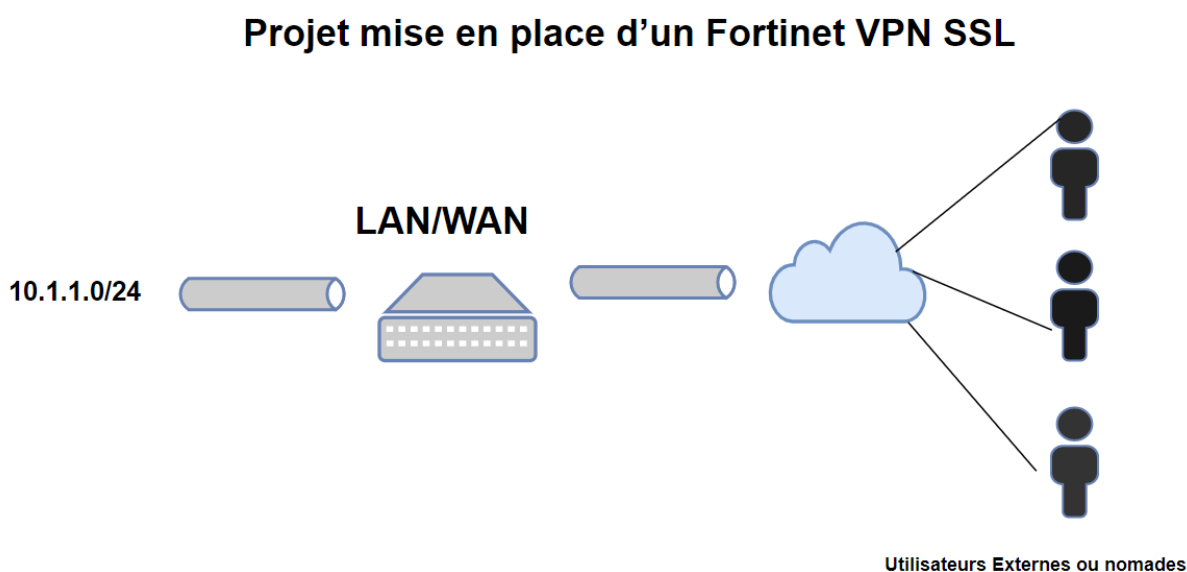


Contexte :

Bonjour je suis dhivina M'bani ,je suis actuellement alternante hébergement et exploitation informatique chez Groupe Avril depuis 2018

Bienvenu dans mon projet, ce projet a pour but permet aux utilisateurs externes ou nomades aient toujours accès aux applications présentes au sein de l'entreprise au travers d'un navigateur web. Dans ce projet, je vais vous montrer comment configurer un Firewall Fortinet (Fortigate) puis nous allons mettre en place un tunnel VPN SSL sur celui-ci afin qu'un utilisateur externe à votre réseau puisse avoir accès à des applications bien spécifiques.

Architecture :

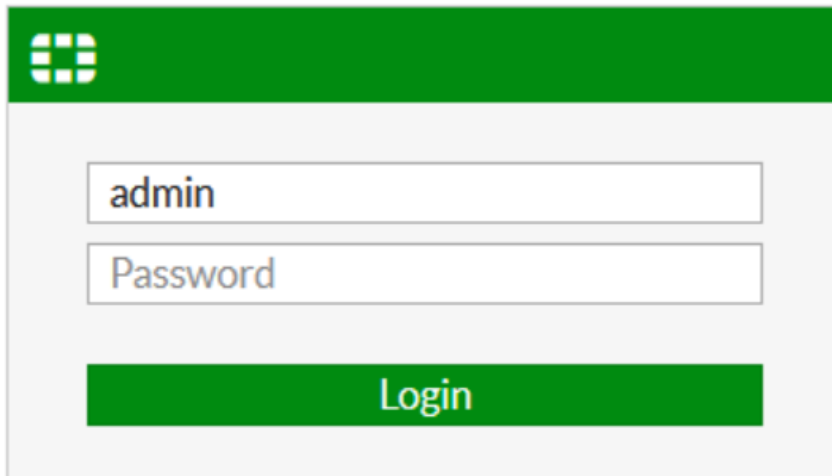


Grâce au **VPN SSL** que je vais configurer et donner l'autorisation aux utilisateurs de se connecter sur certains équipements du réseau interne.

