



NAC i Praktiken

Internetdagarna 2007

Håkan Nohre, CISSP

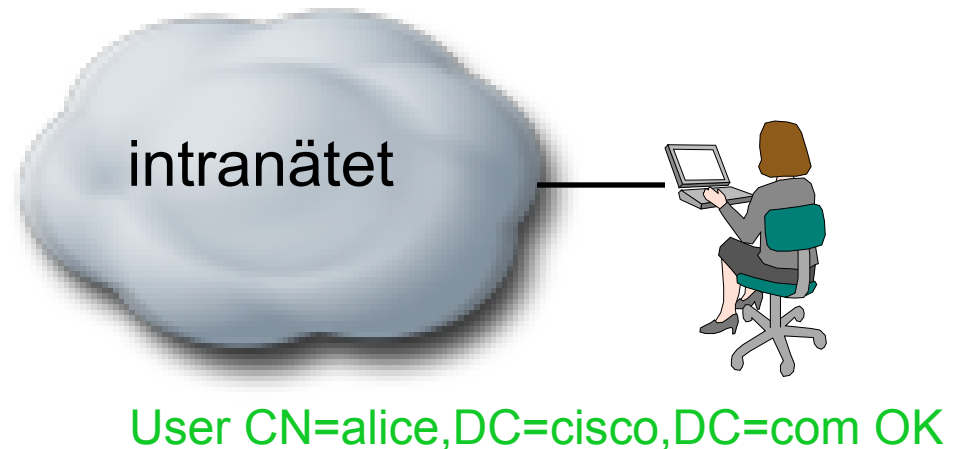
Cisco Systems

NAC : Autensiering av anställda

Autensiering av anställda användare och företagsägda maskiner (med t.e.x Active Directory)

Certifikat, lösenord...

Transparent vid godkänt autensiering



NAC : Stoppa obehöriga

Misslyckad autentisering = ingen åtkomst

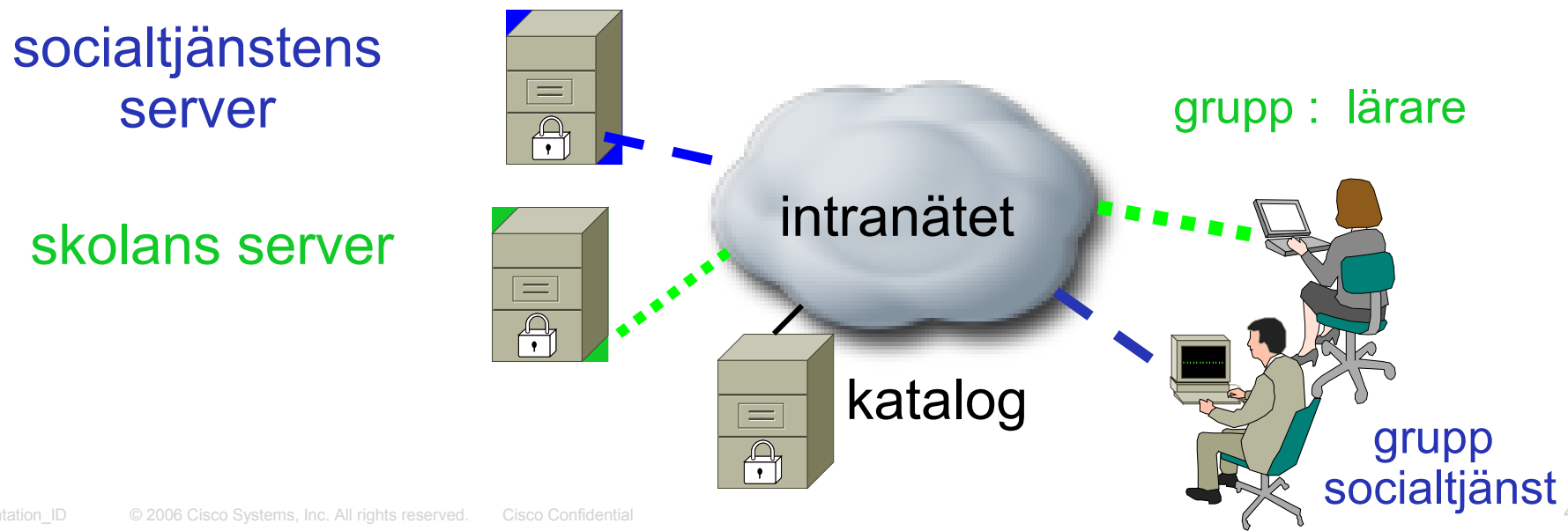


NAC : Auktorisering

Olika åtkomst till nätverket för olika grupper

Accesslistor, VLAN tilldelning...

