Fortinet

- Cheat sheet 7.0
- Cheat sheet 6.4
- KPN IPTV
- Dynamische blocklists
- KPN
    - 01 | KPN PPPoE - IPv4
    - 02 | KPN PPPoE - IPv6
    - 03 | KPN - IPTV
- Ziggo
    - 01 | Ziggo - IPv4
    - 02 | Ziggo - IPv6
- SSL-VPN
    - 01 | SSL-VPN Loopback interface
    - 02 | SSL-VPN FortiToken Push melding
    - 03 | SSL-VPN E-Mail MFA
- ADVPN
- DNS
    - 01 | DDNS
- Policies
    - 01 | Local-in policy
    - 02 | Negate Policy
- Fortimanager

    - Bulk retrieve config
- Dynamische routering
    - 01 | BGP (Draft)
- Security Fabric
    - 01 | External Connectors
- SNMP settings
- Wireless-controller
    - Hitless Rolling AP upgrade
- Troubleshooting
    - 01 | GREP
- Issues
    - BUG 1164092 NP7 FortiGates v7.2.11 may stop sending traffic out on certain interfaces
    - BUG 1128662 BGP peering fails
- IPsec VPN
    - 01 | IPsec Dial Up VPN (Vervanger voor SSL-VPN)
- Public Cloud - Azure
    - 01 | MGMT interface HA cluster

Cheat sheet 7.0

Cheat sheet 6.4

KPN IPTV

```
config system interface
edit "WAN-VLAN4"
        set vdom "root"
        set mode dhcp
        config client-options
            edit 1
                set code 60
                set type string
                set value "IPTV_RG"
            next
            edit 2
                set code 55
                set value "79"
            next
            edit 3
                set code 121
                set type string
                set value "classless-static-routes"
            next
        end
        set distance 6
        set alias "KPN IPTV VLAN"
        set device-identification enable
        set monitor-bandwidth enable
        set role lan
        set snmp-index 15
        set defaultgw disable
        set dns-server-override disable
        set interface "wan"
        set vlanid 4
        next
        end
```

```
 config router static
    edit 0
```

```
        set dst 213.75.112.0 255.255.248.0
        set distance 1
        set device "WAN-VLAN4"
        set dynamic-gateway enable
    next
    end
```

```
config firewall multicast-policy
    edit 1
        set uuid 7f5446ce-6a80-51ee-f08f-1714fb5ee2bc
        set name "Upstream IPTV"
        set logtraffic enable
        set srcintf "WAN-VLAN4"
        set dstintf "LAN"
        set srcaddr "all"
        set dstaddr "all"
        set snat enable
    next
    edit 2
        set uuid 7f585a98-6a80-51ee-aae4-234969492bac
        set name "Downstream IPTV"
        set logtraffic enable
        set srcintf "LAN"
        set dstintf "WAN-VLAN4"
        set srcaddr "all"
        set dstaddr "all"
        set snat enable
    next
end
```

```
config firewall address
    edit "G-IPTV-213.75.112.0/21"
        set subnet 213.75.112.0 255.255.248.0
    next
end
```

```
config firewall policy
    edit 0
        set name "IPTV"
        set srcintf "LAN"
```

```
        set dstintf "WAN-VLAN4"
        set action accept
        set srcaddr "all"
        set dstaddr "G-IPTV-213.75.112.0/21"
        set schedule "always"
        set service "ALL"
        set nat enable
    next
end
```

https://forum.kpn.com/thuisnetwerk-72/instellen-eigen-router-fortigate-60f-met-iptv-options-499669

Dynamische blocklists

Met deze config kun je dynamische lijsten met IPs inladen in de fortigate om vervolgens op basis van deze lijsten verkeer te blokkeren.

```
config system external-resource
    edit "Threadfeed Domains Generic"
        set type domain
        set category 192
        set resource "https://raw.githubusercontent.com/emberstack/threat-
feed/main/Feed/List/ThreatFeed.Domains.Generic.txt"
        set refresh-rate 1
    next
    edit "Threadfeed Domains Advertising"
        set type domain
        set category 193
        set resource "https://raw.githubusercontent.com/emberstack/threat-
feed/main/Feed/List/ThreatFeed.Domains.Advertising.txt"
        set refresh-rate 1
    next
    edit "Russia IP list"
        set type address
        set resource "https://filestore.fortinet.com/fortiguard/russia_reg_ip.list"
        set refresh-rate 1
    next
    edit "Donetsk IP list"
        set type address
        set resource "https://filestore.fortinet.com/fortiguard/dnr_lnr_ip.list"
        set refresh-rate 1
    next
    edit "Iran IP list"
        set type address
        set resource "https://filestore.fortinet.com/fortiguard/iran_reg_ip.list"
        set refresh-rate 1
    next
    edit "Krim IP list"
        set type address
```

```
        set resource "https://filestore.fortinet.com/fortiguard/crimea_ip.list"
        set refresh-rate 1
    next
    edit "Emerging Block List"
        set type address
        set resource "https://rules.emergingthreats.net/fwrules/emerging-Block-IPs.txt"
    next
    edit "Compromised IPs"
        set type address
        set resource "https://rules.emergingthreats.net/blockrules/compromised-ips.txt"
    next
    edit "Threatfox IOC"
        set type address
        set resource "https://raw.githubusercontent.com/elliotwutingfeng/ThreatFox-IOC-
IPs/10fab10d6bf5a8996a0eeb01a840307d6884f554/ips.txt"
end
```

KPN

KPN

01 | KPN PPPoE - IPv4

Deze instructie neemt je stap voor stap mee door de configuratie van KPN PPPoE op je FortiGate.

