

Manuel de tests



N°	Nom du test	But du test	Description du test	Résultat attendu	Status	Problème possible
1	LEDs Party	Vérifier que l'appareil est bien branché	Brancher le FortiG 80F selon manuel d'installation	LEDs ON/OFF, STATUS, POWER, WAN1 et les ports allumés	<input checked="" type="checkbox"/>	-
2	Mise à zéro de l'appareil	Vérifier que l'appareil a bien été mis à zéro	Au login, entrer "admin" et " "	Demande du système d'un changement de mot de passe	<input checked="" type="checkbox"/>	-
3	Adresse IP venant de pare-feu	Vérifier que le PC recoive bien une adresse ip du pare-feu	Faire un ip config et recevoir une adresse du pare-feu	Adresse IP en 192.168.1.XX	<input checked="" type="checkbox"/>	-
4	Atteindre le GUI	Vérifier la connexion au GUI du pare-feu	Se logger en tant qu'admin avec le mdp mis lors du test 2	Login réussi, accès au dashboard	<input checked="" type="checkbox"/>	-
5	Mise à jour du Firmware	Mettre à jour FortiOS	Dans System -> Firmware: Update Firmware	Changement d'OS pour une version plus récente	<input checked="" type="checkbox"/>	Abonnement nécessaire
6	Changement hostname - date	Vérifier que les changements effectués sont pris en compte	Se logger au GUI et vérifier sur la page Dashboard -> Status	Les deux changements sont visible	<input checked="" type="checkbox"/>	-
7	Nouvel administrateur	Vérifier que le nouvel admin peut se logger	Se logger au GUI avec les infos de l'admin créé	Login réussi	<input checked="" type="checkbox"/>	-
8	Accès à internet	Vérifier que l'on a une connexion au WAN	Ouvrir un browser et tester www.lematin.ch	On réussi à atteindre le site	<input checked="" type="checkbox"/>	-
9	Libération des interfaces	Vérifier que les interfaces physique choisi sont disponibles.	Aller dans Network Interfaces et controller le contenu de Physical Interfaces	On doit y trouver les internal1-4 libéré	<input checked="" type="checkbox"/>	-
10	Création de VLAN	Vérifier que la VLAN a bien été créé	Aller dans Network Interfaces Internal1 et vérifier si un VLAN s'y trouve	Le VLAN ROUGE est visible	<input checked="" type="checkbox"/>	-
11	VLAN utilisable	Vérifier que le VLAN créé peut se faire attribuer un port physique	-	-	<input checked="" type="checkbox"/>	Switch manageable nécessaire
12	Création de sous-réseaux	Vérifier que le sous-réseaux a bien été créé	Aller dans Network Interfaces et vérifier si internal3 s'y trouve	internal3 possède IP/netmask, Admin Access et DHCP Range	<input checked="" type="checkbox"/>	-
13	Attribution d'interface	Vérifier que l'interface libérée au test 9 est disponible	Créer une nouvelle adresse et pouvoir lui attribuer l'interface3	Internal3 est disponible dans le menu déroulant d'Interface	<input checked="" type="checkbox"/>	-

14	Connexion à internet sur internal3	Tester si il est possible de se connecter sur ce port	Ouvrir un browser et tester www.lematin.ch	Connexion doit échouer	<input checked="" type="checkbox"/>	-
15	Création d'adresse pour internet	Vérifier qu'il est possible d'accéder au site dont l'adresse a été crée	Ouvrir un browser et tester www.perdu.com	On doit pouvoir se connecter au site perdu.com	<input checked="" type="checkbox"/>	Pas de DNS
16	DNS?	Vérifier que le problème du test 15 est bien lié au DNS	Ouvrir un browser et tester de ping 104.21.5.178	Pinger doit réussir	<input checked="" type="checkbox"/>	-
17	Création DNS	Vérifier que la règle DNS permettent d'atteindre www.perdu.com	Ouvrir un browser et tester www.perdu.com	On doit pouvoir se connecter au site perdu.com	<input checked="" type="checkbox"/>	-
18	Uniquement perdu.com	Vérifier que seul l'accès à perdu.com est possible	Ouvrir un browser et tester www.lematin.ch	On ne doit pas pouvoir se connecter au matin.ch	<input checked="" type="checkbox"/>	-
19	Règle Open bar	Tester l'inverse qu'internal3: accès à tous les sites	Ouvrir un browser et tester un site internet au hasard	On doit pouvoir se connecter à n'importe quel site	<input checked="" type="checkbox"/>	-
20	Règle block loldle	Tester qu'il est possible de bloquer un site bien précis	Ouvrir un browser et tester l'accès à loldle.net	On ne doit pas pouvoir se connecter se connecter à loldle.net	<input checked="" type="checkbox"/>	-
21	Règles similaire CPNV	Tester si il est possible d'utiliser un filtre web	Essayer d'aller sur www.jeuxvideo.com	On ne doit pas pouvoir s'y connecter	<input checked="" type="checkbox"/>	Pas de FortiGuard
22	Switch	Vérifier la bonne connexion entre le pare-feu et un switch	Brancher un PC non sur le pare-feu directement mais sur le switch	On doit être connecté au réseau correspondant	<input checked="" type="checkbox"/>	-
23	DHCP	Vérifier que toutes les machines sur le réseau recoivent une adresse IP	Brancher deux pc sur le switch du test 23	Les deux PCs doivent recevoir des adresses IP	<input checked="" type="checkbox"/>	-

