
NAC deployment @ RTL Belgium

Didier Martin – IT Infrastructure Manager

21 June 2010

A few words about RTL Belgium

belgacom

together with



TV and Radio Broadcasting

RTL-TVI, since 1987



Club RTL



Plug RTL

Bel RTL



Radio Contact



Media House



IP TV, IP Event, IP Plurimedia

NewMedia



Providing contents for emerging broadcasting media (VOD, Smartphones, Internet, etc.)

Diversification



Request from IT Direction Comitee

A lot of ‘flying employees’/freelancers

LAN/IT is now “business critical” (AV production/broadcast)

⇒ Need for more security for LAN access

“The LAN security model has to be defined.”

“All LAN access can then be gradually replaced by a ‘secured’ access.”

Control Network Access:

- “Don’t allow foreign PCs on the network”
- “Ensure RTL Belgium PCs are compliant before getting access”
- “Foresee a remediation zone for non compliant machines”
- “Make the solution transparent for end users”
- “Foresee a solution for freelancers”
- “Have a better view on the network, have an overview of who/what is connected and where”

Initial consultancy phase



Translation of the business needs into technical needs (consultancy)

Combined with practical experience (Proof-of-concept)

→ Belgacom/Telindus offer was selected

Initial consultancy phase (2)



End-user devices covered:

- Desktop & laptops PCs, equipped with windows XP
- Avaya IP Phones
- Non dot1x devices (printers, etc.)
- PDA/Smartphones (Windows Mobile & Symbian) were out of scope as the WLAN aspects weren't covered (there is no Wireless internal LAN at RTL Belgium)

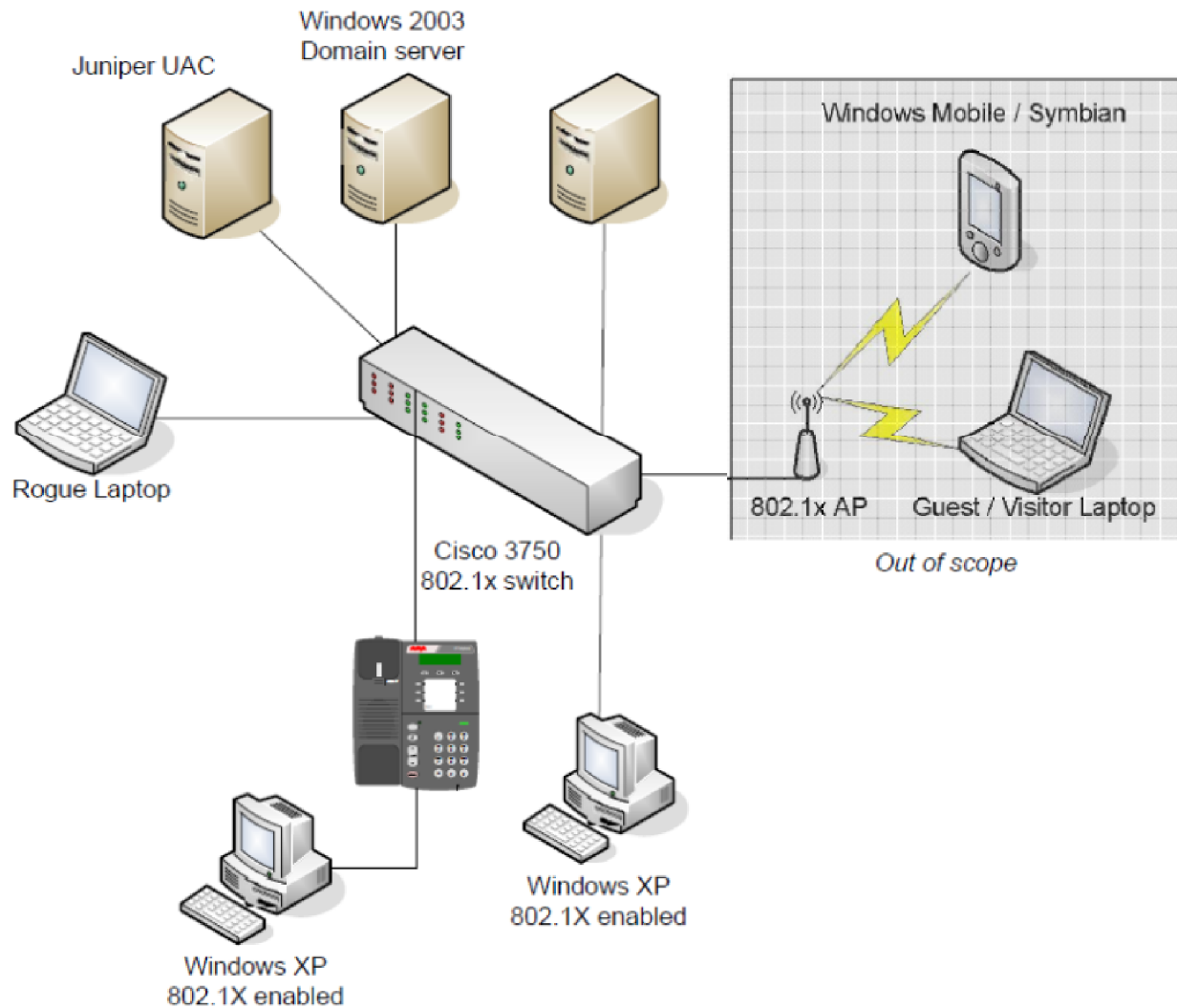
Infrastructure devices covered:

- LAN switches : mainly Cisco Catalyst 3750

Central authentication servers selected:

- Juniper Infranet UAC in Cluster Mode
- Integration with Active Directory

Initial consultancy phase (3)



Initial consultancy phase (4)



Test scenario's:

- Provisioning POC Setup
- 802.1x User and Machine authentication
- Integration of AVAYA IP Phones in 802.1x
- MAC authentication bypass
- Compliancy enforcement for network and port isolation in case of non-conformity

Proposed solution - methodology



- Study of the access methods/client types/ ...
- Based on this, definition of the different use case scenarios
 - RTLBelgium machine, compliant → Full Access
 - RTLBelgium machine, non compliant → Remediation
 - IPPhone, authenticated → Voice vlan
 - RTLBelgium non 802.1x capable devices (printers, badges readers, cameras)
 - restricted access based on MAC address, separate vlan
 - All others (guests, contractors, ...) → no access
- Validation of the access matrix
- Setup of a proof-of-concept for the defined scope
- Validation of technical aspects & documentation
- Deployment

Full Access
Remediation
No access

Actual deployment



Setup/configuration of 2 Juniper Infranet controllers in cluster mode

Creation of MSI packages for the OAC

Deployment on PCs

Switch configuration; step by step (port per port) activation:

->IP Phone configuration

->Authorized MAC database enrichment

Attention points / Lessons learned



Avaya phones

Non dot1x compliant devices

Non dot1x compliant switches (mini switches replaced)

Client software deployments

Machine authentication (Juniper/Microsoft AD integration)

Operational management / Moves-Adds-Changes

⇒ Preparation/testing is crucial

⇒ Deployment should be progressive and carefully managed

Questions & Answers

belgacom

together with



Q&A
