Network Access Control: Case Study

Gaurav Saxena, D.Sarkar, N.C.Samanta, C.D.Datta,
Tapas Samanta, P.S.Roy, Somesh Soni

Presented by: Gaurav Saxena, Computer & Informatics Group, VECC, Kolkata
SACET09, October 28-29, 2009

Network Access Control (NAC): Case Study

- Introduction
- Aim for NAC
- NAC Components
- PacketFence, an open source NAC
- Case Study: VECC LAN
- Getting Started
- PacketFence Implementation
- Custom VLAN Assignment Function
- Working

Network Access Control: Case Study

- Introduction
- Aim for NAC
- NAC Components
- PacketFence, an open source NAC
- Case Study:VECC LAN
- Getting Started
- PacketFence Implementation
- Custom VLAN Assignment Function
- Working

Introduction

- NAC is a way to apply access control policy inside the network, and forces its users to comply with policy before gaining access to the network.
- For eg.
  - "Only registered users, from registered devices, having OS patch level 2 (Windows Vista) with antivirus updated, are allowed to access wired network from Main Building".
- The basic concept behind is "Who you are should govern what you are allowed to do on the network ". It is a "user focused", "network-based", "access control".
- For eg.
- "Who you are" refers not only to the user credentials but also on factors such as

Authentication + Endpoint- Security + Network Environmental Information.

Introduction

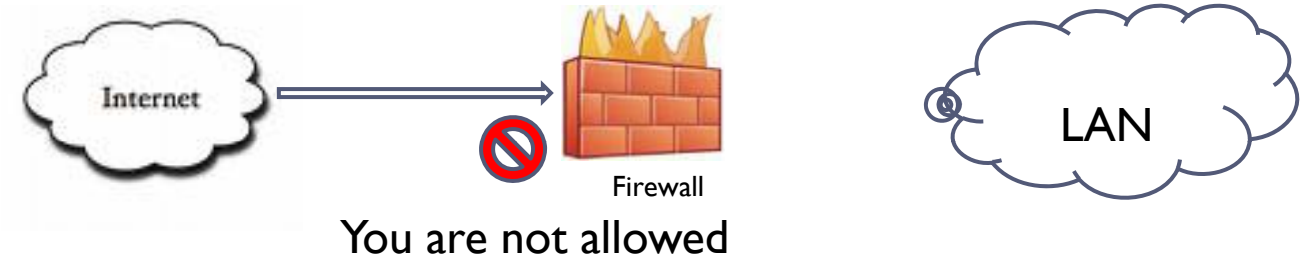
- Access is a function of Authentication and Environment

What you can do =

Who you are
+
How well you comply with the policy
+
How well you behave on the network

Introduction

- The Access Control can also be implemented by Firewall.



- What is the difference between NAC and Firewall?

Introduction

- NAC is basically a way of firewalling.
- In Firewall, the decision taking element are basically the IP addresses, ports, protocols etc., but in NAC, the elements are User Identity, Access Method, Location, End-Point security posture, Destination IP and port.
- Firewall is basically positioned end-points of the two network connecting them, but NAC is being incorporated inside the network, i.e. between the user and the network.

Network Access Control: Case Study

- Introduction
- Why NAC is needed?
- NAC Components
- PacketFence, an open source NAC
- Case Study:VECC LAN
- Getting Started
- PacketFence Implementation
- Custom VLAN Assignment Function
- Working

Need for NAC

- Incorporating Dynamic Environment
- Asset Monitoring
- Forceful Policy Acceptance
- Registration
- Isolation of problematic devices

Network Access Control: Case Study

- Introduction
- Why NAC is needed?
- NAC Components
- PacketFence, an open source NAC
- Case Study:VECC LAN
- Getting Started
- PacketFence Implementation
- Custom VLAN Assignment Function
- Working

NAC Components

- Registration and User Authentication
  - Registration of user and devices
  - User Authentication modes
    - 802.1X and EAP
    - Web-based
    - MAC based
- User Environment
  - Access Method, Time of the day, Client platform, Authentication method, End-Point security posture,
- Access Control
  - On/Off the network
  - VLAN-level assignment
  - Packet filters
  - Stateful firewall
- Management

