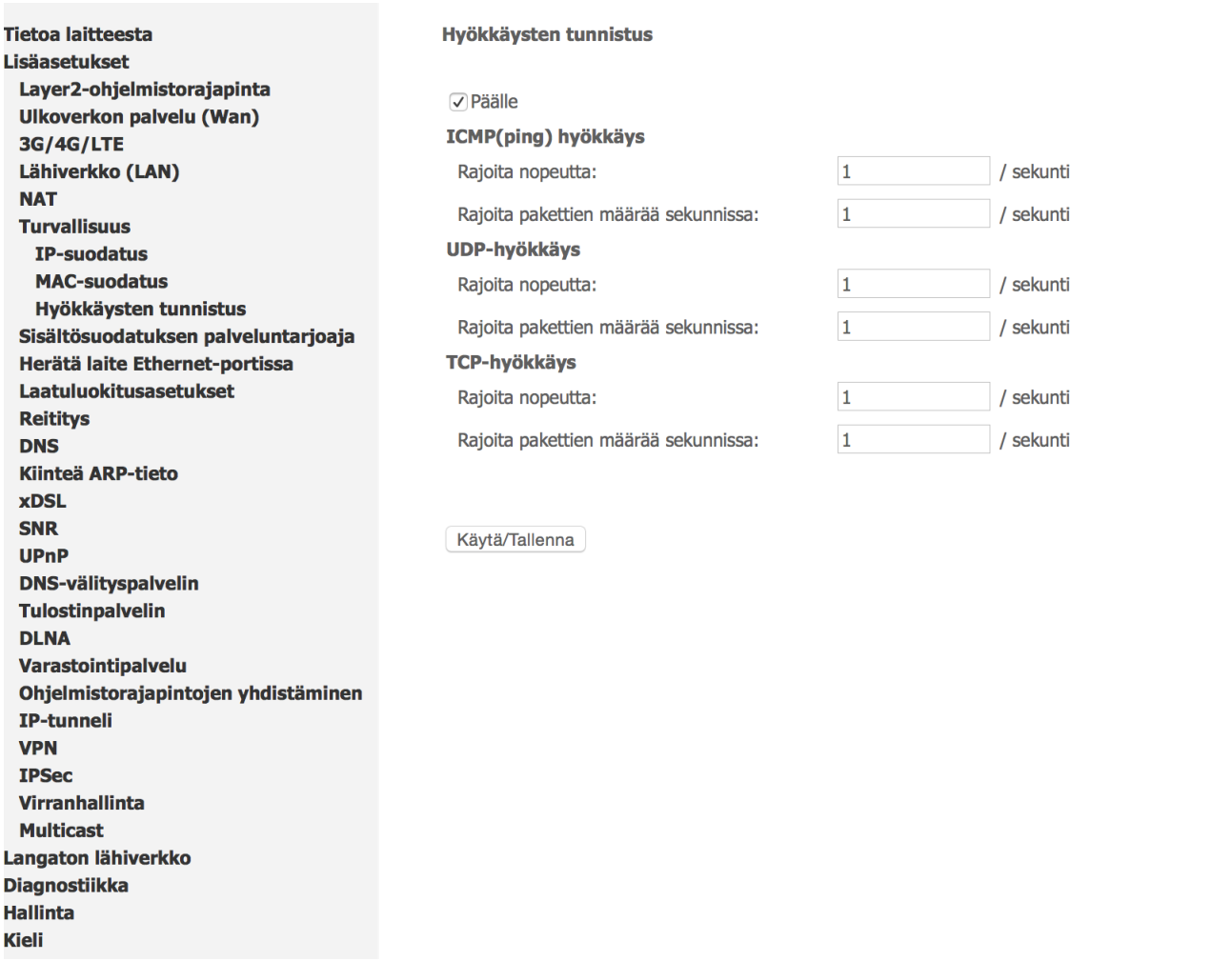
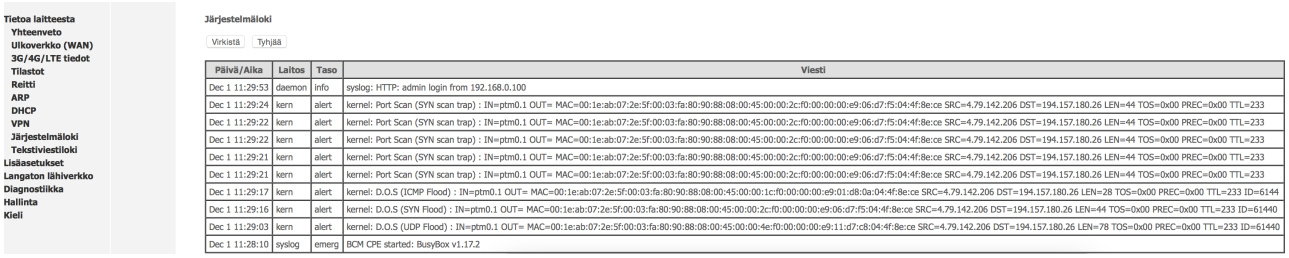
TW-EAV510: HYÖKKÄYSTEN TUNNISTUS

