

1. GUI-clientin asennus

GUI-client saadaan ladattua osoitteesta <https://partnergate.sonera.com/firewall.html>
Asennusohjeet löytyvät myös osoitteesta <https://partnergate.sonera.com/firewall.html>

2. GUI-clienttiin kirjautuminen ja näkymä sovellushallintaan

Määritelkää GUI-kirjautumisikkunaan teille toimituksen aikana kerrottu GUI-hallinnan IP-osoite sekä käyttäjätunnus ja salasana.



Check Point
SmartDashboard®
R75.40VS

Use certificate

Username

Password

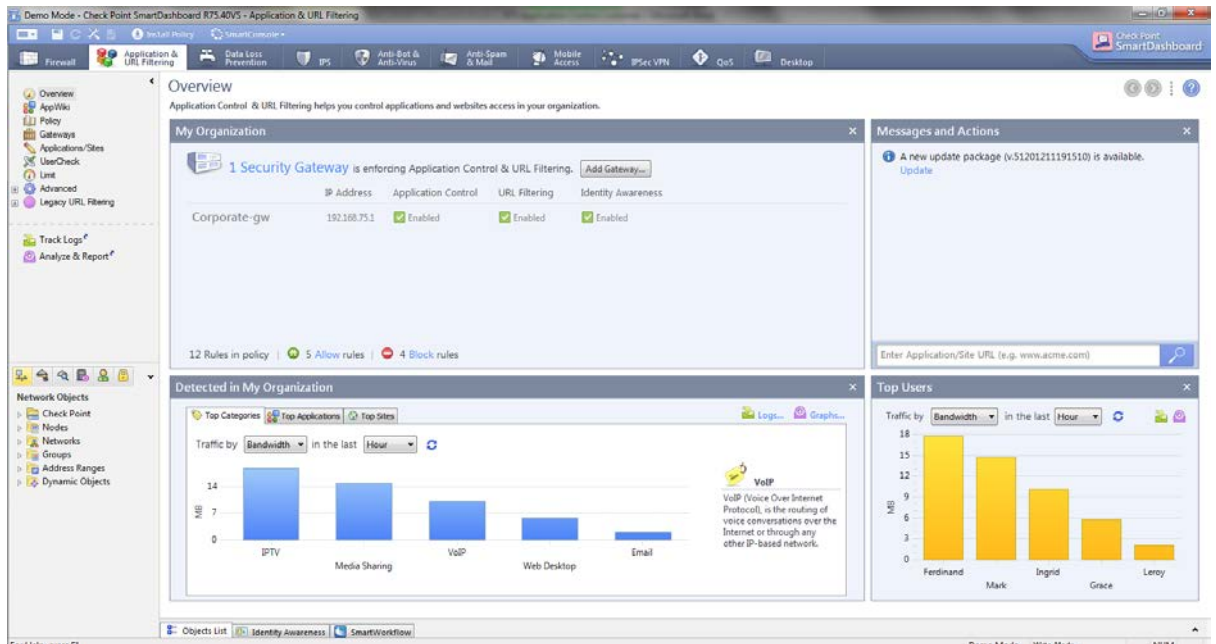
1.1.1.1

Read only Demo mode

Login →

Add session description (optional)

Tämän jälkeen teille avautuu palomuurin yleisnäkymä. Valitkaa ylälaidan välilehdeltä **Application & URL-Filtering** välilehti (kuva 1).



