NAC i Praktiken

Internetdagarna 2007

Håkan Nohre, CISSP

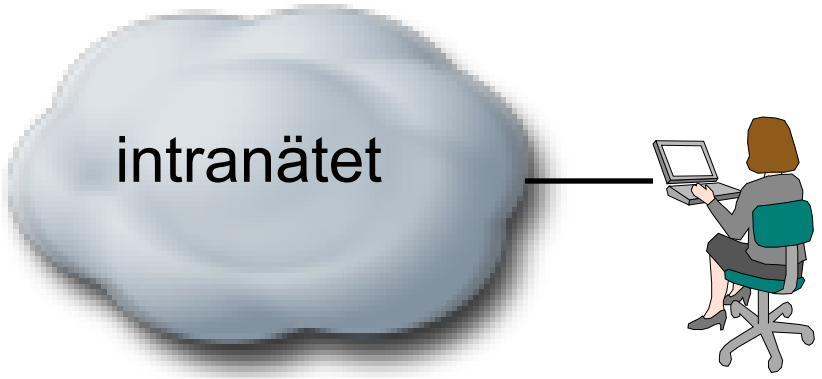
Cisco Systems

NAC : Autensiering av anställda

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

Certifikat, lösenord...

Transparent vid godkänt autensiering



User CN=alice,DC=cisco,DC=com OK

NAC : Stoppa obehöriga

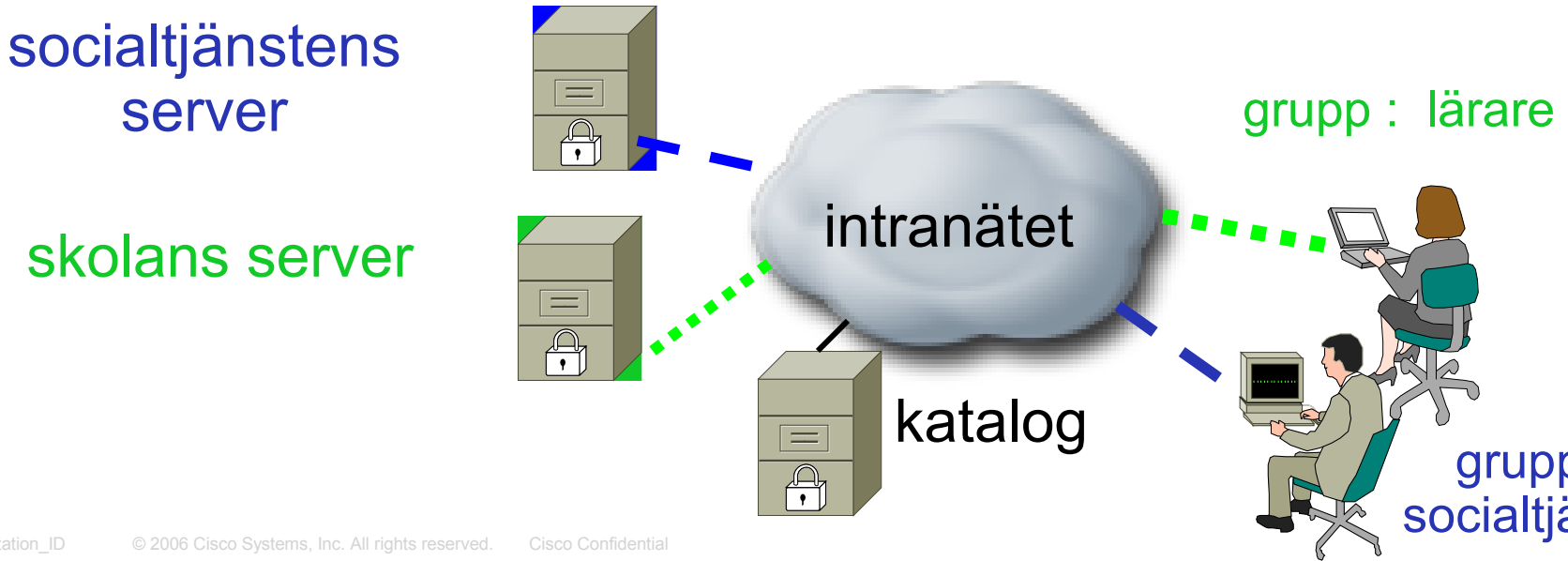
Misslyckad autensiering = ingen åtkomst