Jos haluat nähdä enemmän tapahtumia Internet-puolen liikenteestä, niin laita päälle hyökkäysten tunnistus (Lisäasetukset / Turvallisuus / Hyökkäysten tunnistus) ja siinä alla olevan kuvan mukainen asetus. Tällöin laite näyttää järjestelmälokissa suurimman osan hyökkäysyrityksistä.



Alla esimerkkikuva lokista, kun hyökkäysten tunnistus on päällä.



Päivä/Aika	Laitos	Taso	Viesti
Dec 1 11:29:53	daemon	info	syslog: HTTP: admin login from 192.168.0.100
Dec 1 11:29:24	kern	alert	kernel: Port Scan (SYN scan trap) : IN=ptm0.1 OUT= MAC=00:1e:ab:07:2e:5f:00:03:fa:80:90:88:08:00:45:00:00:2c:f0:00:00:00:e9:06:d7:f5:04:4f:8e:ce SRC=4.79.142.206 DST=194.157.180.26 LEN=44 TOS=0x00 PREC=0x00 TTL=233
Dec 1 11:29:22	kern	alert	kernel: Port Scan (SYN scan trap) : IN=ptm0.1 OUT= MAC=00:1e:ab:07:2e:5f:00:03:fa:80:90:88:08:00:45:00:00:2c:f0:00:00:00:e9:06:d7:f5:04:4f:8e:ce SRC=4.79.142.206 DST=194.157.180.26 LEN=44 TOS=0x00 PREC=0x00 TTL=233
Dec 1 11:29:22	kern	alert	kernel: Port Scan (SYN scan trap) : IN=ptm0.1 OUT= MAC=00:1e:ab:07:2e:5f:00:03:fa:80:90:88:08:00:45:00:00:2c:f0:00:00:00:e9:06:d7:f5:04:4f:8e:ce SRC=4.79.142.206 DST=194.157.180.26 LEN=44 TOS=0x00 PREC=0x00 TTL=233
Dec 1 11:29:21	kern	alert	kernel: Port Scan (SYN scan trap) : IN=ptm0.1 OUT= MAC=00:1e:ab:07:2e:5f:00:03:fa:80:90:88:08:00:45:00:00:2c:f0:00:00:00:e9:06:d7:f5:04:4f:8e:ce SRC=4.79.142.206 DST=194.157.180.26 LEN=44 TOS=0x00 PREC=0x00 TTL=233
Dec 1 11:29:21	kern	alert	kernel: Port Scan (SYN scan trap) : IN=ptm0.1 OUT= MAC=00:1e:ab:07:2e:5f:00:03:fa:80:90:88:08:00:45:00:00:2c:f0:00:00:00:e9:06:d7:f5:04:4f:8e:ce SRC=4.79.142.206 DST=194.157.180.26 LEN=44 TOS=0x00 PREC=0x00 TTL=233
Dec 1 11:29:17	kern	alert	kernel: D.O.S (ICMP Flood) : IN=ptm0.1 OUT= MAC=00:1e:ab:07:2e:5f:00:03:fa:80:90:88:08:00:45:00:00:1c:f0:00:00:00:e9:01:d8:0a:04:4f:8e:ce SRC=4.79.142.206 DST=194.157.180.26 LEN=28 TOS=0x00 PREC=0x00 TTL=233 ID=6144
Dec 1 11:29:16	kern	alert	kernel: D.O.S (SYN Flood) : IN=ptm0.1 OUT= MAC=00:1e:ab:07:2e:5f:00:03:fa:80:90:88:08:00:45:00:00:2c:f0:00:00:00:e9:06:d7:f5:04:4f:8e:ce SRC=4.79.142.206 DST=194.157.180.26 LEN=44 TOS=0x00 PREC=0x00 TTL=233 ID=61440
Dec 1 11:29:03	kern	alert	kernel: D.O.S (UDP Flood) : IN=ptm0.1 OUT= MAC=00:1e:ab:07:2e:5f:00:03:fa:80:90:88:08:00:45:00:00:4e:f0:00:00:00:e9:11:d7:c8:04:4f:8e:ce SRC=4.79.142.206 DST=194.157.180.26 LEN=78 TOS=0x00 PREC=0x00 TTL=233 ID=61440
Dec 1 11:28:10	syslog	emerg	BCM CPE started: BusyBox v1.17.2