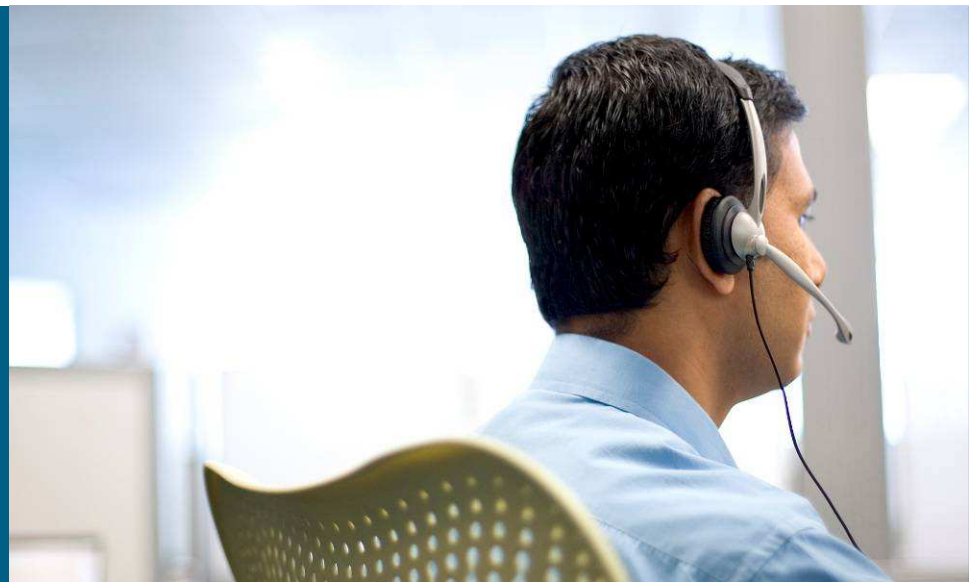
Cisco Expo 2008

Kontrollert nettverkstilgang

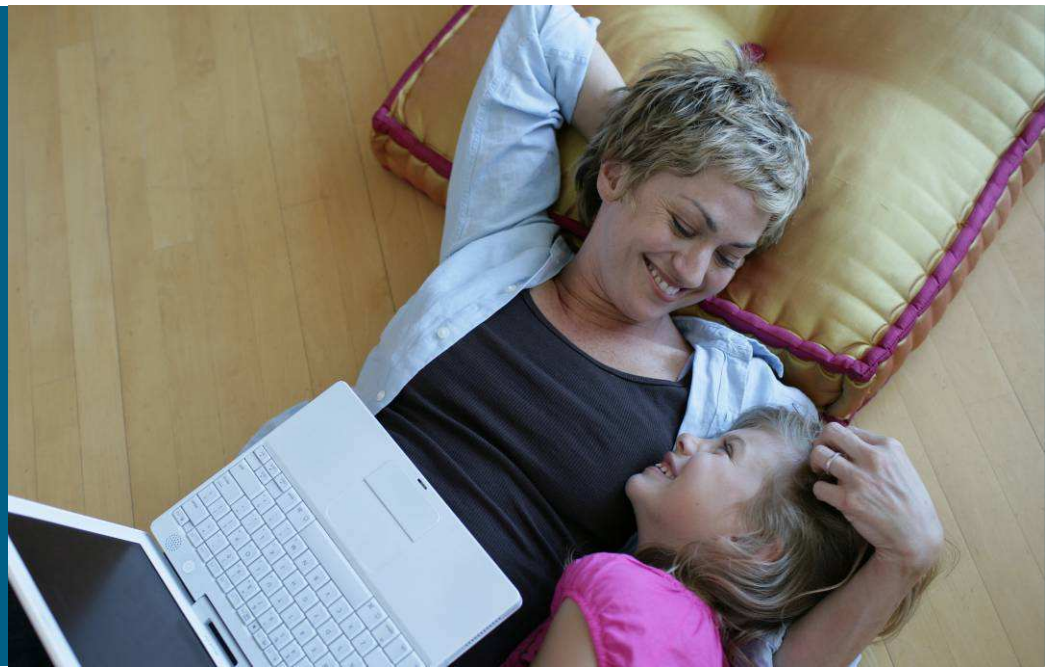
Network Admission Control (NAC)



Kent Støvne

Product Sales Specialist

Risikobildet i dag



Antivirus, Anti-spionvare & kritiske feilrettelser

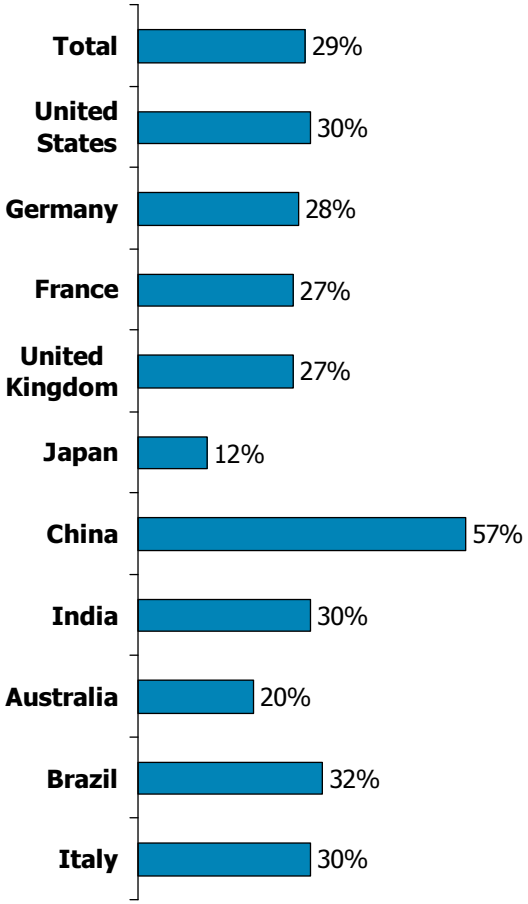
- Installert ?
- Kjører antivirus & anti-spionvare ?
- Oppdatert ?
- Hva med bærbare PC’er og mobile brukere ?

Anbefaling:

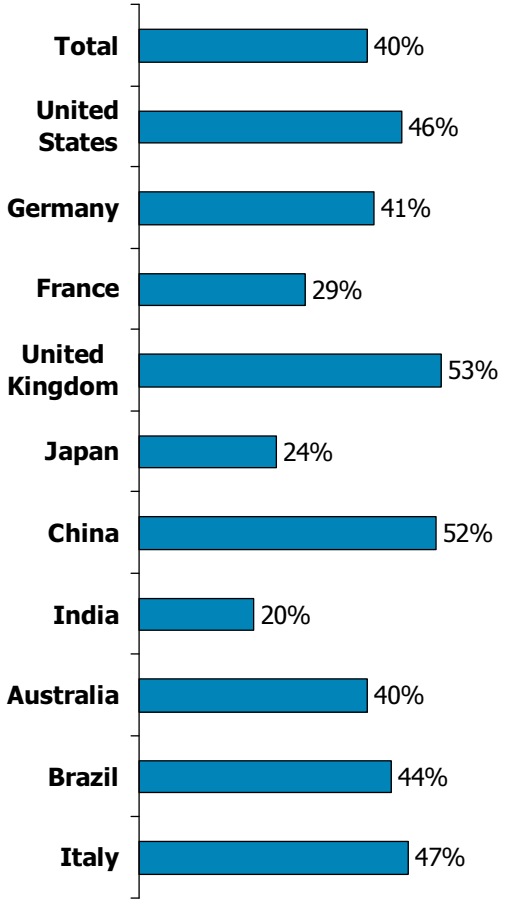
- **Installer fortløpende alle kritiske feilrettelser**
- **Ta i bruk siste generasjon endepunktbeskyttelse**

Den menneskelige faktor

Bruker du jobb PC til private saker?



Bruker du jobb PC til å handle på Internet?



Hva kan vi gjøre ?