NAC : Auktorisering

Olika åtkomst till nätverket för olika grupper

Accesslistor, VLAN tilldelning...

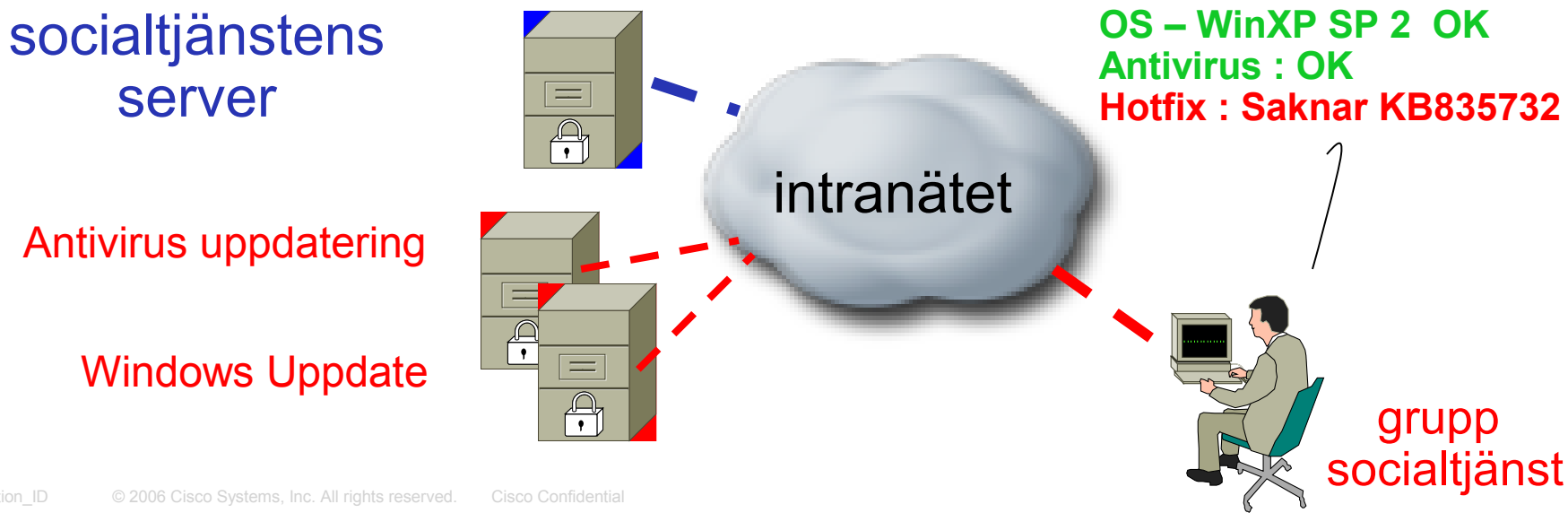
För skalbarhet är virtuella nivå-3 domäner i nätverket en stor fördel



NAC : Kolla datorn med avseende på policy

-OS, Service Pack, Hotfix
-Antivirus , uppdaterad ?
-Applikation X måste vara installerad...
-Applikation Y får inte vara installerad...

