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
```

Revision #2
Created 25 January 2025 12:07:22 by Joshua Bergman | Lighted Networks
Updated 25 January 2025 12:24:22 by Joshua Bergman | Lighted Networks