För skalbarhet är virtuella nivå-3 domäner i nätverket en stor fördel



NAC : Kolla datorn med avseende på policy

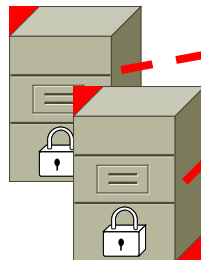
- OS, Service Pack, Hotfix
 - Antivirus , uppdaterad ?
 - Applikation X måste vara installerad...
 - Applikation Y får inte vara installerad...
- Karantän för datorer som ej uppfyller policy

socialtjänstens
server



Antivirus uppdatering

Windows Update



OS – WinXP SP 2 OK
Antivirus : OK
Hotfix : Saknar KB835732

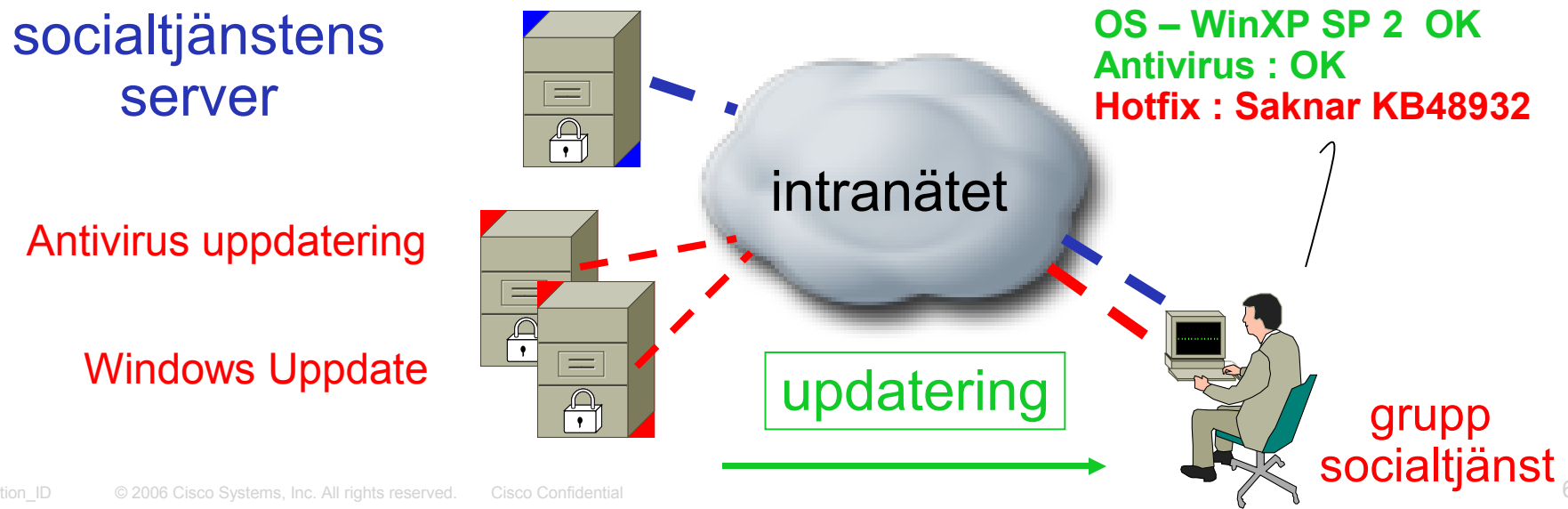


grupp
socialtjänst

NAC : Uppdatera Datorn

Uppdatering av t.e.x Antivirus eller Hotfix

Automatiskt och transparent för användaren



NAC : Enkelhet för administratören

NAC systemet måste hålla reda på vilka fixar som finns, antivirus etc. och integrera med t.e.x WSUS....