Stap 1 - VLAN 6 aanmaken

Bij onderstaand voorbeeld word wan1 gebruikt, let er op dat je het juiste interface koppelt.

```
config system interface
    edit "KPN-INET-VL6"
        set vdom "root"
        set role wan
        set interface "wan1"
        set mtu-override enable
        set mtu 1506
        set vlanid 6
    next
end
```

Stap 2 - PPPoE interface aanmaken

```
config system pppoe-interface
    edit "KPN-PPPoE"
        set device "KPN-INET-VL6"
        set username "internet"
        set password "internet"
    next
end
```

Stap 3 - PPPoE interface configureren

```
config system interface
    edit "KPN-PPPoE"
```

```
        set vdom "root"
        set mode pppoe
        set type tunnel
        set external enable
        set role wan
        set dns-server-override disable
        set interface "KPN-INET-VL6"
    next
end
```

Stap 4 - Statische route aanmaken

```
config router static
  edit 0
    set device KPN-PPPoE
  next
end
```

Stap 5 - Policy aanmaken

```
config firewall policy
    edit 0
        set name "any to internet - IPv4"
        set srcintf "any"
        set dstintf "KPN-PPPoE"
        set action accept
        set srcaddr "all"
        set dstaddr "all"
        set schedule "always"
        set service "ALL"
        set logtraffic all
        set nat enable
    next
end
```

Stap 6 - Internet connectiviteit testen

execute ping google.com

02 | KPN PPPoE - IPv6

Deze instructie gaat er vanuit dat je 01 | KPN PPPoE - IPv4 al gevolgd hebt.

Stap 1 - PPPoE interface voorzien van IPv6 flag

```
config system pppoe-interface
    edit "KPN-PPPoE"
        set ipv6 enable
    next
end
```

Stap 2 - PPPoE interface configureren met IPv6 adres

```
config system interface
    edit "KPN-PPPoE"
        config ipv6
            set ip6-address 2a02:xxxx:yyyy::ffff/128 ## Controleer je IPv6 prefix in de KPN app
        end
    next
end
```

Stap 3 - Statische route aanmaken

```
config router static6
    edit 0
        set device "KPN-PPPoE"
    next
```

```
end
```

Stap 4 - LAN interface configureren met IPv6 adres

```
config system interface
    edit "VLAN2001"
        config ipv6
            set ip6-address 2a02:xxxx:yyyy:2001::1/64
            set ip6-send-adv enable ## Verstuurd router advertisements
            set ip6-manage-flag enable ## Geeft aan dat je DHCP wil gebruiken in plaats van SLAAC
            set ip6-other-flag enable ## Geeft aan dat je middels DHCP de DNS servers mee wil geven
        end
    next
end
```

Stap 5 - DHCP server aanmaken

```
config system dhcp6 server
    edit 0
        set lease-time 86400
        set dns-service default
        set domain "domain.local"
        set subnet 2a02:xxxx:yyyy:2001::/64
        set interface "VLAN2001"
        config ip-range
            edit 1
                set start-ip 2a02:xxxx:yyyy:2001::1000
                set end-ip 2a02:xxxx:yyyy:2001::2000
            next
        end
    next
end
```

Stap 6 - Policy aanmaken

```
config firewall policy
    edit 0
        set name "any to internet - IPv6"
        set srcintf "any"
        set dstintf "KPN-PPPoE"
        set action accept
        set srcaddr6 "all"
        set dstaddr6 "all"
        set schedule "always"
        set service "ALL"
        set logtraffic all
    next
end
```

Stap 7 - Internet connectiviteit testen

```
execute ping6 google.com
```

03 | KPN - IPTV

In deze instructie maken we gebruik van VLAN1003 als IPTV VLAN

Stap 1 - VLAN 4 aanmaken

```
config system interface
    edit "KPN-IPTV-VL4"
        set vdom "root"
        set mode dhcp
        config client-options
            edit 1
                set code 60
                set type string
                set value "IPTV_RG"
            next
            edit 2
                set code 55
                set value "79"
            next
        end
        set distance 10
        set role wan
        set dns-server-override disable
        set interface "wan1"
        set vlanid 4
    next
end
```