1 LEDs Party



2 Mise à zéro de l'appareil

Change Password

⚠ You are required to change the default password.

Old Password

New Password

Confirm Password

OK

Logout

3 Adresse IP venant de pare-feu

```
C:\> Administrateur : Invite de commandes

Microsoft Windows [version 10.0.19044.2728]
(c) Microsoft Corporation. Tous droits réservés.

C:\WINDOWS\system32>ipconfig

Configuration IP de Windows

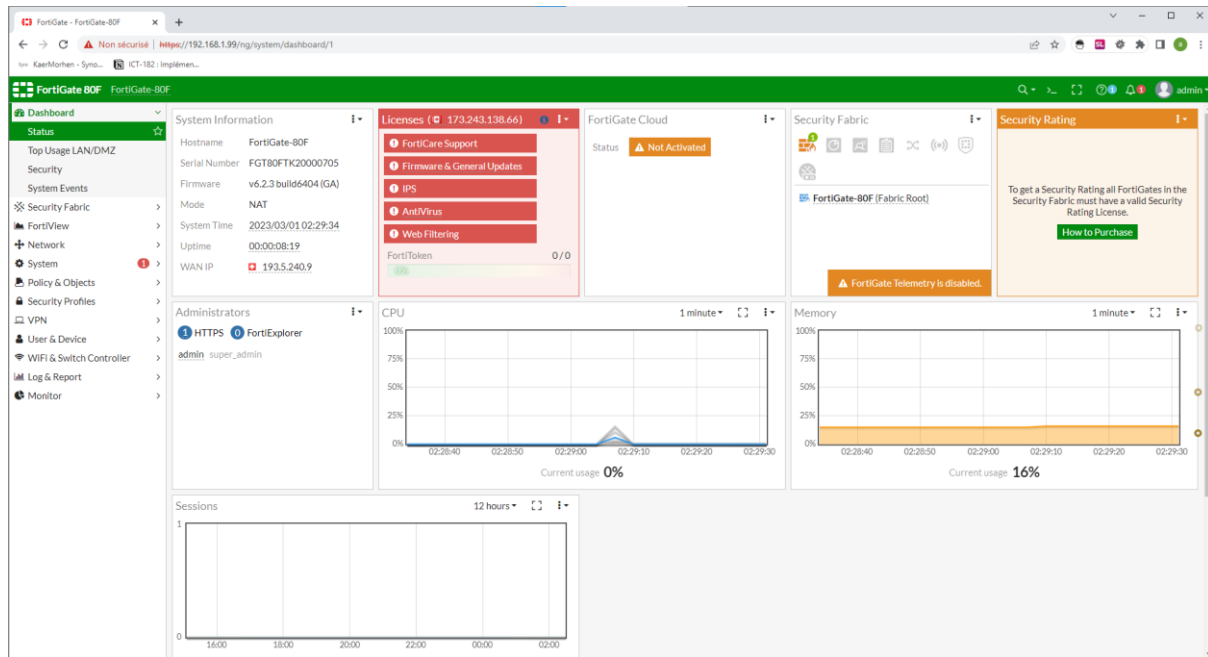