The screenshot shows a configuration window for a NAC requirement. The 'Requirement Type' is set to 'Windows Server Update Services'. The 'Enforce Type' is 'Mandatory' and the 'Priority' is '1'. Under 'Windows Updates Validation by', 'Severity' is selected. A note states: '*Note: Validation by Cisco Rules: Choose OS hotfix rules for validation'. Under 'Windows Updates to be Installed', 'Custom' is selected with a value of 'Critical'. The 'Upgrade to Latest OS Service Pack' checkbox is unchecked. The 'Windows Updates Installation Source' section has a red box around the radio buttons, with 'Managed WSUS Servers' selected. The 'Installation Wizard Interface Setting' has 'Show UI' selected. A note states: '*Note: The Show UI option to show user interface while installing Windows updates will work for privileged users only.'. The 'Requirement Name' is 'wsus_employee' and the 'Description' field is empty. Under 'Operating System', 'Windows 2000', 'Windows XP (All)', and 'Windows Vista (All)' are checked. Under 'Windows XP (All)', 'XP Pro/Home', 'XP Tablet PC', and 'XP Media Center' are unchecked. Under 'Windows Vista (All)', 'Vista Home Basic', 'Vista Home Premium', and 'Vista Business' are unchecked.

Requirement Type: Windows Server Update Services

Enforce Type: Mandatory Priority: 1

Windows Updates Validation by: Cisco Rules Severity
**Note: Validation by Cisco Rules: Choose OS hotfix rules for validation*

Windows Updates to be Installed: Express Custom Critical

Upgrade to Latest OS Service Pack

Windows Updates Installation Source: Microsoft Servers Managed WSUS Servers

Installation Wizard Interface Setting: Show UI No UI
**Note: The Show UI option to show user interface while installing Windows updates will work for privileged users only.*

Requirement Name: wsus_employee

Description:

Operating System: Windows 2000 Windows XP (All) Windows Vista (All)

XP Pro/Home Vista Home Basic

XP Tablet PC Vista Home Premium

XP Media Center Vista Business

NAC för Gäster

Gäst, konsult som behöver komma åt (en del) av nätverket (t.e.x internet)

Gästens PC kommer normalt ej ha någon förinstallerad agent/supplikant

Gästen kommer ofta ej att vara administratör på sin PC

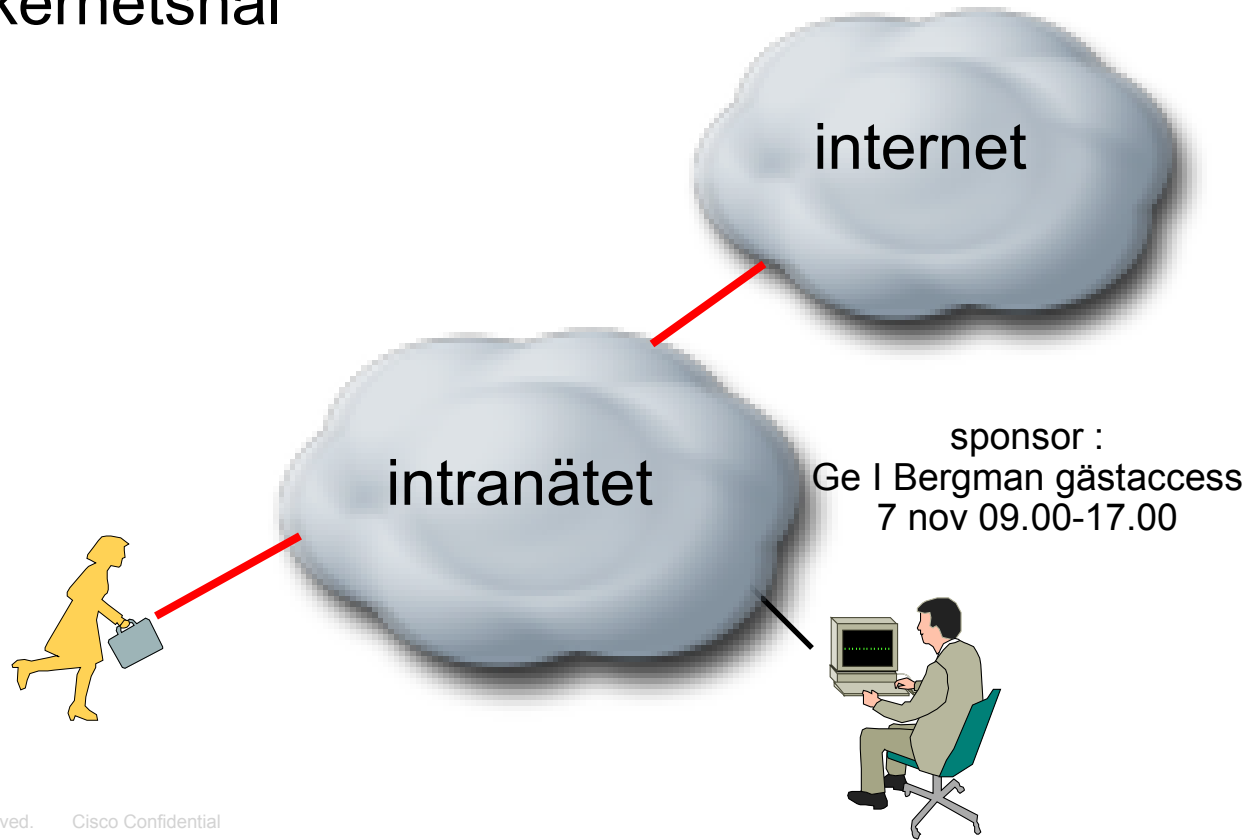
Gäst (t.e.x konsult, leverantör)