Stap 2 - Statische route aanmaken

```
config router static
    edit 0
        set dst 213.75.112.0 255.255.248.0
```

```
        set device "KPN-IPTV-VL4"
        set dynamic-gateway enable
    next
end
```

Stap 3 - IPTV VLAN aanmaken

```
config system interface
    edit VLAN1003
        set vdom "root"
        set ip 10.10.3.6 255.255.255.248
        set role lan
        set interface "LACP" ## Replace with physical interface
        set vlanid 1003
    next
end
```

Stap 4 - DHCP server aanmaken

```
config system dhcp server
    edit 0
        set ntp-service local
        set default-gateway 10.10.3.6
        set netmask 255.255.255.248
        set interface "VLAN1003"
        config ip-range
            edit 1
                set start-ip 10.10.3.1
                set end-ip 10.10.3.5
            next
        end
        set dns-server1 195.121.1.34
        set dns-server2 195.121.1.66
    next
end
```

Stap 5 - Multicast policies aanmaken

```
config firewall multicast-policy
    edit 0
        set name "iTV > KPN"
        set logtraffic enable
        set srcintf "VLAN1003" ## Replace with IPTV VLAN
        set dstintf "KPN-IPTV-VL4"
        set srcaddr "all"
        set dstaddr "all"
        set snat enable
    next
    edit 0
        set name "KPN > iTV"
        set logtraffic enable
        set srcintf "KPN-IPTV-VL4"
        set dstintf "VLAN1003" ## Replace with IPTV VLAN
        set srcaddr "all"
        set dstaddr "all"
    next
end
```

Stap 6 - IPTV policy maken richting KPN

```
config firewall policy
    edit 0
        set name "IPTV to KPN"
        set srcintf "VLAN1003" ## Replace with IPTV VLAN
        set dstintf "KPN-IPTV-VL4"
        set srcaddr "all"
        set dstaddr "all"
        set action accept
        set schedule "always"
        set service "ALL"
        set logtraffic all
        set nat enable
    next
end
```

Stap 7 - Internet policy maken voor TV ontvanger

Deze stap is bedoeld om streamingsdiensten zoals Netflix of Spotify te laten werken

```
config firewall policy
    edit 0
        set name "IPTV to internet"
        set srcintf "VLAN1003" ## Replace with IPTV VLAN
        set dstintf "KPN-INET-VL6"
        set srcaddr "all"
        set dstaddr "all"
        set action accept
        set schedule "always"
        set service "ALL"
        set logtraffic all
        set nat enable
    next
end
```

Ziggo

01 | Ziggo - IPv4

Ziggo is in tegenstelling tot KPN heel simpel op te zetten gezien je bij Ziggo direct een IP krijgt op je WAN ipv op een PPPoE tunnel.

Stap 1 - WAN interface configureren

```
config system interface
    edit "wan1"
        set vdom "root"
        set mode dhcp
        set type physical
        set role wan
        set dns-server-override disable
    next
end
```

Stap 2 - Statische route aanmaken

```
config router static
  edit 0
    set device wan1
  next
end
```

Stap 3 - Policy aanmaken

```
config firewall policy
    edit 0
        set name "any to internet - IPv4"
        set srcintf "any"
        set dstintf "wan1"
        set action accept
```

```
        set srcaddr "all"
        set dstaddr "all"
        set schedule "always"
        set service "ALL"
        set logtraffic all
        set nat enable
    next
end
```

Stap 4 - Internet connectiviteit testen

```
execute ping google.com
```

02 | Ziggo - IPv6

Stap 1 - WAN interface configureren

```
config system interface
    edit "wan1"
        set vdom "root"
        set mode dhcp
        set type physical
        set role wan
        config ipv6
            set ip6-mode dhcp
        end
        set dns-server-override disable
    next
end
```

Stap 2 - Statische route aanmaken

```
config router static6
    edit 0
        set device "wan1"
    next
end
```

Stap 3 - LAN interface configureren met IPv6 adres

IP adressen in het netwerk worden uitgedeeld met SLAAC in deze instructie, hierdoor is er geen DHCP server configuratie nodig.

```
config system interface
    edit "VL2001"
        config ipv6
            set ip6-mode delegated
            set ip6-send-adv enable
            config ip6-delegated-prefix-list
                edit 1
                    set upstream-interface "wan1"
                    set subnet 2001:xxxx:yyyyy:2001::/56
                next
            end
        end
        set interface "LACP" ## Change to physical interface
        set vlanid 2001
    next
end
```

Stap 4 - Policy aanmaken

```
config firewall policy
    edit 0
        set name "any to internet - IPv6"
        set srcintf "any"
        set dstintf "wan1"
        set action accept
        set srcaddr6 "all"
        set dstaddr6 "all"
        set schedule "always"
        set service "ALL"
        set logtraffic all
    next
end
```

