"Design, Development and Analysis of a Comprehensive Open Source System for proactive management of security aspects of control networks"

Authored By

S.S.Tomar, S.N.Chaudhari, H.S.Chouhan, V.K.Maurya and A.Rawat

Affiliated to

"Raja Ramanna Centre for Advanced Technology, Indore, Department of Atomic Energy, India"

Discussion outline

- Introduction
- Risk Analysis of DACN
  - Typical Distributed Architecture Control Networks (DACN) - Assets
  - Security Aspects of DACN – Threats & Vulnerabilities
- Secure DACN using FOSS tools
- Enhancing security of Secure DACN
  - Zero day malware attack detection
  - Distributed Component Overheating Management
- Security analysis of secure DACN
- Conclusions

Introduction

- Modern day control networks are
  - Large
  - Connected to Internet
  - Have distributed architecture
  - Contain both control and information cum resource sharing network components
- COTS PCs with Windows OS are widely used
- Windows OS has a long history of malware infections
  - Duqu, Stuxnet and Flame are recent examples

…Contd.

- Due to Internet connectivity and use of Windows OS, lot of security issues (CIA)
- Proactive and cost effective management of these issues is challenging
- A number of FOSS tools exist
- Two important issues in distributed n/w
  - Proactive and cost effective management of
    - Zero day malware attacks
    - Distributed Component Overheating

Risk Analysis

- Risk = Assets + Threats + Vulnerabilities
- Assets = What we are trying to protect
- Threats = Against which we are trying to protect
- Vulnerabilities = Gaps in our security apparatus

Typical DACN - Assets

- COTS PC, with windows OS
- Ethernet network with wide usage of Quality of Service (QoS) feature
- Modern messaging servers like name, email and web for publishing information
- Data acquisition and control hardware
- Alarm generation system
- Storage system for storing events
- Redundant components for
  - Computation, Decision making, Communication and Data acquisition & Control.

