Tietoturva F-Secure : Palvelin ja hallintakonsoli

Asenna palvelimeen hallintaa varten F-Secure Policy Manager Server ja työasemaan F-Secure Policy Manager Console:

1. Hallintapalvelimen työasemia palvelevaksi portiksi asetetaan 81 oletusarvon sijasta. Hallintakonsolin palvelinportiksi asetetaan 8090 ja webraportoinnin palvelinportiksi 8091

2. Aseta työasemien pollausväliksi 30 sekuntia oletuksen sijaan, muista asettaa palvelimen osoite keskitettyyn hallintaan.

3. Luo Policy Manageriin työasemia ja palvelimia varten omat kansiot hallintapuuhun.

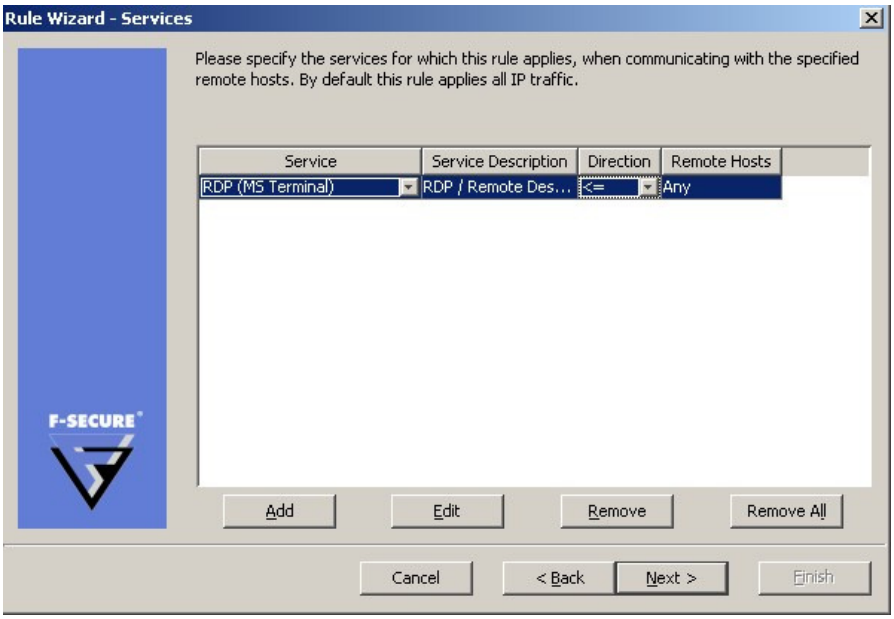
4. Siirrä hallittavat tietokoneet oikeisiin kansioihin.