Stap 5 - Internet connectiviteit testen

```
execute ping6 google.com
```

SSL-VPN

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
```

ADVPN

DNS

01 | DDNS

```
config system ddns
    edit 1
        set ddns-server FortiGuardDDNS
        set ddns-domain "<fqdn>.fortiddns.com"
        set use-public-ip enable
        set monitor-interface "KPN-PPPoE"
    next
end
```

Policies

01 | Local-in policy

Met de functie *Local in Policy* op een FortiGate apparaat kun je de toegang tot de administratieve interfaces van de firewall beheren. Deze policy maakt het mogelijk om specifieke toegangspaden voor beheerders te configureren, zodat je kunt bepalen welke IP-adressen of netwerken wel of niet toegang krijgen tot de beheermogelijkheden van het apparaat. Dit is een belangrijk hulpmiddel voor het versterken van de beveiliging, aangezien het het risico op ongeautoriseerde toegang tot de device instellingen vermindert.

```
config firewall local-in-policy
    edit 1
        set intf "<WAN interface>"
        set srcaddr "<Firewall address>"
        set dstaddr "all"
        set action accept
        set service "ALL_ICMP" "SNMP"
        set schedule "always"
    next
    edit 2
        set intf "<WAN interface>"
        set srcaddr "all"
        set dstaddr "all"
        set service "ALL"
        set schedule "always"
    next
end
```

Deze regels zorgen ervoor dat alleen verkeer voor ICMP (ping) en SNMP (voor netwerkbeheer) wordt toegestaan naar de firewall via de opgegeven WAN-interface, terwijl al het andere verkeer wordt geblokkeerd. De eerste regel staat specifiek ICMP en SNMP toe vanaf een bepaald IP-adres, terwijl de tweede regel alle andere diensten voor elke bron blokkeert.

02 | Negate Policy

Negate kun je gebruiken als omgekeerd policy object.
Geef je bijvoorbeeld aan dat je RFC1918 als destination Negate, dan word alles toegestaan behalve RFC1918.

Deze functie gebruik je bijvoorbeeld als je al het internet verkeer wil toestaan behalve bepaalde URL's, hiermee heb je dan maar 1 policy in plaats van 2.

In het voorbeeld hieronder kun je naar alle internet adressen toe, behalve 1.1.1.1

```
config firewall policy
    edit 0
        set srcintf "VLAN2001"
        set dstintf "wan1"
        set action accept
        set srcaddr "N-10.20.1.0/24"
        set dstaddr "H-1.1.1.1"
        set schedule "always"
        set service "ALL"
        set logtraffic all
        set nat enable
        set dstaddr-negate enable
    next
end
```

Fortimanager

Fortimanager

Bulk retrieve config

1. Create a script in **FortiManager -> Device Manager -> Scripts -> Create New**.

2.png
Image not found or type unknown

- **Type**: CLI Script.
- **Run script on**: Remote ForitGate Directly (via CLI):

`diagnose fdsm cfg-upload 'comment'` <----- Any comment can be set, it will be used to identify the retrieve in the revision history.

- Select **OK** to save.

Note:

For FortiGates with VDOMs enabled, the script should be modified to this:

```
config global
diagnose fdsm cfg-upload 'comment'
```

3.png
Image not found or type unknown

2. Running the script on all FortiGates:

4.png
Image not found or type unknown

- Select the FortiGates and select the right arrow:

5.png
Image not found or type unknown

- Select Run:

run_now.png
Image not found or type unknown

- Select OK:

click_ok.png
Image not found or type unknown

- The script will start running:

start_run.png
Image not found or type unknown

run_success.png
Image not found or type unknown

3. Go to Device Manager and the configuration status of FortiGates should show synchronized. If any FortiGate is not showing synchronized, 'right-click' on the device and select 'Refresh Device'.

sync.png
Image not found or type unknown

4. In the Total Revisions for each FortiGate, there will be a 'Retrieve' entry with the 'comment' in the comments section.

11.png
Image not found or type unknown

Note 1:

Script Status/logs can also be checked from: **System Settings -> Task Monitor**:

TM.png
Image not found or type unknown

Note 2:

Bulk retrieval can also be done by selecting the notification icon on the top, **but it only works if the devices are either in a 'conflict' or 'out-of-sync' state**.

13.png
Image not found or type unknown

Dynamische routering

01 | BGP (Draft)

Security Fabric

01 | External Connectors

GEO

Je kan onder Security Fabric -> External Connectors allerlei lijsten toevoegen die niet afhankelijk zijn van een FortiGuard licentie.
Zo kan je bijvoorbeeld een IP lijst opvoeren met alle IP reeksen uit een bepaald land, hieronder staan er een aantal gespecificeerd.

Stel dat je de IP lijst van Nederland importeert, dan kan je deze bijvoorbeeld aan je SSL-VPN hangen zodat je alleen mag verbinden vanuit Nederland.

Hier kan je alle landen vinden: rir-ip/country at master · ipverse/rir-ip
Let op, de lijsten zijn niet van Fortinet, er is geen garantie dat deze lijsten actief bij worden gehouden.

