

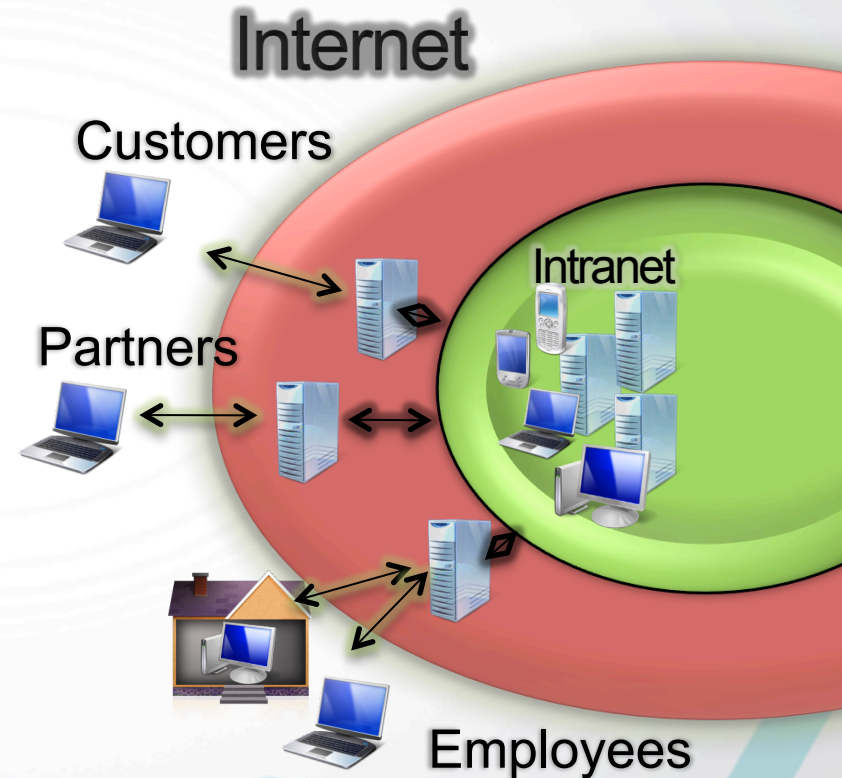
# Overcoming Challenges in Deploying NAC Solutions in Highly Distributed Networks with 100.000+ End Points: A Case Study



*Necati Ertuğrul*  
*CTO, NATEK Technologies GmbH*



- 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



- 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**



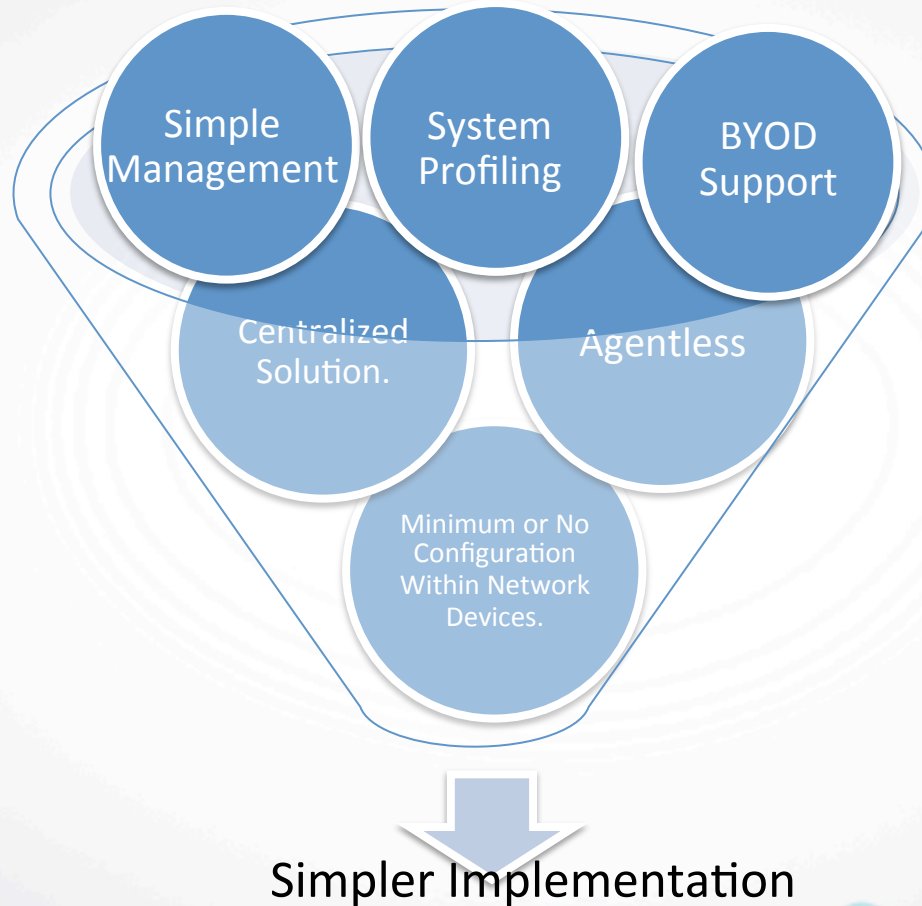
- Chosen as the Most Valuable Brand between 2009-2014 by Brand Finance.
- 13.3 Million Land Telephone Subscribers.
- 7.5 Broadband Internet Subscribers.
- 16.2 Million Mobile Phone Subscribers.
- 5.5 Billion USD Investment Between 2005-2014.
- 34000 Employees.