Carte Ethernet Ethernet 2 :

    Statut du média. . . . . : Média déconnecté
    Suffixe DNS propre à la connexion. . . :

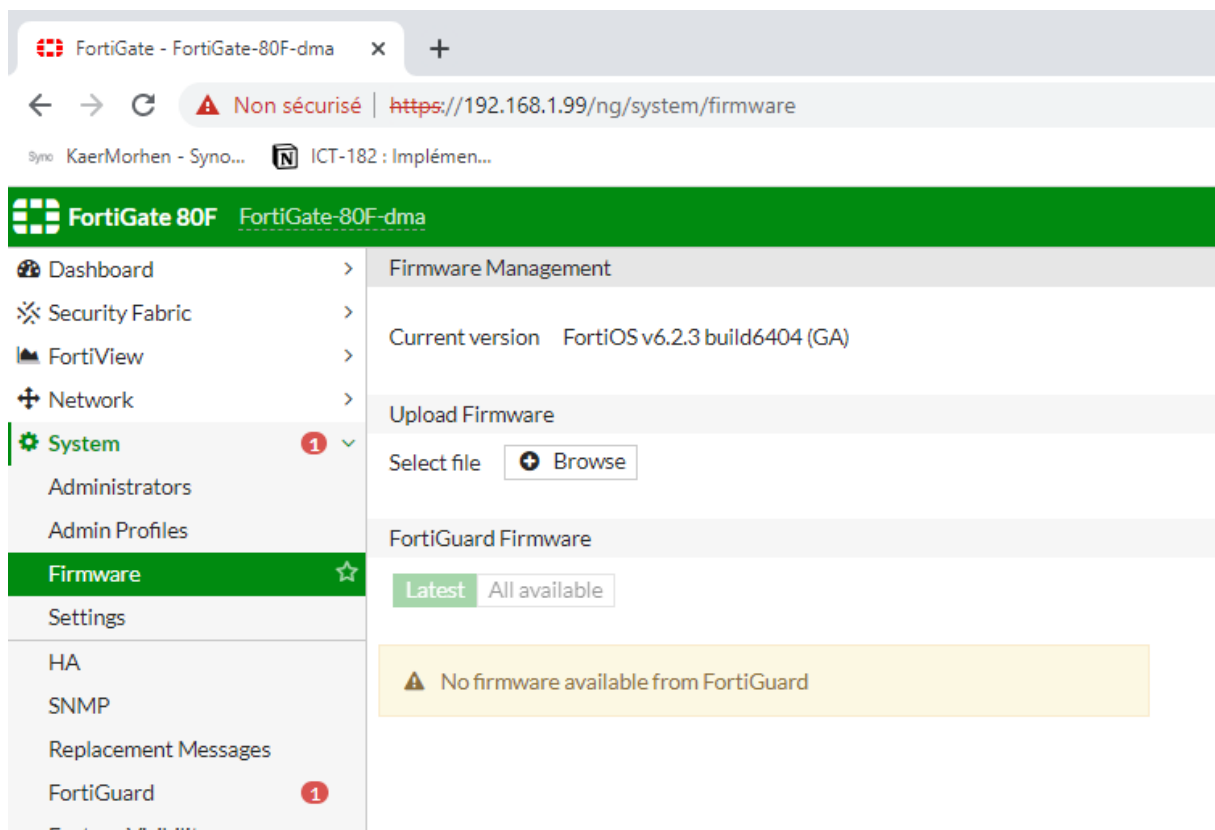
Carte Ethernet Ethernet :

    Suffixe DNS propre à la connexion. . . :
    Adresse IPv6 de liaison locale. . . . : fe80::f98:2aeb:9ab2:3cb1%5
    Adresse IPv4. . . . . : 192.168.1.110
    Masque de sous-réseau. . . . . : 255.255.255.0
    Passerelle par défaut. . . . . : 192.168.1.99
```