```
config system external-resource
    edit "BE - IPs"
        set uuid 65632f48-e71e-51ef-b723-04eddcdc6642
        set type address
        set resource "https://raw.githubusercontent.com/ipverse/rir-ip/refs/heads/master/country/be/ipv4-aggregated.txt"
    next
    edit "BE - IPv6"
        set uuid 50cd53fa-f14c-51ef-c9ad-c1f65978f354
        set type address
        set resource "https://raw.githubusercontent.com/ipverse/rir-ip/refs/heads/master/country/be/ipv6-aggregated.txt"
    next
    edit "DE - IPs"
        set uuid a2eb10a6-e71e-51ef-7c05-a2a8d9ffd6d9
        set type address
        set resource "https://raw.githubusercontent.com/ipverse/rir-ip/refs/heads/master/country/de/ipv4-aggregated.txt"
```

```
    next
    edit "DE - IPv6"
        set uuid 5f5cdeea-f14c-51ef-1691-3ea3b4749926
        set type address
        set resource "https://raw.githubusercontent.com/ipverse/rir-ip/refs/heads/master/country/de/ipv6-
aggregated.txt"
    next
    edit "NL - IPs"
        set uuid 272a92d4-e71e-51ef-932d-7c06156001c2
        set type address
        set resource "https://raw.githubusercontent.com/ipverse/rir-ip/refs/heads/master/country/nl/ipv4-
aggregated.txt"
    next
    edit "NL - IPv6"
        set uuid 3ee5463e-f14c-51ef-1367-705307682e46
        set type address
        set resource "https://raw.githubusercontent.com/ipverse/rir-ip/refs/heads/master/country/nl/ipv6-
aggregated.txt"
    next
end
```

APR - Apple Private Relay

Als je een iCloud abbonement hebt dan kan je gebruik maken van APR, dit houd in dat al je internetverkeer via proxies van Apple geleid word, hierdoor ben je minder zichtbaar op het internet. Er is echter wel een nadeel, namelijk dat die servers niet opgenomen zijn in de lijsten van hierboven. Om APR toe te staan op je FortiGate zijn hieronder de lijsten voor IPv4 en IPv6

Apple heeft hiervoor een CSV gedeeld: mask-api.icloud.com/egress-ip-ranges.csv

Github gebruiker hroost heeft hiervoor een script gemaakt om dit om te zetten naar lijsten die door de FortiGate gelezen kunnen worden: hroost/icloud-private-relay-iplist: List of iCloud Private Relay egress IP addresses in various formats for easy integration into your network infrastructure

```
config system external-resource
    edit "Apple Private Relay - IPs"
        set uuid 9848b88a-e721-51ef-aaed-c07a4bdf73ca
        set type address
        set resource "https://raw.githubusercontent.com/hroost/icloud-private-relay-
```

```
iplist/refs/heads/main/ipv4/ipv4-ranges.txt"
    next
    edit "Apple Private Relay - IPv6"
        set uuid 1e638452-f14c-51ef-2e76-18c2765d2308
        set type address
        set resource "https://raw.githubusercontent.com/hroost/icloud-private-relay-
iplist/refs/heads/main/ipv6/ipv6-ranges.txt"
    next
end
```

SNMP settings

Fortigate

To gather Port IP info & routing info for Fortigates, disable the append-index feature. This feature appends VDOM to the index, breaking standard MIBs.

```
config system snmp sysinfo
    set append-index disable
end
```

https://docs.fortinet.com/document/fortigate/7.2.0/new-features/742119/enabling-the-index-extension-7-2-8

Wireless-controller

Hitless Rolling AP upgrade

This release introduces Hitless Rolling upgrades for FortiAPs. When upgrading FortiAPs, an algorithm considers the reach of neighboring APs and their locations. The APs are then upgraded in staggered process with some APs being immediately upgraded while others continue to provide Wi-Fi service to clients and are placed in a standby queue. Once the SSIDs on the initial upgraded APs are able to serve clients, the APs in the standby queue begin upgrading.

CLI changes

The following CLI commands for configuring Hitless Rolling AP upgrades have been added to both global settings and per-VDOM settings:

Enabling Hitless Rolling Upgrade at the global level

```
config wireless-controller global
  set rolling-wtp-upgrade {Enable | disable}
  set rolling-wtp-upgrade-threshold <integer>
end
```

rolling-wtp-upgrade	Enable/disable rolling WTP upgrade (default = disable). **Note:** Enabling this at the global-level will enforce all managed FortiAPs in all VDOMs to implement the rolling upgrade, regardless of the VDOM-level settings.
rolling-wtp-upgrade-threshold	Minimum signal level/threshold in dBm required for the managed WTP to be included in rolling WTP upgrade (-95 to -20, default = -80).

Enabling Hitless Rolling Upgrade at the per-VDOM level