Network Access Control: Case Study

- Introduction
- Why NAC is needed?
- NAC Components
- PacketFence, an open source NAC
- Case Study:VECC LAN
- Getting Started
- PacketFence Implementation
- Custom VLAN Assignment Function
- Working

Packetfence

- Packetfence is an opensource NAC solution available
- Some of its important features includes: Registration of the user and the devices, Detection of abnormal network activities through snort sensors, Nessus proactive vulnerability scans, Isolation of problematic devices through VLAN Isolation technique, 802.1X support through FreeRADIUS and DHCP fingerprinting for automatically registration of specific type of devices.

Network Access Control: Case Study

- Introduction
- Why NAC is needed?
- NAC Components
- PacketFence, an open source NAC
- Case Study:VECC LAN
- Getting Started
- PacketFence Implementation
- Custom VLAN Assignment Function
- Working

Case Study: VECC LAN

- Following discussion takes up the case study of VECC LAN and presents the steps that have been taken to implement NAC
- A test-bed has been created to demonstrate the NAC implementation

Network Access Control: Case Study

- Introduction
- Why NAC is needed?
- NAC Components
- PacketFence, an open source NAC
- Case Study: VECC LAN
- Getting Started
- PacketFence Implementation
- Custom VLAN Assignment Function
- Working

Getting Started

- Policy Formation
  - Identification of Users
    - Guest
    - Student
    - VECC Staff
    - Temporary Staff

      Again Guest and Students are further classified as group (ex. C&I Group) specific and non-group specific personnel's
  - End-Point Security Information
    - User/Device Registration to Portal
    - Anti-Virus Definition Update

Getting Started

- Policy Formation 2
  - Network Environment Information
    - Location of the User from which he/she has logged on
      - Common Client Area
      - Group Client Area
      - Common Server Area
      - Group Server Area
      - Other Area

      These categories depend on the user itself, as a particular location in VECC may be considered as a "Group Client Area" for a staff member, but at the same time it is "Other Area" for another staff member who doesn't belong to the same group

Getting Started

- Policy Formation 3
  - Identification of services
    - Internet Access
    - Mail Access
    - Common Intranet Services
    - Group-specific Intranet Services
    - Light-weight registration
    - Extra light-weight registration
    - Remedial Access to network

Getting Started

- Policy for User Guest

User Identification	End-Point Security	Environment	Access Control
Unauthenticated	Don't care	Don't care	No Access
Auth, Guest	System Registered	Common Area	Internet Access Only
Auth, Guest	System Not Registered	Common Area	Light weight Registration
Auth, Guest	Don't care	Other than Common Area	No Access
Auth, Guest Special	System Registered, A/V Don't care	Anywhere	Internet + Mail + Group Intranet all + Common Intranet.
Auth, Guest Special	System Not Registered, A/V Don't care	Anywhere	Extra light weight Registration
Auth, Guest of Group Special	System Registered, A/V updated	Particular Group Area	Internet + Mail + Group Intranet + Common Intranet.
Auth, Guest of Group Special	System Registered, A/V not Updated	Particular Group Area	Remedial Access Only
Auth, Guest of Group Special	System not Registered, A/V Don't care	Particular Group Area, Common Area	Light Weight Registration.
Auth, Guest of Group Special	System Registered, A/V don't care	Common Area	Internet + Mail Access Only
Auth, Guest of Group Special	Don't care	Other than Common Area, Particular Group Area	No Access
Auth, Guest of Group	System Registered, A/V updated	Particular Group Area	Internet + Mail + Common Intranet.
Auth, Guest of Group	System Registered, A/V not updated	Particular Group Area	Remedial Access Only
Auth, Guest of Group	System not Registered, A/V don't care	Particular Group Area, Common Area	Light Weight Registration.
Auth, Guest of Group	System Registered, A/V don't care	Common Area	Internet + Mail Only
Auth, Guest of Group	Don't care	Other than Common Area,	No Access

