

## 1 Sonera Palomuri säännöstö- ja reaaliaikainenloki näkymä

Asenna **GUI palomuri säännöstö- ja lokiraportointi sovellus** osoitteesta <https://partnergate.sonera.com/firewall.html>. Ohjeet asennukselle löytyy samasta osoitteesta **GUI asennusohje** pdf-tiedostosta.

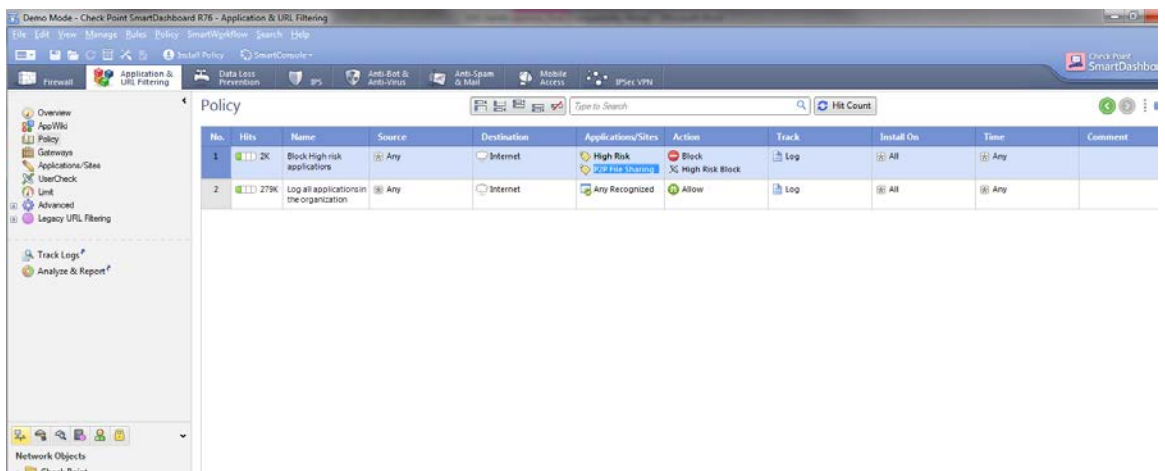
## 2 Säännöstö näkymään kirjautuminen ja käyttö

Kun asennus on suoritettu pääset kirjautumaan säännöstö näkymään Smart Dashboard sovelluksen avulla.

Määritellä Smart Dashboard -kirjautumisikkunaan teille toimituksen aikana kerrottu Smart Dash board säännöstönäkymän IP-osoite sekä käyttäjätunnus ja salasana.



Tämän jälkeen teille avautuu palomuurin yleisnäkymä. Ylälaidan välilehdiltä pääsette katsomaan eri toiminnallisuuksien (Sovelluhallinta, web-sisällönsuodatus jne.) sääntöjä.

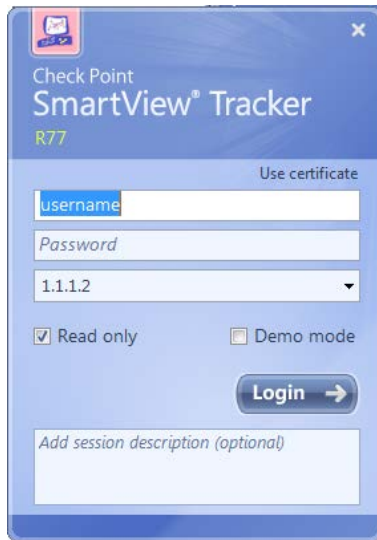


No.	Hits	Name	Source	Destination	Applications/Sites	Action	Track	Install On	Time	Comment
1	2K	Block High risk applications	Any	Internet	High Risk	Block	Log	All	Any	
2	279K	Log all applications in the organization	Any	Internet	Any Recognized	Allow	Log	All	Any	

Ohjeet muutoshallintaa varten löytyy <https://partnergate.sonera.com/firewall.html> otsikon "Palomuri lisäpalveluiden muutoshallintaohjeet" alta.