```
config wireless-controller setting
  set rolling-wtp-upgrade {Enable | disable}
end
```

rolling-wtp-upgrade	Enable/disable rolling WTP upgrade (default = disable). **Note:** Enabling this at the VDOM-level will let managed FortiAPs in the current VDOM to implement the rolling upgrade, regardless of the global-level setting.

Executing Hitless Rolling Upgrade

```
exec wireless-controller rolling-wtp-upgrade <all>|<SN>|<wtp-group>
```

rolling-wtp-upgrade	Select which APs you want to upgrade with the Hitless Rolling upgrade. You can select all APs, by their WTP serial number, or WTP group.

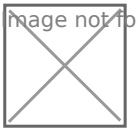
To configure Hitless Rolling AP upgrade - GUI

1. Before you can run Hitless Rolling AP upgrade from the GUI, you must first enable `rolling-wtp-upgrade` and configure the `rolling-wtp-upgrade-threshold` level in the CLI.

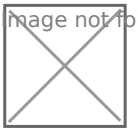
```
config wireless-controller global
  set rolling-wtp-upgrade enable
  set rolling-wtp-upgrade-threshold -70
end
```

```
config wireless-controller setting
  set rolling-wtp-upgrade enable
end
```

2. From the FortiGate GUI, go to *WiFi & Switch Controller* > *Managed FortiAPs*.
3. Select multiple FortiAPs of the same model, and then right-click and select *Upgrade*. The *Upgrade FortiAPs* window loads.
4. Upload the FortiAP image file and click *Upgrade*.



The FortiAPs are automatically upgraded using the Hitless Rolling upgrade method.
5. Some FortiAPs immediately begin upgrading while others are marked with "ISSU queued". In-Service Software Upgrade (ISSU) indicates that these are the standby APs that continue to provide Wi-Fi service to clients and are queued to be upgraded later.



6. Once the first batch of FortiAPs are upgraded and can provide service, the ISSU queued FortiAPs will begin upgrading.

To configure Hitless Rolling AP upgrade - CLI

1. Enable `rolling-wtp-upgrade` at either the global or VDOM level and configure the `rolling-wtp-upgrade-threshold` level.

```
config wireless-controller global
  set rolling-wtp-upgrade enable
  set rolling-wtp-upgrade-threshold -70
end
```

```
config wireless-controller setting
  set rolling-wtp-upgrade enable
end
```

2. Upload FortiAP images to FortiGate and check the image list. In this example, FAP231F is uploaded:

```
execute wireless-controller upload-wtp-image tftp /FortiAP/v7.00/images/build0626/FAP_231F-v7-build0626-F
```

3. Verify the uploaded FortiAP images:

```
execute wireless-controller list-wtp-image
WTP Images on AC:
ImageName                        ImageSize(B)   ImageInfo           ImageMTime
...
FP231F-v7.4.2-build0626-IMG.wtp       37605058       FP231F-v7.4-build0626  Mon Nov 27 10:39:53 2023
```

4. Run the Rolling WTP Upgrade and prepare to check the FortiAP upgrade status.

```
exec wireless-controller rolling-wtp-upgrade all
```

5. Promptly check the FortiAP upgrade status to verify that the APs are upgrading:

```
diagnose wireless-controller wlac -c ap-upd

1,50,66 0-FP231FTF23037012 FP231F-v7.4-build0591 ==> FP231F-v7.4-build0626 ws (0-10.233.10.7:5246)
upd-download,3 5%
<- The image download has started (may still be blocked by concurrent AP image downloading limit)
2,50,66 0-FP231FTF23037026 FP231F-v7.4-build0591 ==> FP231F-v7.4-build0626 ws (0-10.233.10.3:5246) u
3,50,66 0-FP231FTF23037047 FP231F-v7.4-build0591 ==> FP231F-v7.4-build0626 ws (0-10.233.10.24:5246)
...
15,50,66 0-FP431FTF23000559 FP431F-v7.4-build0591 ==> FP431F-v7.4-build0626 ws (0-10.233.30.40:524
upd-enqueue-issu,4 0%      <- In queue for rolling AP upgrade to avoid Wi-Fi service drop
16,50,66 0-FP431FTF23021146 FP431F-v7.4-build0591 ==> FP431F-v7.4-build0626 ws (0-10.233.30.42:524
upd-enqueue-issu,4 0%
...
19,50,66 0-FP433FTF21001215 FP433F-v7.4-build0591 ==> FP433F-v7.4-build0626 ws (0-10.233.30.41:524
upd-enqueue-issu,4 0%
...
```

6. After a few minutes, check the FortiAP upgrade status again to see any changes:

```
diagnose wireless-controller wlac -c ap-upd

1,44,66 0-FP231FTF23037012 FP231F-v7.4-build0626 ws (0-10.233.10.7:5246) upd-ap-up,58
<- The AP has reconnected after image upgrade
...
7,44,66 0-FP231FTF23037232 FP231F-v7.4-build0626 ws (0-10.233.10.36:5246) upd-ssid-up,5
<- The AP's SSIDs are UP after image upgrade
...
15,44,66 0-FP431FTF23000559 FP431F-v7.4-build0591 ==> FP431F-v7.4-build0626 ws (0-10.233.30.40:524
upd-enqueue-issu,404 0%      <- Still in queue for rolling AP upgrade to avoid Wi-Fi service drop
16,44,66 0-FP431FTF23021146 FP431F-v7.4-build0591 ==> FP431F-v7.4-build0626 ws (0-10.233.30.42:524
upd-enqueue-issu,404 0%
...
19,44,66 0-FP433FTF21001215 FP433F-v7.4-build0591 ==> FP433F-v7.4-build0626 ws (0-10.233.30.41:524
upd-enqueue-issu,404 0%
...
```

7. After a few more minutes, check the FortiAP upgrade status again to see APs in the queue begin upgrading:

```
diagnose wireless-controller wlac -c ap-upd

1,48,66 0-FP231FTF23037012 FP231F-v7.4-build0626 ws (0-10.233.10.7:5246) upd-ssid-up,6
...
15,48,66 0-FP431FTF23000559 FP431F-v7.4-build0591 ==> FP431F-v7.4-build0626 ws (0-10.233.30.40:524
upd-download,12 48%
<- Previously queued APs have begun the upgrade process since enough SSIDs from other APs are up to pro

16,48,66 0-FP431FTF23021146 FP431F-v7.4-build0591 ==> FP431F-v7.4-build0626 ws (0-10.233.30.42:524
upd-download,12 49%
...
19,48,66 0-FP433FTF21001215 FP433F-v7.4-build0591 ==> FP433F-v7.4-build0626 ws (0-10.233.30.41:524
upd-download,12 47%
```

Troubleshooting

Troubleshooting

01 | GREP

De FortiGate CLI biedt een ingebouwde versie van het `grep`-commando waarmee je output efficiënt kunt filteren.

GREP | Opties

```
Usage: grep [-invfcABC] PATTERN
Options:
    -i      Ignore case distinctions
    -n      Print line number with output lines
    -v      Select non-matching lines
    -f      Print fortinet config context
    -c      Only print count of matching lines
    -A      Print NUM lines of trailing context
    -B      Print NUM lines of leading context
    -C      Print NUM lines of output context
```

GREP | Simpele query

Met een simpele GREP query kan je zien of de waarde voor komt in de config

```
LNNLROSEBFW001 (JP) # show sys int | grep VLAN2001
    edit "VLAN2001"
```

GREP | Configuratie blok query

Door middel van de -f flag kan je de volledige config zien van waar de waarde in voor komt

```
LNNLROSEBFW001 (JP) # show sys int | grep -f VLAN2001
config system interface
    edit "VLAN2001" <---
        set vdom "JP"
```

```
        set ip 10.20.1.254 255.255.255.0
        set alias "Intern VLAN"
        set device-identification enable
        set monitor-bandwidth enable
        set role lan
        set interface "ae1"
        set vlanid 2001
    next
end
```

GREP | Meerdere waardes

Door middel van '<waarde1>\|<waarde2>' kan je meerdere waardes opvragen, hierbij kan je uiteraard ook weer de -f flag gebruiken

```
LNNLROSEBFW001 (JP) # show sys int | grep 'VLAN2001\|VLAN2002'
    edit "VLAN2001"
    edit "VLAN2002"
```

Issues

BUG 1164092 NP7 FortiGates v7.2.11 may stop sending traffic out on certain interfaces

https://community.fortinet.com/t5/FortiGate/Troubleshooting-Tip-NP7-FortiGates-on-v7-2-11-may-stop-sending/ta-p/396301

1128652, 1164092	On NP7 platforms, a change in the destination MAC address or fib change may cause traffic to stop on certain interfaces. **Workaround**: Disable offload on policy rules.

BUG 1128662 BGP peering fails

1128662	BGP peering fails to establish when a race condition occurs between FortiGate OS and NPU driver during IPsec SA updates for dynamic hub-to-static spoke VPNs.

FIX

Restart vpn tunnel

IPsec VPN

01 | IPsec Dial Up VPN (Vervanger voor SSL-VPN)

SSL-VPN is voortaan niet meer beschikbaar op de entry level modellen van Fortinet.
Tevens is het gebruik van SSL-VPN ook niet altijd even veilig gebleken in het verleden.
Hieronder staan een aantal stappen om de IPsec Dial Up VPN te configureren op basis van lokale gebruikers.

Stap 1 - Phase 1 interface aanmaken