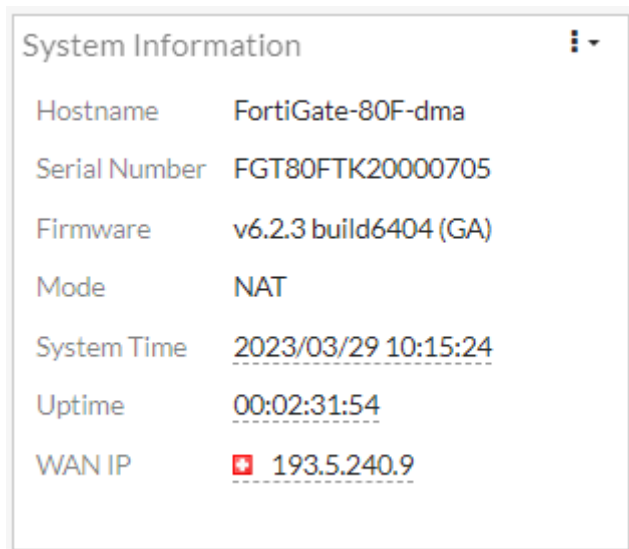
4 Atteindre le GUI



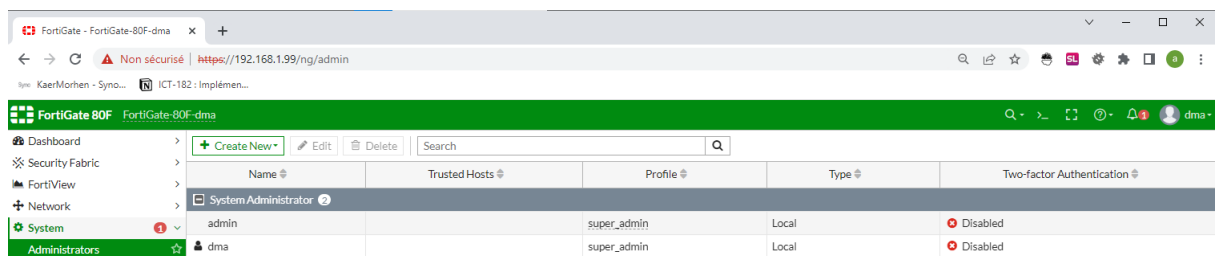
5 Mise à jour du Firmware



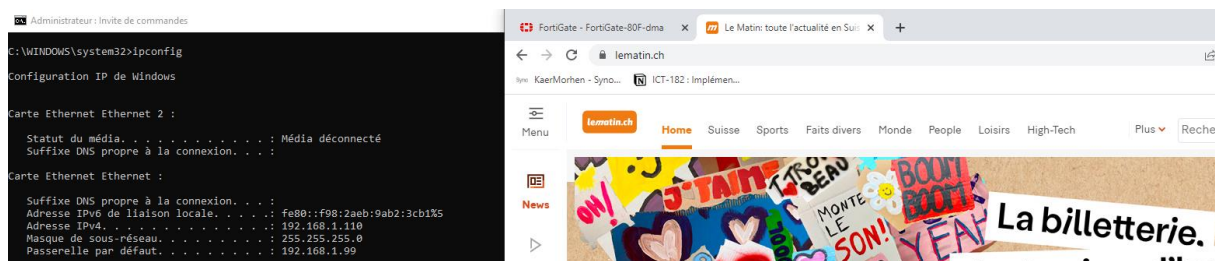
6 Changement hostname – date



7 Nouvel administrateur



8 Accès à internet



9 Libération des interfaces

FortiGate - FortiGate-80F-dma x +

Non sécurisé | https://192.168.1.99/ng/interface

KaerMorhen - Syno... ICT-182 : Implémen...

FortiGate 80F FortiGate-80F-dma

Dashboard
Security Fabric
FortiView
Network

Interfaces

Create New Edit Delete Search

Name	Type	Members	IP/Netmask	Transceiver(s)	Administrative Access	DHCP Clients	DHCP Ranges	Ref.
Hardware Switch								
fortilink	Hardware Switch	a b	Dedicated to FortiSwitch		PING Security Fabric Connection		169.254.1.2-169.254.1.254	2
Internal	Hardware Switch	Internal5 Internal6	192.168.1.99/255.255.255.0		PING HTTPS SSH HTTP	1	192.168.1.110-192.168.1.210	2
Physical Interface								
Internal1	Physical Interface		0.0.0.0/0.0.0.0					2
ROUGE	VLAN		192.168.10.1/255.255.255.0					1
BLEU	VLAN		192.168.20.1/255.255.255.0					1
Internal2	Physical Interface		0.0.0.0/0.0.0.0		PING HTTPS SSH SNMP			0
Internal3	Physical Interface		192.168.30.1/255.255.255.0		PING HTTPS SSH SNMP		192.168.30.2-192.168.30.254	4
Internal4	Physical Interface		192.168.40.1/255.255.255.0		PING HTTPS SSH SNMP		192.168.40.2-192.168.40.254	5

10 Création de VLAN

FortiGate - FortiGate-80F-dma x +

Non sécurisé | https://192.168.1.99/ng/interface

KaerMorhen - Syno... ICT-182 : Implémen...