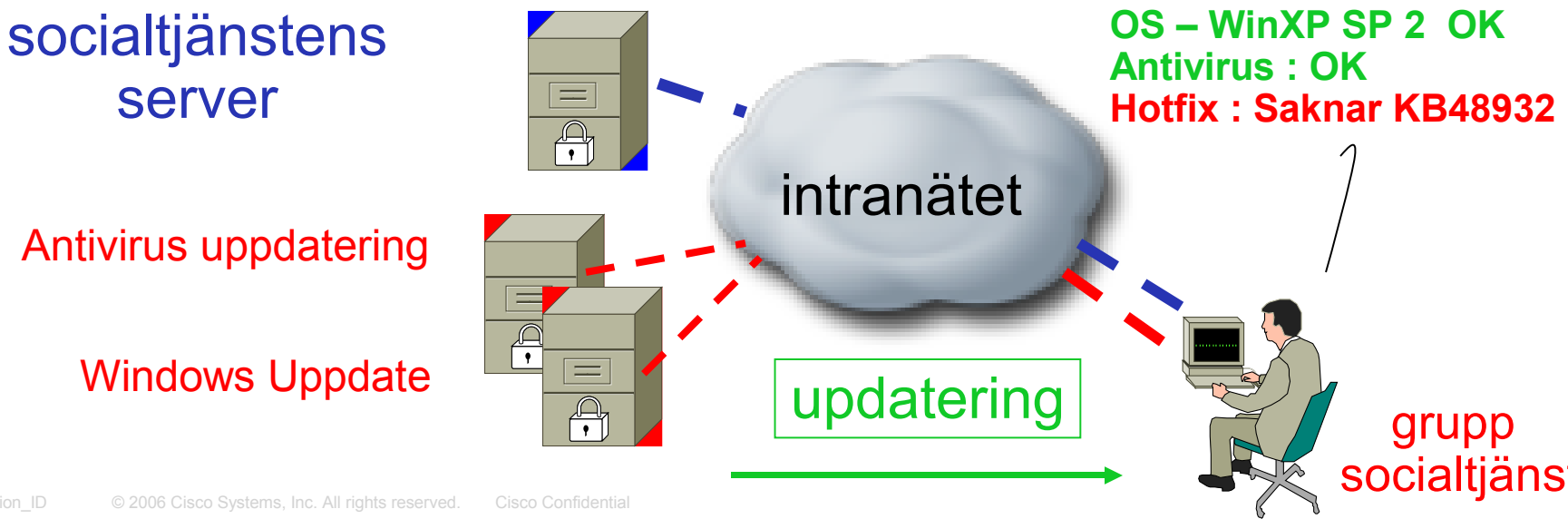
-Karantän för datorer som ej uppfyller policy