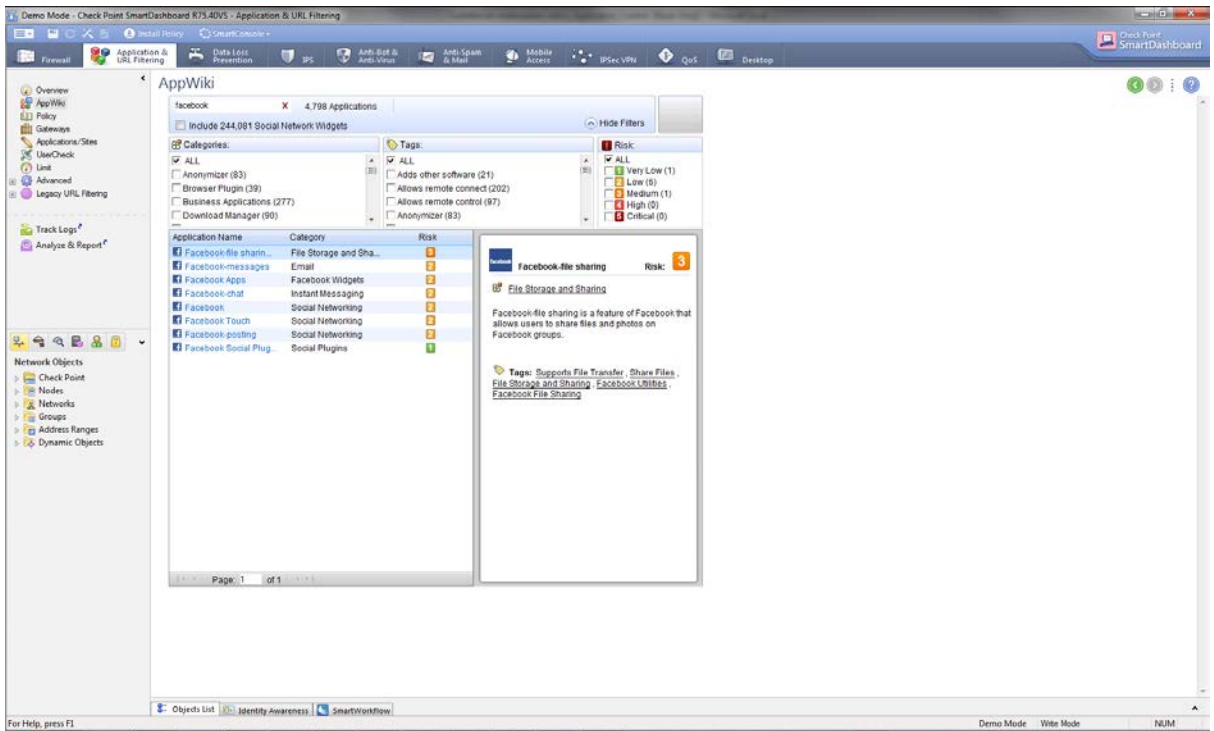
1. Yleiskuva sovellushallinta välilehdeltä

Sovellushallinnan avulla on mahdollista

- Tunnistaa, sallia tai estää tuhansia erilaisia sovelluksia
- Sovellukset sisältää
 - o Ohjelmat joita on asennettu päätelaitteeseen, esim. Microsoft Office
 - o Ohjelmat joita käytetään Internetselaimella, esim. Google chat
 - o Sosiaalisen median widgetit, esim. Farmville Facebookissa
- Jokainen sovellus on kategorioitu käyttötarkoituksen mukaan
- Sovellus voi pitää sisällään useita tageja: Gmail pitää sisällään esim. seuraavia tageja: tiedostojen siirto, mailin lähetys, pika chattaus jne.
- AppWiki antaa lyhyen kuvauksen sovelluksesta, riskitasosta ja kategoriasta ja muita ominaisuuksia