Bruke de tre sikkerhetsskjoldene:

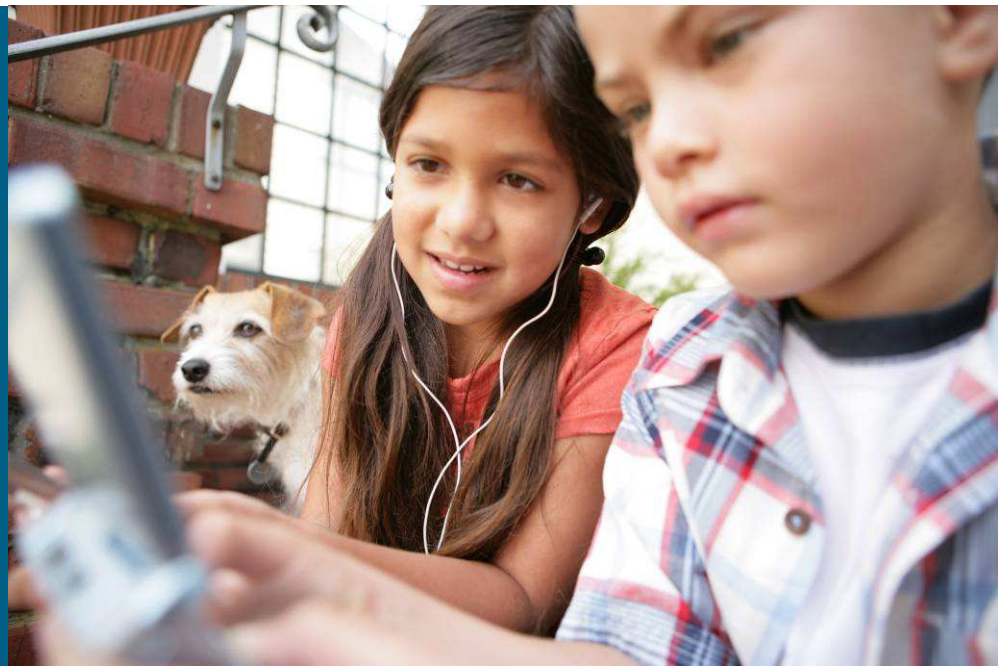
Etablere sikkerhets policy

Kontrollere tilgang til nettverket

Beskytte endepunkt

Nettverks tilgangskontroll –

Network Admission Control (NAC)



En liten begrepsavklaring

IEEE 802.1x ≠ NAC

Viktige kriterier for tilgang

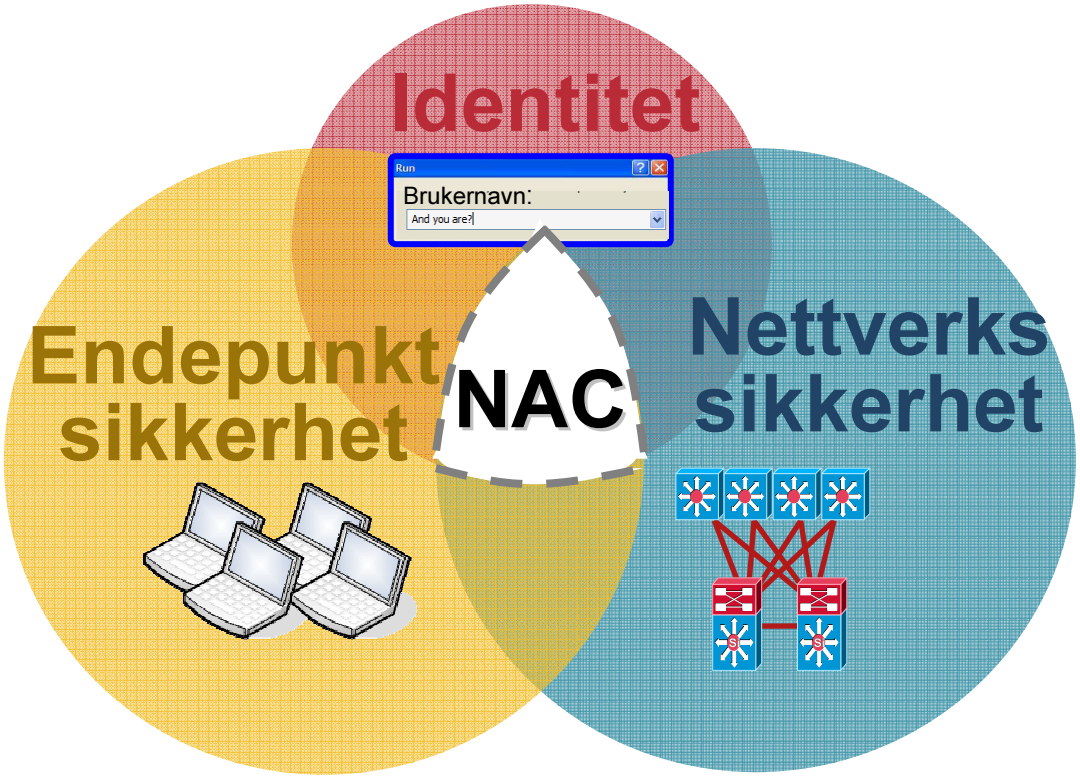
Hva slags enhet er det ?	**Windows, Mac eller Linux** **Laptop, Desktop eller PDA** **Skriver eller andre enheter**
Hvem eier enheten ?	**Virksomheten** **Den ansatte** **Konsulent** **Gjest** **Ukjent**
Hvordan er den tilknyttet ?	**VPN** **LAN** **WLAN** **WAN**
Sikkerhetsfunksjoner installert ? **Kjører de ? Er de oppdatert ?**	**Antivirus, anti-spionvare** **personlig brannmur** **oppdateringsverktøy**
Foretrukket måte for sikkerhetssjekk/oppdatering ?	**Egendefinert** **Ferdige maler** **Automatisk eller manuell oppdatering** **3'dje parts programvare**

Komplekse løsninger krever bred beskyttelse

Disse virkemidlene - brukt enkeltvis - kan feile og derved utsette alle for risiko !

Nettverks tilgangskontroll

Nettverket håndhever vår sikkerhetspolicy og sikrer at tilknyttede enheter oppfyller våre krav



Fire nøkkelegenskaper ved NAC

Fire nøkkelegenskaper ved NAC

	Sikker identifikasjon av enheter og brukere	Håndheve konsistent policy	Karantene og oppretting	Konfigurere og adminstrere
Hva betyr det ?	Knytter brukere til enheter	Aksessenheter i nettverket håndhever policy	Isolerer og retter opp (“patcher”) endepunkter utenfor policy	Enkelt å lage og vedlikeholde sikkerhetspolicy
Hvorfor er det viktig ?	Det muliggjør fleksibel håndheving av policy i henhold til rolle og/eller gruppe	Håndheving på nettverkslaget reduserer risiko fra kompromitterte endepunkt	Karantene er kritisk for å stoppe spredningen av ondsinnet kode; Oppretting/ ”patching” adresserer roten til det hele	En sikkerhetspolicy som er enkel å vedlikeholde gir bedre drift og lavere kostnader

En fullstendig NAC løsning må ha alle fire egenskapene ovenfor: Bortfall av en funksjon svekker hele sikkerhetsløsningen

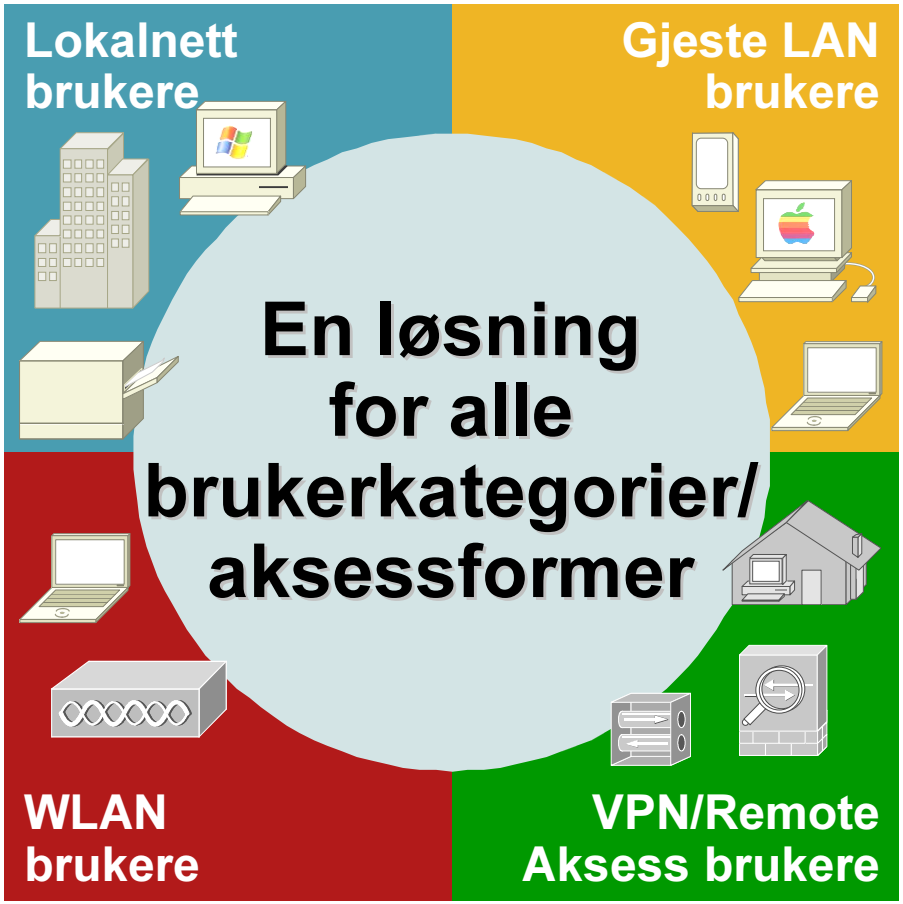
Spørsmål før vi fortsetter …

- Trenger jeg forskjellige produkter for VPN brukere, LAN brukere, trådløse brukere og gjestebrukere ?
- Er vi forsøkskaniner ? Hvilken erfaring har dere med utrulling av Cisco NAC Appliance ?
- Vil installasjon ta flere måneder ?
- Hvordan kan jeg være sikker på at denne løsningen passer i vårt nettverk ?
- Må vi oppgradere hele nettverks infrasturkturen ?

