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
```

Revision #1
Created 16 August 2025 08:44:26 by Jehrlander
Updated 16 August 2025 09:20:22 by Jehrlander