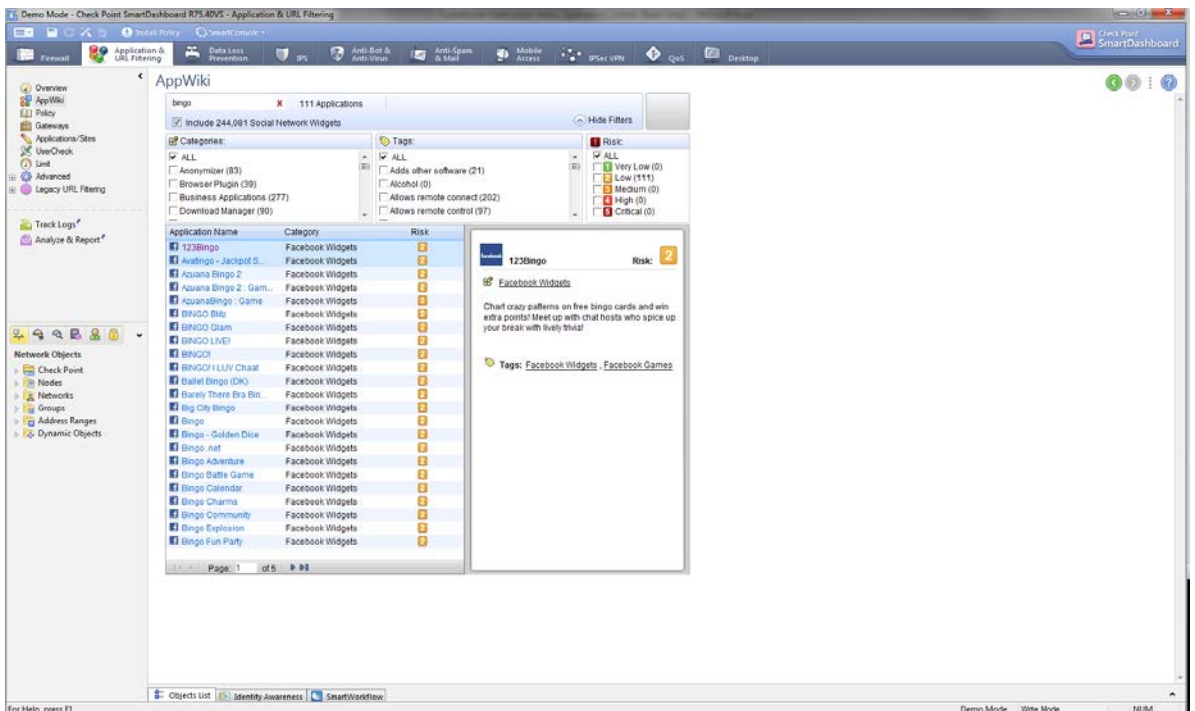
3. Uuden sovellushallinta säännön määrittäminen

Käytä AppWikiä löytääksesi sovelluksen, esimerkiksi Facebook-sovelluksen (kuva 2).