- **En prérequis**

Connexion

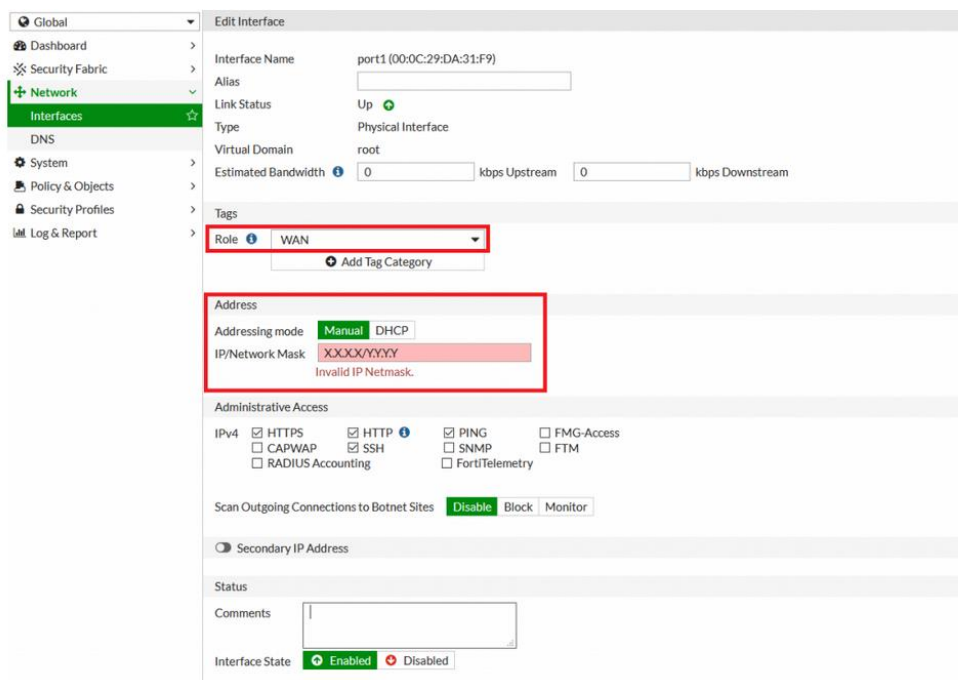
Commencez par vous connecter sur l'interface d'administration du Firewall. Entrez l'adresse IP de votre firewall sur un navigateur Web. Pour vous connecter, les identifiants par défaut sont « admin » pour le login et le champ password sera vide.



The image shows the FortiGate login interface. It features a green header with the FortiGate logo. Below the header, there are two input fields: one for the username 'admin' and another for the password, labeled 'Password'. At the bottom, there is a large green button labeled 'Login'.

1. Configuration des interfaces

Je commence par configurer l'interface WAN qui sera connectée sur mon port physique. Pour le champ « Role » sélectionnez « WAN » et dans la partie « IP/Network Mask » remplacez « X.X.X.X » par l'adresse IP et « Y.Y.Y.Y » par le masque associé.



The image shows the 'Edit Interface' configuration page in the FortiGate web interface. The left sidebar contains a menu with options like Global, Dashboard, Security Fabric, Network, Interfaces, DNS, System, Policy & Objects, Security Profiles, and Log & Report. The 'Interfaces' option is selected. The main area is titled 'Edit Interface' and shows the configuration for the 'port1 (00:0C:29:DA:31:F9)' interface. The 'Role' is set to 'WAN'. The 'Address' section shows the 'Addressing mode' set to 'Manual' and the 'IP/Network Mask' field containing 'X.X.X.X/Y.Y.Y.Y' with a red error message 'Invalid IP Netmask.' below it. The 'Administrative Access' section shows various protocols like HTTPS, HTTP, PING, CAPWAP, SSH, SNMP, RADIUS Accounting, FMG-Access, and FTM. The 'Scan Outgoing Connections to Botnet Sites' section has buttons for 'Disable', 'Block', and 'Monitor'. The 'Secondary IP Address' section is currently disabled. The 'Status' section shows the 'Interface State' as 'Enabled'.

