Network access control and management solution
Summary

- Current situation
- What is openNAC?
- What does openNAC can do?
- openNAC architecture
- openNAC components
- openNAC services
- Contact us
openNAC solution

- 2 year+ of active development
- Opensource Network Access Control solution
- Enterprise support services available
- CentOS based
Current situation

- Corporate network access management is poorly controlled
- Mobile Workers. Users become more mobile
- More type of different devices like Smartphones, tablets,...
- This scenarios generate security and availability problems due to non-controlled LAN access
- The security of the workstations is constantly threatened by new vulnerabilities
- Security, network management and monitoring tools of expensive and poorly integrated
What is openNAC?

- Network Access Control for corporate LAN / WAN environments
- Enables **authentication, authorization** and **audit** policy-based all access to network
- Multivendor solution
- Based on open source components and self-development
- Based on industry standards such as FreeRadius, 802.1x, ldap, ...
- Extensible, new features can be incorporated
- Easily integrated with existing systems
- It provides value added services such as configuration management, network, backup configurations, Network Discovery and Network Monitoring
What does openNAC can do?

- Corporate network access based on a set of rules (access policy)
- The availability of Notifications or Quarantine to users regardless of the client device (via browser)
- Access accounting and audit
- Real time monitoring of users, allowing to instantly locate users, ip, mac, switch, port and physical location
- Value-added services such as monitoring, discovery and configuration of network infrastructure
Features

- Authentication of 802.1x enable devices
- Authentication backend based on ldap or AD
- Support to detect rogue devices using 802.1x or SNMP traps
- Bulk configuration of network devices using module onNetConf
- Bulk backup of configuration of network devices using module onNetBackup
- Detection of os, antivirus, firewall and os updates of devices connected to enforce an access policy
onNAC Architecture

- **Access Requestor (AR)**
  - Set of client devices such as PCs, Smartphones, Tablets, printers, others.
  - Different types of OS such as Windows, Linux, MacOS, IOS, Android, etc ...
  - Wired LAN, WiFi, VPN

- **Policy Enforcement Point (PEP)**

- **Policy Decision Point (PDP)**

- **Metadata Access Point (MAP)**

- **External Sensors**

@opennac
onNAC Architecture

- **Policy Enforcement Point (PEP)**
  - Network access for all devices that connect to the network (Edge Network)
  - Composed by wired LAN and Wi-Fi equipment (Access Points)
  - Multivendor

- **Policy Decision Point (PDP)**

- **Metadata Access Point (MAP)**

- **External Sensors**

---

onNAC

@opennac
onNAC Architecture

- **Policy Decision Point**
  - Service that allows system to take policy decisions that apply to each type of access based on identity, device, location, time, ...

- **Policy Enforcement Point (PEP)**

- **Policy Decision Point (PDP)**

- **Metadata Access Point (MAP)**

- **External Sensors**

@opennac
Metadata Access Point

- Service that stores all data relating to incoming events
- All information is related to each other in order to maximize the utility
- Real time access to the information

onNAC Architecture

@opennac
- **External Sensors**
  - Services such as IDS sensors or firewalls that can both provide new information to the platform as consulting onNAC information to make better decisions.
openNAC components
Modular architecture

- All information is stored in a CMDB
- Queue-based, allowing for greater scalability and traceability
- Very flexible identity backend, ldap, databases, etc ...
- Based in a REST APIs
- Frontend web based in DOJO
- Scripteable command line
onNAC Component

onNETDISCO
onNETCONF
onNETBACKUP
onMON

onMETAREPO

onCMDB

@opennac
onNAC description

- Is the main module, with the services of Authentication, Authorization and Audit Product
- Enables 802.1X authentication or captive web portal for all devices
- All security policy is defined and applied in this module
- Rogue devices detection
onNAC screenshots

Overall dashboard
onNAC screenshots

State of users logged into the platform
Comprehensive security policy to apply to all users
onNAC screenshots - Policy

Dashboard  ON NAC  ON NetConf  ON NetBackup  ON NAC RADIUS  ON NAC Status  ON NAC Policy