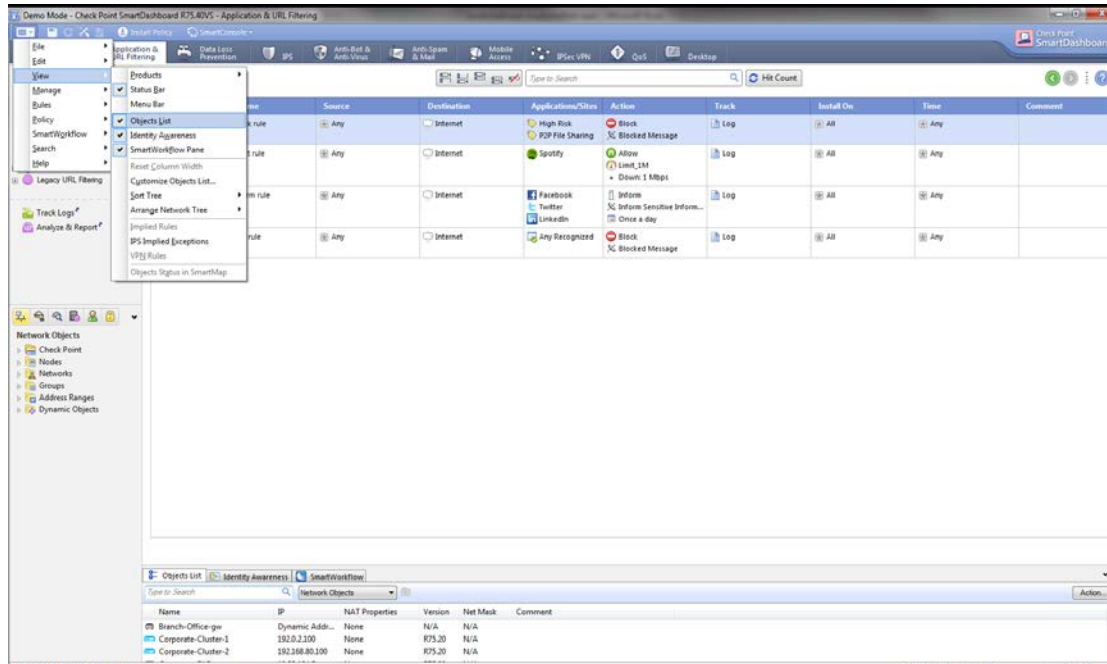
2. Sovelluksen hakeminen

Käytä AppWikiä etsiessä sovelluksen widgettiä sääntöön, alla olevassa esimerkissä Bingo widgettiä (kuva 3). Huomaa, että Social Network Widgets on valittu hakuun.



3. Widgetin hakeminen

Sovellushallinnan säännöt saadaan näkyään vasemmasta laidasta valitsemalla **Policy** (kuva 4). Jos haluat nähdä kaikki lähde- ja kohdepuolelle valittavat objektit valitse ylälaidasta **View** (kuva 4) valinta ja täppää **Object List** valinta. Objektit näkyvät nyt alalaidan Object List välilehdellä.



4. Säännöstönäkymä

Alla (Kuva 5) on ns. default sääntö, joka kieltää organisaation verkosta kaiken ulospäin menevän korkean riskin ja P2P (vertaisverkon) liikenteen käytön sekä ilmoittaa siitä käyttäjä. Lisäksi liikenne lokitetaan.

No.	Hits	Name	Source	Destination	Applications/Sites	Action	Track
1	7M	Default rule	Any	Internet	High Risk P2P File Sharing	Block Blocked Message	Log

5. Default sääntö

Sääntöjen sisältö esim. säännössä 1:

- **Source** - Voidaan käyttää kaikkia objekti listassa olevia objekteja.
- **Destination** - Voidaan käyttää kaikkia objekti listassa olevia objekteja.
- **Application** - Sovellus jonka sääntö tarkistaa
- **Action** - Tässä kiellä ja informoi. Voi olla salli (Allow), informoi (Inform), kysy (Ask), rajoita (Limit).
- **Track** – Lokitus päälle tai pois
- Jos sääntö halutaan tarkemmin määritellä, niin tilataan asiantuntijatyönä, jolloin laskutus Surfmanager asiantuntija laskutuksen mukaan.

Kuvassa 6 on rajoitettu organisaation verkosta ulospäin menevä Spotify sovelluksen liikenteen kaista 1 Megabittiin sekunnissa. Lisäksi liikenne lokitetaan. Kaistaa voidaan määritellä tapauskohtaisesti.

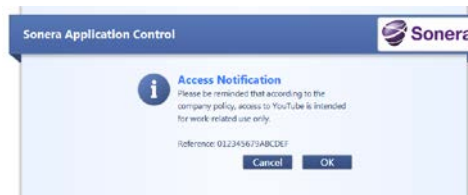
2	1M	Limit rule	Any	Internet	Spotify	Allow Download_1Mb... Down: 1 Mbps	Log
---	----	------------	-----	----------	---------	--	-----

6. Kaistan rajoitus sääntö

Kuvassa 7 sovellus sääntö, joka sallii organisaation verkosta Facebook-, Twitter ja LinkedIn sovellusten käytön, mutta ilmoittaa siitä käyttäjää kerran päivässä. Tiedonanto ikkuna käyttäjälle kuvassa 8, ilmoitusta voidaan kustomoida.

3	91K	Application control	Any	Internet	Facebook Twitter LinkedIn	Inform Access Notificati... Once a day	Log
---	-----	---------------------	-----	----------	---------------------------------	--	-----

7. Sovellushallinta sääntö



8. Tiedonanto ilmoitus

Kuvassa 9 on kuvattu sääntö joka kieltää kaiken muun organisaation verkosta ulospäin lähtevän liikenteen ja antaa siitä käyttäjälle ilmoituksen. Lisäksi liikenne lokitetaan. Tämä sääntö oletuksena viimeisenä sääntönä.

