ePO 4.5 og Anti-Virus/Anti-Spam

Peter Helms
Senior Security Engineer

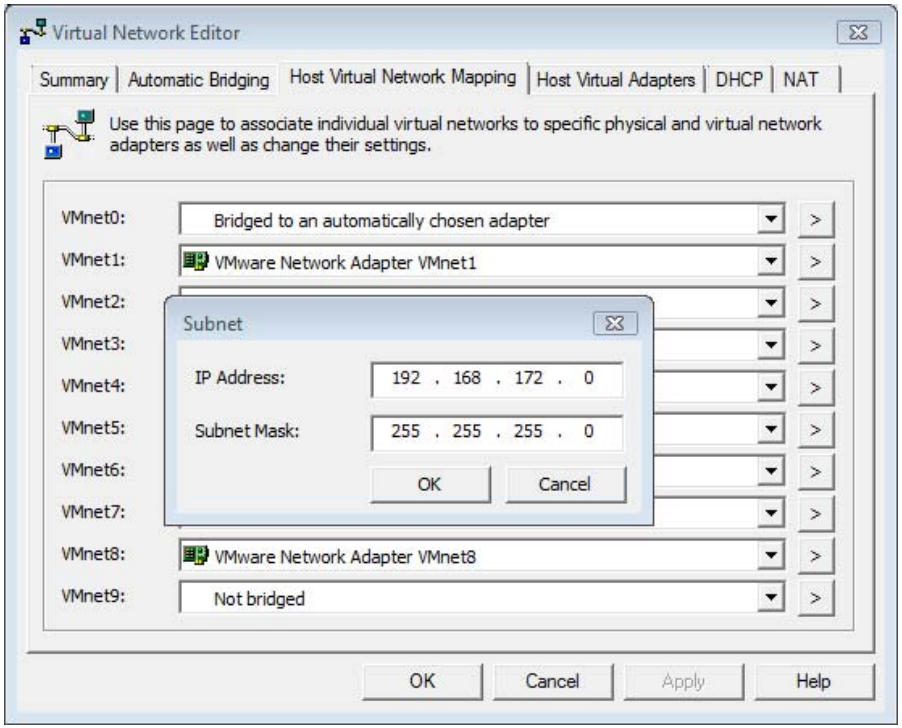
September 15, 2009

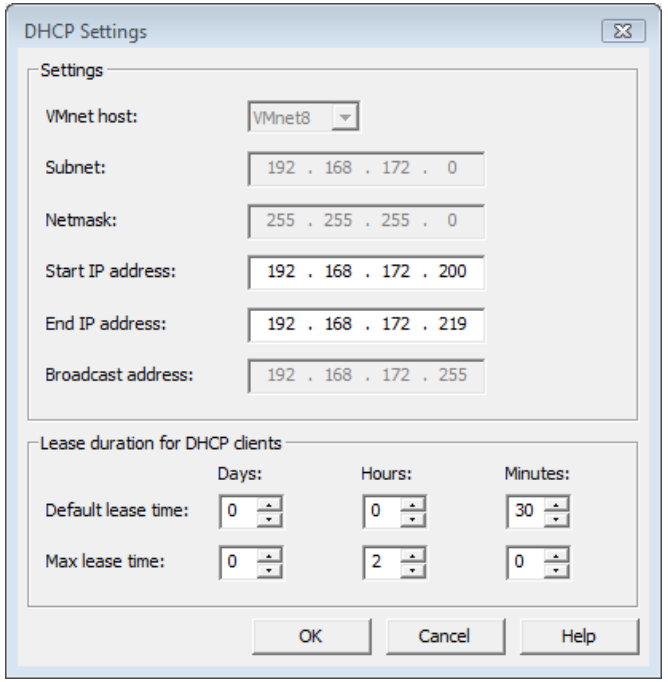
Agenda

- McAfee ePolicy Orchestrator (ePO) – vision - funktionsmåde
- Opsætning af ePO
  - User name: admin
  - Password: mcafee
- Udrulning af McAfee Agent
- Udrulning af Anti-virus og Anti-spam produkter

Vmware konfiguration

- Tilretning i VMvares netværksopsætning til VM-image
  - ”Edit->Virtual Network Editor->Host Virtual Network Mapping”
    - Vmware Network Adapter VMnet8->Subnet: 192.168.172.0 (Apply)
    - DHCP->Start IP & End IP address: 192.168.172.200-219





ePO 4.5

- Installation
  - (er foretaget på Vmware image)
- ePO overview

- Opsætning
  - Menu->Configuration->Server Settings
    - Ports
    - Email Server
    - Printing and Exporting (A4 paper)
  - Menu->Automation->Server Tasks
    - Update Maser Repository (selected packages only, every 3-4 hours)
  - Downloads med Grant Number
    - Tjek om ny Agent, ny Anti-Virus el. patches til samme, ny ePO el. patches til samme

ePO 4.5

- Initial tasks
  - Set up System Tree (groups, sub-groups)
  - Install new McAfee Agent (Menu->Software->Master Repository->Check In Package)
  - Policy Catalog
    - McAfee Agent Settings
      - Enable remote access to log
  - Import Systems (manual, AD sync etc)
  - Deploy Agent
    - System Tree->(group name in System tree)->Client Tasks
    - New Client Tasks
      - Product Update (logon) – at logon
      - Product Update (daily) - daily

ePO 4.5

- Prepare Deployment
  - Check in software (AV, Anti-Spam)
    - VSE870LMLRP1.Zip
    - ASEM870LALL.zip
    - VSE87HF464768.zip (hotfix til AV 8.7i patch 1)
  - Install extensions
    - VIRUSCAN8700.zip (AV)
    - VSEMAS870000.zip (AV)
    - VIRUSCANREPORTS.zip (Anti-Spam)

    - Bemærk at extensions og hot-fixes ligger pakket i de downloadede zip-filer (eks. VSE870LMLRP1.Zip og ASEM870LALL.zip)

ePO 4.5

- Deploy software
  - Policy Catalog->VirusScan Enterprise 8.7.0
    - On-Access General Policies
      - Herustic network check: ”very low” (Workstation and Server)
        - » Anvender McAfees Artemis teknologi (se links)
  - Deploy software
    - System Tree->(group name in System tree)->Client Tasks
      - Install McAfee Agent - Run immediately
      - Install AV og Anti-Spam - Run immediately
  - Deploy Rogue Sensor
    - Eks. på Windows DHCP server. Kan med fordel installeres på een server/arbejdsstation i hvert fysisk adskilte netværkssegment
    - System Tree->Systems->(Vælg System)->Actions knappen->Rogue Sensor->Install Rogue Sensor

Windows 7 og Windows Server 2008 R2 info

- Følgende software pakker vil have Windows 7 og Windows Server 2008 R2 kompabilitiet, men er d.d. (pr. 10.09.2009) ikke frigivet
  - McAfee Agent 4.0 patch 3
  - McAfee Agent 4.5
  - McAfee VSE (anti-virus) 8.7i patch 2
  - McAfee MSAE (anti-spyware) 8.7 (patch 1?)

Nyttige McAfee links

- Download Software (anvend Grant Number)
  - https://secure.nai.com/apps/downloads/my_products/login.asp?region=us&segment=enterprise
- Artemis
  - http://www.mcafee.com/us/enterprise/products/artemis_technology/index.html
- McAfee Security Innovation Alliance (SIA)
  - http://www.mcafee.com/sia
- End-of-Life information
  - http://www.mcafee.com/us/products/mcafee/end_of_life.htm
- Submission of Anti-virus sample
  - http://vil.nai.com/vil/submit-sample.aspx


McAfee®