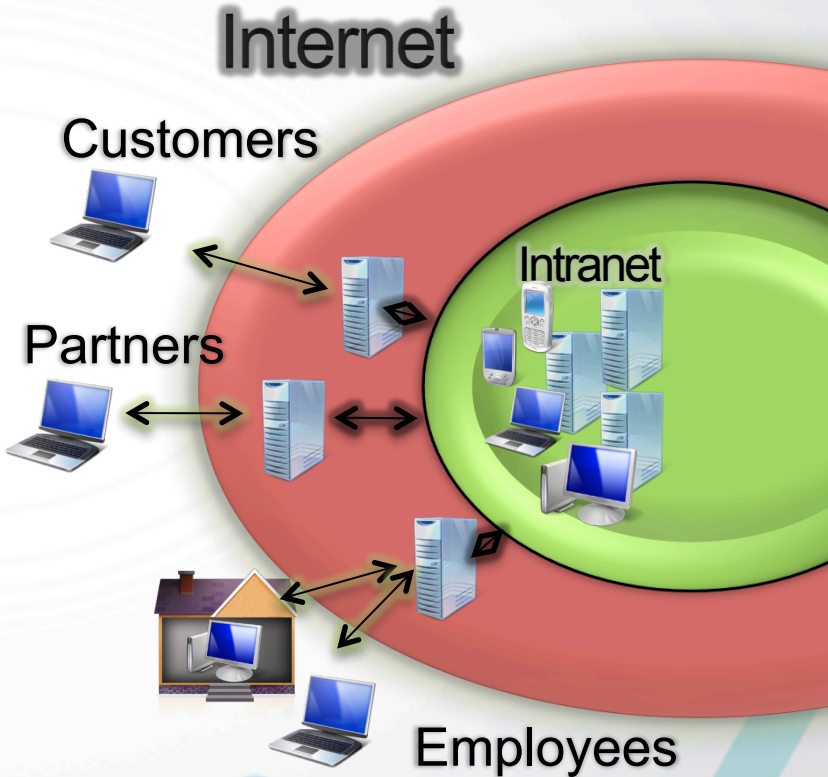
Overcoming Challenges in Deploying NAC Solutions in Highly Distributed Networks with 100.000+ End Points: A Case Study

Necati Ertuğrul
CTO, NATEK Technologies GmbH

Why NAC?

- Common Requirements
  - ❑ Different Authorizaton Requirements for Users
  - ❑ Manage BYOD Effectively
- New Challanges
  - ❑ 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.