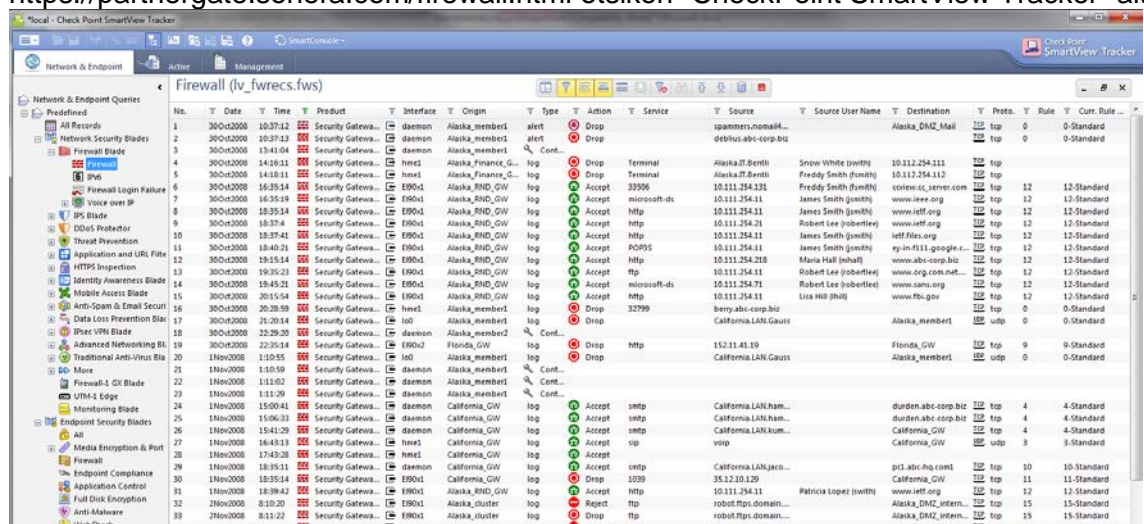
## 3 Reaaliaikainen lokinäkymään kirjautuminen ja käyttö

Määritellä SmartView -kirjautumisikkunaan teille toimituksen aikana kerrottu reaaliaikaloki näkymän IP-osoite sekä käyttäjätunnus ja salasana. **Raportointi pitää käynnistää aina SmartView Trackerilla, reaaliaika lokeihin ei pääse Smart Dashboard näkymän kautta**



Tämän jälkeen avautuu reaaliaika lokin yleisnäkymä. Oikeasta laidasta pääsee valitsemaan mitä Bladea filtteroidään. Lisäksi päänäkymässä pääsee tekemään tarkempaa filtteriointiä esim. IP-osoitteiden avulla.

Tarkempia ohjeistuksia SmartView Trackerin käytölle löytyy <https://partnergate.sonera.com/firewall.html> otsikon "CheckPoint SmartView Tracker" alta.