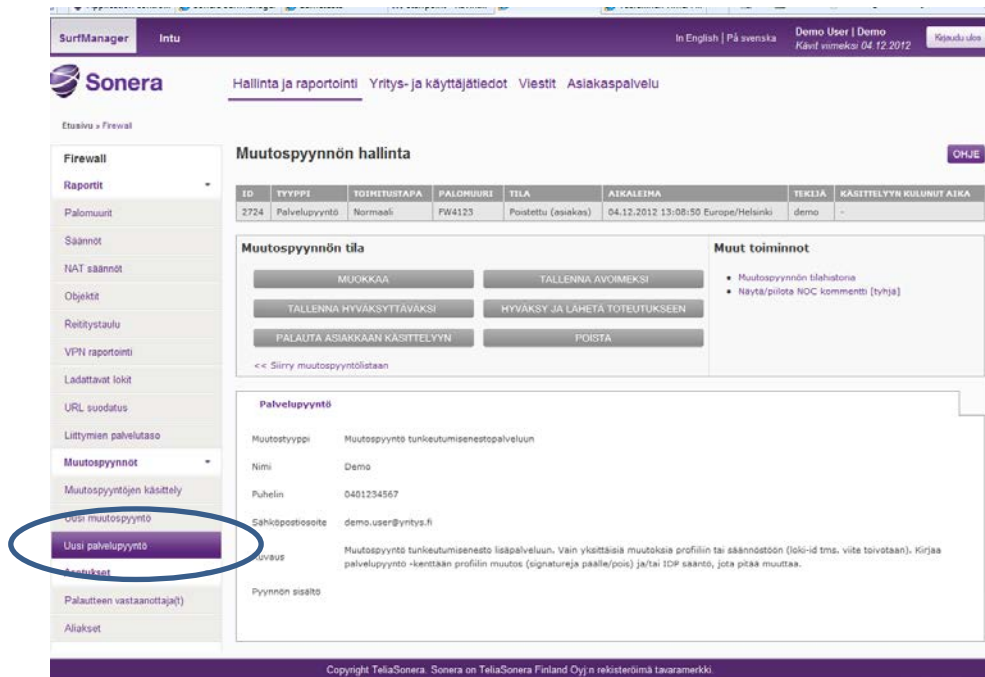
4	108	Block rule	Any	Internet	Any Recognized	Block Blocked Message	Log
---	-----	------------	-----	----------	----------------	--------------------------	-----

9. Kaiken muun kieltävä ja lokittava sääntö

4. Sovellushallintasäännön tilaus

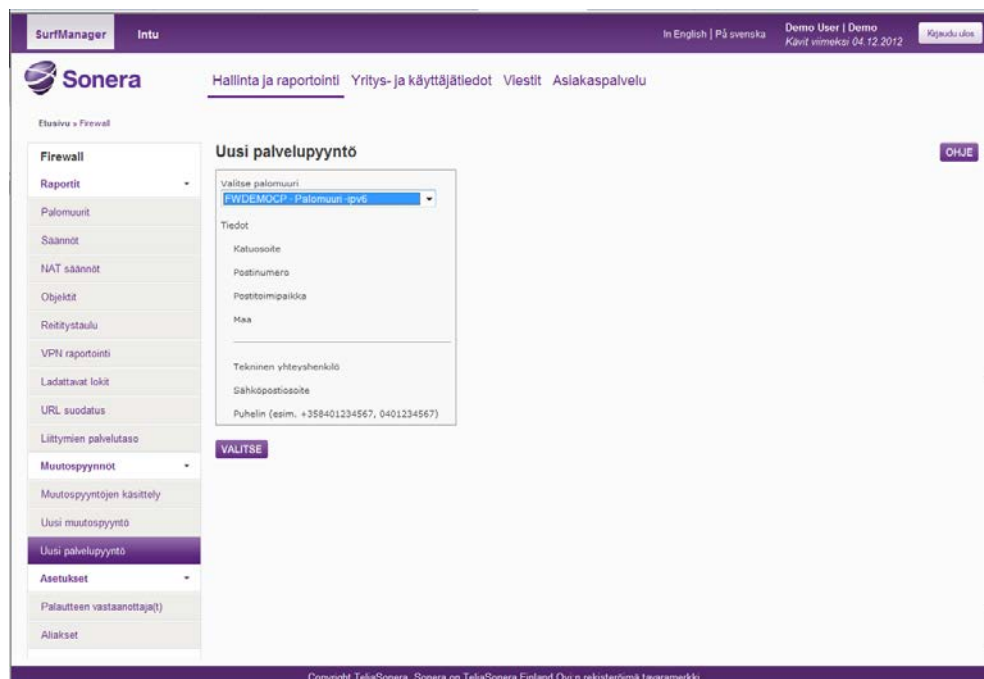
Sovellushallinta säännöt tilataan Surfmanagerilla, joka löytyy osoitteesta <https://surfmanager.sonera.com/>

