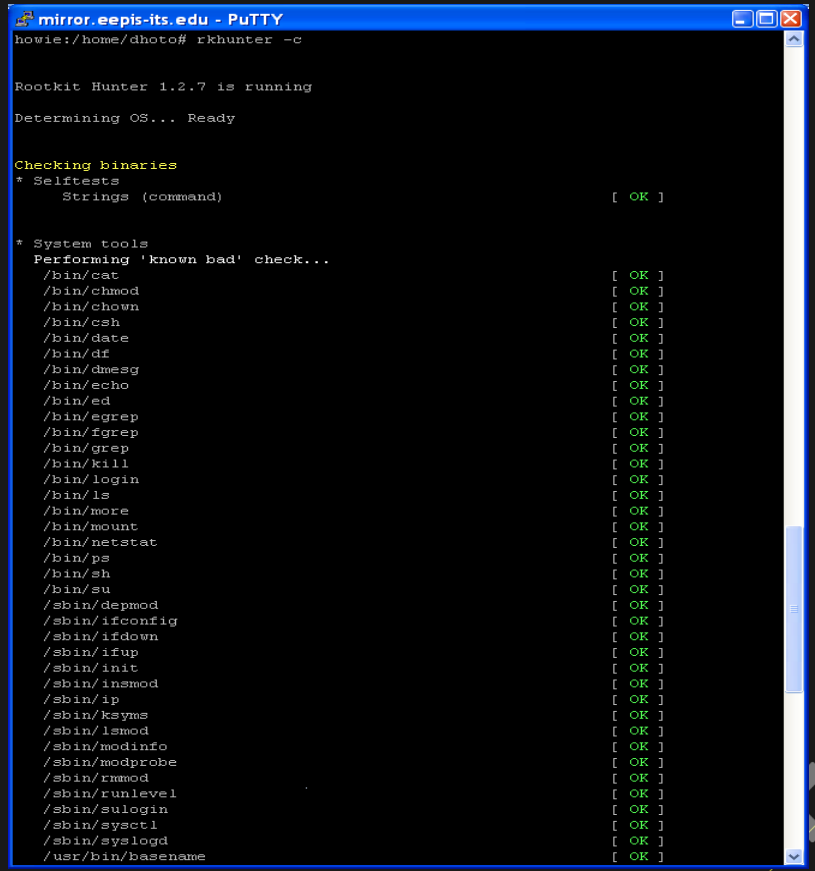
from	to	src port	dst port	proto	rule
*	www	*	80	tcp	allow
*	mail-gw	*	25	tcp	allow
squids	proxy	*	8080, 3128	*	allow
mynet	*	*	*	*	allow
*	*	*	*	*	deny

Securing from Rootkit, Spoofing, DoS

Rootkit

Let hacker to:

- Enter a system at any time
- Open ports on the computer
- Run any software
- Become superuser
- Use the system for cracking other computer
- Capture username and password
- Change log file
- Unexplained decreases in available disk space
- Disk activity when no one is using the system
- Changes to system files
- Unusual system crashes



Spoof Protect

Debian way to protect from spoofing
/etc/network/options

Spoofprotect=yes

/etc/init.d/networking restart

DoS Prevention

- IDS
- IPS
- Honeypots
- firewall

Intrusion Detection System (IDS)