FortiGate 80F FortiGate-80F-dma

Dashboard
Security Fabric
FortiView
Network

Interfaces

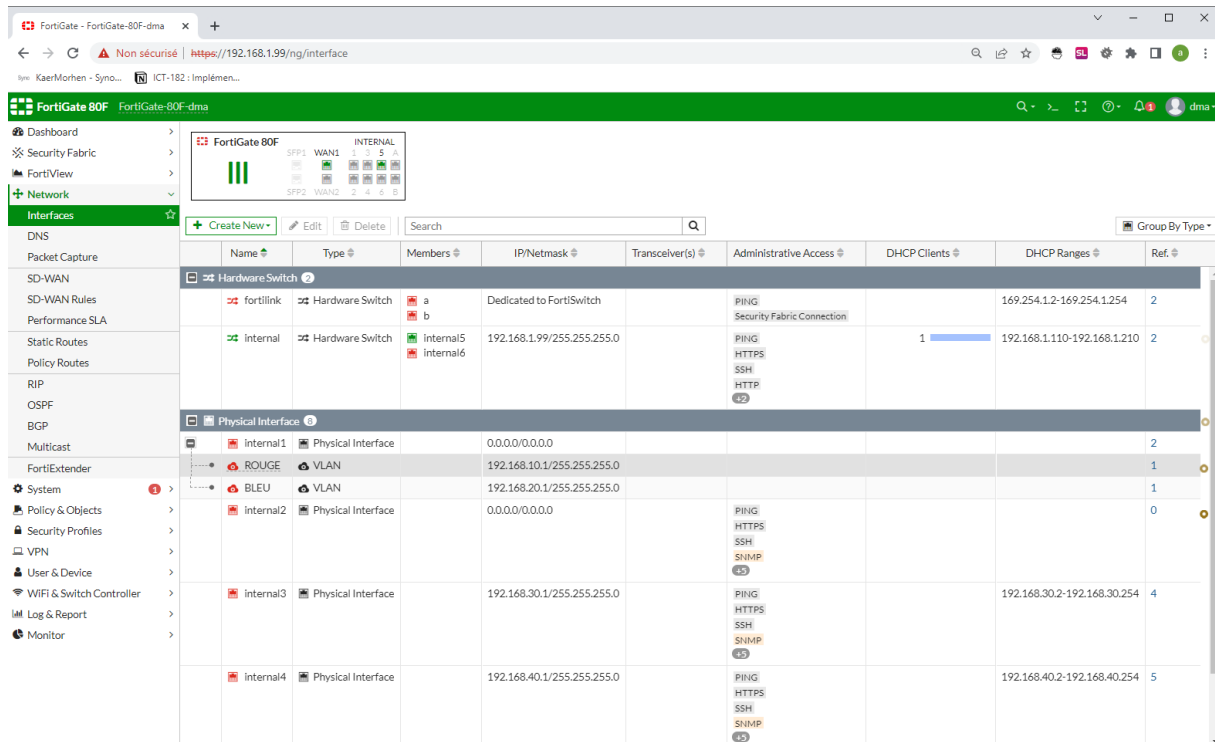
Create New Edit Delete Search

Name	Type	Members	IP/Netmask	Transceiver(s)	Administrative Access	DHCP Clients	DHCP Ranges	Ref.
Hardware Switch								
fortilink	Hardware Switch	a b	Dedicated to FortiSwitch		PING Security Fabric Connection		169.254.1.2-169.254.1.254	2
Internal	Hardware Switch	Internal5 Internal6	192.168.1.99/255.255.255.0		PING HTTPS SSH HTTP	1	192.168.1.110-192.168.1.210	2
Physical Interface								
Internal1	Physical Interface		0.0.0.0/0.0.0.0					2
ROUGE	VLAN		192.168.10.1/255.255.255.0					1
BLEU	VLAN		192.168.20.1/255.255.255.0					1
Internal2	Physical Interface		0.0.0.0/0.0.0.0		PING HTTPS SSH SNMP			0
Internal3	Physical Interface		192.168.30.1/255.255.255.0		PING HTTPS SSH SNMP		192.168.30.2-192.168.30.254	4
Internal4	Physical Interface		192.168.40.1/255.255.255.0		PING HTTPS SSH SNMP		192.168.40.2-192.168.40.254	5

11 VLAN utilisable


Pas d'illustration

12 Création de sous-réseaux



Name	Type	Members	IP/Netmask	Transceiver(s)	Administrative Access	DHCP Clients	DHCP Ranges	Ref.
Hardware Switch								
fortilink	Hardware Switch	a, b	Dedicated to FortiSwitch		PING Security Fabric Connection		169.254.1.2-169.254.1.254	2
internal	Hardware Switch	internal5, internal6	192.168.1.99/255.255.255.0		PING HTTPS SSH HTTP	1	192.168.1.110-192.168.1.210	2
Physical Interface								
internal1	Physical Interface		0.0.0.0/0.0.0.0					2
ROUGE	VLAN		192.168.10.1/255.255.255.0					1
BLEU	VLAN		192.168.20.1/255.255.255.0					1
internal2	Physical Interface		0.0.0.0/0.0.0.0		PING HTTPS SSH SNMP			0
internal3	Physical Interface		192.168.30.1/255.255.255.0		PING HTTPS SSH SNMP		192.168.30.2-192.168.30.254	4
internal4	Physical Interface		192.168.40.1/255.255.255.0		PING HTTPS SSH SNMP		192.168.40.2-192.168.40.254	5

13 Attribution d'interface

Name	Sous-Réseau3
Color	 <input type="button" value="Change"/>
Type	Subnet
IP/Netmask	192.168.30.0/24
Interface	internal3
Show in address list	<input checked="" type="checkbox"/>
Static route configuration	<input type="checkbox"/>
Comments	création adresse Sous-Réseau3 dma