Il faut ensuite configurer l'interface LAN. Dans le champ « Role », renseignez « LAN » puis dans la partie « IP/Network Mask » renseignez l'adresse IP que vous allez affecter à votre firewall ainsi que le masque associé.

Edit Interface

Interface Name: port2 (00:0C:29:45:7E:D2)
 Alias:
 Link Status: Up 🟢
 Type: Physical Interface

Tags

Role: LAN ⌵
 Add Tag Category:

Address

Addressing mode: Manual DHCP One-Arm Sniffer Dedicated to FortiSwitch
 IP/Network Mask: 10.1.1.1/255.255.255.0

Administrative Access

IPv4: ☐ HTTPS ☐ HTTP ☐ PING ☐ FMG-Access
☐ CAPWAP ☐ SSH ☐ SNMP ☐ FTM
☐ RADIUS Accounting ☐ FortiTelemetry

☐ DHCP Server

Networked Devices

Device Detection: ☐

Admission Control

Security Mode: None ⌵

☐ Secondary IP Address

Status: OK Cancel

2. Liaison LAN – WAN

Nous allons maintenant créer une règle afin d'autoriser le trafic du LAN vers le WAN. Allez dans le menu « IPv4 Policy » et cliquez sur « Create New » :

Policy & Objects

IPv4 Policy ☆

IPv4 DoS Policy

Addresses

Wildcard FQDN Addresses

Internet Service Database

Services

Schedules

Virtual IPs

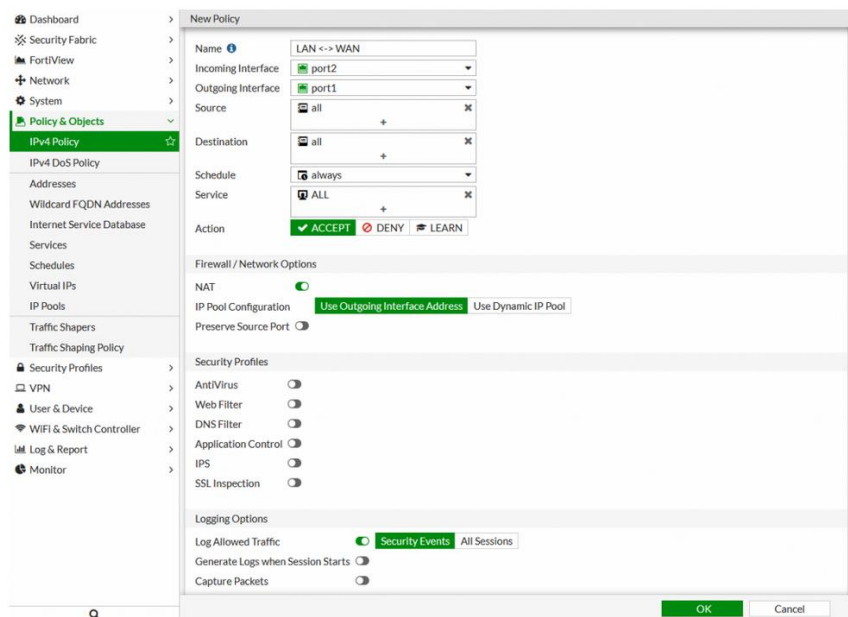
IP Pools

+ Create New

ID

+ Implicit 1

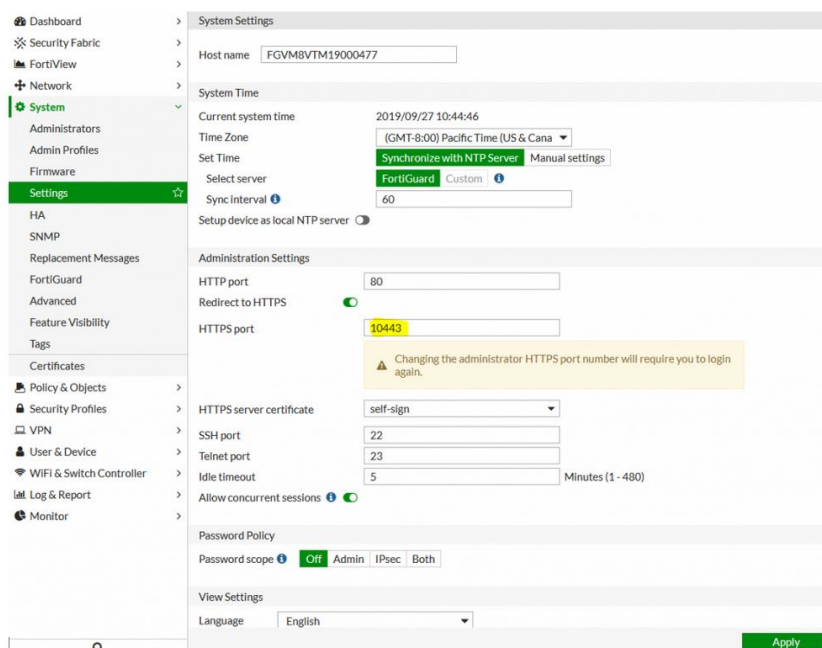
Dans cette règle, je vais autoriser tout le trafic du LAN à aller sur le WAN. Dans un environnement réel, vous devez restreindre les flux selon vos besoins.



3. Configuration VPN SSL sous Fortigate

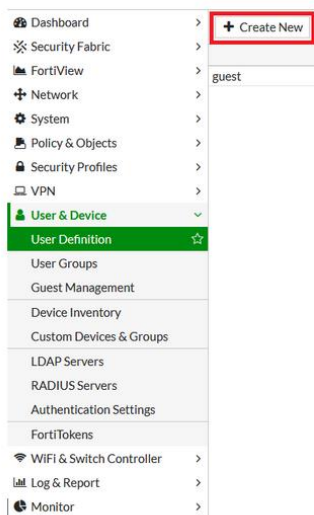
Changement du port d'administration du firewall

Le port par défaut de l'interface d'administration qui est configuré de base sur le port 443.

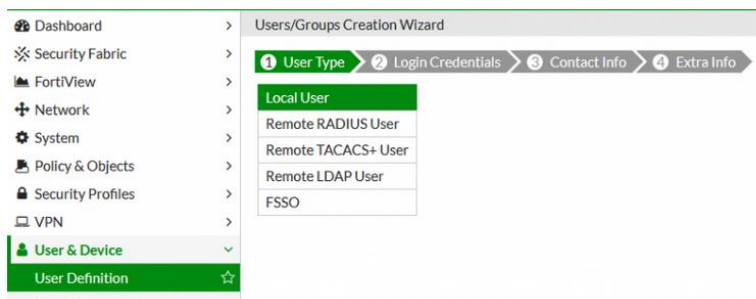


4. Création d'un utilisateur

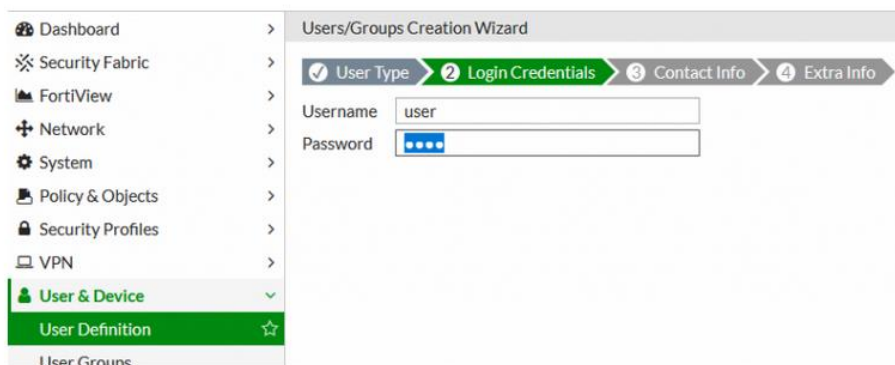
Je vais à présent créer un utilisateur que j' autoriserais par la suite sur le portail **VPN SSL**. Dans le menu cliquez sur « User & Device » puis sur « User Definition » et sélectionnez « Create New ».



