Overcoming Challenges in Deploying NAC Solutions in Highly Distributed Networks with 100,000+ End Points: A Case Study

Necati Ertuğrul
CTO, NATEK Technologies GmbH
Why NAC?

- Common Requirements
  - Different Authorization Requirements for Users
  - Manage BYOD Effectively

- New Challenges
  - Mobile Devices
  - Increased Threat for Malicious Software
  - Auditing Other Stakeholders Accessing Network

- Strategy
  - User Authentication & Authorization
  - Remediation Management
  - Compliance Tracking
Challenges in Deploying NAC in Distributed Networks

- Difficulty in Using a Single Solution for Wired & Wireless Networks.
- Network Problem’s Can Effect NAC Infrastructure.
- Agent Deployment Becomes a Major Problem.
- Some Products Require Appliance on LAN’s.

Deploy NAC in Headquarters Only
Türk Telekom

• Chosen as the Most Valuable Brand between 2009-2014 by Brand Finance.
• 13.3 Million Land Telephone Subscribers.
• 7.5 Broadband Internet Subscribers.
• 16.2 Million Mobile Phone Subscribers.
• 5.5 Billion USD Investment Between 2005-2014.
• 34000 Employees.
Challenges in Türk Telekom

- Many Different Devices from Different Network Vendors.
- More than 3000 Sites With Less Than 20 Users.
- 10+ Regional Headquarters.
- Many Visitors.
- Many Consultants Working With Their Own Devices.
- Common Usage of Personal Devices.
Major Requirements

- Simple Management
- System Profiling
- BYOD Support
- Centralized Solution
- Agentless
- Minimum or No Configuration Within Network Devices

Simpler Implementation
How System Works?

Traffic Redirection

Update Retrieval

Remediation Request


Remediation Servers

Detector

Detector Server

Computer Uncompliant. Traffic is Redirected and ACL is Applied.

Network Devices

Corporate Network

NAC Server


Captive Portal (Optional)

User Access Approved

Client

NAC Server

Request for Retrieving Updates

Request for Network Devices

Remediation

Servers

User Access Approved
How System Works?

<table>
<thead>
<tr>
<th>Mac Address</th>
<th>Ip Address</th>
<th>Host Name</th>
<th>Object Type</th>
<th>IsCategory</th>
<th>IsLegal</th>
<th>MacVendor</th>
<th>Detection Time</th>
<th>Last Collection Date</th>
<th>Credential Name</th>
<th>Operating Systems</th>
<th>Enumeration Error</th>
<th>DetectorId</th>
</tr>
</thead>
<tbody>
<tr>
<td>000c2893f646d</td>
<td>192.168.20.16</td>
<td>VCENTER</td>
<td>WINDOWS</td>
<td>Yes</td>
<td>Legal</td>
<td>VMware</td>
<td>23.12.2014 15:18:30</td>
<td>30.11.2014 11:33:05</td>
<td>Ntek.demo Domain</td>
<td>Microsoft Windows 7 SP0 - SP1</td>
<td>-</td>
<td>DETECTOR01</td>
</tr>
<tr>
<td>000c289499b02</td>
<td>192.168.20.22</td>
<td>NSM</td>
<td>WINDOWS</td>
<td>Yes</td>
<td>Legal</td>
<td>VMware</td>
<td>23.12.2014 15:18:30</td>
<td>30.11.2014 11:33:04</td>
<td>Ntek.demo Domain</td>
<td>Microsoft Windows 7 SP0 - SP1</td>
<td>-</td>
<td>DETECTOR01</td>
</tr>
<tr>
<td>000c2894f7710</td>
<td>192.168.20.23</td>
<td>THER</td>
<td>WINDOWS</td>
<td>Yes</td>
<td>Legal</td>
<td>Fortinet</td>
<td>23.12.2014 15:11:58</td>
<td>30.11.2014 11:33:14</td>
<td>-</td>
<td>Fortinet FortiGate 51B or 310B</td>
<td>RPC Connection Failed</td>
<td>DETECTOR01</td>
</tr>
</tbody>
</table>
• Device Management is Delegated to Regional Administrators.
• Regional Administrators Can Track Activity Within Their Responsible Segments.
• Device Formatting and Image Downloads Can Take Place Without Any Configuration Change on NAC.
How Devices are Enumerated?

- WMI, RPC, SSH and SNMP Used for Device Identification.
- Agentless Inventory Collection for Windows, Linux & Mac Operating Systems.
- Ability to Use Different Methods for Integrating with Network Devices
  - SNMP
  - SSH
- ACL’s are applied on network devices by SSH.
- NMAP Used for Understanding Types of Devices Inside the Network.
Implementation Steps

- Performed a Detailed Design.
- Started Enumeration by polling ARP Tables & Network Sniffing.
- Discovered All Components in the Network.
- Activated From Up to Down.
- Followed a Staged Approach.
Final Recommendations

- Detailed Design Based on Requirements Should be Made in Detail.
- Strong Coordination Between Units.
- Staged Approach Makes Life Easier.
- Captive Portal Is a Life Saver.
- Minimum Disruption is Critical.
- Ability to Disable The System With One Click Can be Important.