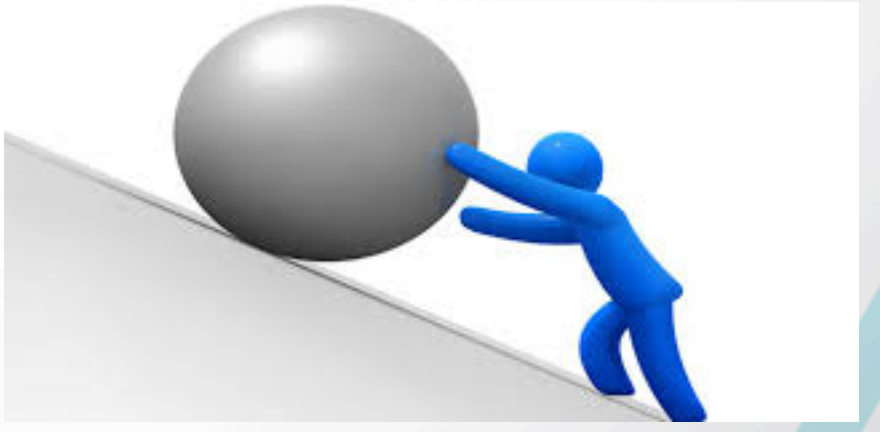
Deploy NAC in Headquarters Only

Türk Telekom

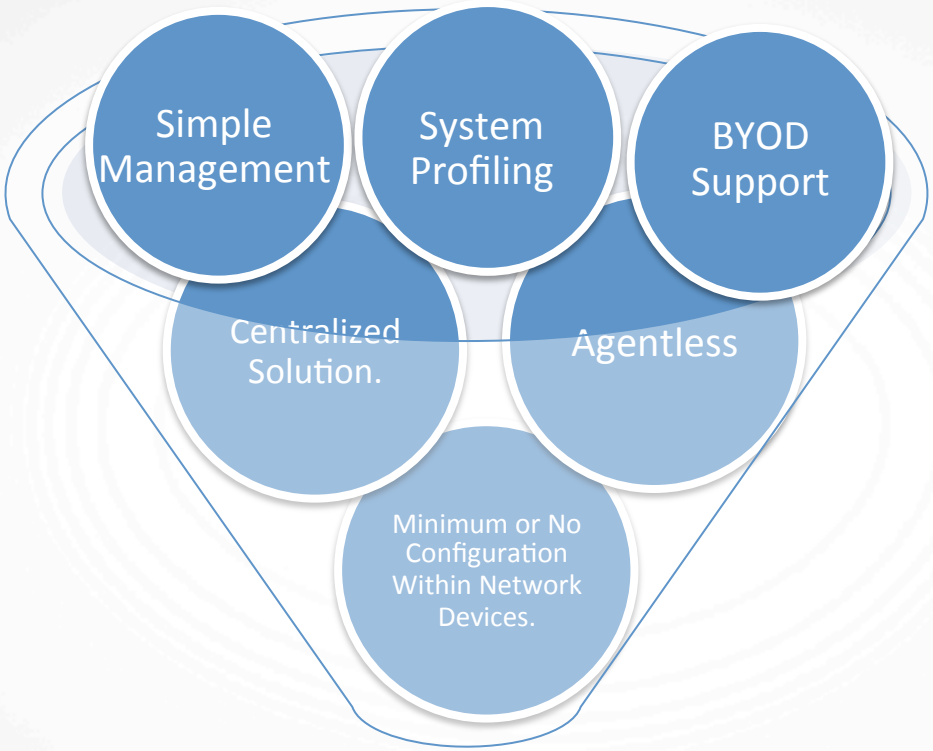
- Chosen as the Most Valuable Brand between 2009-2014 by Brand Finance.
- 13.3 Million Land Telephone Subscribers.
- 7.5 Broadband Internet Subscribers.
- 16.2 Million Mobile Phone Subscribers.
- 5.5 Billion USD Investment Between 2005-2014.
- 34000 Employees.

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.