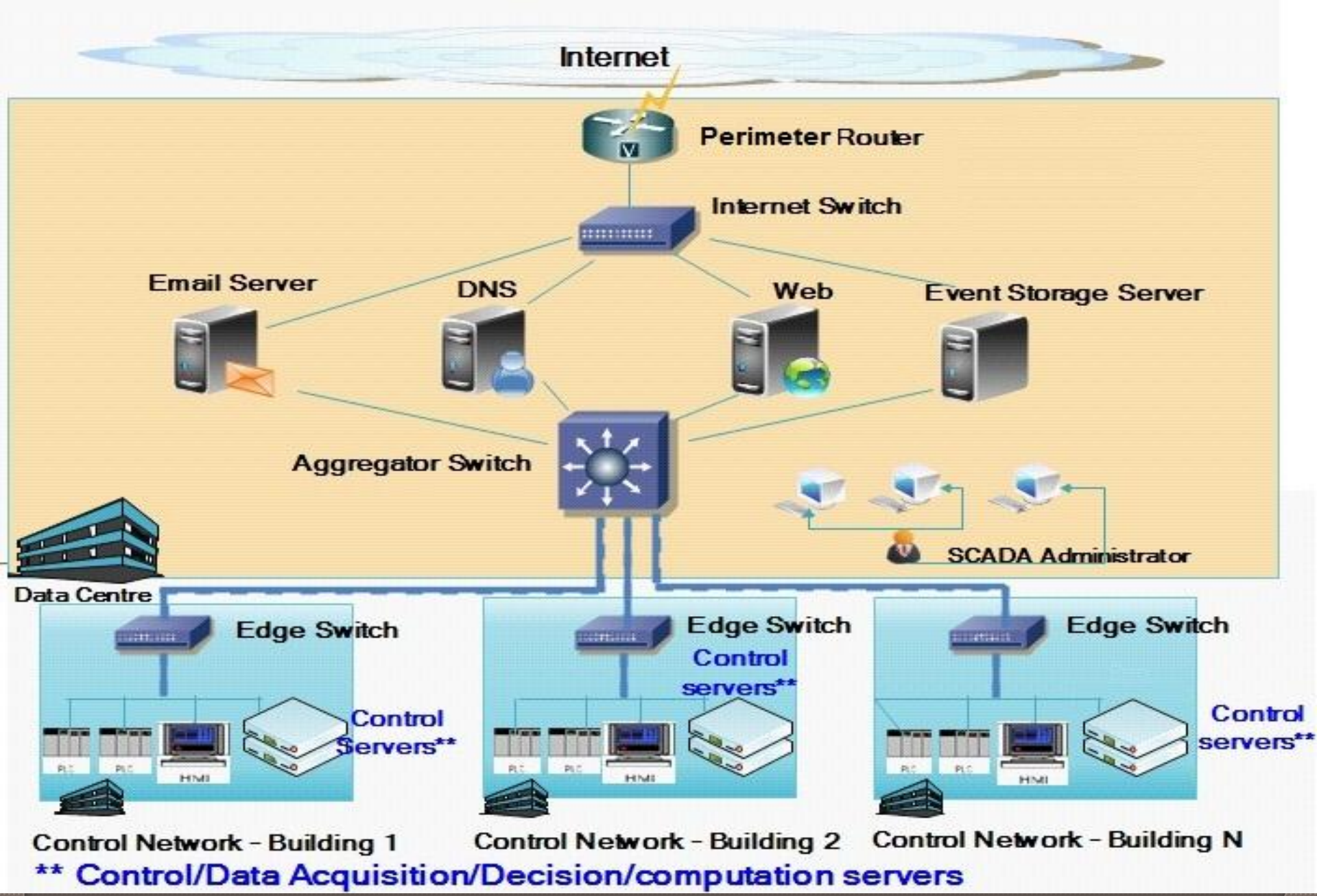


Figure 1: Typical DACN

Security Aspects of DACN – Threats and Vulnerabilities

- COTS PC with Windows OS, has threats from malwares.
- Ethernet technology based networks have CIA issues.
- Internet on a DACN has CIA issues.
- Environmental changes in Distributed locations of the DACN components
- Mail/web/name servers have numerous threats from malwares

Areas for proactive management

- Authentication Authorization Accounting (AAA)
- Firewall and DeMilitarized Zone (DMZ)
- Network Access Control (NAC)
- Network traffic encryption
- Network traffic monitoring
- Virus/SPAM/Malware **detection**
- Network fabric management (Servers/Routers/Switches/PC /Software)
- Log monitoring and analysis
- Alarm communication management