33/255

14 Connexion à internet sur internal3

Pas d'illustration

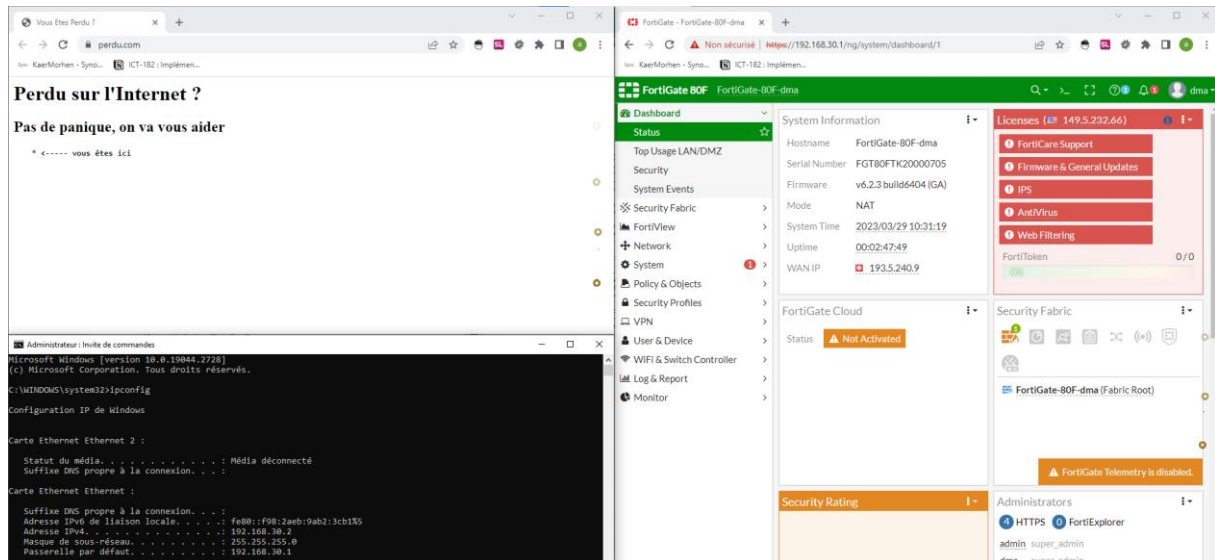
15 Création d'adresse pour internet

Pas d'illustration

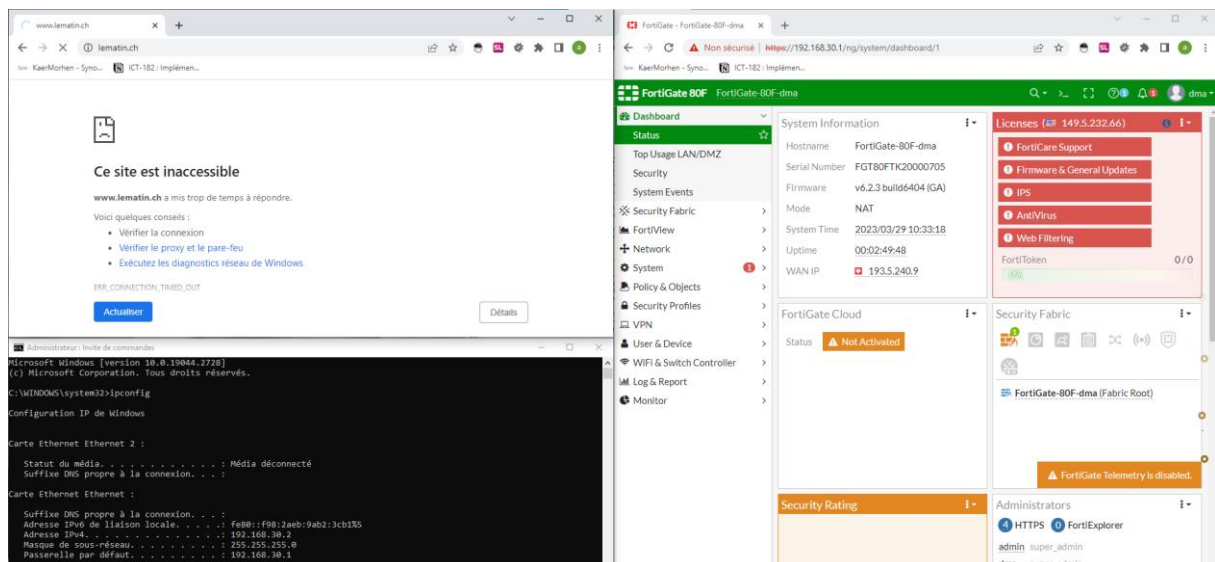
16 DNS?