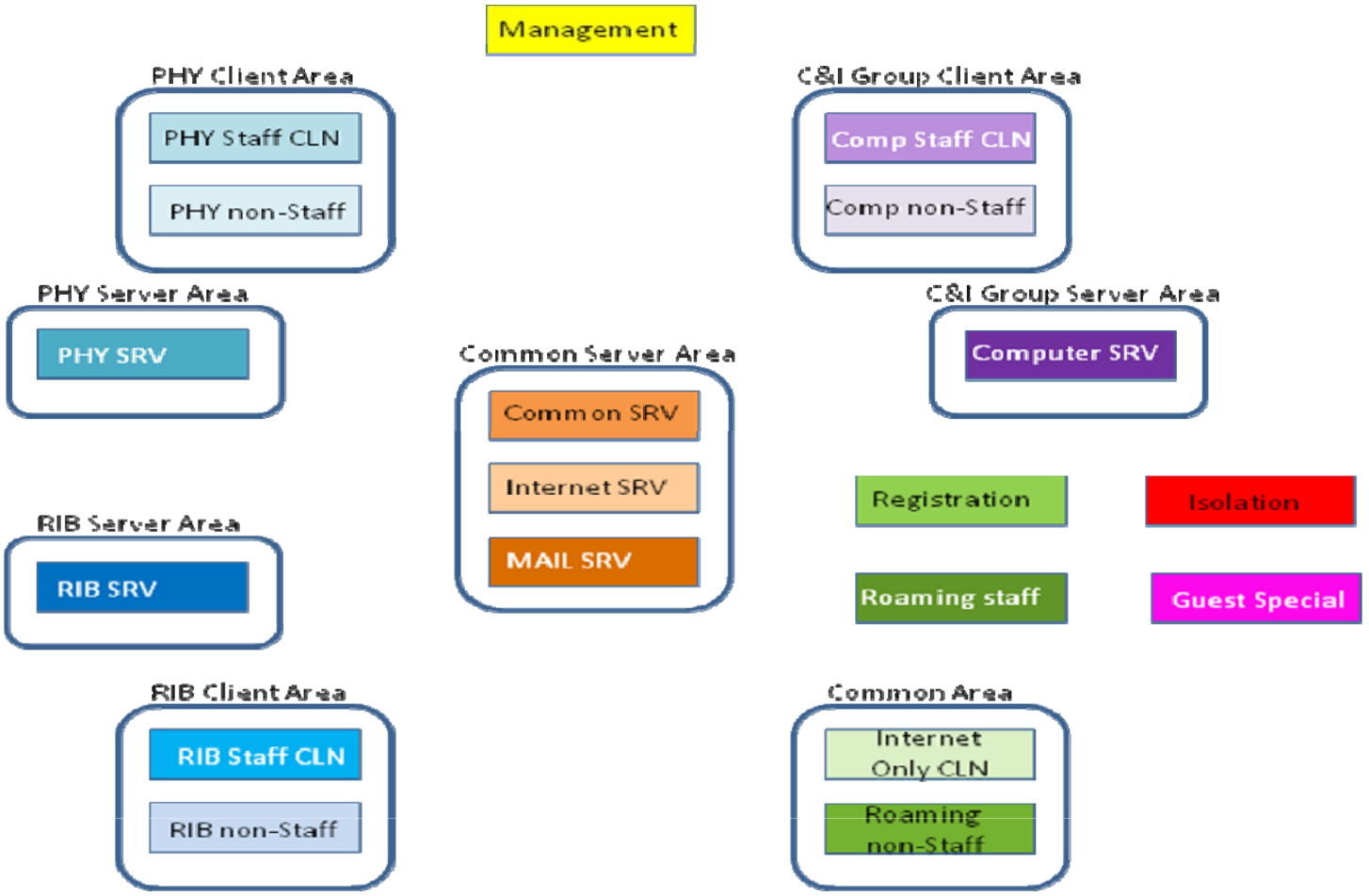
Getting Started

- Authentication Mechanism
  - 802.1X based authentication
  - Web-based authentication
  - Combination of both

    For the devices that are not complied with NAC, MAC based authentication can be used and they must statically register to the Network