Secure DACN using FOSS tools

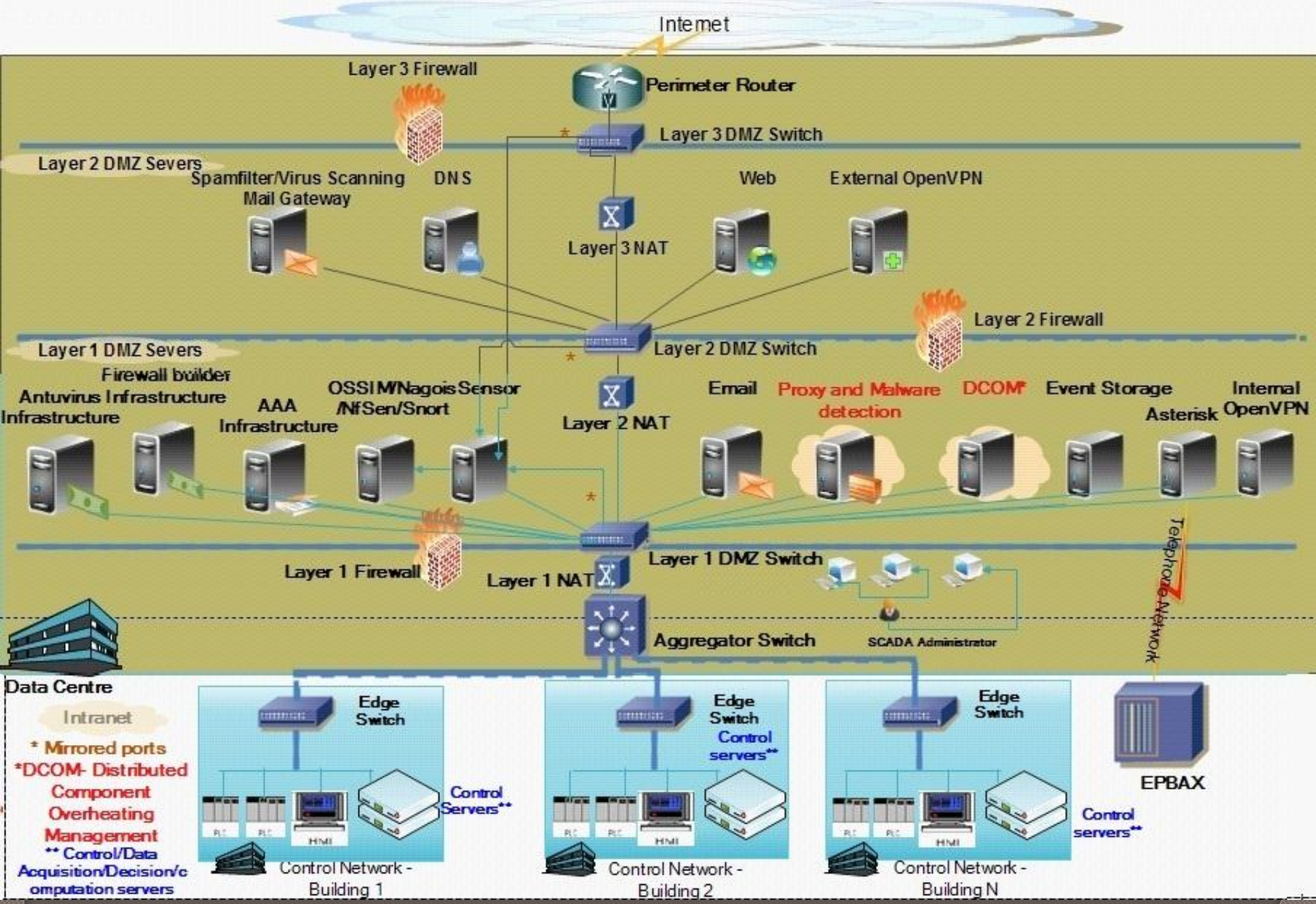


Figure 2: Secure DACN

Sailent Features of the Secure DACN

- Follows multi layered (DMZ) approach
- Follows proxy based Internet access approach
- Filtering of web traffic for virus and SPAM
- AAA of every access to the network
- Reduced Visibility of the resources
- Network traffic encryption
- Network monitoring systems in every DMZ, to detect unusual/ unwanted zero day attack traffic
- Log analysis systems to detect unusual system behaviour
- Abnormal network event related real time multimode alarm generation & comm. system

FOSS tools used for Development

- **Linux (CentOS) as OS**
- AAA – CentOS Directory Server and FreeRadius
- Firewall and DMZ – IPtables with Bastille and firewall builder
- Network Access Control – PacketFence and Authenticated Squid Proxy server
- Network traffic encryption – OpenVPN and Apache with secure hypertext transfer protocol

- Network traffic monitoring –Open Source Security Information Management (OSSIM) with nagios/snort, NfSen plugins
- Virus/SPAM mgmt. – Clam AntiVirus (ClamAV) for virus filtering, SpamAssassin for SPAM control on servers. ClamAV and Microsoft Security Essentials on PCs
- Network fabric management – OSSIM to monitor host and service availability. Bastille for server hardening and NetDisco for asset discovery

- Log Analysis – OSSEC with automated log analysis feature
- Alarm communication system – Asterisk for communicating alarms using the telecommunication network, emails using email network, web server for status information display in the form of web pages

Enhancing Security of DACN

- Zero day malware attack detection system
- Distributed Component Overheating management system

Zero day malware attack detection system

Basic Idea

- Malware are characterized by following:
  - Designed to proliferate
  - Use Internet/Intranet as channel of communication
  - Leave footprints in authenticated proxy logs in the form of excessive TCP_DENIED log lines
- Analyze proxy logs
- Manipulate routing table for blocking access
- Program portals can be used to guide users to check status and unblock access

Pre requisites

- Use Squid as proxy server for access to public networks from DACN
- Authentication and logging options should be enabled in the squid proxy server
- All PCs in DACN should be configured to use proxy server for public network access

Design of Complete system

- Consists of three subsystems
  - Malware infected PC detecting and blocking subsystem.
  - User PC status checking subsystem.
  - User controlled PC unblocking subsystem

