SSL-VPN

- 01 | SSL-VPN Loopback interface
- 02 | SSL-VPN FortiToken Push melding
- 03 | SSL-VPN E-Mail MFA

01 | SSL-VPN Loopback interface

Als je je SSL-VPN interface veranderd naar een Loopback interface dan kan je L7 firewalling toepassen middels reguliere firewall policies in plaats van enkel L3 en L4 middels local-in policies.

Stap 1 - Loopback interface aanmaken

```
config system interface
    edit "SSL-VPN-LO"
        set vdom "root"
        set ip 172.25.100.1 255.255.255.255
        set allowaccess ftm
        set type loopback
        set role dmz
    next
end
```

Stap 2 - DNAT aanmaken middels VIP

```
config firewall vip
    edit "SSL-VPN-LO-IP4"
        set extip <external IP> ## Check with myip.nl for example
        set mappedip "172.25.100.1"
        set extintf "any"
        set portforward enable
        set extport 8443 ## Change to a different port if SSL-VPN is running on a different port
        set mappedport 8443 ## Change to a different port if SSL-VPN is running on a different port
    next
```

Stap 3 - Policy aanmaken

```
config firewall policy
    edit 0
        set name "INET to Loopback SSL-VPN"
        set srcintf "KPN-INET-VL6"
        set dstintf "SSL-VPN-LO"
        set action accept
        set srcaddr "all"
        set dstaddr "SSL-VPN-LO-IP4"
        set schedule "always"
        set service "T8443"
        set logtraffic all
    next
end
```

Stap 4 - SSL-VPN configuratie aanpassen met loopback interface

```
config vpn ssl settings
    set port 8443
    set source-interface "SSL-VPN-LO"
end
```

02 | SSL-VPN FortiToken Push melding

Er zijn meerdere manieren om MFA authenticatie aan te zetten voor je gebruikers om te verbinden met de SSL-VPN, hieronder behandelen we de FortiToken. Standaard krijg je er twee gratis.

Stap 1 - FortiToken toekennen aan gebruiker

```
config user local
    edit "joshua.bergman"
        set type password
        set two-factor fortitoken
        set fortitoken "XXXXXXXXXXXXXX"
        set email-to "josh.bergman@xxxxxxxx.com"
    next
end
```

Stap 2 - FortiToken Push activeren

Ik ga er hier van uit dat je 01 | SSL-VPN Loopback interface gevolgd hebt

```
config system interface
    edit "SSL-VPN-LO"
        set allowaccess ftm
    next
end
```

Stap 3 - FortiToken Mobile App installeren

Gebruiker krijgt een mailtje om de FortiToken te activeren.
Gebruiker dient hiervoor de FortiToken Mobile App te hebben geinstalleerd op een mobiel apparaat

Stap 4 - DNAT aanmaken middels VIP

```
config firewall vip
    edit "SSL-VPN-LO-IP4-FTM"
        set extip <external IP>
        set mappedip "172.25.100.1"
        set extintf "any"
        set portforward enable
        set extport 4433
        set mappedport 4433
    next
end
```

Stap 5 - Service aanmaken

```
config firewall service custom
    edit "FTM"
        set category "Remote Access"
        set tcp-portrange 4433
    next
end
```

Stap 6 - Policy aanmaken

```
config firewall policy
    edit 0
        set name "INET to Loopback SSL-VPN - FTM"
        set srcintf "KPN-INET-VL6"
        set dstintf "SSL-VPN-LO"
        set action accept
        set srcaddr "all"
        set dstaddr "SSL-VPN-LO-IP4-FTM"
        set schedule "always"
        set service "FTM"
        set logtraffic all
    next
end
```

03 | SSL-VPN E-Mail MFA

Ik ga er in deze instructie van uit dat de gebruiker al bestond en al toegang had tot de SSL-VPN tunnel

Stap 1 - E-Mail MFA toekennen aan gebruiker

```
config user local
    edit "joshua.bergman"
        set type password
        set two-factor email
        set email-to "josh.bergman@outlook.com"
    next
end
```