Cisco NAC Appliance
(aka Cisco Clean Access)

Cisco NAC Appliance

1.



2. **Trolig den mest selgende NAC-løsningen: 3500+ løsninger levert til dato !**

3. **Mange installasjoner gjennomføres på under 5 dager**

4. **Skalerer fra under 100 til over 100.000 brukere, spredt over 150+ lokasjoner**

5. **Kan installeres uten oppgradering av infrastruktur**

NAC Appliance håndhever vår sikkerhetspolicy

Kontroll av endepunkt i NAC

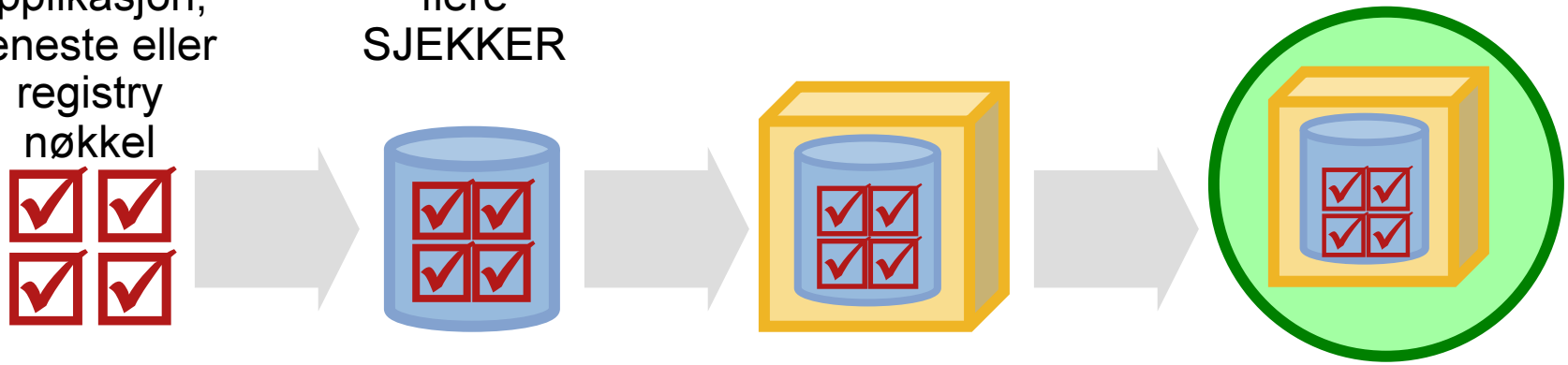
Verifisering i henhold til policy er en hierarkisk prosess

SJEKK
status på en file, applikasjon, tjeneste eller registry nøkkel

REGLER
består av en eller flere SJEKKER

KRAV
omfatter en eller flere REGLER

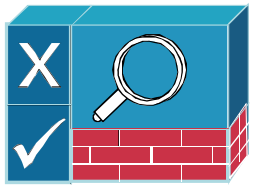
ROLLER
har en eller flere KRAV



NAC Appliance komponenter

- **NAC Appliance Server**

  Kontrollerer tilgang til nettverket. Står in-band eller out-of-band



- **NAC Appliance Manager**

  Sentralisert adminstrasjon for sikkerhetsansvarlig, brukerstøtte personell og driftspersonell

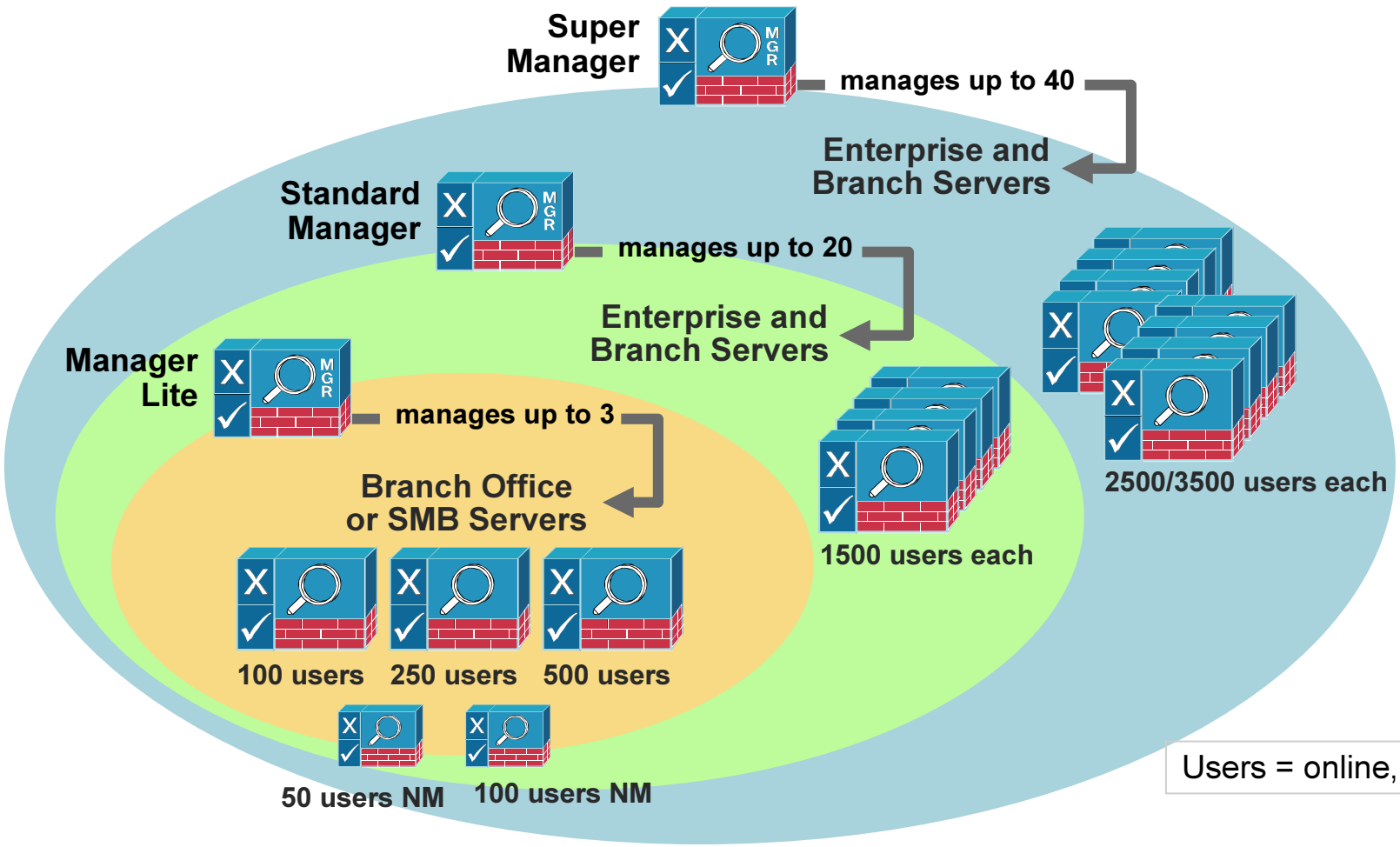
- **NAC Appliance Agent**
  (Cisco Clean Access Agent)

  Lettvekts klient for autentisering og scanning (opsjon)

- **Oppdatert regelsett**

  Automatisk oppdatering av prekonfigurerte regelsett for antivirus, kritiske hot-fixes og andre sikkerhetsapplikasjoner