Getting Started

- VLAN Formations



Getting Started

- VLAN Routing
  - Clients in each of the VLAN are associated with the specific set of services that he/she can access
  - This is described by the NAC Policy for that particular category of the user
  - Taking into account the NAC policy and the VLAN, proper routing has to be done within VLANs
  - For eg.
    - Isolation VLAN doesn't have to route anywhere because no access being given to its clients
    - Internet Only VLAN of Common Area is only routed to Internet Servers VLAN at Common Server Area

Network Access Control: Case Study

- Introduction
- Why NAC is needed?
- NAC Components
- PacketFence, an open source NAC
- Case Study: VECC LAN
- Getting Started
- PacketFence Implementation
- Custom VLAN Assignment Function
- Working

PacketFence Implementation

- Switch configuration
  - Proper VLANs have been configured onto the switch depending on physical location of the Switch, the Area to which it is associated and VLANs associated with that Area.
  - All the switches have been configured to send SNMP Traps to PacketFence Server.
  - Two important VLANs, i.e. "Registration" and "Isolation", have been configured on all the switches.
  - Other VLANs such as "Management", "Guest Special" and "Roaming Staff" have also been spanned through out the network.
  - As per policy, routing has been done.

PacketFence Implementation

- PacketFence Server Configuration
  - NICs of the Sever have been configured to host different virtual interfaces to directly connect to the VLANs "Registration VLAN" and "Isolation VLAN"
  - Server has been properly configured to attach to all the switches through "Management VLAN"
  - Authentication Mechanism: Flat file mechanism has been chosen (initially) as method for authentication. Later it was extended to incorporate 802.1X through FreeRADIUS.

PacketFence Implementation

- DHCP Server
  - To distribute IPs in Registration and Isolation VLAN
- Rogue DNS Server
  - To trap the Internet/Intranet access request of the client and divert the client to Registration or Isolation Portal.

Network Access Control: Case Study

- Introduction
- Why NAC is needed?
- NAC Components
- PacketFence, an open source NAC
- Case Study:VECC LAN
- Getting Started
- PacketFence Implementation
- Custom VLAN Assignment Function
- Working

Custom VLAN Assignment Function

- A custom function has to be designed as a part of customizing PacketFence.
- This function will assign the correct VLAN to particular user, as per our policy, at the time of initial connection.
- There are different inputs to this function such as Switch IP, Switch Port, Switch Location, User Credentials, and End-Point Security Information etc.
- These inputs are to be analysed at the time of initial connection and proper decision should be taken accordingly

Custom VLAN Assignment Function

Network Access Control: Case Study

- Introduction
- Why NAC is needed?
- NAC Components
- PacketFence, an open source NAC
- Case Study: VECC LAN
- Getting Started
- PacketFence Implementation
- Custom VLAN Assignment Function
- Working

Working of NAC

- A new device connects to the network.
- The associated Switch sends SNMP trap to the Packetfence Server.
- The associated Switch-Port has been put up in Registration VLAN.
- Each and every user request to access network is trapped, and user is being directed to the Registration Portal.
- After receiving user credentials and other information for the user, custom function acts to assign appropriate VLAN.
- Snort server is continuously monitoring the traffic of the user/device.
- Whenever there is an anomaly, the user/device is isolated from the network by putting it into Isolation VLAN.
- After remedial action has been taken, it is put back to the designated VLAN.
- Schedule scan of Nessus may also be configured to look up the vulnerabilities

References

- [1]. Network Access Control Interoperability Lab, What is NAC http://www.opus1.com/nac/teamwhitepapers/2008-01WhatisNAC.pdf.
- [2].Joel M Snyder, Welcome to NAC Day http://www.opus1.com/nac/nac-day-interop.pdf
- [3].Network Access Control Interoperability Lab, Getting Started with Network Access Control. http://www.opus1.com/nac/teamwhitepapers/2008-02GettingStarted.pdf
- [4].Interop Labs NAC Class Las Vegas 2008, http://www.opus1.com/nac/2008-nacilabsclass.pdf
- [5].PacketFence, http://www.packetfence.org

Thanks