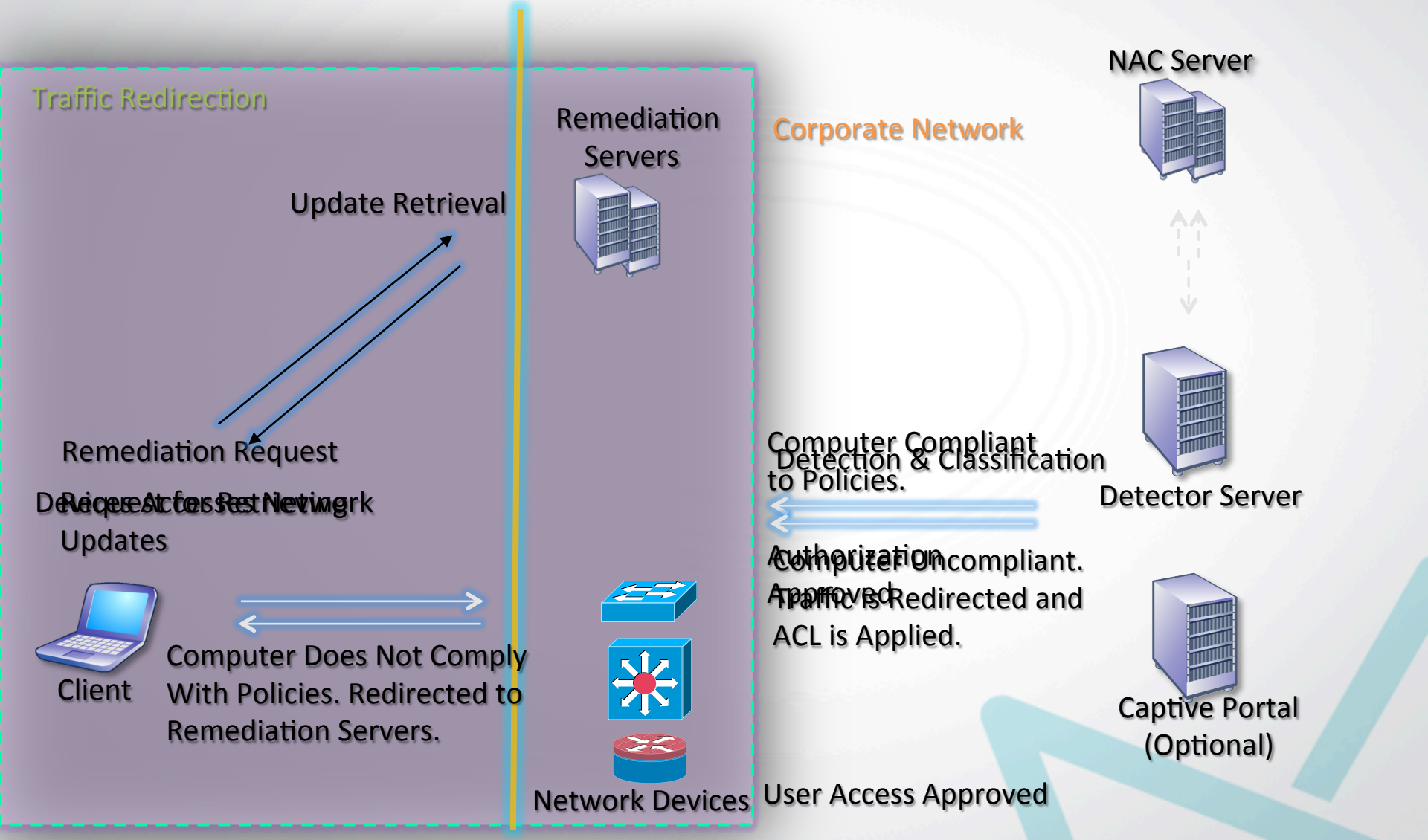


Major Requirements



Simpler Implementation

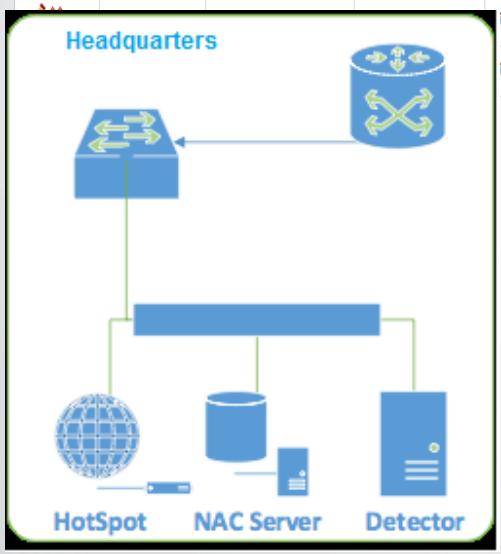
How System Works?



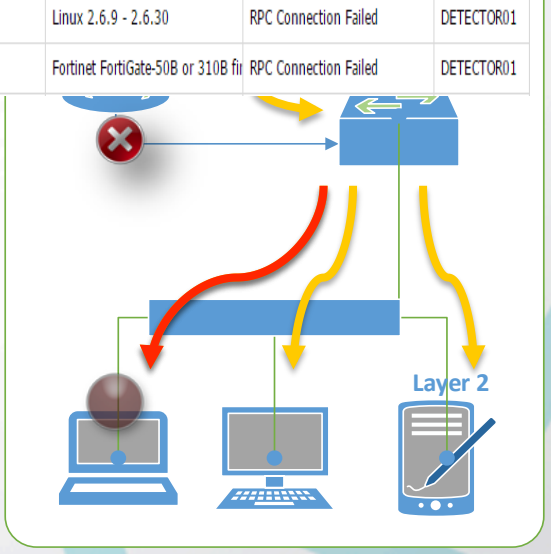
How System Works?