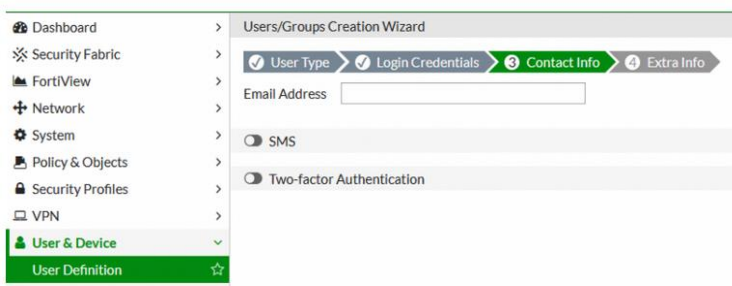
Sélectionnez « Local User » :



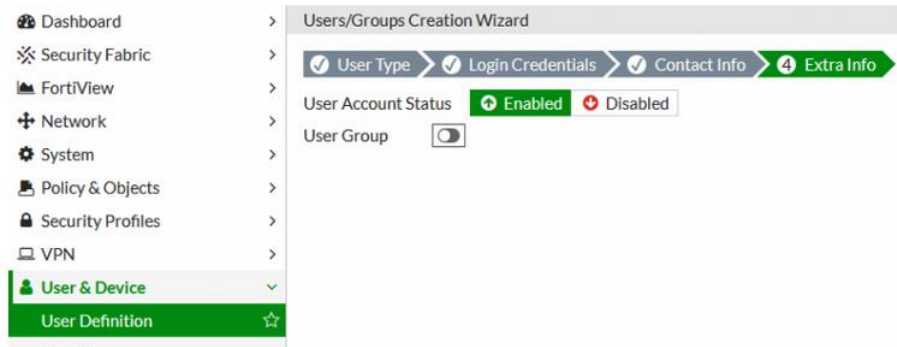
Renseignez le nom d'utilisateur et le mot de passe associé :



Sur la page suivante, laissez par défaut :

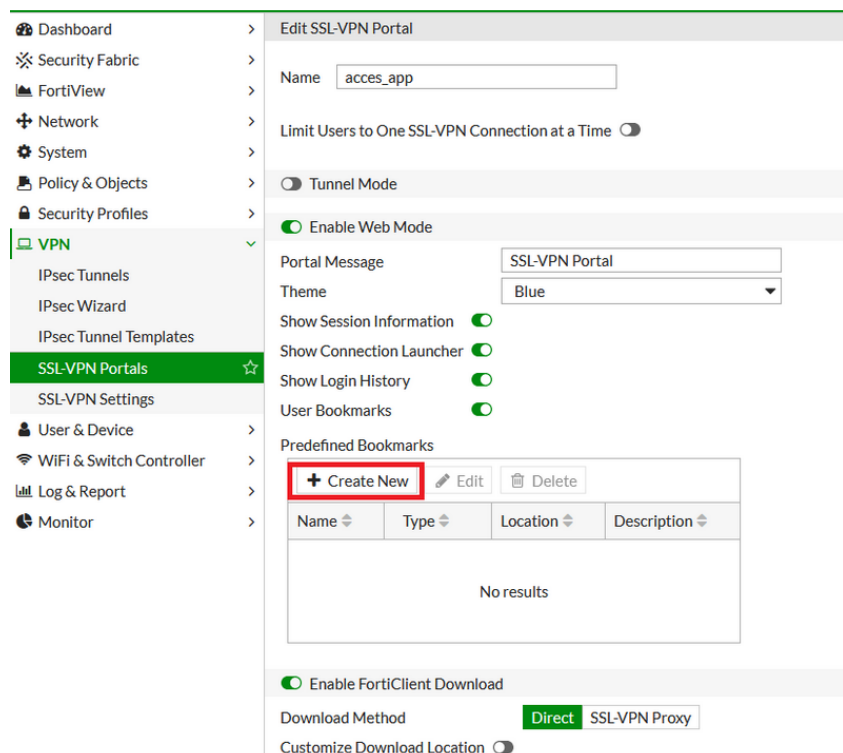


Laissez également par défaut sur la dernière page.