Skalering

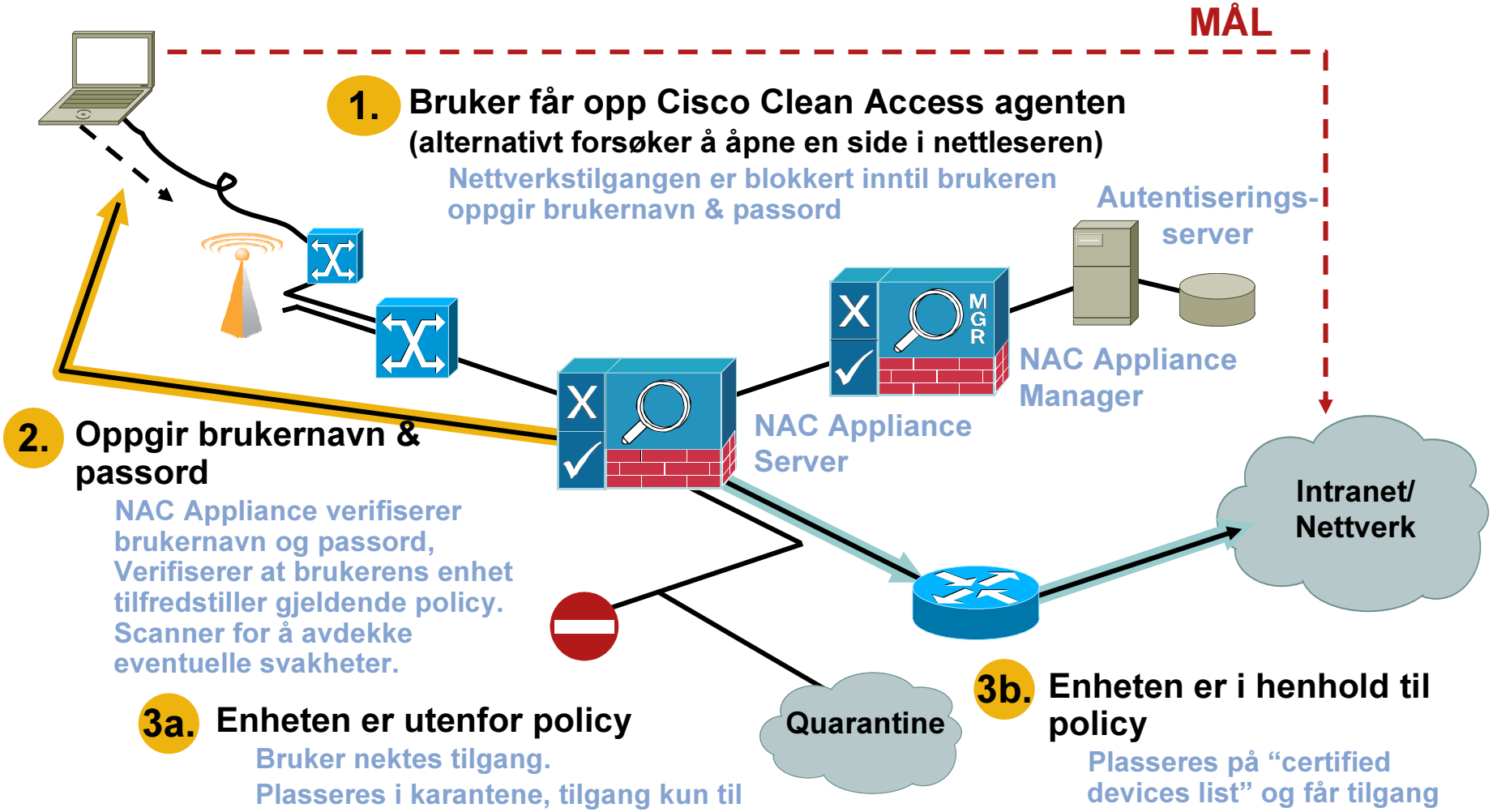


Users = online, concurrent

Cisco NAC Appliance –

Virkemåte

Virkemåte

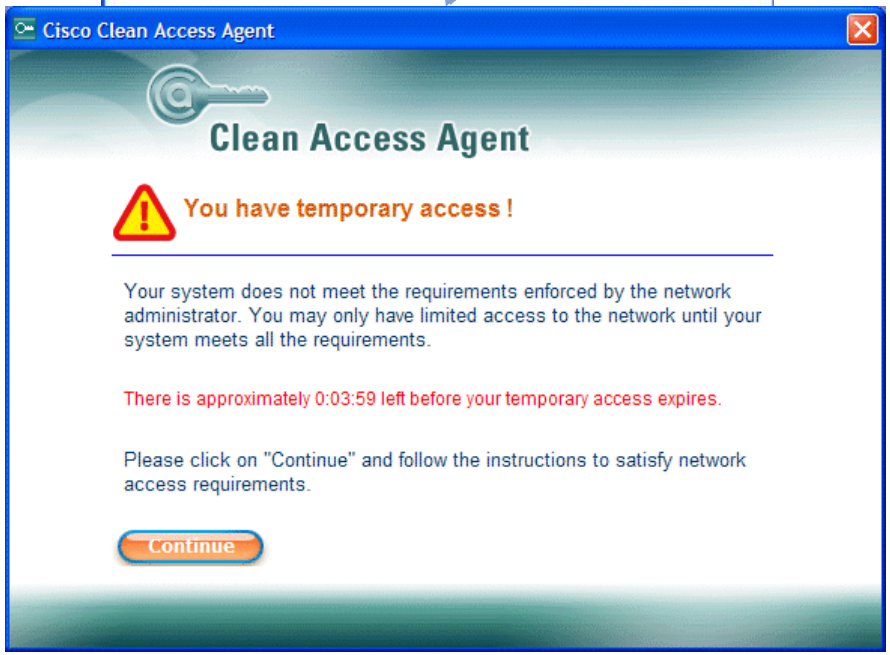


Eksempel på brukeropplevelse - Agent

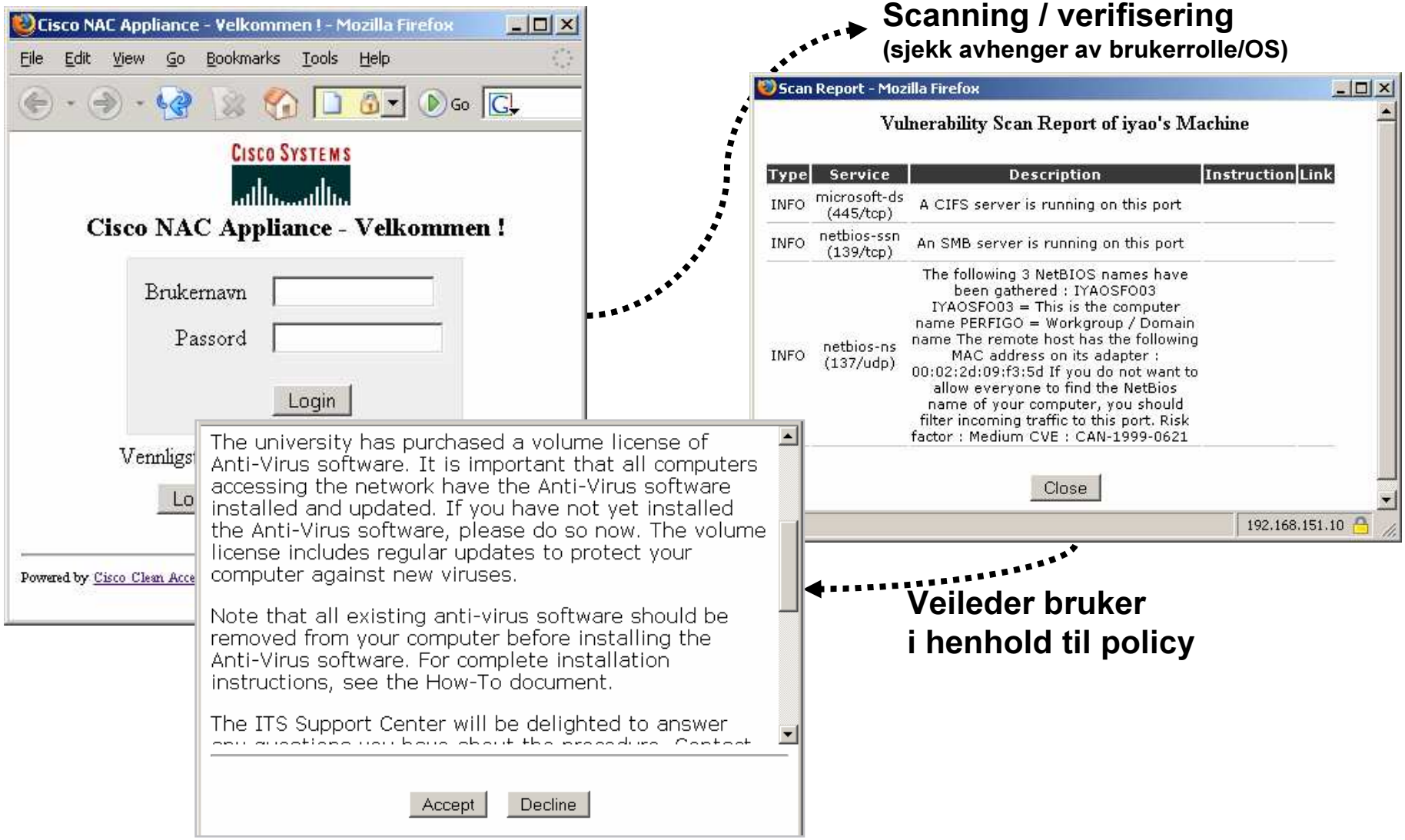
Scanning/verifisering
(sjekk avhenger av brukerrolle/OS)