www.natektech.com

Mac Address	Ip Address	Host Name	Object Type	IsCategorize	Alien/Legal	MacVendor	Detection Time	Last Collection Date	Credential Name	Operating Systems	Enumeration Error	DetectorId
005056B16412	192.168.20.23	NAC01	WINDOWS	Yes	Legal	VMware	23.12.2014 15:18:30	30.11.2014 11:33:06	Natek.demo Domain	No OS Information	WMI Failed	DETECTOR01
000C29457710	192.168.20.15	ROOT	WINDOWS	Yes	Legal	VMware	23.12.2014 15:18:30	30.11.2014 11:33:41	Natek.demo Domain	Microsoft Windows Phone 7.5,Mi	-	DETECTOR01
000C29330A5F	192.168.20.16	VCENTER	WINDOWS	Yes	Legal	VMware	23.12.2014 15:18:30	30.11.2014 11:33:05	Natek.demo Domain	Microsoft Windows 7 SP0 - SP1,	-	DETECTOR01
000C29499E02	192.168.20.22	NSM	WINDOWS	Yes	Legal	VMware	23.12.2014 15:18:30	30.11.2014 11:33:04	Natek.demo Domain	Microsoft Windows 7 SP0 - SP1,	-	DETECTOR01
000C29AFE20B	192.168.20.21	HELPDESKDEMO	WINDOWS	Yes	Legal	VMware	23.12.2014 15:18:29	30.11.2014 11:34:13	Natek.demo Domain	Microsoft Windows Server 2008 S	-	DETECTOR01
005056B138AF	192.168.20.20	SCSUITE	WINDOWS	Yes	Legal	VMware	23.12.2014 15:18:29	30.11.2014 11:33:36	Natek.demo Domain	Microsoft Windows 7 SP0 - SP1,	-	DETECTOR01
005056B139CC	192.168.20.27	NA	OTHER	Yes	Legal	VMware	23.12.2014 15:16:45	30.11.2014 14:41:09	-	No OS Information	RPC Connection Failed	DETECTOR01
24FD52F48509	192.168.20.55	NA	OTHER	Yes	Legal	NA	23.12.2014 15:15:03	30.11.2014 13:26:47	-	No OS Information	RPC Connection Failed	DETECTOR01
			THER	Yes	Legal	AirTies Wireless Netw	23.12.2014 15:13:04	30.11.2014 11:33:24	-	Linux 2.6.9 - 2.6.30	RPC Connection Failed	DETECTOR01
			THER	Yes	Legal	Fortinet	23.12.2014 15:11:58	30.11.2014 11:33:14	-	Fortinet FortiGate-50B or 310B fi	RPC Connection Failed	DETECTOR01

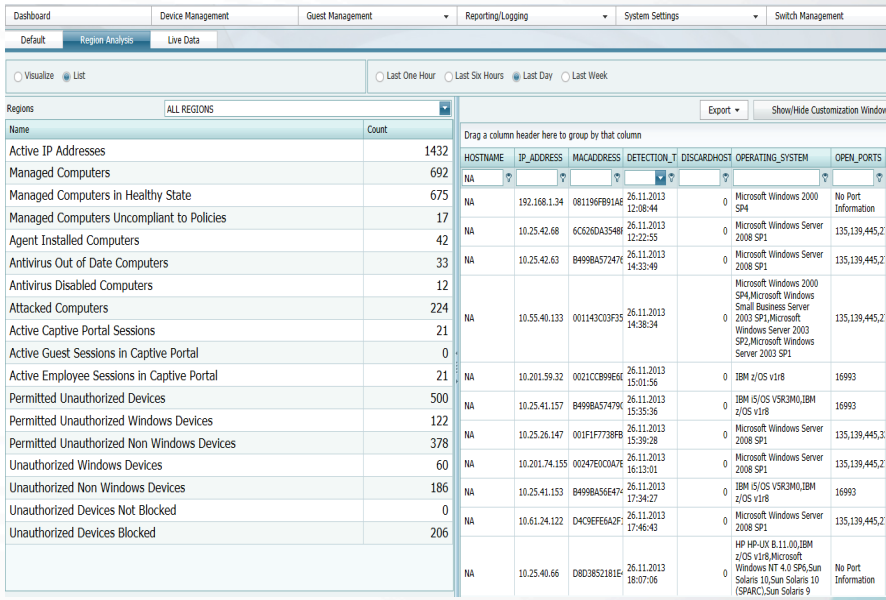


Vlan	Mac Address	Type	Ports
10	000d.9dd2.b5a5	DYNAMIC	Fa0/1
10	000e.3834.b638	DYNAMIC	Fa0/21
10	000e.3834.b954	DYNAMIC	Fa0/19
10	000e.3888.d251	DYNAMIC	Fa0/1
10	000e.3892.ddd1	DYNAMIC	Fa0/4
10	0012.8053.f49c	DYNAMIC	Fa0/15
10	0012.8053.f6e4	DYNAMIC	Fa0/12
10	0012.8053.f76f	DYNAMIC	Fa0/9
10	0012.8053.f77b	DYNAMIC	Fa0/10
10	0012.8055.becf	DYNAMIC	Fa0/22
10	0012.8055.c076	DYNAMIC	Fa0/7
10	0012.8055.cc42	DYNAMIC	Fa0/20
10	0012.8081.e07c	DYNAMIC	Po1
10	0012.80b5.a124	DYNAMIC	Fa0/23
10	0012.80bb.e3d4	DYNAMIC	Fa0/3
10	0012.80bb.e3d5	DYNAMIC	Fa0/8
10	0012.80bb.e457	DYNAMIC	Fa0/13
10	0012.da8a.c496	DYNAMIC	Fa0/6



Region Based Administration

- 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.