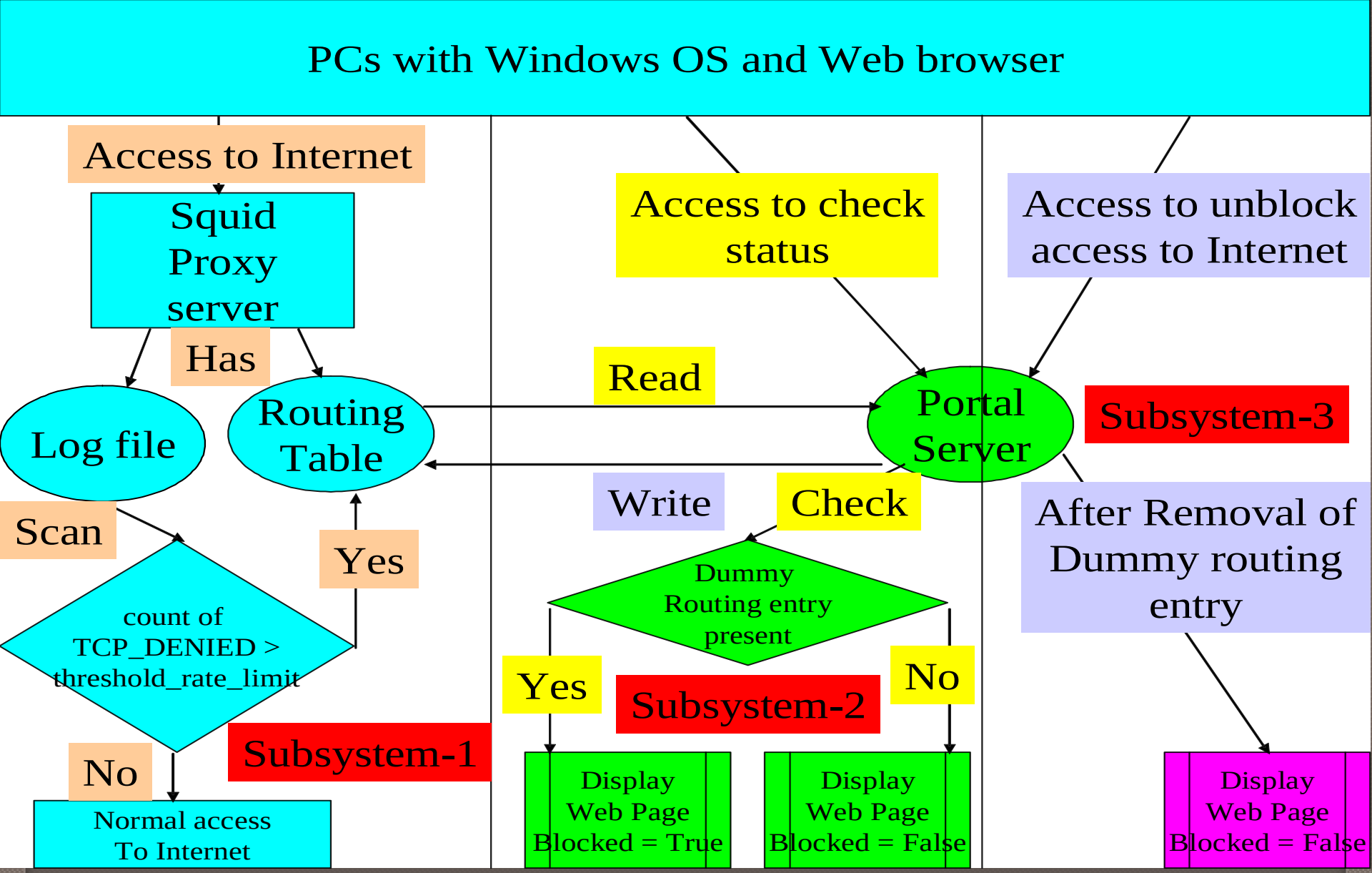
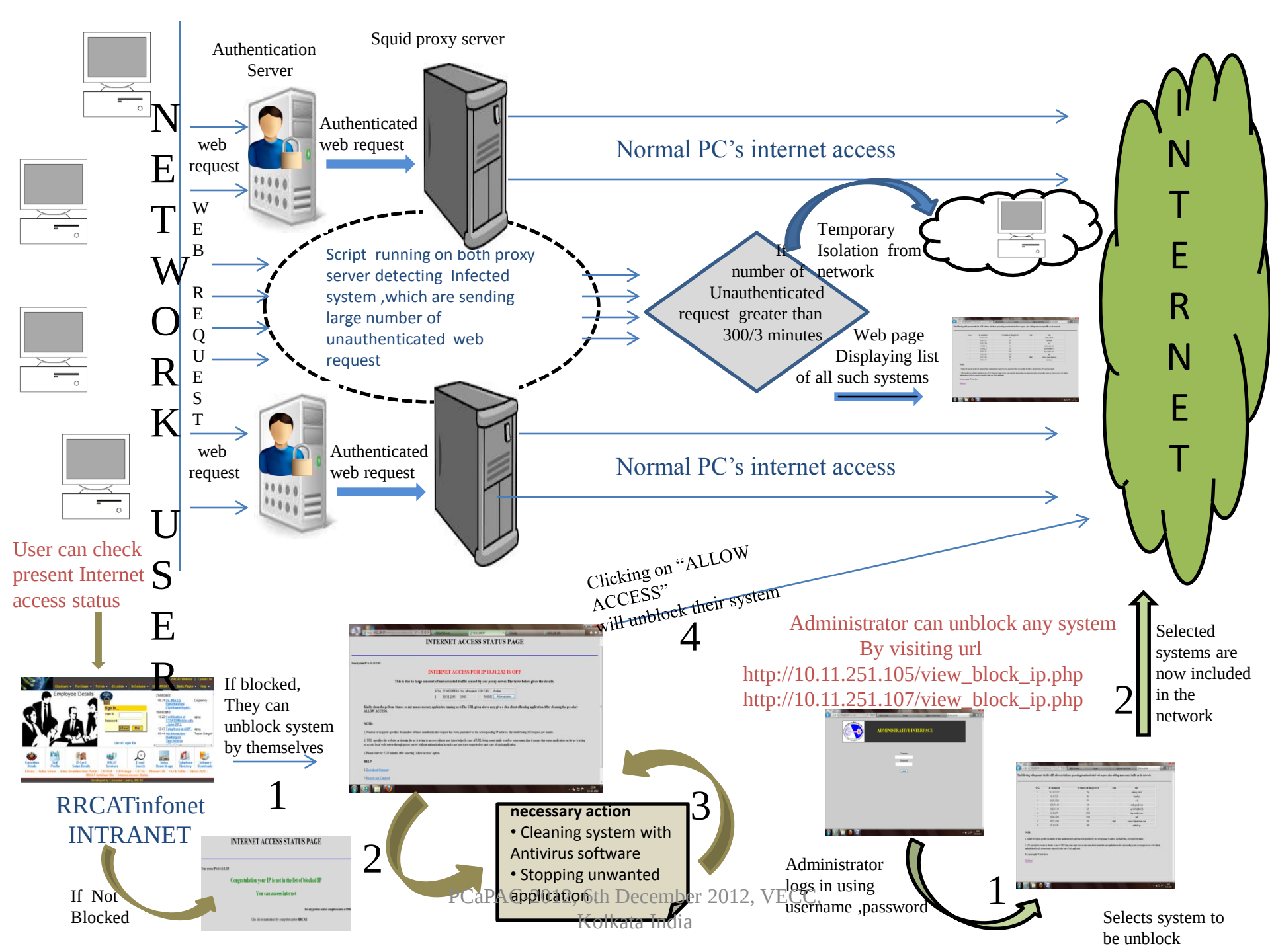