Utenfor policy

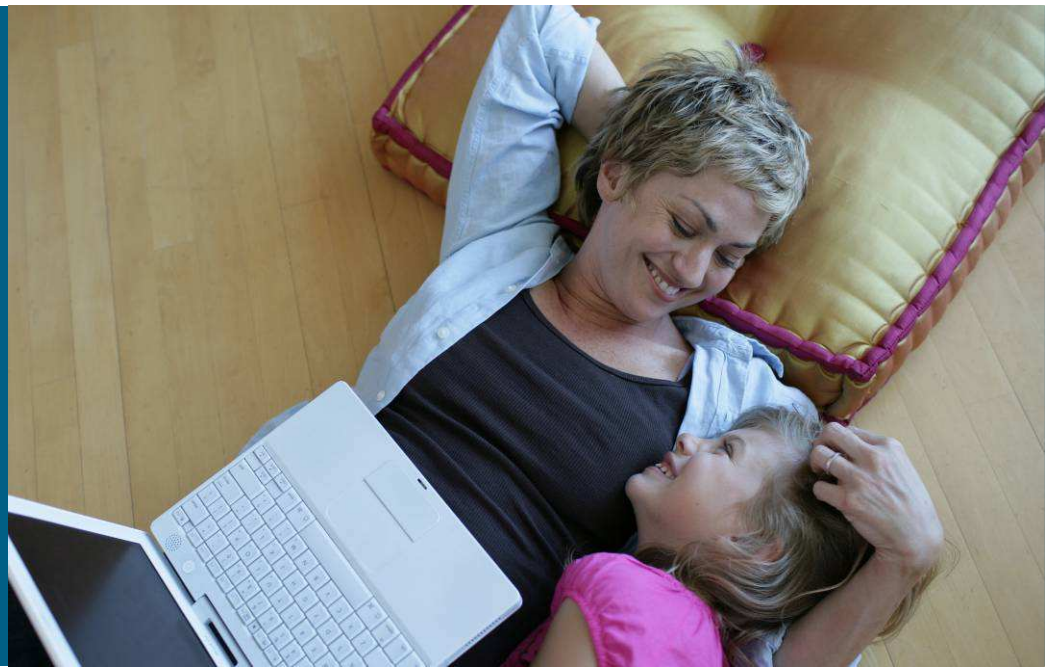
Veileder bruker



Eksempel på brukeropplevelse - nettleser



Hva er viktig med en NAC løsning ?



Forhåndsdefinerte regler

Kritiske Windows oppdateringer

Windows XP, Windows 2000, Windows 98, Windows ME

Antivirus oppdateringer

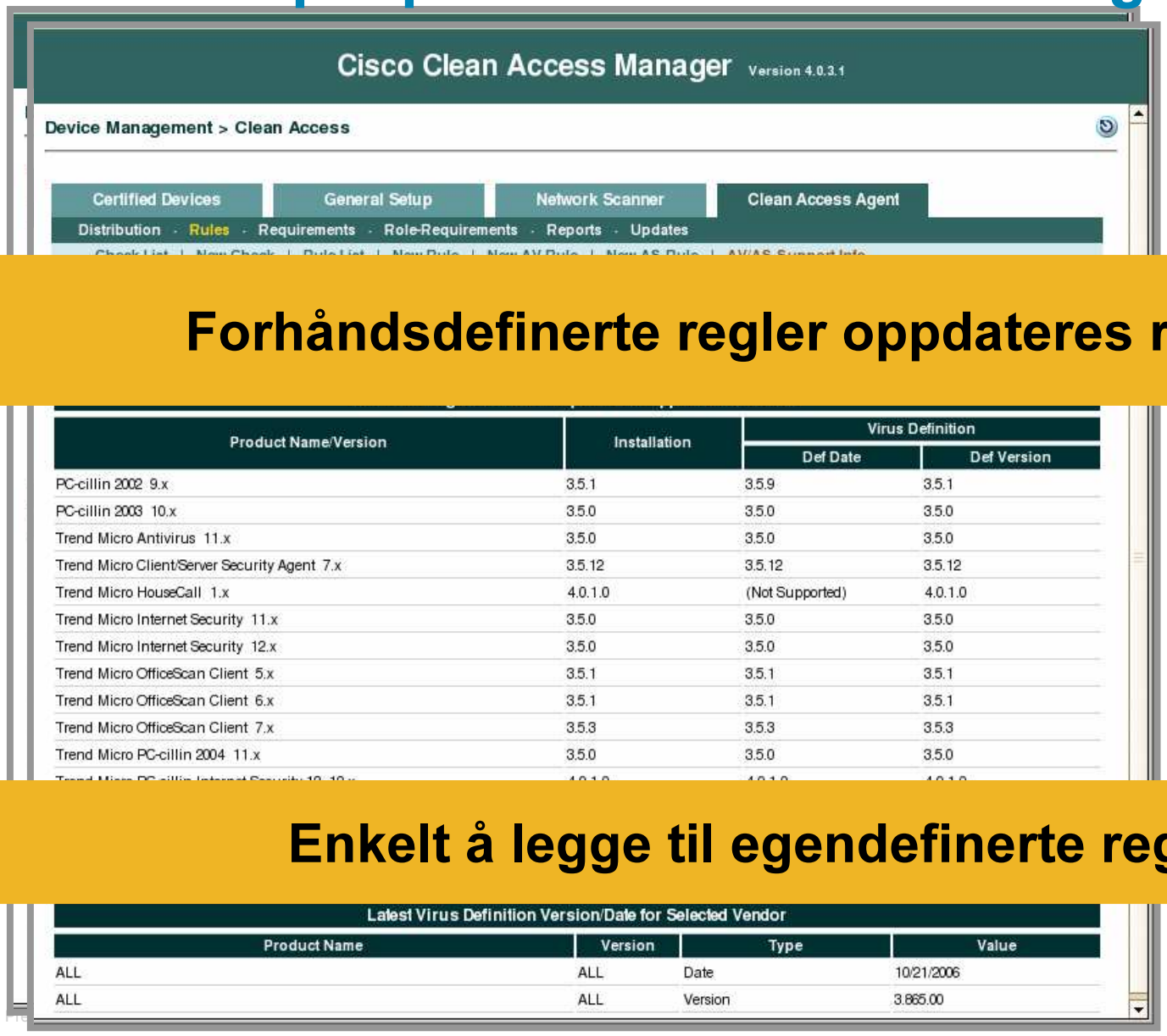
Anti-spionvare oppdateringer

3'dje parts oppdateringer

Forhåndsdefinerte regler

NAC Appliance støtter 350+ applikasjoner fra blant annet følgende leverandører:

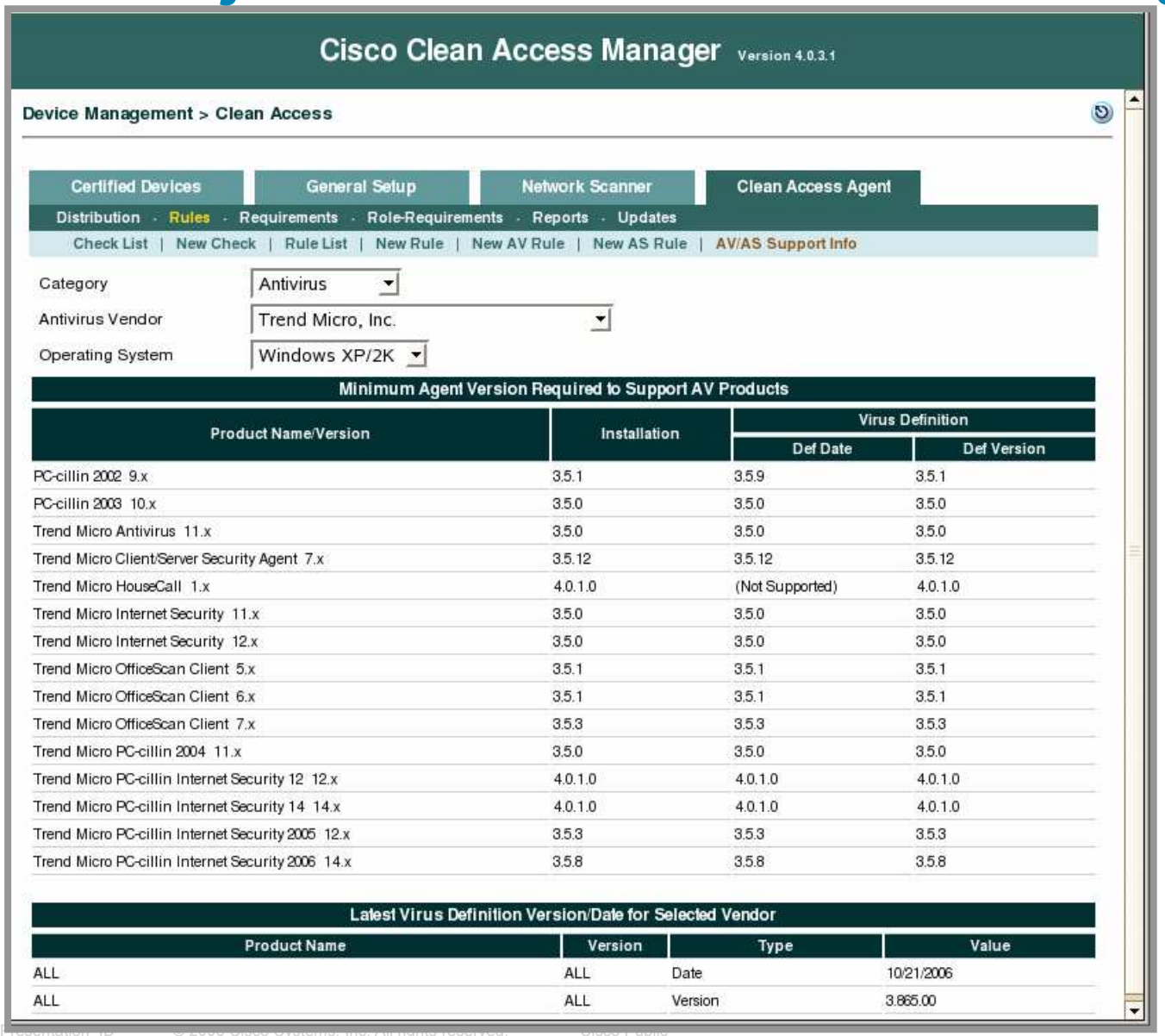
Eksempel på forhåndsdefinerte regler



Forhåndsdefinerte regler oppdateres regelmessig

Enkelt å legge til egendefinerte regler

Eksempel:
Versjon/dato i forhåndsdefinerte regler



Cisco Clean Access Manager Version 4.0.3.1

Device Management > Clean Access

Certified Devices | General Setup | Network Scanner | Clean Access Agent

Distribution · Rules · Requirements · Role-Requirements · Reports · Updates

Check List | New Check | Rule List | New Rule | New AV Rule | New AS Rule | AV/AS Support Info

Category: Antivirus

Antivirus Vendor: Trend Micro, Inc.

Operating System: Windows XP/2K

Minimum Agent Version Required to Support AV Products

Product Name/Version	Installation	Virus Definition	
		Def Date	Def Version
PC-cillin 2002 9.x	3.5.1	3.5.9	3.5.1
PC-cillin 2003 10.x	3.5.0	3.5.0	3.5.0
Trend Micro Antivirus 11.x	3.5.0	3.5.0	3.5.0
Trend Micro Client/Server Security Agent 7.x	3.5.12	3.5.12	3.5.12
Trend Micro HouseCall 1.x	4.0.1.0	(Not Supported)	4.0.1.0
Trend Micro Internet Security 11.x	3.5.0	3.5.0	3.5.0
Trend Micro Internet Security 12.x	3.5.0	3.5.0	3.5.0
Trend Micro OfficeScan Client 5.x	3.5.1	3.5.1	3.5.1
Trend Micro OfficeScan Client 6.x	3.5.1	3.5.1	3.5.1
Trend Micro OfficeScan Client 7.x	3.5.3	3.5.3	3.5.3
Trend Micro PC-cillin 2004 11.x	3.5.0	3.5.0	3.5.0
Trend Micro PC-cillin Internet Security 12 12.x	4.0.1.0	4.0.1.0	4.0.1.0
Trend Micro PC-cillin Internet Security 14 14.x	4.0.1.0	4.0.1.0	4.0.1.0
Trend Micro PC-cillin Internet Security 2005 12.x	3.5.3	3.5.3	3.5.3
Trend Micro PC-cillin Internet Security 2006 14.x	3.5.8	3.5.8	3.5.8

Latest Virus Definition Version/Date for Selected Vendor

Product Name	Version	Type	Value
ALL	ALL	Date	10/21/2006
ALL	ALL	Version	3.865.00

Fordeler med en Cisco NAC løsning

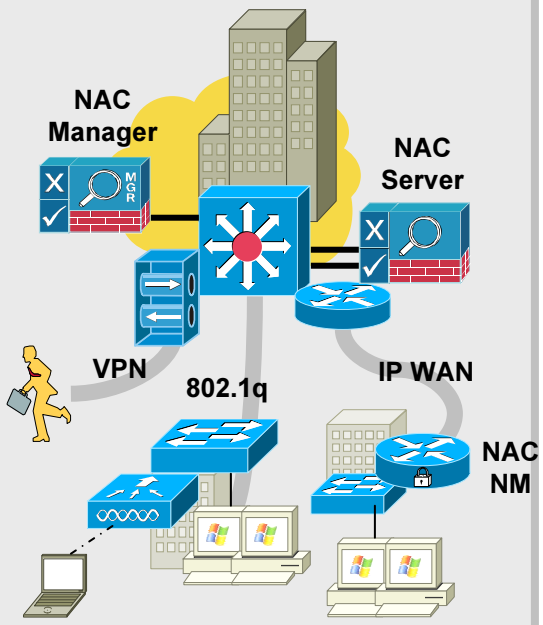
- Gir brukeren anledning til å oppdatere sitt system i henhold til policy
- Sentralisert adminstrasjon og vedlikehold av policy
- Forhåndsdefinerte regler reduserer kostnaden ved “dag 2” adminstrasjon og vedlikehold
- Egendefinerte regler gir mulighet til å stille krav til hvilken som helst applikasjon
- Reduserer belastning på IT-avdeling / brukerstøtte

Løsningsalternativer

NAC løsningsalternativer

Tilgjengelig

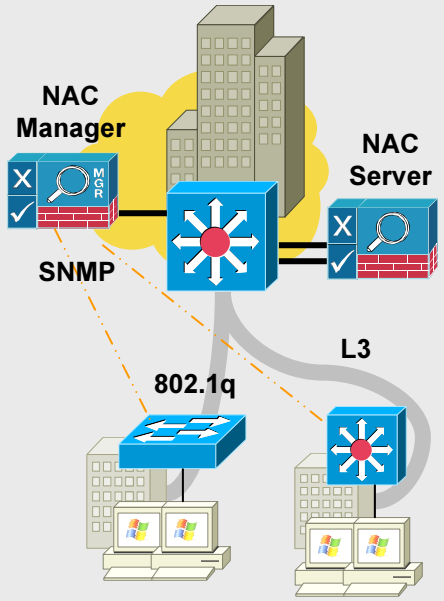
NAC In-Band



- Installer & kjør (basic)
- VPN, WLAN, campus & Remote Access
- Støtter også ikke-Cisco enheter
- Håndheving via appliance

Tilgjengelig

NAC Out-of-Band

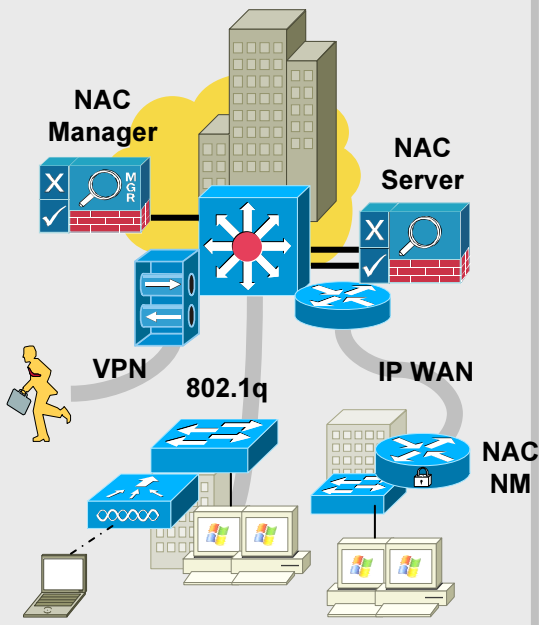


- Installer & kjør (intermediate)
- Campus LANS (L2, L3)
- Bygger på Cisco infrastruktur
- SNMP som kontrollplan
- Håndheving via switch eller appliance

