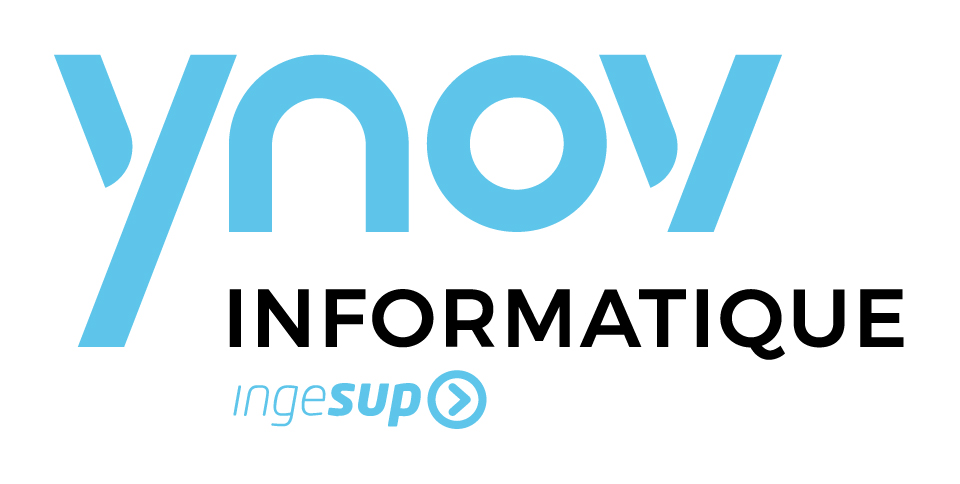
Projet Infrastructure et Cybersécurité

2021



Marie DRAVIGNY

Mohamed MAATOUG

Jean-Maxime ALEXANDRE

Sommaire

I.) Présentation du projet. P.2

II.) Constitution du réseau. P.3

III.) Schéma réseau agnostique. P.4

IV.) Plan d’adressage par environnement. P.5

V.) VM routeur. P.6

VI.) Maquette GNS3. P.7

VII.) Cybersécurité P.7

VIII.) Démo : traçage de paquets avec routage/filtrage fonctionnel. P.11

IX.) Problème rencontré. P.13

X.) Annexe P.14

I.) Présentation du projet.

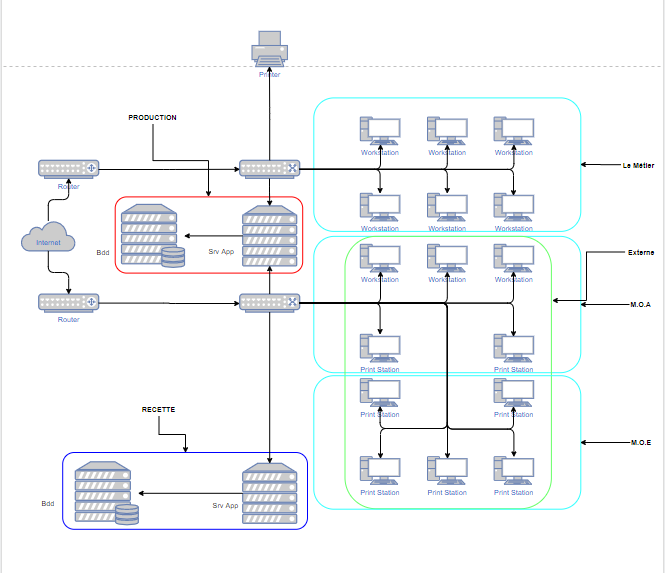
Notre projet consiste à mettre en place une architecture réseau avec des fonctionnalités avancées et de haute disponibilité et d'assurer le paramétrage et le bon fonctionnement du système.

Pour cela nous utilisons le logiciel GNS3 qui nous servira de plateforme de présentation et de test virtuel car nous n’avons aucune possibilité de réaliser le projet en physique.

Nous travaillons sur une machine Windows 10 version …

le réseau est configuré comme suit :

II.) Constitution du réseau.



Nous avons créé un environnement de travail virtuel réparti en fonction des différents services d’une entreprise fictive.