Figure 3: Conceptual block diagram of the zero day malware Detection/blocking/unblocking solution


Authentication Server
Squid proxy server
NETWORK USER
web request
WEB REQUEST
web request
Authenticated web request
Authenticated web request
Normal PC's internet access
Normal PC's internet access
Script running on both proxy server detecting Infected system ,which are sending large number of unauthenticated web request
If number of Unauthenticated request greater than 300/3 minutes
Temporary Isolation from network
Web page Displaying list of all such systems
INTERNET
User can check present Internet access status
Employee Details
If blocked, They can unblock system by themselves
1
RRCATinfonet INTRANET
INTERNET ACCESS STATUS PAGE
INTERNET ACCESS FOR IP 10.31.2.93 IS OFF
2
If Not Blocked
INTERNET ACCESS STATUS PAGE
Congratulation your IP is not in the list of blocked IP
You can access internet
necessary action
• Cleaning system with Antivirus software
• Stopping unwanted application
3
Clicking on "ALLOW ACCESS" will unblock their system
4
Administrator can unblock any system By visiting url
http://10.11.251.105/view_block_ip.php
http://10.11.251.107/view_block_ip.php
ADMINISTRATIVE INTERFACE
Administrator logs in using username ,password
1
Selects system to be unblock
2
Selected systems are now included in the network

Malware infected PC detecting and blocking subsystem

- For detecting and blocking, a script in the proxy server is executed using a scheduler at fixed intervals with following algorithm:

Step 1. Define a threshold limit for generated TCP_DENIED requests for a PC/IP.