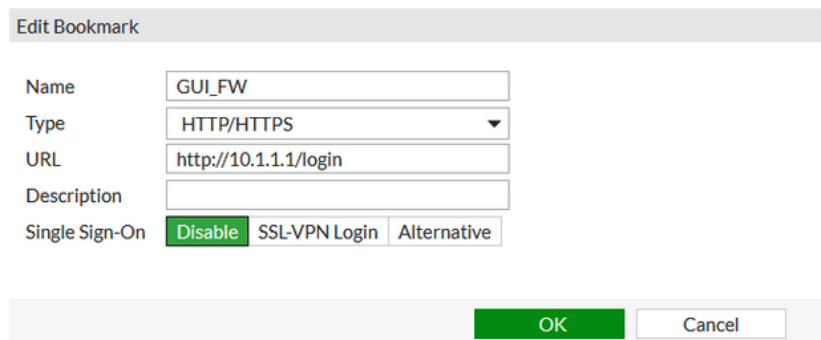


5. Configuration du portail SSL-VPN

Je vais à présent passer à la configuration du portail SSL-VPN. Dans le menu, sélectionnez « SSL-VPN Portals » puis cliquez sur « Create New » :



Dans cet exemple, je vais créer un raccourci pour se connecter sur l'interface Web de mon Firewall. Prérequis, n'oubliez pas d'activer les protocoles HTTP et HTTPS sur l'interface LAN du firewall (menu Network -> Interfaces) :

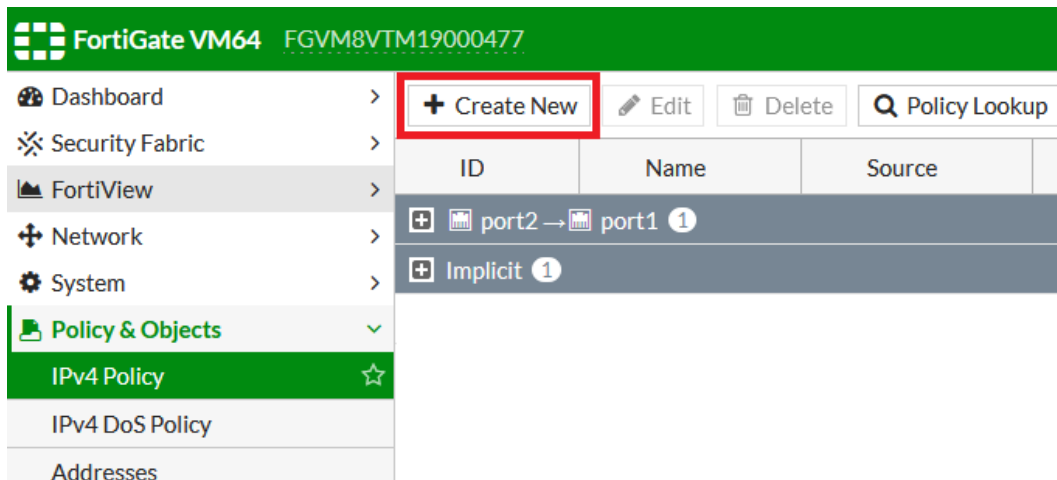


Resultat :

Dans le menu « SSL-VPN Settings », remplissez les champs comme ci-dessous. Sélectionnez bien l'interface Wan pour l'écoute (port 1) :

6. Création des règles de Firewall

Retournez dans le menu « IPv4 Policy » et cliquez sur « Create New » :



Remplissez les champs comme ci-dessous puis validez la règle :

Dashboard > Edit Policy

Security Fabric >

FortiView >

Network >

System >

Policy & Objects >

IPv4 Policy

IPv4 DoS Policy

Addresses

Wildcard FQDN Addresses

Internet Service Database

Services

Schedules

Virtual IPs

IP Pools

Traffic Shapers

Traffic Shaping Policy

Security Profiles

VPN

User & Device

WiFi & Switch Controller

Log & Report

Monitor

Name: access_to_portal

Incoming Interface: SSL-VPN tunnel interface (ssl.root)