Les Service de M.O.A et M.O.E doivent travailler sur le développement et la maintenance d’un logiciel utilisé par les employés sur le serveur applicatif et la base de données Recette puis ils les livrent pour la production. Le réseau que nous avons mis en place permet de faciliter les échanges et une interopérabilité des services.

Pour les outils :

Postes de type :

- windows 7

- ubuntu

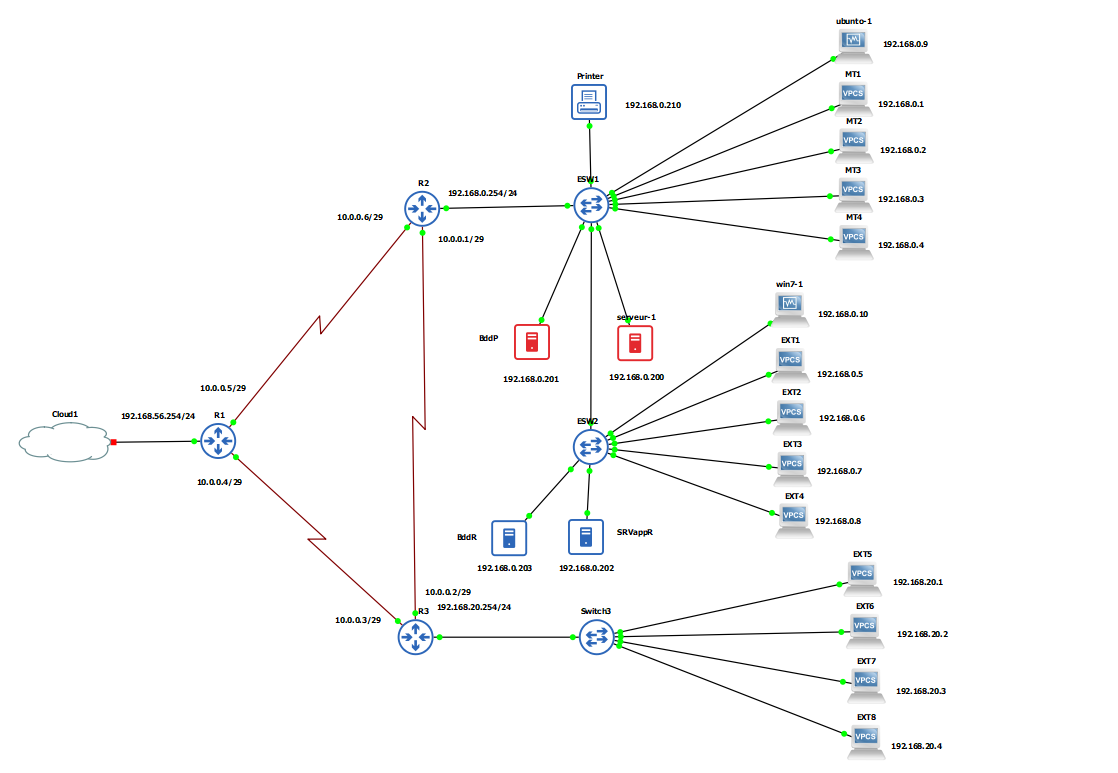
- virtual pc simulateur

- windows serveur 2012

routeur et switch cisco

imprimante

IV.) Plan d’adressage par environnement.



L'adressage du réseau est défini selon son groupe de travail :

Emplyés et M.O.A : 192.168.0.0/24

Le M.O.E : 192.168.20.0/24

Communication possible dans le réseau local ( mais bloqué par le Vlan mis en place )

Par convention elles ne sont pas routées sur Internet (juste en interne)

V.) VM routeur.

nom : Cisco 3725

catégorie : router

platform : c3725

ram : 128

nvram : 256

startup\_config : ios\_base\_startup-config.txt

slot0 : GT96100-FE

configuration des interfaces routeur :

R1 Serial 0/0 10.0.0.5/29 ; Serial 0/1 10.0.0.4/29 ; FastEthernet 0/0 172.16.1.254/16