NAC løsningsalternativer

Tilgjengelig

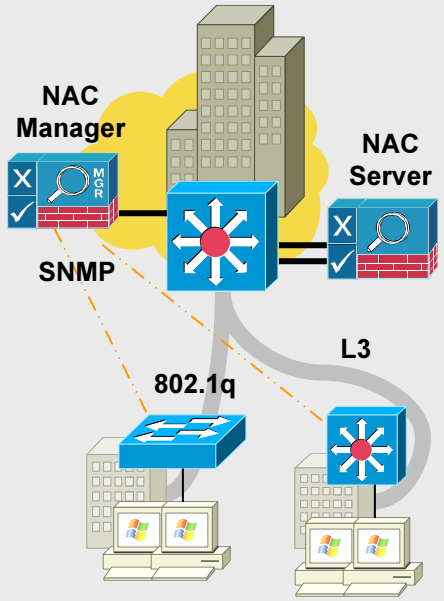
NAC In-Band



- Installer & kjør (basic)
- VPN, WLAN, campus & Remote Access
- Støtter også ikke-Cisco enheter
- Håndheving via appliance

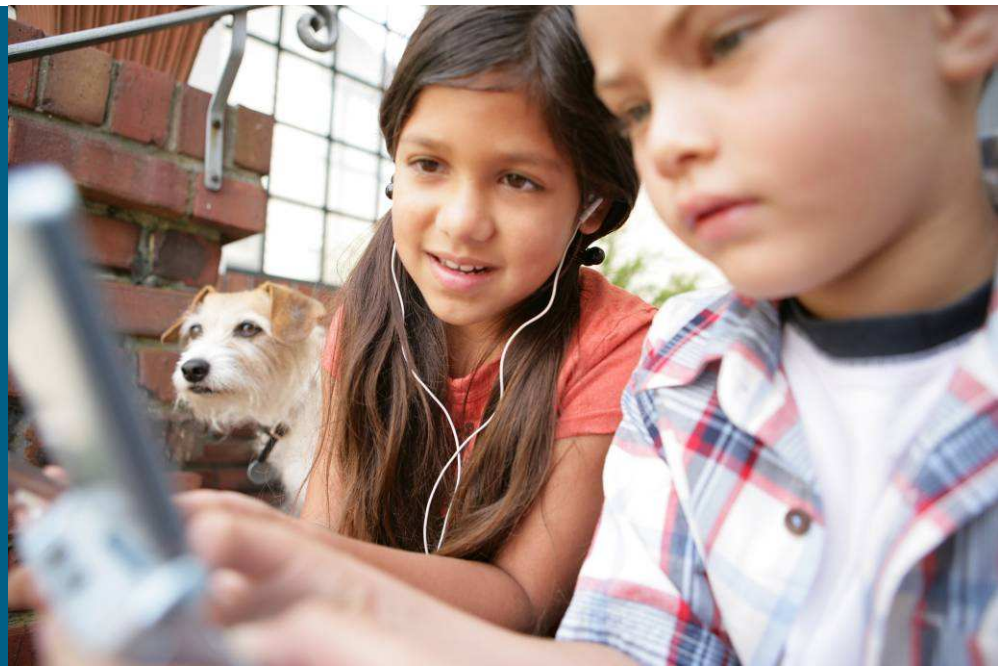
Tilgjengelig

NAC Out-of-Band



- Installer & kjør (intermediate)
- Campus LANS (L2, L3)
- Bygger på Cisco infrastruktur
- SNMP som kontrollplan
- Håndheving via switch eller appliance

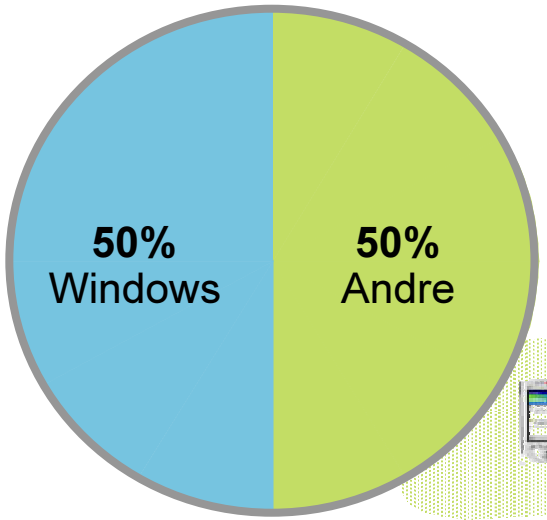
Cisco NAC Profiler



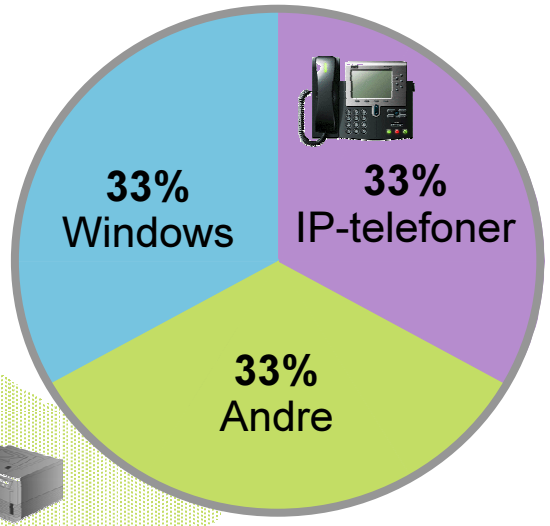
Utfordring: Hva med andre nettverksenheter

Det er en myriade av ulike enheter tilkoblet et nettverk.
Mange er noe helt annet enn en PC med Windows.
De fleste er udokumenterte … (ref. DHCP).

Organisasjoner uten IP-telefoni
Fordeling av endepunkter



Organisasjoner med IP-telefoni
Fordeling av endepunkter



Eksempel på nettverksenheter


Skrivere


Faxmaskiner


Video konferanse utstyr


IP-telefoner


HUB'er


IP-kamera


Trådløse aksess-punkter (WLAN)


UPS


Kassaregister


Medisinsk utstyr


Alarmsystemer


Adgangskontroll


Smarthus


RMON-prober


Automater

. . . pluss mange flere.

Traditional Method

- Dedicated full-time employee:
  - Surveys facilities/wiring closets to determine port usage
  - Manual recording process

- Challenges:
  - By the time survey for Wiring Closet F is complete, Wiring Closet A survey is out-of-date
  - Additions, changes, removals require manual interaction = non scalable method
  - Manual method prone to errors