NAC : Uppdatera Datorn

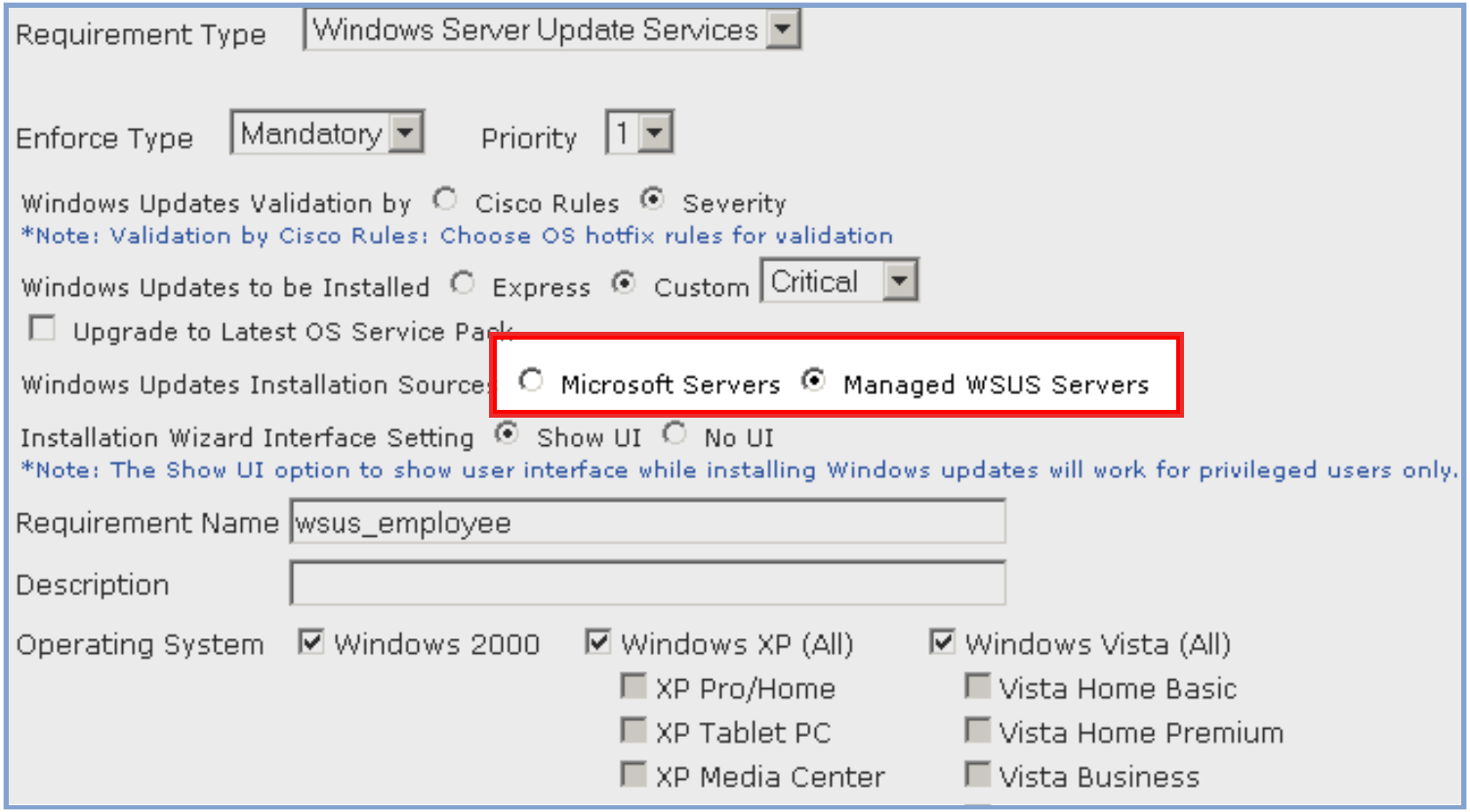
Uppdatering av t.e.x Antivirus eller Hotfix

Automatiskt och transparant 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....