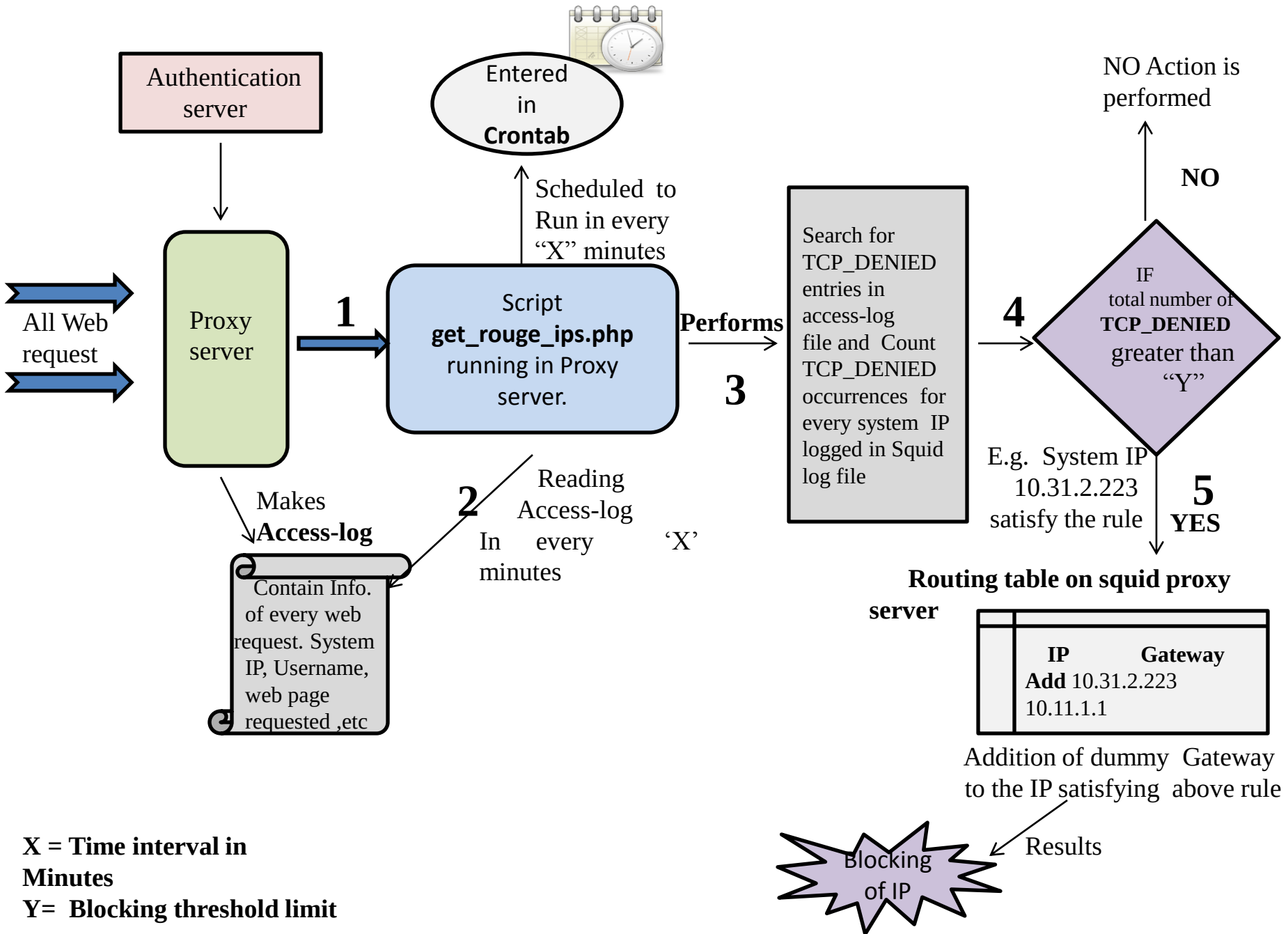
Step 2. Read the squid access log file for lines containing TCP_DENIED word. Only consider the lines that have got augmented since the last read.

Step 3. Read each line containing TCP_DENIED tag and count the number of such lines generated for each PC/IP.

Step 4. Compare the count of such lines with the threshold rate limit as defined in step 1.

Step 5. If the count of such lines generated by a PC/IP is more that the set threshold limit then mark the PC/IP as malware infected.

Step 6. For IPs listed in step 5, make a non routable entry in the routing table of the proxy server for each of them for blocking their access.



X = Time interval in Minutes

Y= Blocking threshold limit

User status checking subsystem

- **A portal with** necessary web pages to publish the status of the user PC/IP.
- This subsystem is residing on another server, configured with a portal/web server, which is accessible to the PCs even when proxy access is not present.
- A script with the following algorithm is used to provide the required functionality:

Step 1. Get the IP details of the PC from where the status check function is being performed.

Step 2. Read the routing table of the proxy server which was modified by the detecting/blocking subsystem.

Step 3. Check for the routing table entry related to the PC/IP from where the status is being checked.