- 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.

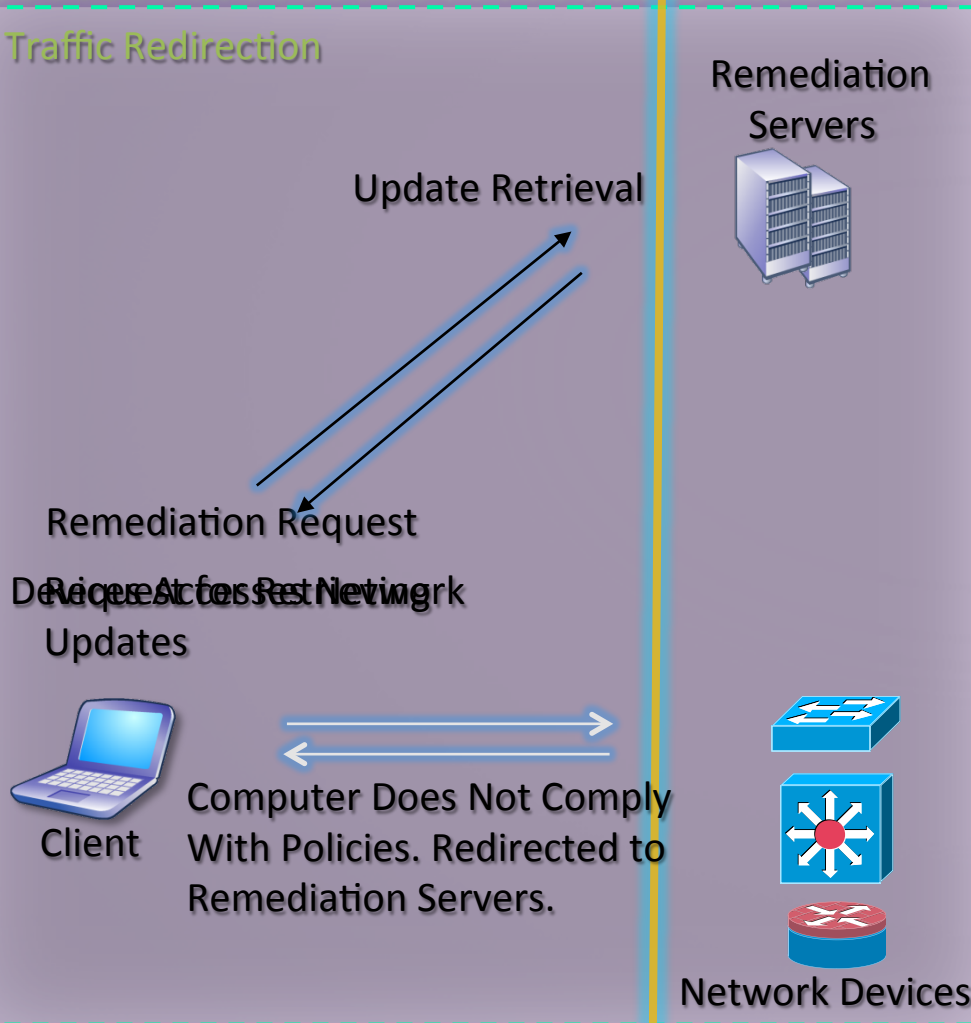




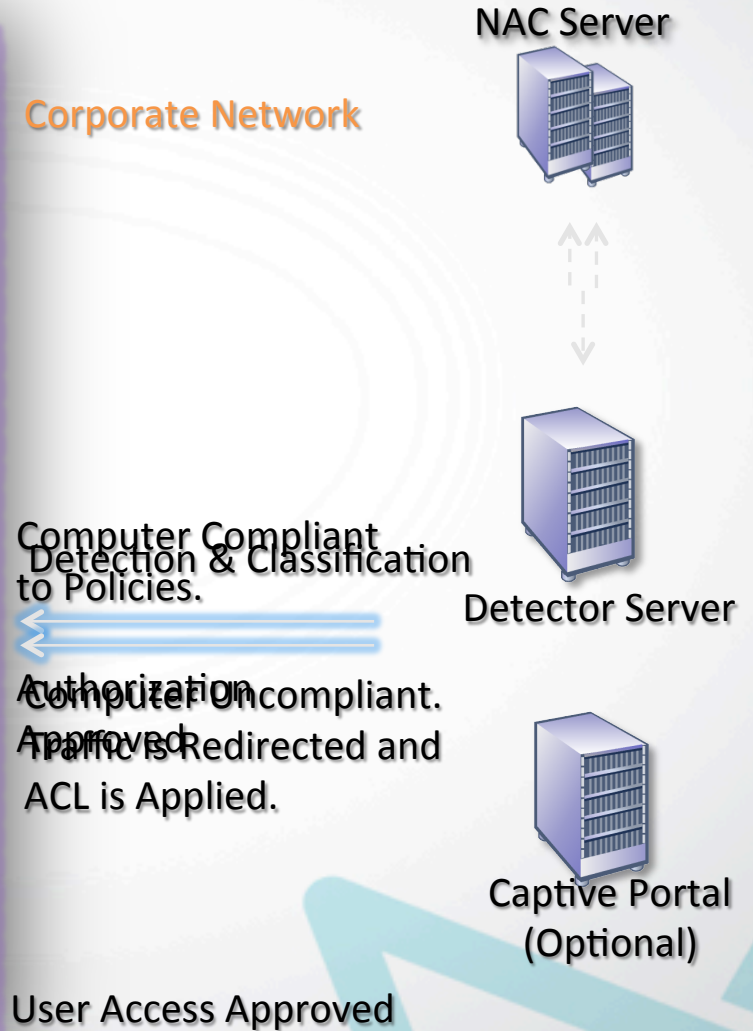


# How System Works?

## Traffic Redirection



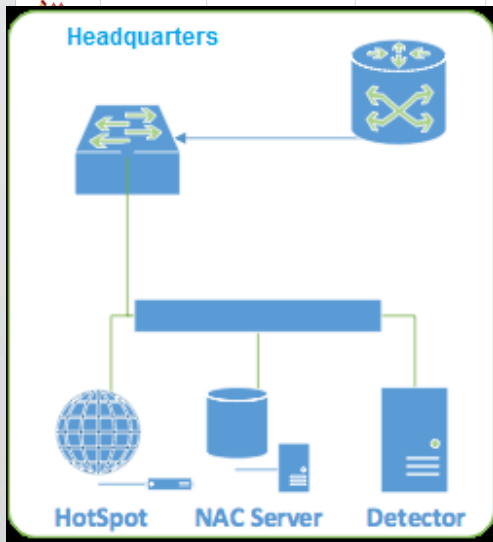
## Corporate Network



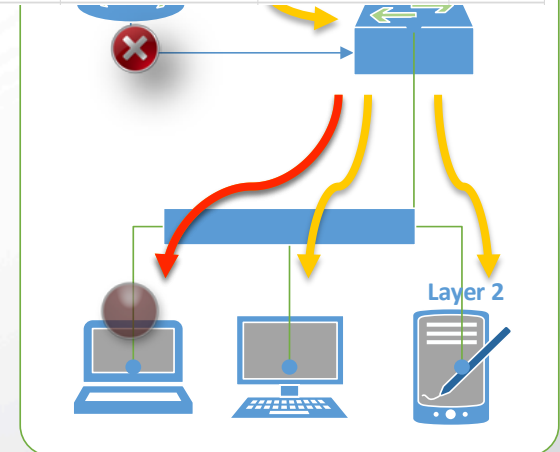


# How System Works?

	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
	000C294FE20B	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
			OTHER	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
			OTHER	Yes	Legal	Fortinet		23.12.2014 15:11:58	30.11.2014 11:33:14	-	Fortinet FortiGate-50B or 310B fir	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

www.natektech.com

- 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.

Dashboard | Device Management | Guest Management | Reporting/Logging | System Settings | Switch Management

Default | **Region Analysis** | Live Data

Visualize |  List |  Last One Hour |  Last Six Hours |  Last Day |  Last Week

Regions: ALL REGIONS

Name	Count
Active IP Addresses	1432
Managed Computers	692
Managed Computers in Healthy State	675
