Feasibility Study NAC for Vanderlande Industries

Network based NAC in a flexible environment

Stefan Roelofs

February 3, 2009

Table of contents

Research Questions

- What is the best architecture for a NAC solution in this environment?
- What elements and services should be part of this architecture?
- What organizational processes should be in place for an introduction of this technique?
- Is network based NAC feasible technology for this situation?

Company Introduction

- Project based company in material handling market
- Many different users:
  - Employees
  - External employees
  - Subcontractors, partners (long term)
  - Guests (short term)
- Locations: worldwide branches and customer locations
- Current infrastructure: collapsed core network with high portability of static IP devices
- Endpoints: PLC, SCADA, real-time (Unix based) OS, Windows
- IP Addresses: private, public and customer IP space

Some false assumptions...

- Everybody is in our 10.0.0.0/8 network (detection)
- Everybody is running TCP/IP (inspection)
- Every endpoint runs Windows/Unix/Linux based OS (agent)
- Every endpoint is capable of DHCP assignment (enforcement)
- The physical location is under supervision of an administrative body (authentication)
- Every endpoint has a user controlling it (authentication)

NAC Introduction

"Network Access Control (NAC) is a set of technologies and defined processes, which its aim is to control access to the network allowing only authorized and compliant devices to access and operate on a network"

- Goals: protect network or protect host itself
- Agent & agentless concepts

NAC Components

1. Element detection
2. Registration & authentication
3. Policy enforcement
4. Pre-admission evaluation
5. Access classification
6. Post admission scanning

Element Detection

- 802.1x: only 802.1x capable clients
- SNMP: dependable on MAC table entries
- Mapping of MAC - IP address static IP devices
  - Inverse ARP
  - ARP Table Layer 3
  - Port mirroring port
  - Manual registration
- Practical verifications
  - Gratuitous ARP to fill MAC table
  - No core activity assured

Registration & Authentication

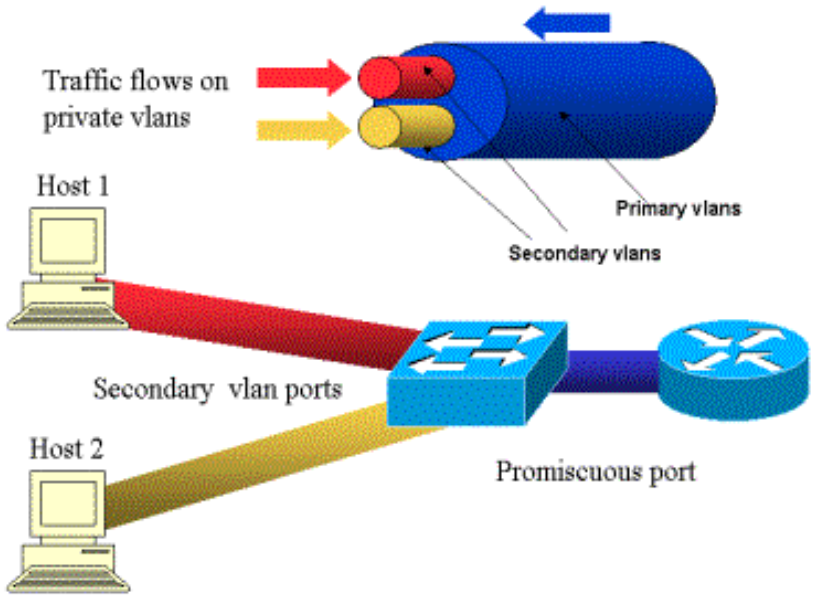
- User based approach registration
- 802.1x: client support/configuration
- Captive portal: unified way and remediation instructions
- Static IP clients & no browser clients: pre-registration

Policy Enforcement

- 802.1x
- ARP
- In-line devices
- DHCP
- Dynamic VLAN

Dynamic VLAN

- Random VLAN
- Private VLAN
- Practical verifications:
  - DHCP VLAN behavior

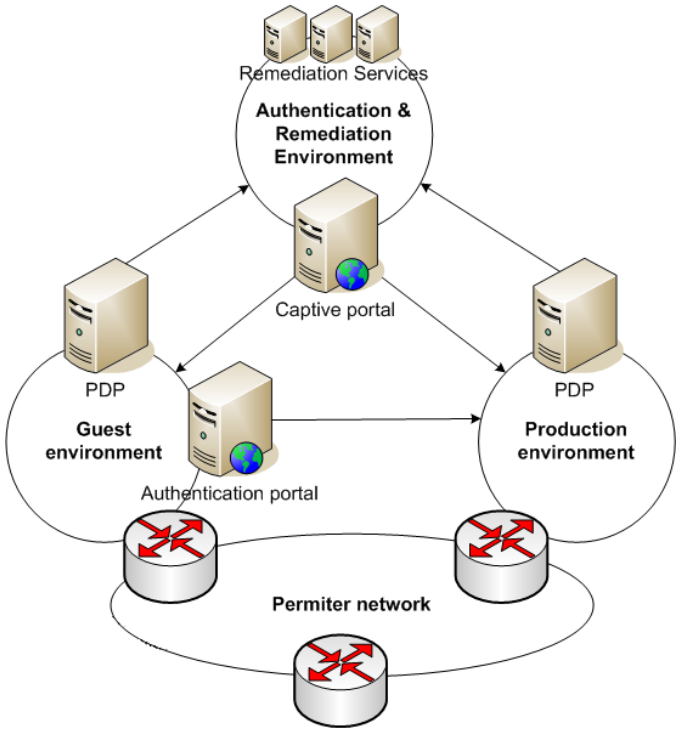


Pre Admission Evaluation

- Evaluation time <30 seconds
- Guest users: network threats
- Production users: also self-threats (administrative rights required)
- Vulnerability scanning
- Intrusion Detection System
- Practical verifications
  - Vulnerability scanning time
  - Snort on PLC/SCADA equipment

Access Classification

- Remediation & authentication environment
- Guest environment
- Production environment



Post Admission Evaluation

- No time boundary, continues scanning
- Different approach in guest VLAN and production VLAN
- Vulnerability scanning with application vulnerabilities
- Intrusion detection throughput

Organizational Processes

- Registration & authentication limits
- Asset management
- Hardening clients
- Extra network equipment policy
- Management effort

Conclusion

- What is the best architecture for a NAC solution in this environment?
  - SNMP with dynamic VLAN, captive portal with IDS/Vulnerability scanning.
- What elements and services should be part of this architecture?
  - Critical network services, authentication and web services, update (remediation) repositories, IDS and vulnerability scanning.

Conclusion (continued)

- What organizational processes should be in place for an introduction of this technique?
  - Client hardening, asset management, authentication & registration limits.
- Is network based NAC feasible technology for this situation?
  - Yes but agent needed to provide administrative access.
- Future work
  - Check patch level through scripting
  - Project locations
  - Wifi networks & VoIP services
  - Inspection on IRT traffic

Discussion

- Questions?