Threat detection, remote access

För att skydda från botar och intrångsförsök kan man använda sig av threat protection. Threat protection placerar IP-adresser i en shun-lista vid för många inloggningsförsök och/eller för många initationer av klient-tunnel.

Det kräver att man är på rätt ASA-kod:

```
9.16 version train -> supported from 9.16(4)67 and newer versions within this specific train.
9.18 version train -> supported from 9.18(4)40 and newer versions within this specific train.
9.20 version train -> supported from 9.20(3) and newer versions within this specific train.
9.22 version train -> supported from 9.22(1.1) and any newer versions.
```

Konf:

```
threat-detection service invalid-vpn-access
threat-detection service remote-access-authentication hold-down 10 threshold 20
threat-detection service remote-access-client-initiations hold-down 10 threshold 30
```

Validering:

```
show threat-detection service
show threat-detection service entries
show threat-detection service remote-access-authentication entries
show shun x
no shun x = ta bort shun för viss IP
clear shun = ta bort shun för samtliga
```

Om man har PAT på vägen till en vpn-ASA kan det bli problem. Det går inte att rensa en specifik entry som är i recording, det går att rensa samtliga men inte specifik. Jag har ful-löst det här med ett EEM skript som rensar shun-listan var femte sekund:

```
event manager applet Clear_Shun_PATIP
 description Clear  PAT IP every 5 seconds
 event timer watchdog time 5
 event none
```

```
 action 1 cli command "no shun 1.3.3.7"
 output none
```

Man kan också vilja rensa hela shun-listan varje vecka, då den ej rensas automatiskt.

```
event manager applet Clear_Shun_Weekly
 description Clear shunned IPs every 7 days
 event none
 event timer watchdog time 604800
 action 1 cli command "clear shun"
 output none
```

Revision #1
Created 26 April 2025 12:07:03 by Jehrlander
Updated 26 April 2025 12:07:09 by Jehrlander