Pas d'illustration

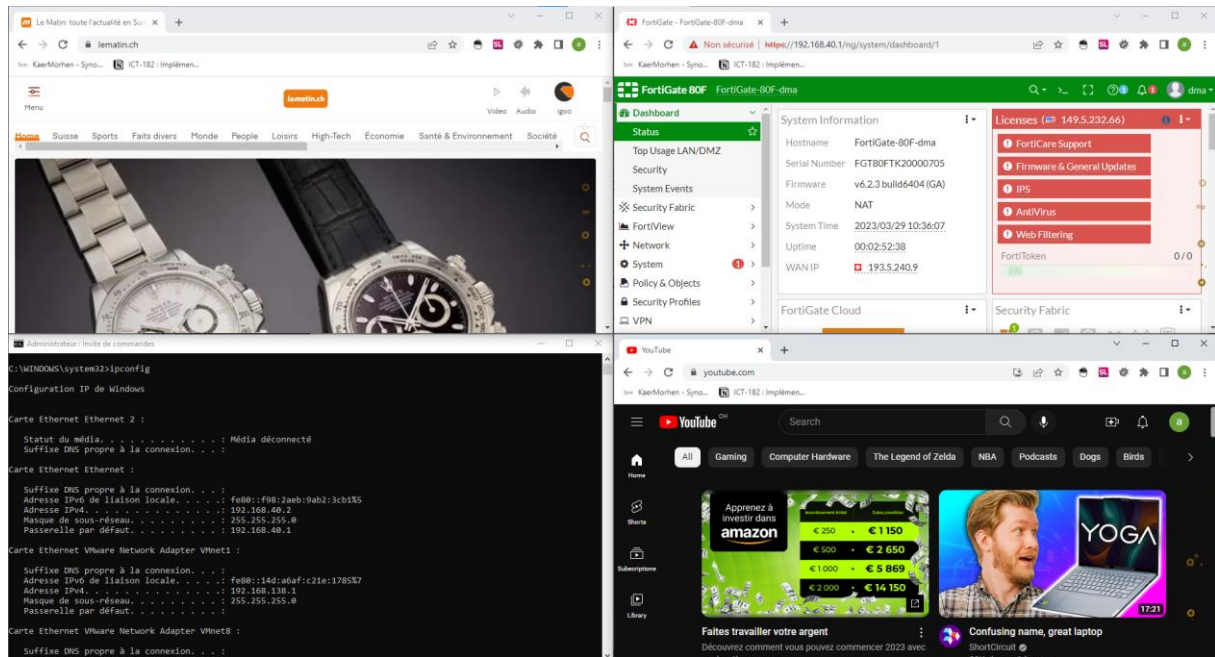
17 Création DNS



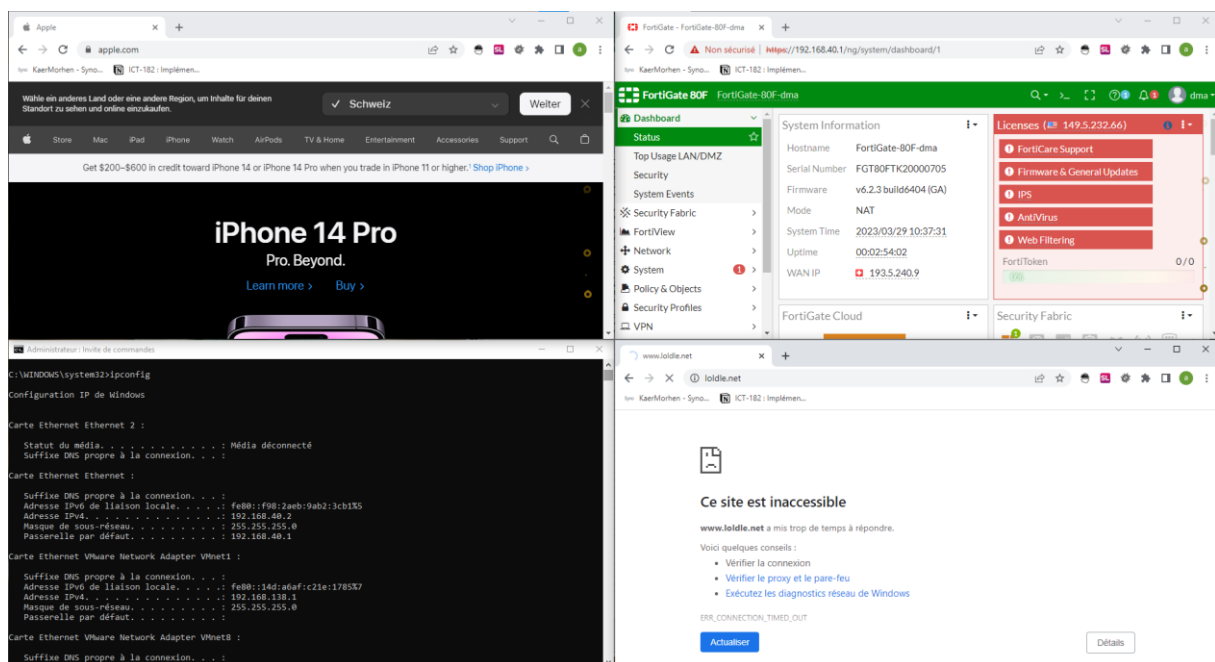
18 Uniquement perdu.com



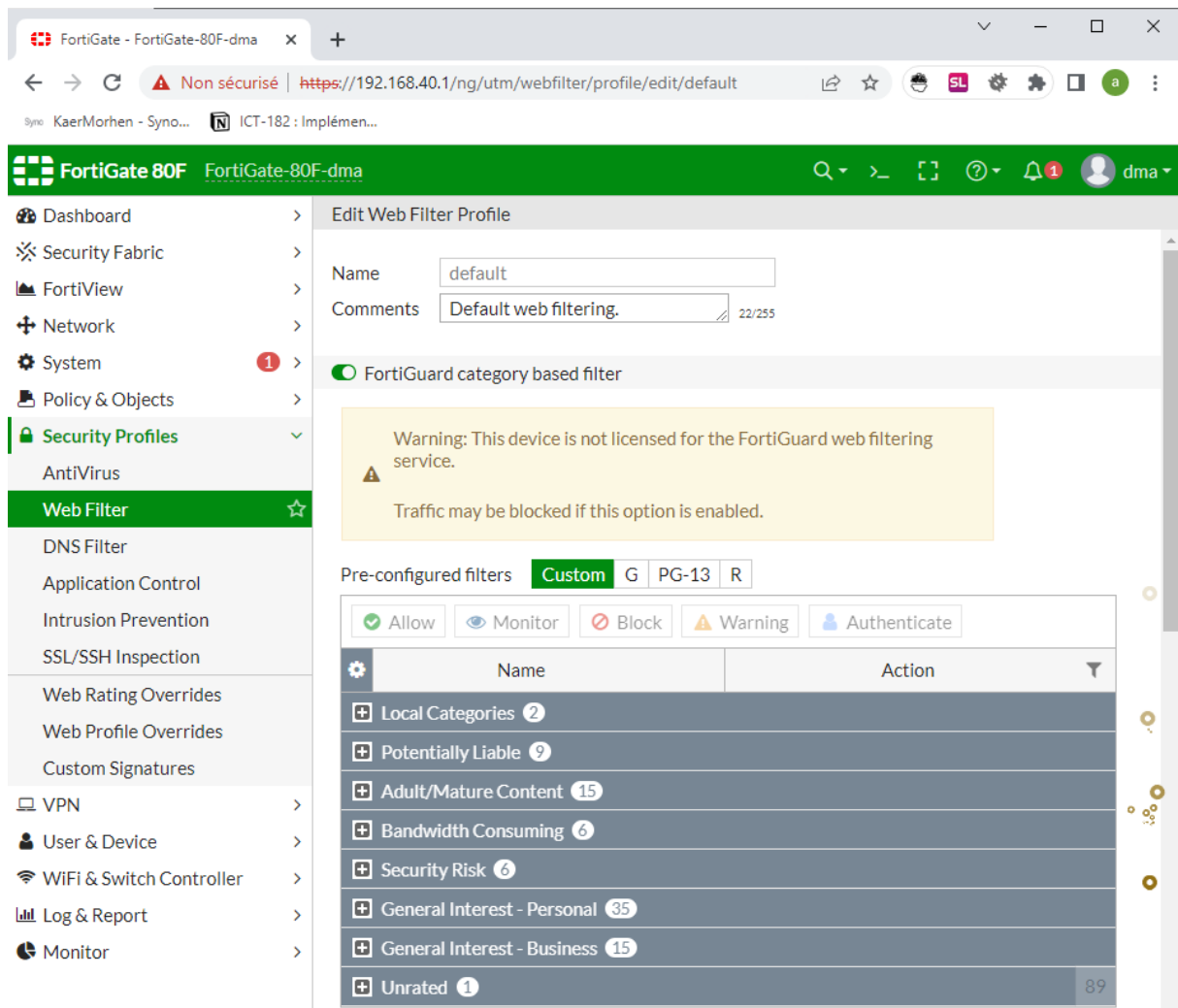
19 Règle Open bar



20 Règle block loldle



21 Règles similaire CPNV



FortiGate 80F FortiGate-80F-dma

Dashboard > Edit Web Filter Profile

Security Fabric >

FortiView >

Network >

System >

Policy & Objects >

Security Profiles >

AntiVirus

Web Filter ☆

DNS Filter

Application Control

Intrusion Prevention

SSL/SSH Inspection

Web Rating Overrides

Web Profile Overrides

Custom Signatures

VPN >

User & Device >

WiFi & Switch Controller >

Log & Report >

Monitor >

Name: default

Comments: Default web filtering. 22/255

FortiGuard category based filter

Warning: This device is not licensed for the FortiGuard web filtering service.

Traffic may be blocked if this option is enabled.

Pre-configured filters Custom G PG-13 R

Allow Monitor Block Warning Authenticate

Name	Action
Local Categories 2	
Potentially Liabile 9	
Adult/Mature Content 15	
Bandwidth Consuming 6	
Security Risk 6	
General Interest - Personal 35	
General Interest - Business 15	
Unrated 1	

89

22 Switch

Pas d'illustration

23 DHCP

Pas d'illustration