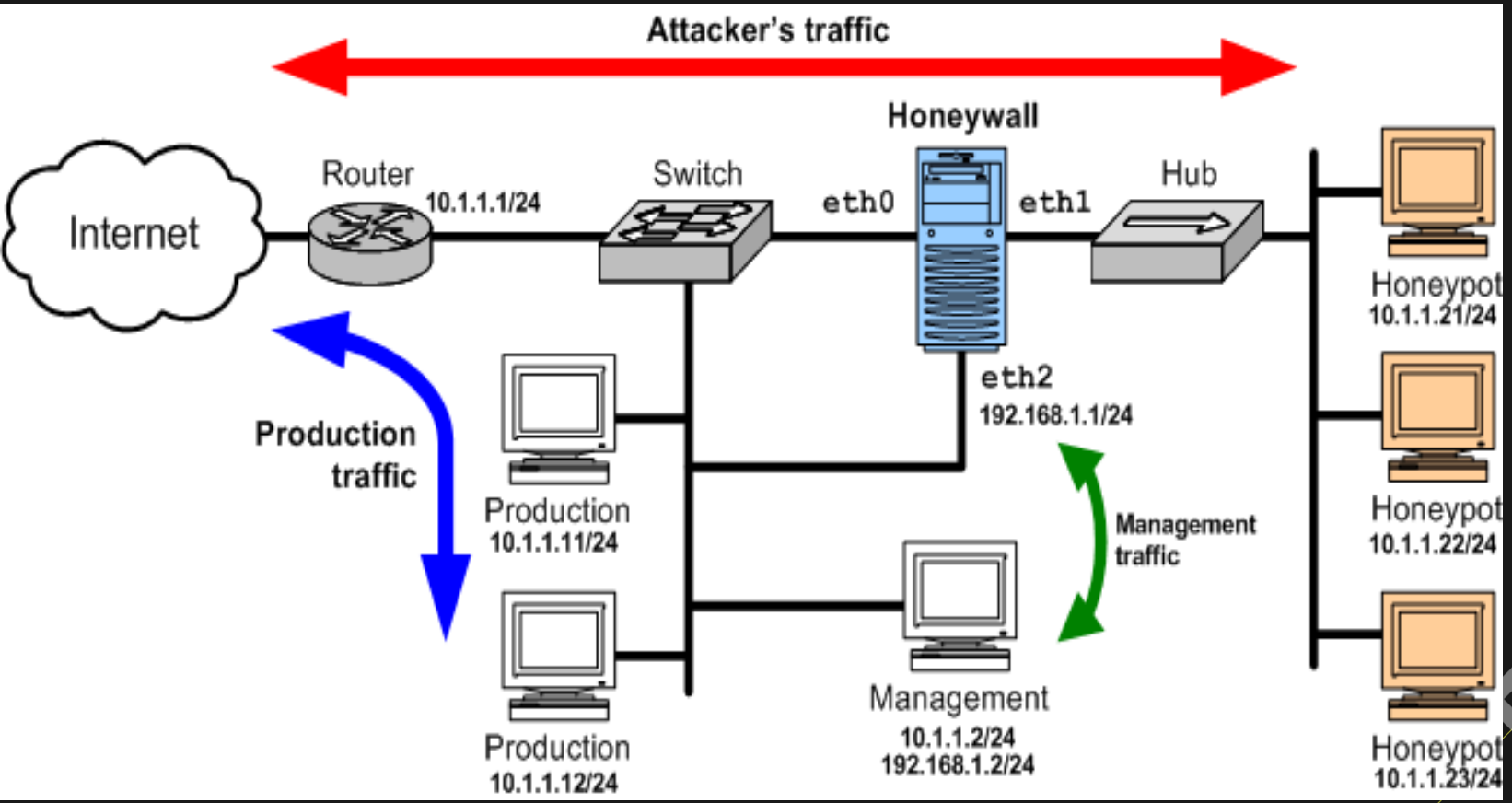
- Examining system logs (host based)
- Examining network traffic (network based)
- A Combination of the two
- Implementation: snort

Intrusion Prevention System (IPS)

- Upgrade application
- Active reaction (IDS = passive)
- Implementation: portsentry

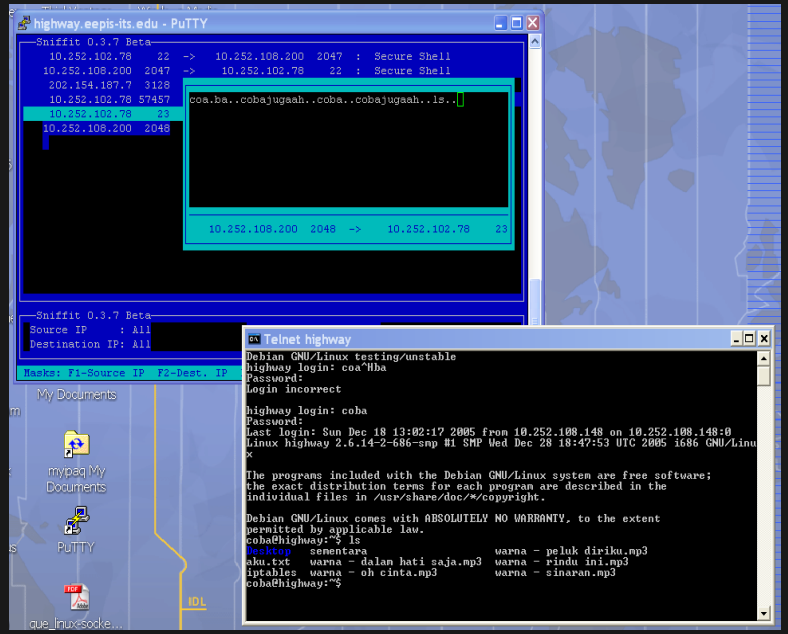
HoneyPots

Source: www.honeynet.org



Secure Remote Access

- Telnet vs SSH
- VPN:
  - Ipsec
    - Freeswan
    - Racoon
- CIPE
- PPTP
- OpenVPN



Wireless Security

- Signal bleed & insertion attack
- Signal bleed & interception attack
- SSID vulnerabilities
- DoS
- Battery Exhaustion attacks - bluetooth

Securing Wireless-LAN: 802.11x Security

- WEP – Wired Equivalency Privacy
- 802.11i security and WPA – Wifi Protected Access
- 801.11 authentication
- EAP (Extensible Authentication Protocol)
- Cisco LEAP/PEAP authentication
- Bluetooth security – use mode3

Hands on for Wireless Security

- Limit signal bleed
- WEP
- Location of Access Point
- No default SSID
- Accept only SSID
- Mac filtering
- Audit
- DHCP
- Honeypot
- DMZ wireless