Outgoing Interface: port2

Source: SSLVPN_TUNNEL_ADDR1, user

Destination: all

Schedule: always

Service: ALL

Action: ACCEPT, DENY, LEARN

Firewall / Network Options

NAT: ON

Security Profiles

AntiVirus: ON

Web Filter: ON

DNS Filter: ON

Application Control: ON

IPS: ON

SSL Inspection: ON

Logging Options

Log Allowed Traffic: ON Security Events All Sessions

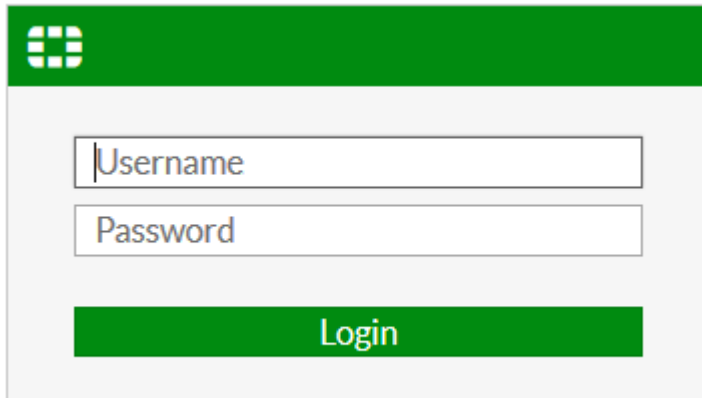
Generate Logs when Session Starts: ON

Comments: Write a comment... 0/1023

OK Cancel

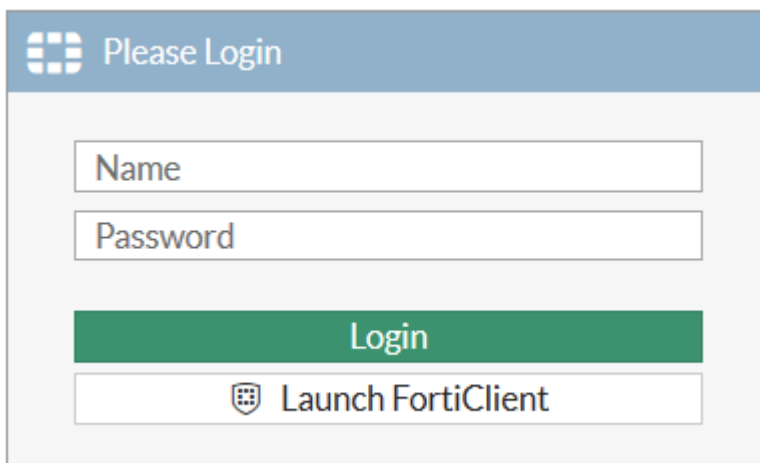
Test

Après toute cette configuration, c'est le moment de tester ! Vous arriverez sur la page d'administration :



A screenshot of a web login interface. It features a green header bar with a white Fortinet logo on the left. Below the header, there are two white input fields: the first is labeled 'Username' and the second is labeled 'Password'. At the bottom of the form is a solid green button with the word 'Login' in white text.

Accédez à votre **VPN SSL** via un navigateur web en saisissant l'adresse suivante : [https://\[VOTRE_IP_PUBLIQUE\]](https://[VOTRE_IP_PUBLIQUE]). Vous devriez voir une page de demande de login s'afficher. Saisissez les identifiants de l'utilisateur créé au début de ce tutoriel :



A screenshot of a 'Please Login' web page. The header is blue with the Fortinet logo and the text 'Please Login'. The main content area is white and contains two input fields: 'Name' and 'Password'. Below these fields are two buttons: a green 'Login' button and a white button with a shield icon and the text 'Launch FortiClient'.

Maintenant que vous êtes connecté à votre **VPN SSL**, vous allez pouvoir tester que le raccourci que vous avez créé fonctionne. Cliquez sur « GUI_FW ».



00:00:11 0 B ↓ 0 B ↑


SSL-VPN Portal


 Download FortiClient ▾

Bookmarks



GUI_FW

 Quick Connection

 New Bookmark

History