Step 4. If routing table entry for the IP exists then generate a web page showing Blocked = true as the PC status else
generate a page with Blocked=false message

File containing blocked IPs

Blocked_ips.txt

populates

10.31.2.223,,500,,john,,google.com
10.28.2.223,,458,david,,orkut.com

Squid proxy server

If System with these IP, checks their "Internet Access Status" on Intranet. Message like below will appear

Network Users

1

Logs on Intranet

2

blocked

Page displays System IP along with the reason for blocking.

If unblocked

User controlled PC unblocking subsystem

- Extends the functionality of the portal setup with an additional script with the following algorithm:

Step 1. Get the IP of the PC from where the user requested for unblocking.
Step 2. Read the routing table of the proxy server.
Step 3. If the IP related routing entry is present in the proxy server’s routing table then delete it.

Development details

- Linux (Centos 5.7) as the OS
- Scripts written using linux bash, awk, grep and PHP scripting language
- Server side scripting for web pages done using PHP
- Web pages designed using HTML
- Routing table reading/modifications using route command of linux
- CRON scheduler for scheduling

Distributed Component Overheating Management System

Design goals

- To develop an system which can:
  - Continuously monitor the temperature of the switches deployed on network and display it on webpage.
  - Generate automatic phone calls and send emails to concerned persons in case the temperature of a switch exceeds threshold.
  - Perform automatic shutdown of the registered servers when ambient temperature exceeds the shutdown threshold.