Using Encryption to protect Network

- Single key – shared key

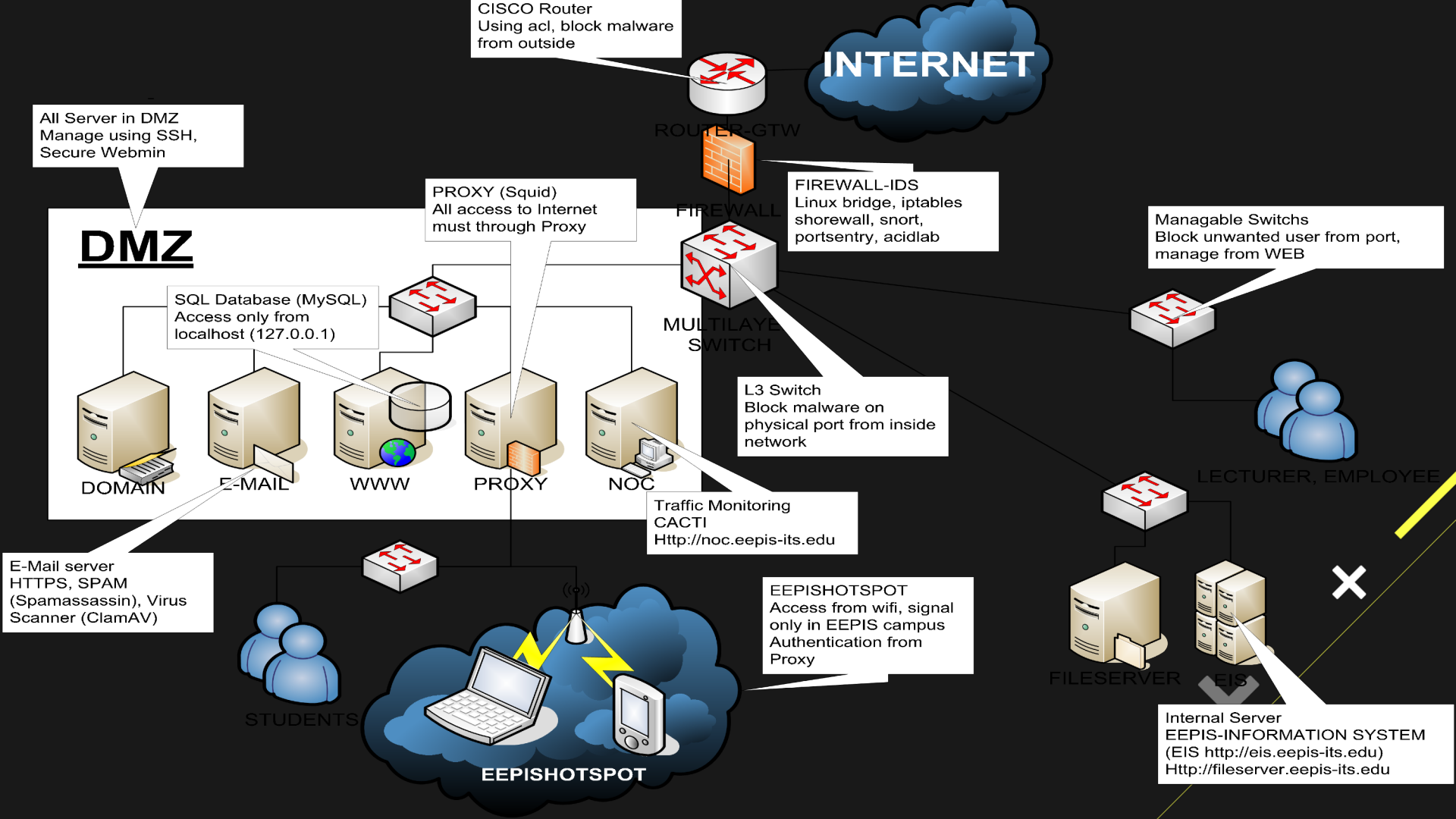
  DES, 3DES, AES, RC4 …

- Two-key encryption schemes – Public key

  PGP

- Implementation

  HTTPS


CISCO Router
Using acl, block malware from outside
INTERNET
ROUTER-GTW
All Server in DMZ
Manage using SSH, Secure Webmin
PROXY (Squid)
All access to Internet must through Proxy
FIREWALL-IDS
Linux bridge, iptables shorewall, snort, portsentry, acidlab
FIREWALL
DMZ
SQL Database (MySQL)
Access only from localhost (127.0.0.1)
MULTILAYER SWITCH
Managable Switchs
Block unwanted user from port, manage from WEB
L3 Switch
Block malware on physical port from inside network
DOMAIN
E-MAIL
WWW
PROXY
NOC
LECTURER, EMPLOYEE
Traffic Monitoring
CACTI
Http://noc.eepis-its.edu
E-Mail server
HTTPS, SPAM (Spamassassin), Virus Scanner (ClamAV)
EEPISHOTSPOT
Access from wifi, signal only in EEPIS campus
Authentication from Proxy
FILESERVER
EIS
STUDENTS
EEPISHOTSPOT
Internal Server
EEPIS-INFORMATION SYSTEM
(EIS http://eis.eepis-its.edu)
Http://fileserver.eepis-its.edu

THANK YOU!

Any questions?
You can find me at
niel.vanrooyen@voxtelecom.co.za