ASA

- Threat detection, remote access
- Placering av ASA bakom annat brandväggskluster
- vpn load-balancing, klient VPN
- ACME, Lets Encrypt

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
```

Placering av ASA bakom annat brandväggskluster

Om man fortfarande kör ASA för exempelvis VPN S2S eller VPN RA så kan det vara bra att placera ASAn bakom ett mer modernt brandväggskluster för att nyttja säkerhetsfunktioner.

En sak man ska ta med sig är att för S2S bör brandväggen fortsatt ha de publika IPv4 adresserna på interfacet, ej använda NAT för att komma åt Internet. Detta då brandväggen injicerar information i IKE-meddelandena gällande vilken IP som finns på utgående interface. Om andra sidan matchar på publika IPn kommer då uppsättningen att misslyckas. Se debug-loggar från en Cisco 4k ISR nedan där den förväntade sig en publik IPv4 adress:

```
Aug 15 08:39:08: IKEv2:(SESSION ID = 1,SA ID = 1):Process auth response notify
Aug 15 08:39:08: IKEv2:(SESSION ID = 1,SA ID = 1):Searching policy based on peer's identity '172.31.52.4' of type 'IPv4 address'
Aug 15 08:39:08: IKEv2-ERROR:(SESSION ID = 1,SA ID = 1):: Failed to locate an item in the database
Aug 15 08:39:08: IKEv2:(SESSION ID = 1,SA ID = 1):Verification of peer's authentication data FAILED
Aug 15 08:39:08: IKEv2:(SESSION ID = 1,SA ID = 1):Auth exchange failed
Aug 15 08:39:08: IKEv2-ERROR:(SESSION ID = 1,SA ID = 1):: Auth exchange failed
Aug 15 08:39:08: IKEv2:(SESSION ID = 1,SA ID = 1):Abort exchange
Aug 15 08:39:08: IKEv2:(SESSION ID = 1,SA ID = 1):Deleting SA
Aug 15 08:39:11: IPSEC(crypto_ipsec_received_invalid_spi): SPI present in Transient Tree, not sending INVSPI KMI to IKE
Aug 15 08:39:19: IKEv2-ERROR:Address type 2147516258 not supported
```

vpn load-balancing, klient VPN

Har man flera ASA-brandväggar kan man använda sig av en teknik som heter vpn load-balancing. Det gör att man kan använda sig av samtliga burkar istället för att köra active/standby. Se exempelkonf nedan.

```
vpn load-balancing
 redirect-fqdn enable
 priority 3
 interface lbpublic Outside
 interface lbprivate Inside
 cluster key password
 cluster ip address 1.1.1.1
 cluster encryption
 participate
```

Vill man ta ur en medlem ur klustret kan man slå no participate i läget ovan.

Verifiering sker med `show vpn load-balancing`.

Erfarenheter

Vid patchning har jag fått problem med att medlemmar inte ser varandra. Det är inte utrett om det här är på grund av att det är olika mjukvarnivåer eller på grund av att transportnätet är VXLAN/EVPN. Men med 4 vpn load-balacing brandväggar har jag först patchat två av dem, när de är klara har jag fått ta ut de två opatchade ur particiate och "parka" på de två patchade genom no participate följt av participate.

ACME, Lets Encrypt

Fungerade konfiguration för att få certifikat till ASA-brandväggar via ACME-protokollet från Lets Encrypt:

```
crypto ca trustpoint LETSENCRYPT_TEST
enrollment protocol acme authentication http01 outside
enrollment protocol acme url LetsEncrypt

crypto ca trustpoint LETSENCRYPT_TEST
enrollment interface outside
enrollment protocol acme authentication http01 outside
enrollment protocol acme url https://acme-v02.api.letsencrypt.org/directory
fqdn vpn.jehrlander.net
alt-fqdn vpn.jehrlander.net
subject-name CN=vpn.jehrlander.net
keypair rsa modulus 4096
auto-enroll 80 regenerate

! Tänk på att ALLA fqdn-objekt ovanför behöver kunna slås upp på Internet

! Enroll
crypto ca enroll LETSENCRYPT_SMHI

! Verifiering
show crypto ca certificates LETSENCRYPT_TEST
```

Debug:

- **debug crypto ca acme <1-255>**
- **debug crypto ca <1-14>**