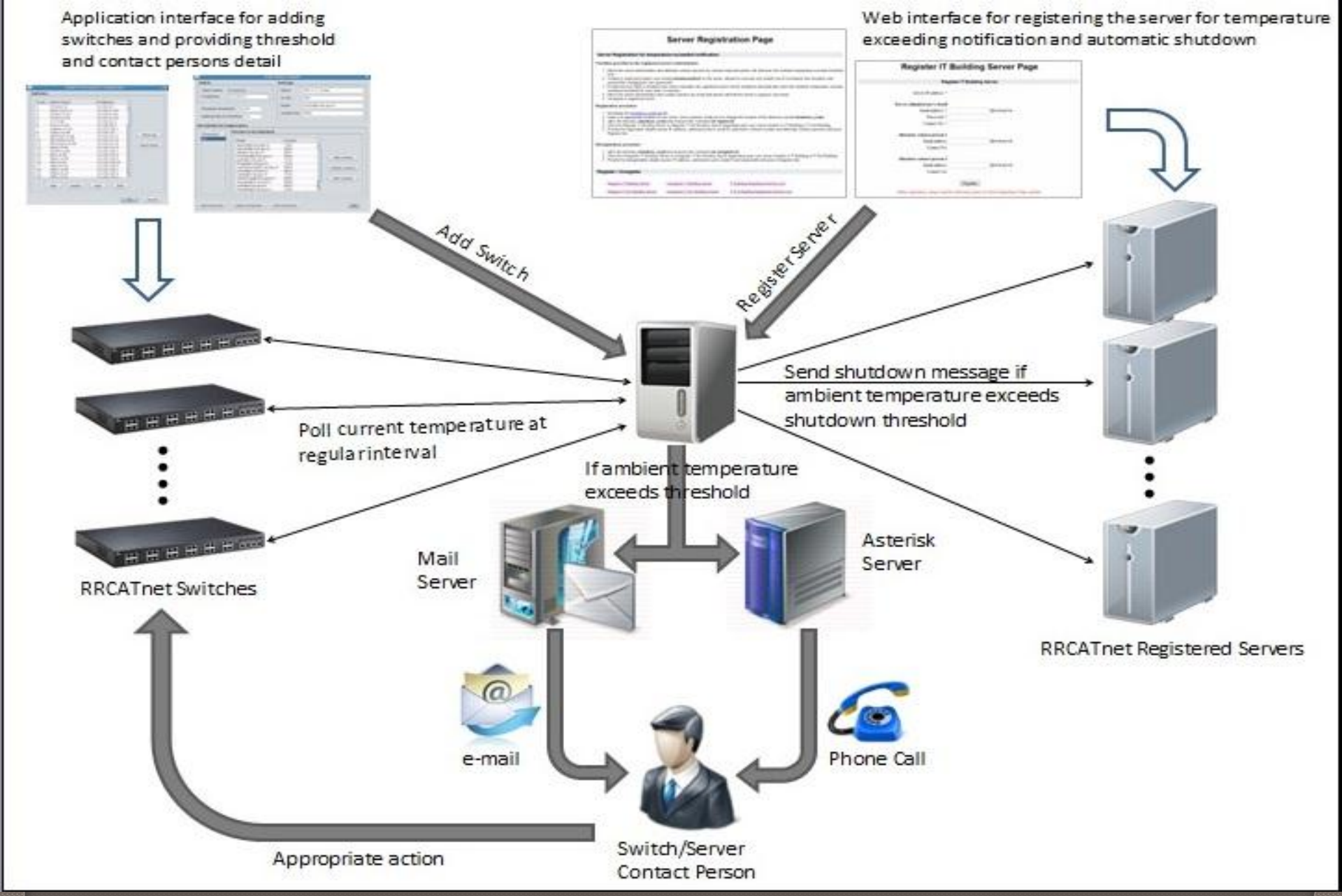


Figure 4: Conceptual block diagram of DCOMS

Design of the System

- Desktop application for configuring network switch details registration and storing it in database (XML format)
  - Temperature threshold
  - Contact details (IP, Phone no.,email id.)
- Web application for server registration
  - Server shutdown threshold
  - Contact details (IP, Phone no.,email id.)
- DCOMS notification generation application with the following algorithm

a. Read the database of registered switches and get IPs of the registered switches.

b. For each switch IP.

   i. Connect to switch using the SNMP client and get SNMP variable value of the temperature variable.

   ii. Read the email-ids and phone numbers associated with the switches.

   iii. Read the shutdown threshold value of the switch

   iv. Read the registered server IPs associated with the switch

   v. If the current temperature exceeds shutdown threshold then

      1. Send shutdown message to the servers

      2. Send email to the concerned persons using the email server

      3. Generate a phone call to the concerned persons using the asterisk server

- Automatic server (linux) shutdown is performed using the following algorithm:

Step 1. On the server (one time)

a. Execute a program/script (register.sh) with the following algorithm:

i. Create a restricted shell user in the server and copy the root public key of the DCOMS server to its authorized users list.

ii. Install a script (shutdown_ server.sh) with the following algorithm:

1. Read the message file as sent by DCOMS server.
2. If the value of shutdown flag is true then initiate shutdown.

b. Make an entry in cron scheduler to schedule the program for execution in every minute interval

c. Make an entry in rc.local file to reset the shutdown flag value.

d. Copy the DCOMS server root public key into the .ssh folder of the restricted shell user.

Step 2. On the DCOMS server (for every switch)

a. If the current temperature of the associated switch exceeds server shutdown threshold then

i. Send shutdown message to the servers

ii. Send email to the concerned persons using the email server

iii. Generate a phone call to the concerned persons using the asterisk server.

Step 3. On the server (for deregistration, one time)

a. Delete the cron entry related to shutdown_server.sh script

b. Delete the rc.local entry for changing the shutdown flag.

c. Delete the shutdown_server.sh script.

d. Delete the restricted shell user.

Development of the system

- Linux – CentOS 5.7 as Operating System.
- Apache as web server.
- JAVA for developing desktop GUI, the Switch Threshold Configurator.
- HTML and JavaScript for developing web interfaces.
- XML for storing information in the database.
- CRON for scheduling.
- PHP and BASH scripts.
- *scp* for message passing or copying file to remote hosts (registered servers).
- SNMP for polling switches current temperature.
- Asterisk (FOSS) as telephony system.
- Qmail as MTA on the mail server.

Security Analysis of secure DACN

- Confidentiality controls
- Integrity controls
- Availability controls

Security of Internet connected N/W -Prime requirements

- Confidentiality
  - Only intended user can decipher message
- Integrity
  - Message not changed during transfer
- Availability
  - Service always available 24X7

Confidentiality controls

- AAA infrastructure
- Network access control
- Traffic encryption
- Authenticated Proxy
- Firewalls, DMZ, NAC, NAT provides access control for additional authorization

Integrity controls

- Dual authentication using digital certificate and password in OpenVPN
- HMAC in OpenVPN provides integrity of data at network layer level
- AAA infrastructure supports password expiry, strong password and md5 storage of password for ISO 27001 compliance
- Antivirus and Antimalware systems at all entry and exit points of data
- OSSEC ensures integrity of important configuration files

Availability controls

- Malware detection system ensures higher availability by reducing, spreading of malware and hence DoS
- DCOMS ensures continuous availability of healthy components
- Network monitoring setup using snort, OSSIM, nfSen and nagios ensures failures and security breaches are reported in time
- Alarm generation and communication setup using OSSEC and Asterisk further improves availability

Conclusions

- Achieving foolproof security is challenging
- Security aspects of such networks is to be managed proactively and cost effectively
- A number of FOSS tools exist
- In DACN handling zero day malware attacks and overheating management are to be given importance
- Proxy log analysis technique for zero day malware detection presented
- SNMP technique for DCOMS was presented

Thank You!!