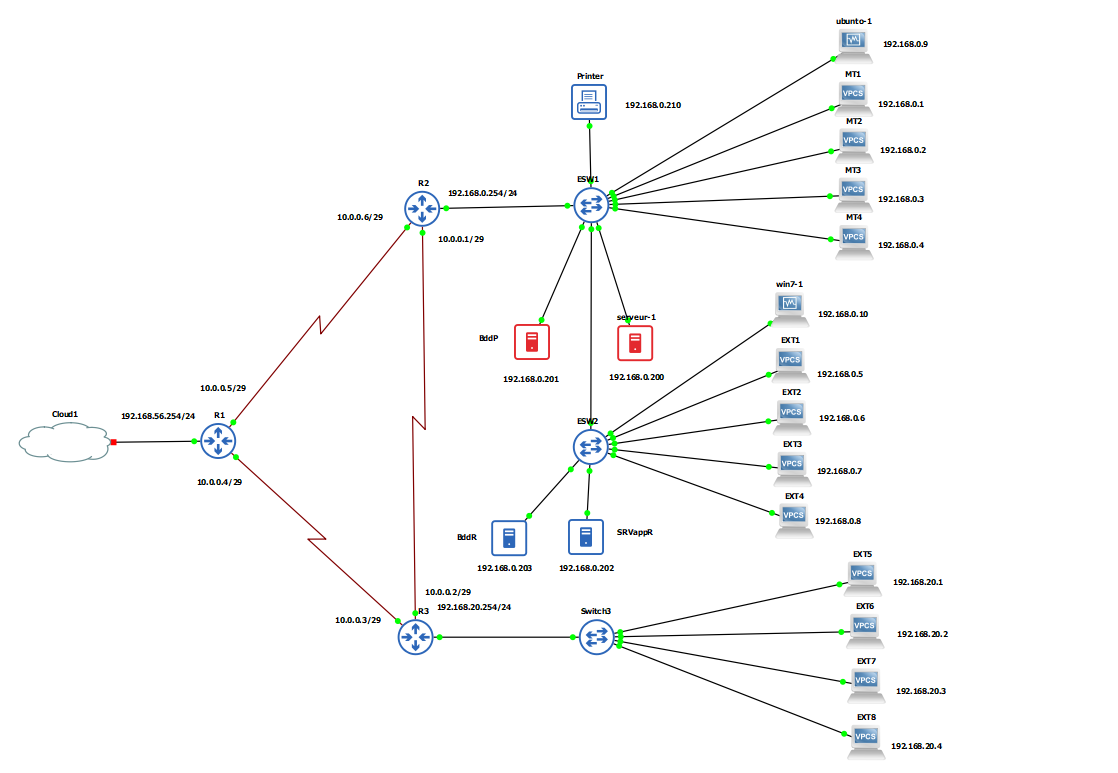
R2 Serial 0/0 10.0.0.1/29 ; Serial 0/1 10.0.0.6/29 ; FastEthernet 0/0 192.168.0.254/24

R3 Serial 0/0 10.0.0.2/29 ; Serial 0/1 10.0.0.3/29 ; FastEthernet 0/0 192.168.20.254/24

Un Ospf a été mise en place pour prendre la route plus courte comme indiqué son nom Open Shortest Path First



VI.) Maquette GNS3.



**VII - ) Partie Cybersécurité :**

**1 - ) Firewall :**

D’après nous la première solution à mettre en place, c’est le firewall : un logiciel et/ou un matériel permettant de faire respecter la politique de sécurité du réseau (document générique qui définit des règles à suivre pour les accès au réseau). Il surveille et contrôle les applications et les flux de données, aussi appelés “paquets”.

C’est une carte maîtresse de la sécurité informatique, et il a pour principale tâche de contrôler le trafic entre différentes zones de confiance (entre nulle et importante), en filtrant les flux de données qui y transitent. Par exemple, entre l’Internet, une zone de confiance à valeur nulle, et un réseau domestique, une zone de confiance à valeur élevée. Il va également être capable d’isoler le réseau en plusieurs zones de sécurité (cf. DMZ plus bas)

**Mise en place du pare-feu :** Après avoir configuré l’infrastructure, nous avons donc commencé à mettre en place la sécurité, et en particulier le pare-feu. Nous avons donc téléchargé ce pare-feu [ici](https://www.gns3.com/marketplace/appliances/cisco-asav) (premier lien) car compatible avec notre version de GNS3. Cependant, après l’avoir installé, notre GNS, et bientôt notre VM, a commencé à planter entièrement (cf. partie Problèmes rencontrés plus bas).