Cisco NAC Profiler: Automatisert oversikt

Cisco NAC Profiler

PCer	Ikke-PCer			
	UPS	Telefon	Skriver	AP

Discovery

Endepunktsprofilering

Identifiserer alle nettverks endepunkt etter type og lokasjon

Vedlikeholder data om endepunkt i sanntid, samler historikk

Monitoring

Overvåker oppførsel

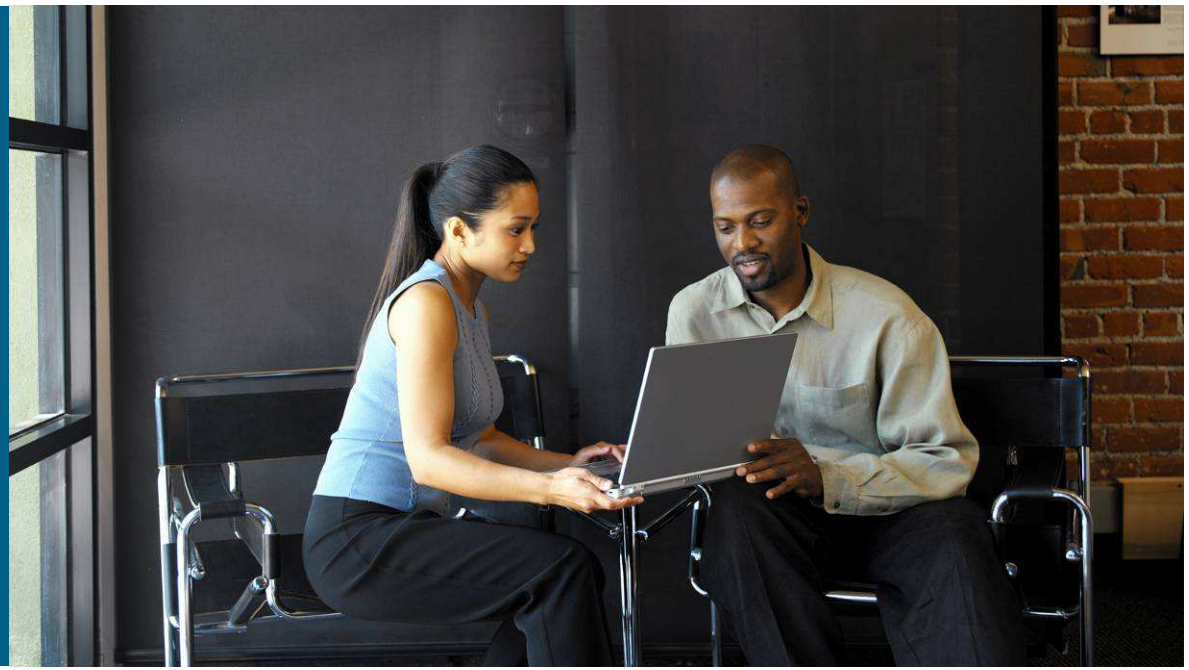
Overvåker tilstanden til alle nettverks endepunkt

Detekterer hendelser som MAC adresse spoofing, port swapping etc.

Automatisert prosess oppdaterer enhets-informasjonen i NAC Manager

Informasjonen går videre til korresponderende NAC policy

NAC Guest Server

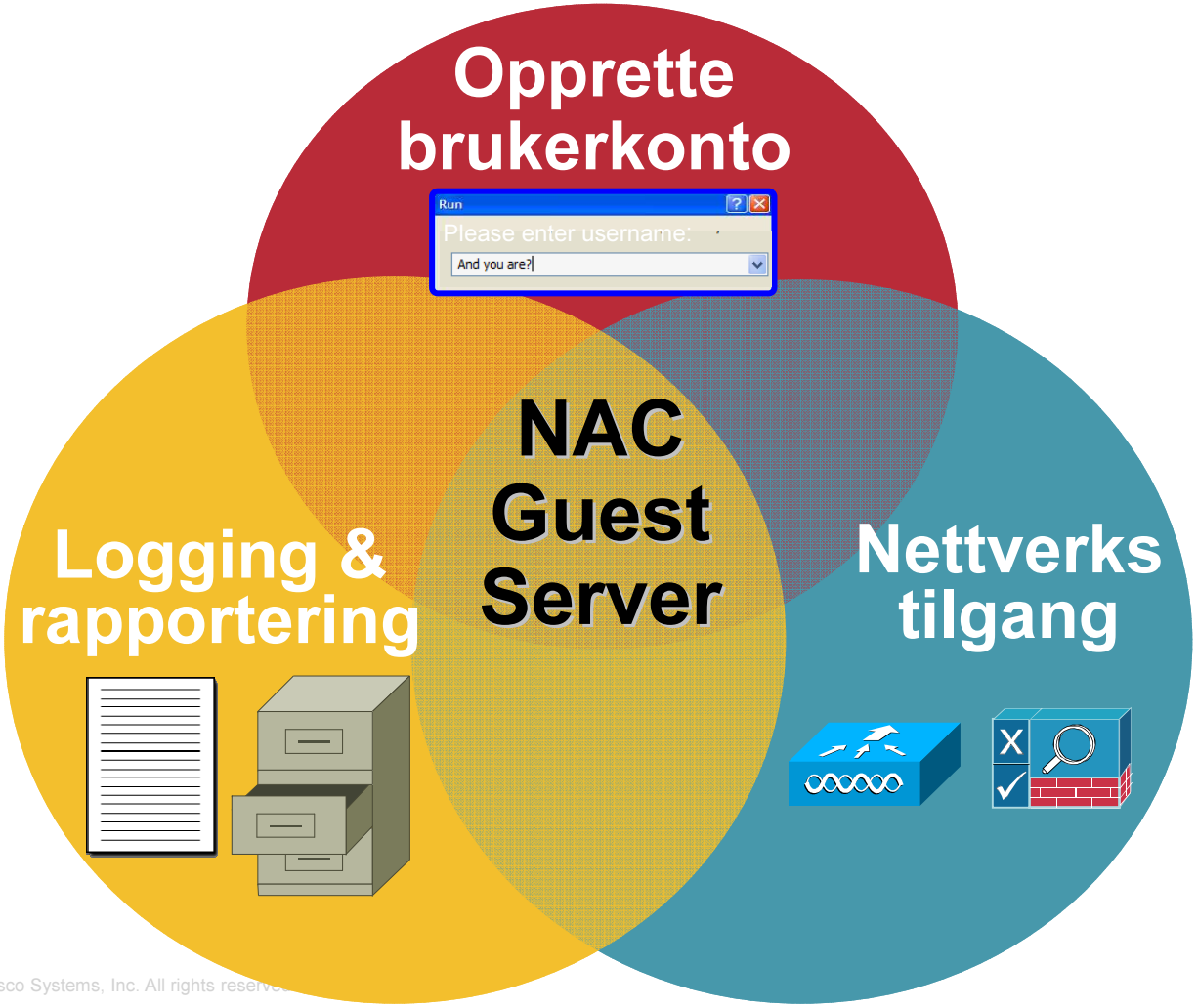


Viktige sider ved en gjesteløsning

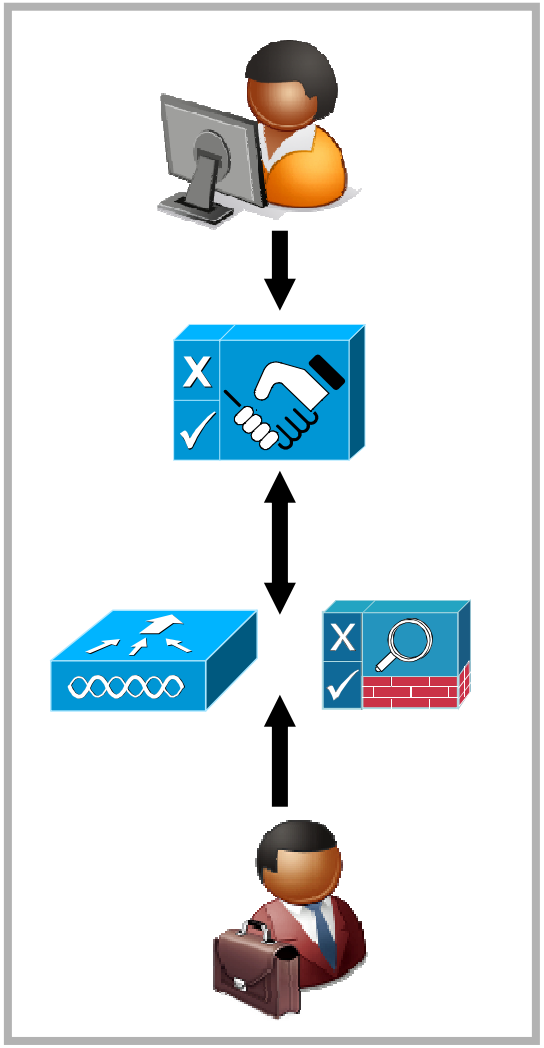
Brukerterskel	Opprette gjestebrukerkonto Resepsjonist, assistent, ansatte
Integrasjon med eksisterende nettverk	Unngå parallell nettverks infrastruktur
Logging og sporbarhet	Hvem gjør hva Hvem har opprettet hvilken konto
Kostnad	Implementasjon Drift

Gjestetilgang

Cisco NAC Guest Server forener gjestetilgangsfunksjoner



Fire nøkkelkomponenter for gjestetilgang



Sponsor

Intern(e) bruker(e) som ønsker å tilby Internett-tilgang til sine gjester

NAC Guest Server

Lar sponsor opprette gjestebruker konto, forbereder gjestekonto på nettverksenhet, logger bruk

Nettverksenhet

Redirigerer web, autentiserer og gir nettverkstilgang Wireless LAN Controller (WLC) eller NAC Appliance

Gjest

Gjestebruker som trenger nettverkstilgang (vanligvis kun Internett, kan være mer)

Oppsummering

Oppsummering

- Husk de tre skjoldene:
- Implementer NAC

  NAC = håndheving av policy

- Kommentar fra Gartner Group:

  Strategic Planning Assumption:

  Through 2008, enterprises that do not implement network access control (NAC) policies on network connections will experience 200 percent more network downtime than those that do (0.7 probability)

  Source: www.gartner.com


CISCO