No.	Date	Time	Product	Interface	Origin	Type	Action	Service	Source	User Name	Destination	Proto.	Rule	Curr. Rule
1	30Oct2008	10:37:12	Security Gateway...	daemon	Alaska_member1	alert	Drop		spammers.nomail4...		Alaska_DMZ_Mail	tcp	0	0-Standard
2	30Oct2008	10:37:13	Security Gateway...	daemon	Alaska_member1	alert	Drop		debilus-abc-corp.biz		Alaska_member1	tcp	0	0-Standard
3	30Oct2008	13:41:04	Security Gateway...	daemon	Alaska_member1	Cont.								
4	30Oct2008	14:48:11	Security Gateway...	hms1	Alaska_Finance_G...	log	Drop	Terminal	Alaska.IT.Bentli	Snow White (jswth)	10.112.254.111	tcp	12	12-Standard
5	30Oct2008	14:48:11	Security Gateway...	hms1	Alaska_Finance_G...	log	Drop	Terminal	Alaska.IT.Bentli	Fredy Smith (fsmith)	10.112.254.112	tcp	12	12-Standard
6	30Oct2008	16:35:14	Security Gateway...	E990d	Alaska_RND_GW	log	Accept	33066	10.111.254.331	Fredy Smith (fsmith)	coxnet.cs_server.com	tcp	12	12-Standard
7	30Oct2008	16:35:19	Security Gateway...	E990d	Alaska_RND_GW	log	Accept	microsoft-ds	10.111.254.11	James Smith (jsmith)	www.iver.org	tcp	12	12-Standard
8	30Oct2008	18:25:54	Security Gateway...	E990d	Alaska_RND_GW	log	Accept	http	10.111.254.11	James Smith (jsmith)	www.ietf.org	tcp	12	12-Standard
9	30Oct2008	18:37:41	Security Gateway...	E990d	Alaska_RND_GW	log	Accept	http	10.111.254.21	Robert Lee (jrobertlee)	www.ietf.org	tcp	12	12-Standard
10	30Oct2008	18:37:41	Security Gateway...	E990d	Alaska_RND_GW	log	Accept	http	10.111.254.11	James Smith (jsmith)	ietf.files.org	tcp	12	12-Standard
11	30Oct2008	18:40:21	Security Gateway...	E990d	Alaska_RND_GW	log	Accept	POP3S	10.111.254.11	James Smith (jsmith)	ry.in.f11.google.c...	tcp	12	12-Standard
12	30Oct2008	19:25:54	Security Gateway...	E990d	Alaska_RND_GW	log	Accept	http	10.111.254.218	Maria Hall (mhall)	www.abc-corp.biz	tcp	12	12-Standard
13	30Oct2008	19:35:23	Security Gateway...	E990d	Alaska_RND_GW	log	Accept	ftp	10.111.254.11	Robert Lee (jrobertlee)	www.org.com.net...	tcp	12	12-Standard
14	30Oct2008	19:45:21	Security Gateway...	E990d	Alaska_RND_GW	log	Accept	microsoft-ds	10.111.254.71	Robert Lee (jrobertlee)	www.sams.org	tcp	12	12-Standard
15	30Oct2008	20:15:54	Security Gateway...	E990d	Alaska_RND_GW	log	Accept	http	10.111.254.11	Lisa Hill (lhill)	www.fhs.gov	tcp	12	12-Standard
16	30Oct2008	20:38:09	Security Gateway...	hms1	Alaska_member1	log	Drop	32799	berry-abc-corp.biz		Alaska_member1	tcp	0	0-Standard
17	30Oct2008	21:30:14	Security Gateway...	iso	Alaska_member1	log	Drop		California.LAN.Gauss		Alaska_member1	udp	0	0-Standard
18	30Oct2008	22:39:30	Security Gateway...	daemon	Alaska_member2	Cont.								
19	30Oct2008	22:35:14	Security Gateway...	E990d	Florida_GW	log	Drop	http	152.11.41.19		Florida_GW	tcp	9	9-Standard
20	11Nov2008	1:05:55	Security Gateway...	iso	Alaska_member1	log	Drop		California.LAN.Gauss		Alaska_member1	udp	0	0-Standard
21	11Nov2008	1:08:59	Security Gateway...	daemon	Alaska_member1	Cont.								
22	11Nov2008	1:11:02	Security Gateway...	daemon	Alaska_member1	Cont.								
23	11Nov2008	1:11:29	Security Gateway...	daemon	Alaska_member1	Cont.								
24	11Nov2008	15:00:41	Security Gateway...	daemon	California_GW	log	Accept	smtp	California.LAN.han...		burden-abc-corp.biz	tcp	4	4-Standard
25	11Nov2008	15:00:39	Security Gateway...	daemon	California_GW	log	Accept	smtp	California.LAN.han...		California.LAN.han...	tcp	4	4-Standard
26	11Nov2008	15:41:29	Security Gateway...	daemon	California_GW	log	Accept	smtp	California.LAN.han...		California_GW	tcp	4	4-Standard
27	11Nov2008	16:43:13	Security Gateway...	hms1	California_GW	log	Accept	voip			California_GW	udp	3	3-Standard
28	11Nov2008	17:43:28	Security Gateway...	hms1	California_GW	log	Accept							
29	11Nov2008	18:35:11	Security Gateway...	daemon	California_GW	log	Accept	smtp	California.LAN.jaro...		pc1.abc-hq.com	tcp	10	10-Standard
30	11Nov2008	18:35:14	Security Gateway...	E990d	California_GW	log	Drop	1039	35.12.10.20		California_GW	tcp	11	11-Standard
31	11Nov2008	18:39:42	Security Gateway...	E990d	Alaska_RND_GW	log	Accept	http	10.111.254.11	Patricia Lopez (jswth)	www.ietf.org	tcp	12	12-Standard
32	21Nov2008	8:10:20	Security Gateway...	E990d	Alaska_cluster	log	Reject	ftp	robot.rps.domain...		Alaska_DMZ_inter...	tcp	15	15-Standard
33	21Nov2008	8:11:23	Security Gateway...	E990d	Alaska_cluster	log	Reject	ftp	robot.rps.domain...		Alaska_DMZ_inter...	tcp	15	15-Standard
34	21Nov2008	8:11:30	Security Gateway...	E990d	Alaska_cluster	log	Reject	ftp	robot.rps.domain...		Alaska_DMZ_inter...	tcp	15	15-Standard