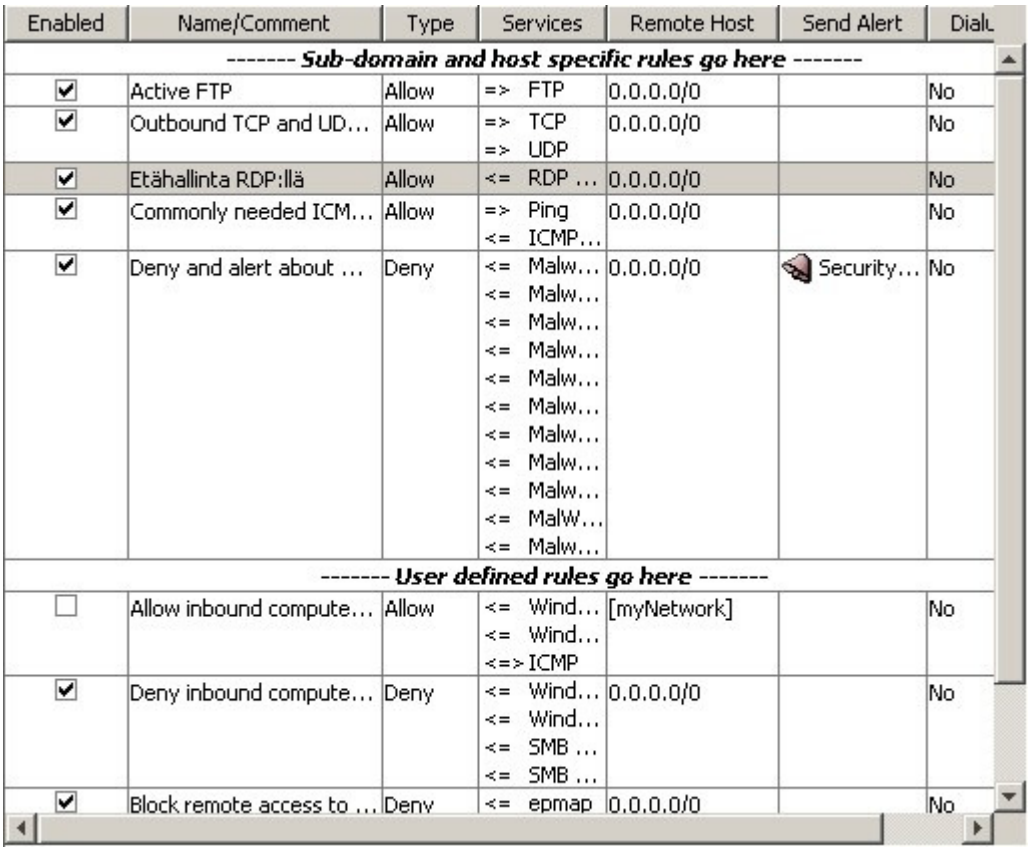
5. Jaa policyt

Asenna järjestelmä siten, että palvelin hakee virus- ja vakoiluohjelmatunnisteet automaattisesti ja jakaa ne kaikille koneille.

Tee seuraavat määritykset keskitetyn hallinnan avulla:

1. Työasemiin voi ottaa yhteyttä etätyöpöytäohjelmalla (rdp)
- vinkki: Firewall Services sisältää valmiin määrityksen rdp:lle





Enabled	Name/Comment	Type	Services	Remote Host	Send Alert	Dialu
------- *Sub-domain and host specific rules go here* -------						
☑	Active FTP	Allow	=> FTP	0.0.0.0/0		No
☑	Outbound TCP and UD...	Allow	=> TCP => UDP	0.0.0.0/0		No
☑	Etähallinta RDP:llä	Allow	<= RDP ...	0.0.0.0/0		No
☑	Commonly needed ICM...	Allow	=> Ping <= ICMP...	0.0.0.0/0		No
☑	Deny and alert about ...	Deny	<= Malw... <= Malw... <= Malw... <= Malw... <= Malw... <= Malw... <= Malw... <= Malw... <= Malw... <= MalW... <= Malw...	0.0.0.0/0	Security...	No
------- *User defined rules go here* -------						
☐	Allow inbound compute...	Allow	<= Wind... <= Wind... <=> ICMP	[myNetwork]		No
☑	Deny inbound compute...	Deny	<= Wind... <= Wind... <= SMB ... <= SMB ...	0.0.0.0/0		No
☑	Block remote access to ...	Deny	<= epmap	0.0.0.0/0		No

2. Työasemien pitää voida jakaa levyä ja kirjoittimia ollessaan paikallisverkossa

3. Työasemissa otetaan käyttöön verkkokaranteeni, jos työasemien virustunnisteet ovat 10 päivää vanhempia.

4. Käyttäjä ei saa kytkeä reaaliaikaista virustorjuntaa ja palomuuria pois päältä.

5. Http-liikenteen skannaus on oltava päällä kaikissa työasemissa.

6. Jaa policyt

Taitaja 2007 JOENSUU

Työasema

Työasemaan tulee asentaa F-Secure Client Security. Yrityksen mikrotuki haluaa, että ohjelmisto asennetaan etäkäytöllä (Push-install) työasemalle.
- vinkki: mitää pitää XP-työasemassa tehdä, että rpc-käsky pääsee läpi?

Mene selaimella osoitteeseen eicar.org ja lataa sieltä testitiedosto eicar.com.

Tarkastele työaseman selaimen avulla hallintapalvelimen tilaa, jätä selain näkyviin.