Managed Computers Uncompliant to Policies	17
Agent Installed Computers	42
Antivirus Out of Date Computers	33
Antivirus Disabled Computers	12
Attacked Computers	224
Active Captive Portal Sessions	21
Active Guest Sessions in Captive Portal	0
Active Employee Sessions in Captive Portal	21
Permitted Unauthorized Devices	500
Permitted Unauthorized Windows Devices	122
Permitted Unauthorized Non Windows Devices	378
Unauthorized Windows Devices	60
Unauthorized Non Windows Devices	186
Unauthorized Devices Not Blocked	0
Unauthorized Devices Blocked	206

Export | Show/Hide Customization Window

Drag a column header here to group by that column

HOSTNAME	IP_ADDRESS	MACADDRESS	DETECTION_T	DISCARDHOST	OPERATING_SYSTEM	OPEN_PORTS
NA	192.168.1.34	081196F891A6	26.11.2013 12:08:44	0	Microsoft Windows 2000 SP4	No Port Information
NA	10.25.42.68	6C620A23548F	26.11.2013 12:22:55	0	Microsoft Windows Server 2008 SP1	135,139,445,2
NA	10.25.42.63	B499BA572474	26.11.2013 14:33:49	0	Microsoft Windows Server 2008 SP1	135,139,445,2