```
config vpn ipsec phase1-interface
    edit "DU-VPN"
        set type dynamic                ## Dynamic allows multiple clients to connect
        set interface "wan1"            ## Bind to the incomming interface
        set ike-version 2               ## use IKEv2 for negotiation
        set peertype one                ## Only allow one specific peer ID
        set net-device disable
        set mode-cfg enable             ## Mode cfg, allow clients to dynamically get an IP and DNS settings
        set proposal aes256-sha256      ## Encryption/authentication proposal
        set localid <redacted>>         ## Local ID (remote ID on client)
        set dhgrp 16                    ## Diffie-Hellman group
        set eap enable                  ## Enable EAP (Username / Password authentication)
        set eap-identity send-request   ## how to handle EAP identity requests from the client
        set fec-egress enable           ## Forward Error Correction (FEC), for noisy links such as 4G/5G
        set fec-codec rs
        set fec-ingress enable
        set peerid <redacted>           ## Peer ID (local ID on client)
        set ipv4-start-ip 10.32.250.10
        set ipv4-end-ip 10.32.250.30
        set ipv4-netmask 255.255.255.224    ## Subnet mask for mode cfg
        set dns-mode auto               ## Add DNS to mode cfg
        set save-password enable        ## Allow user to store password on client
        set client-auto-negotiate enable    ## Allow client to auto-negotiate the tunnel at startup
```

```
        set client-keep-alive enable        ## Keepalive to maintain idle tunnel
        set psksecret <redacted>            ## Pre-shared key
        set dpd-retryinterval 60            ## Dead Peer Detection
    next
end
```

Stap 2 - Phase 2 configureren

```
config vpn ipsec phase2-interface
    edit "DU-VPN-IPv4"
        set phase1name "DU-VPN"             ## link back to the phase1 interface defined earlier
        set proposal aes256-sha256          ## ESP proposal for the IPsec tunnel (AES-256 + SHA-256)
        set dhgrp 16                        ## DH group for PFS (set to match policy requirements)
        set replay disable
        set keepalive enable                ## keepalive will try to maintain the tunnel association
    next
end
```

Stap 3 - Phase 1 interface configureren

```
config system interface
    edit "DU-VPN"
        set vdom "root"                         ## VDOM the interface belongs to (single VDOM named root here)
        set ip 10.32.250.1 255.255.255.255      ## Local IP assigned to the firewall side of the tunnel (/32
common)
        set type tunnel                         ## mark as a tunnel interface
        set remote-ip 10.32.250.1 255.255.255.224   ## define the remote subnet that clients will be in
(pool/netmask)
        set interface "wan1"
    next
end
```

Stap 4 - Zone aanmaken (optioneel)

```
config system zone                      ## Zone to group the VPN interface for easier firewall policy management
    edit "Z-VPN-DU"
```

```
        set interface "DU-VPN"              ## add the virtual DU-VPN interface to this zone
    next
end
```

Stap 5 - Lokale gebruiker aanmaken

```
config user local
    edit "firstname.lastname"
        set type password
        set email-to "firstname.lastname@example.com"
        set passwd <redacted>
    next
end
```

Stap 6 - Firewall groep aanmaken

```
config user group
    edit "DU-VPN-USERS"
        set member "firstname.lastname"
    next
end
```

Stap 7 - Policy aanmaken

```
config firewall policy
    edit 48
        set name "Dial-up VPN user -> INET"
        set srcintf "Z-VPN-DU"
        set dstintf "wan1"
        set action accept
        set srcaddr "N-10.32.250.0/27"
        set dstaddr "all"
        set schedule "always"
        set service "ALL"
        set logtraffic all
        set nat enable
        set groups "DU-VPN-USERS"
```

```
next
```

Public Cloud - Azure

01 | MGMT interface HA cluster

Inleiding

Standaard heeft een FortiGate in Azure 4 netwerk poorten, namelijk;

- Port1 - Extern
- Port2 - Intern
- Port3 - HA
- Port4 - MGMT

Middels een UDR laat je al het verkeer binnen komen op het IP van Port2.
Internetverkeer gaat naar buiten via Port1

De HA koppeling maakt gebruik van Port3 en MGMT gaat via Port4

Wanneer een FortiGate (Azure) in HA geplaatst word dan worden alle instellingen gesynct, waaronder dus de interfaces.
Dit is voor het MGMT interface niet wenselijk wanneer je beide nodes apart wil monitoren.

Hier is een trucje voor :)

Stap 1 - Log in op de FortiGate (via de Azure console)

Stap 2 - Controleer de VDOM's

```
diag sys vd list
```

Hier zou je het volgende VDOM moeten zien: vsys_ha, dit is het "hidden HA" VDOM

Stap 3 - Navigeer naar het HA VDOM

```
diag sys vd set vsys_ha
```

Stap 4 - Conigureer het MGMT interface

```
config system ha
  set ha-mgmt-status enable
  config ha-mgmt-interfaces
    edit 1
      set interface port4
      set gateway x.x.x.x
    next
  end
  set ha-direct enable
end
```

Stap 5 - Navigeer terug naar het root VDOM

```
diag sys vd set root
```

Tip: ha-direct zorgt ervoor dat onder andere je FortiAnalyzer en FortiManager verkeer via het MGMT interface lopen.