Add new  Edit  Delete  Save order  Discard order  Refresh

<table>
<thead>
<tr>
<th>Time</th>
<th>User/Identity</th>
<th>Device</th>
</tr>
</thead>
<tbody>
<tr>
<td>00:00:01:00</td>
<td>albert.sole</td>
<td></td>
</tr>
<tr>
<td>03:00:40:00</td>
<td>albert.sole</td>
<td></td>
</tr>
<tr>
<td>00:00:24:00</td>
<td>albert.sole</td>
<td>test15000</td>
</tr>
<tr>
<td>00:00:24:00</td>
<td>test15000</td>
<td></td>
</tr>
<tr>
<td>00:00:24:00</td>
<td>guest</td>
<td></td>
</tr>
</tbody>
</table>

Edit

- Time: 0 item(s) selected
- User/Identity: albert.sole
- User group: any
- LDAP filter: any
- Device: any
- Device group: test15000
- VLAN: service
- VLANID: 330
- Security Profile: any
- Plugins: 0 item(s) selected
- On error: 0 item(s) selected
- Message: message
- Comment: comment

Accept  Cancel

Mozilla Firefox

http://192.168.104.253/admin/

192.168.104.253/admin/

@opennac

Copyright OpenNAC.org 2013 - Report bug/suggestion - Rev. 2713M
onNAC screenshots - CMDB
onNETDISCO component
onNETDISCO

- Allows discovery of network devices
- Store discovered devices in the CMDB
- Maintains the inventory updated
- Discover the network topology, detecting devices without redundant links
- Allows periodic discovery tasks
- Queue-based
- Allows you to export the results to csv
onNETCONF component

onNETDISCO

onNETCONF

onNETBACKUP

onMON

onMETAREPO

onCMDB

@opennac
Network Equipment Configurator allows you to define configuration templates and apply them to sets of network equipment.

- Frontend web or Web Service
- Based on a service queue to ensure traceability and integrity of any action
- Very useful for applying settings to large amount of network equipment
- Very useful to install and configure NAC service
Create a configuration template to send a group of network devices
onNETCONF Screenshots - Devices

Network device list

Equipment selection
onNETCONF Screenshots - Results

Viewing the results of configuration tasks

@opennac
onNETBACKUP component

@opennac
Make backups and automatic archiving of network devices configurations

- Allows programming device groups copies
- Allows define retention policy
- Based on a service queue to ensure traceability and integrity of any action
Selection of devices to perform backups

<table>
<thead>
<tr>
<th>IP</th>
<th>Manufacturer</th>
<th>Family</th>
<th>Model</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.128.0.250</td>
<td>ALCATEL</td>
<td>82244</td>
<td>ONERACK</td>
</tr>
<tr>
<td>10.128.0.249</td>
<td>ALCATEL</td>
<td>82244</td>
<td>ONERACK</td>
</tr>
<tr>
<td>10.128.0.250</td>
<td>ALCATEL</td>
<td>82244</td>
<td>ONERACK</td>
</tr>
<tr>
<td>10.128.0.249</td>
<td>ALCATEL</td>
<td>82244</td>
<td>ONERACK</td>
</tr>
</tbody>
</table>
onNETBACKUP

Display planning backups
onMON component

onNAC

onNETDISCO
onNETCONF
onNETBACKUP
onMON

onMETAREPO

onCMDB
- Monitoring is provisioned automatically from the CMDB
- Monitoring profiles available based on device type
- Real time network devices status
- Generates alerts if any of the parts of the network is not working properly
Viewing the status of a network computer
onCMDB component

onNAC

onNETDISCO
onNETCONF
onNETBACKUP
onMON

onMETAREPO

onCMDB
- The module CMDB is the repository of all information of the inventory
- Allows you to easily share information with other platforms
- It stores all the basic elements that use the platform as network devices, security rules, networks, groups, VLAN, ...
onMETAREPO component

onNETDISCO
onNETCONF
onNETBACKUP
onMON

onNAC

onMETAREPO

onCMDB
• METADATA Access Point server module
• It uses protocol IF-MAP
openNAC services

- **Security Consulting**
  - Set architecture and methodology appropriate for a client to improve the security of access and authorization from your network

- **Roll out**
  - openNAC setups in companies and organizations

- **Support**
  - 7x24 support to openNAC installations

- **Development and customization**
  - Creating specific modules and functionality to customers
  - Support new infrastructure

- **Integration**
  - Integrating the solution with third tools
Contact

- http://www.opennac.org
- info@opennac.org
- Twitter: @opennac