NAC för Gäster

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

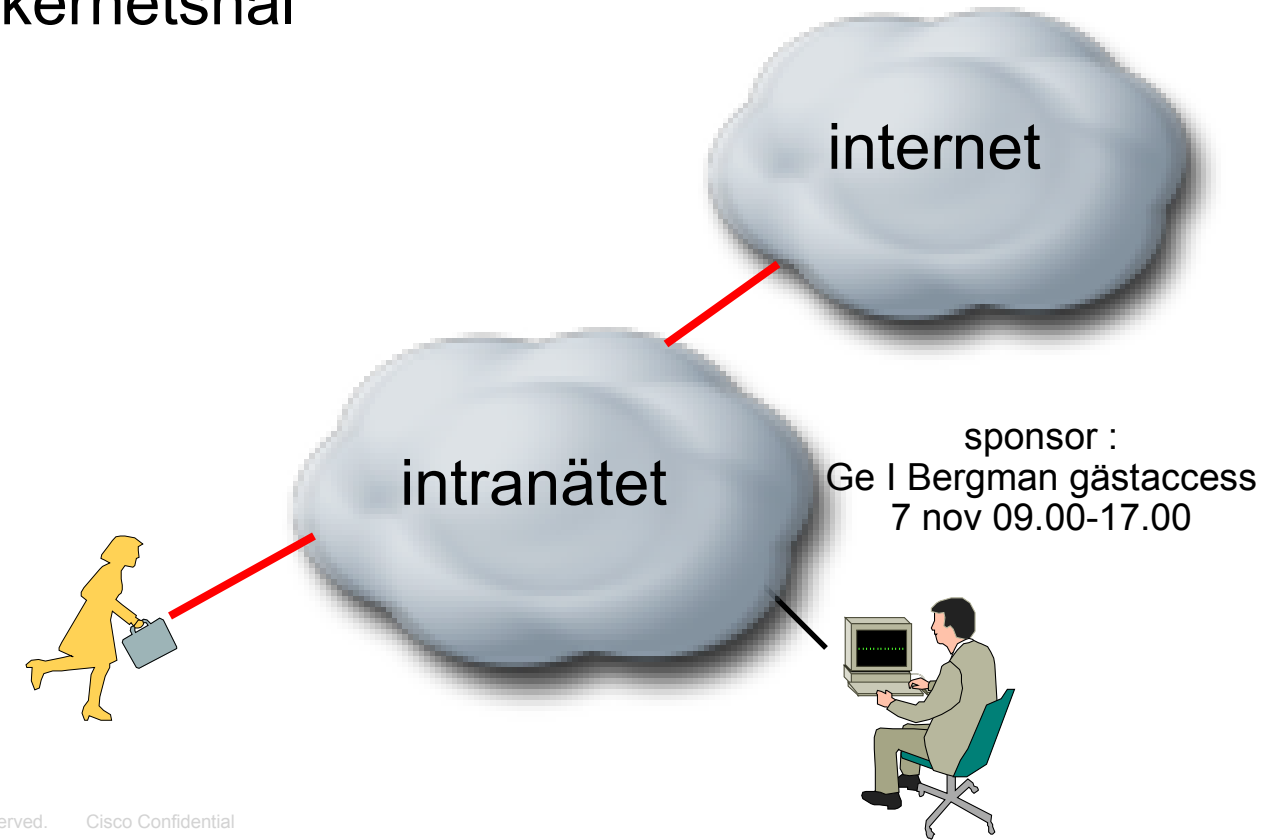
Gästens PC kommer normalt ej ha någon förinstallerad agent/supplikant

Gästen kommer ofta ej att vara administratör på sin PC

NAC för Gäster, forts.

Webinlogging (konto skapas av ”sponsor”)

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



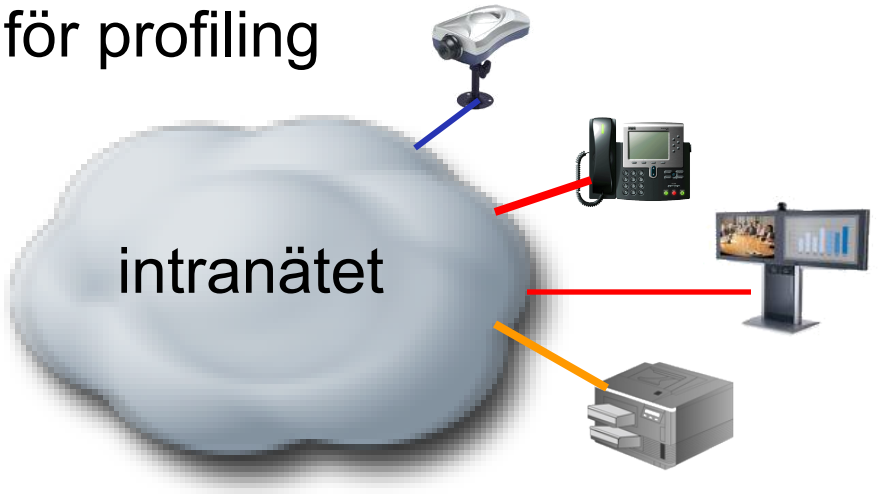
NAC för övrig IP utrustning

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