Sääntöjen tilaus aloitetaan valitsemalla SM/C:n Firewall näkymästä **Uusi palvelupyyntö** (kuva 10).



10. Valitaan uusi palvelupyyntö.

Tämän jälkeen valitaan muuri johon sovellushallinta sääntöä ollaan lisäämässä (kuva 11).



11. Valitaan palomuri, johon muutosta ollaan tekemässä.

Muuri valinnan jälkeen valitse **Muokkaa** painike

The screenshot shows the Sonera SurfManager interface. The main content area is titled 'Muutospyynnön hallinta'. At the top, there is a table with the following data:

ID	TYYPPI	TOIMITUSTAPA	PALOMUURI	TIILA	AIKALEIHA	TEKIJÄ	KÄSITTELYYN KULUNUT AIKA
2725	Palvelupyynnö	Normaali	FW4123	Uusi	04.12.2012 13:14:37 Europe/Helsinki	demo	-

Below the table, there is a section 'Muutospyynnön tila' with several buttons: 'MUOKKAA' (circled in blue), 'TALLENNA AVOIMEKSI', 'TALLENNA HYVÄKSYTTÄVÄKSI', 'HYVÄKSY JA LÄHETÄ TOTEUTUKSEEN', 'PALAUTA ASIAKKAAN KÄSITTELYYN', and 'POISTA'. To the right, there is a 'Muut toiminnot' section with a list: 'Muutospyynnön tilahistoria' and 'Näytä/piilota NOC kommentti [tyhjä]'. Below this, there is a 'Palvelupyynnö' section with a text input field.

12. Valitaan Muokkaa

Seuraavaksi valitse **Lisää uusi palvelupyynnö** (kuva 13).

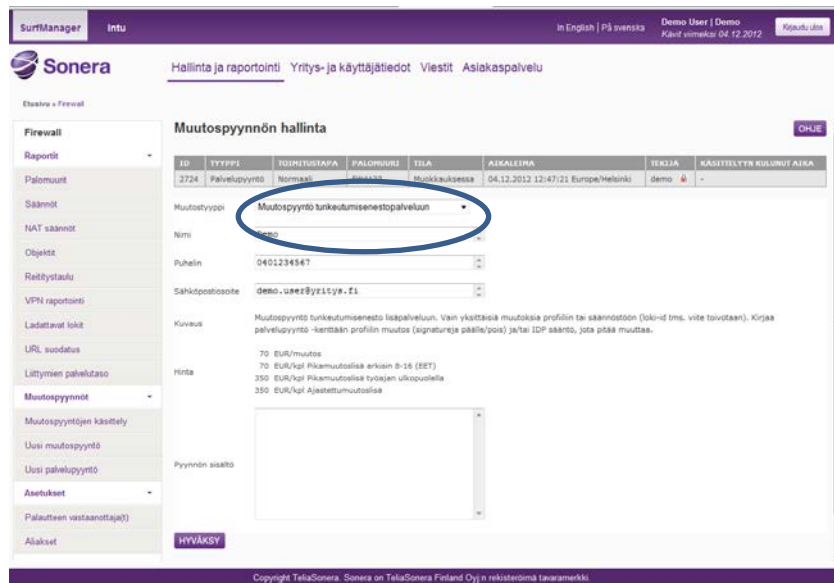
The screenshot shows the Sonera SurfManager interface. The main content area is titled 'Muutospyynnön hallinta'. At the top, there is a table with the following data:

ID	TYYPPI	TOIMITUSTAPA	PALOMUURI	TIILA	AIKALEIHA	TEKIJÄ	KÄSITTELYYN KULUNUT AIKA
2725	Palvelupyynnö	Normaali	FW4123	Muokkauksessa	04.12.2012 13:15:36 Europe/Helsinki	demo	-

Below the table, there is a section 'Muutospyynnön tila' with several buttons: 'MUOKKAA', 'TALLENNA AVOIMEKSI', 'TALLENNA HYVÄKSYTTÄVÄKSI', 'HYVÄKSY JA LÄHETÄ TOTEUTUKSEEN', 'PALAUTA ASIAKKAAN KÄSITTELYYN', and 'POISTA'. To the right, there is a 'Muut toiminnot' section with a list: 'Muutospyynnön tilahistoria' and 'Näytä/piilota NOC kommentti [tyhjä]'. Below this, there is a 'Palvelupyynnö' section with a list: 'Lisää uusi palvelupyynnö' (circled in blue).

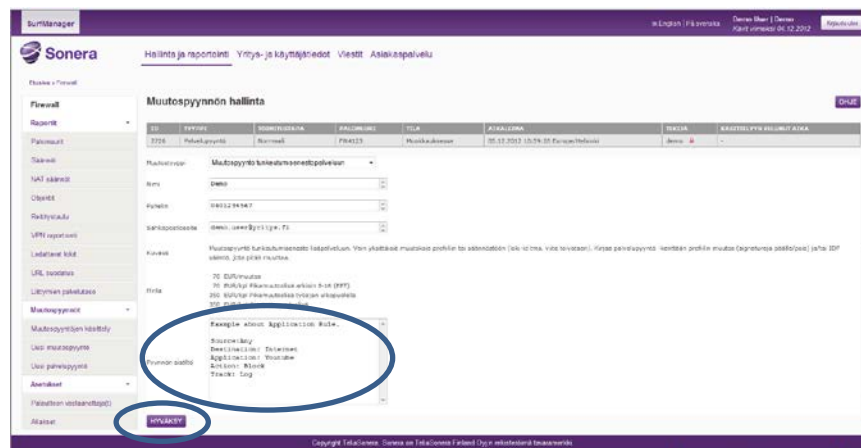
13. Valitaan lisää uusi palvelupyynnö

Valitaan **Muutospyyntö tunkeutumisenestopalveluun** (kuva 14) . HUOM. Tilausta ei laskuteta!



14. Vapaamuotoisen sääntömuutoksen valinta

Pyynnön sisältö kenttään (kuva 15) kerrotaan mitä säännössä tilataan.



15. Pyyntönsisältö

Kuvan 15 Pyyntönsisältö kenttään on määritelty säännön sisältö.

Pyyntönsisältö kentässä pitää olla vähintään alla mainitu asiat:

- Source: Any (Any applies to all traffic from the organization)
- Destination: Internet (Internet applies to all traffic going to the internet or DMZ)
- Application: YouTube (Applications from AppWiki)
- Action: Block/Allow
- Track: Log/None

Jos halutaan tarkemmin määritellä säännön sisältöä, niin laskutus Surfmanager asiantuntija laskutuksen mukaan.

Kun sisältö on kerrottu painetaan **Hyväksy** valintaa, jonka jälkeen sääntö lähtee Soneralle toteutettavaksi.