NAC för Gäster, forts.

Webinlogging (konto skapas av "sponsor")

Ev. skannas datorn innan den ges tillträde
för att leta efter säkerhetshål



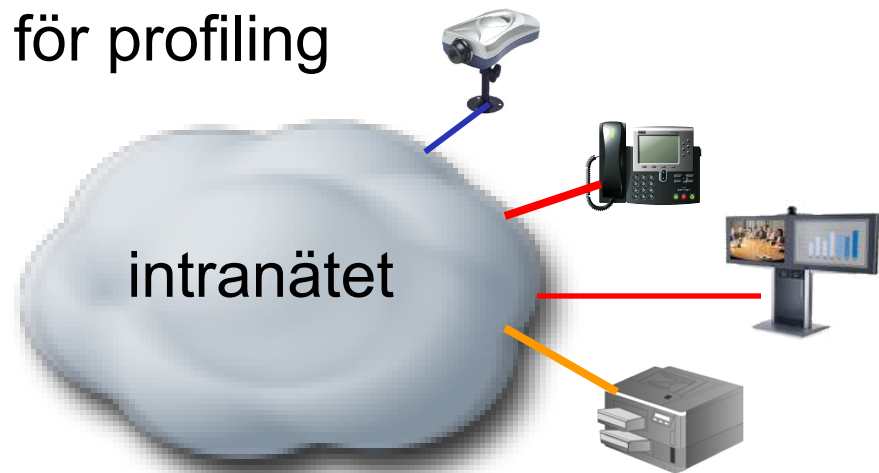
NAC för övrig IP utrustning

Telefoner, Videosystem, Skrivare, Kameror, Faxar

Manuellt hålla reda på portar och mac adresser ?

Automatisk "profiling" av utrustning för att ge rätt behörighet till viss typ av utrustning (t.e.x skrivare)

Använder t.e.x Netflow data för profiling



Att tänka på !

- NAC är **inte** bara ett nätverksprojekt, det omfattar Nätverket, PC-support, Säkerhetsavdelningen.....
- Politiken kan bli komplicerad....
- Tekniken mycket lättare ! 😊

Standarder

- Cisco NAC fungerar med alla större Operativsystem
- Cisco NAC fungerar med nästan alla anti-virus, personliga brandväggar, anti-spyware etc.
- Cisco strategiskt samarbete med Microsoft NAP+NAP
- Cisco aktiva i IETF standardiseringsarbete för NAC, NEA (Network Endpoint Assessment)

[draft-ietf-nea-requirements-05.txt](#)