NA	10.55.40.133	001143C03F35	26.11.2013 14:38:34	0	Microsoft Windows 2000 SP4;Microsoft Windows Small Business Server 2003 SP1;Microsoft Windows Server 2003 SP2;Microsoft Windows Server 2003 SP1	135,139,445,2
NA	10.201.59.32	0021CC899E62	26.11.2013 15:01:56	0	IBM z/OS v1r8	16993
NA	10.25.41.157	B499BA574794	26.11.2013 15:35:36	0	IBM i5/OS V5R3M0;IBM z/OS v1r8	16993
NA	10.25.26.147	001F1F7738FB	26.11.2013 15:39:28	0	Microsoft Windows Server 2008 SP1	135,139,445,3
NA	10.201.74.155	00247E0C0A7E	26.11.2013 16:13:01	0	Microsoft Windows Server 2008 SP1	135,139,445,2
NA	10.25.41.153	B499BA56E474	26.11.2013 17:34:27	0	IBM i5/OS V5R3M0;IBM z/OS v1r8	16993
NA	10.61.24.122	D4C3EFE6A4D7	26.11.2013 17:46:43	0	Microsoft Windows Server 2008 SP1	135,139,445,2
NA	10.25.40.66	D8D3852181E2	26.11.2013 18:07:06	0	HP HP-UX B.11.00;IBM z/OS v1r8;Microsoft Windows NT 4.0 SP6;Sun Solaris 10;Sun Solaris 10 (SPARC);Sun Solaris 9	No Port Information



# 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.





- 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.





- 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.