**2 - ) Honeypot :**

En informatique, ce qui est appelé “honeypot”, c’est un “faux réseau” créé uniquement pour attirer les trafics réseaux malintentionnés. Plus grossièrement, on va créer un appât, en faisant d’un honeypot un réseau attrayant en termes de data à voler, afin que les attaquants tentent d’y accéder.

La raison principale pour laquelle un honeypot est mis en place, c’est les précieuses informations qu’il peut retenir des différentes attaques dont il est la cible, qu’aucune autre technique de détection d’intrusion ou de prévention n’est capable de glaner (comme le username, le rôle, les privilèges et l’adresse IP de l’attaquant, ainsi que les données qui sont visées et ce que tape directement l’attaquant sur son clavier lors de l’attaque.)

Avec les informations recueillies par l’honeypot, nous pouvons alors savoir de quelle type d’attaque nous sommes la cible, et ainsi mieux nous préparer en conséquence si une tendance particulière en sort.

De plus, c’est une solution peu coûteuse à mettre en place, et surtout qui peut donner des informations précieuses sur les attaques subies par l’entreprise.

Il y a 2 sortes d’honeypot :

* **L’honeypot “Corporate”** : il va être mis en place en amont dans un environnement de production et va servir à l’analyse des attaques dont il est la cible, afin de renforcer le véritable réseau interne de l’entreprise.
* **L’honeypot de recherche** : toujours dans cet esprit d’analyse, il va aider à voir les différents pattern d’attaques informatiques, ainsi que les raisons de telles attaques, afin que l’entreprise puisse une nouvelle fois mettre en place des solutions spécialement adaptées.

**3 - ) DMZ :**

La troisième solution qui selon nous est à intégrer est la DMZ, qui sert à protéger les éléments les plus vulnérables du réseau, ceux-ci ont un accès extrêmement restreint aux autres services du réseau interne. Les communications entre les hôtes hébergés dans la DMZ et le réseau externe sont très limitées afin de garantir une plus large zone tampon.

Cela permet aux hôtes qui sont dans la partie de réseau qui est protégé d'interagir avec les réseaux internes et externes tandis que le pare-feu se charge de répartir et de gérer le trafic partagé entre la DMZ et le réseau interne.

Dans la DMZ on retrouve les service suivant :

* Les serveur web
* Les serveur de messagerie
* Les serveur FTP

Dans notre projet, nous utilisons un pare-feu unique car cela permet de réduire les coûts mais aussi la complexité du réseau puisque nous avons seulement trois interfaces.

La zone démilitarisée sera alors placée à l'intérieur de ce pare-feu. Son fonctionnement est le suivant : le périphérique réseau externe établit la connexion à partir du FAI (Fournisseur d’Accès Internet), le réseau interne est connecté par le deuxième périphérique, puis les connexions établies dans la DMZ sont gérées par le troisième périphérique réseau.

Les DMZ sont un composant essentiel de tout système de sécurité des réseaux et permettent de protéger les utilisateurs individuels comme les grandes entreprises. Ces zones offrent un niveau de protection supplémentaire en restreignant l'accès distant aux serveurs et aux informations internes, dont la violation serait particulièrement préjudiciable.

**4 - ) La redondance :**

La redondance de routeurs est le fait de mettre plusieurs routeurs dans un même réseau pour que, si l’un tombe en panne, l’autre le remplace. Cela permet de ne pas avoir d’interruption dans l'acheminement du trafic réseau.

Pour mettre en place la redondance de routeurs dans un réseau, il existe deux protocoles. Le premier protocole est appelé HSRP. C’est le premier qui a été créé. Il n’est configurable que sur des routeurs Cisco. Le deuxième, appelé VRRP, est, quant à lui, configurable sur les routeurs de n’importe quel constructeur.

Ces deux protocoles fonctionnent en créant un ou plusieurs routeurs virtuels, communs à plusieurs routeurs réels. Cela permet aux équipements, qui veulent communiquer avec un élément hors du réseau dans lequel ils se trouvent, de le faire en transmettant les données à une passerelle par défaut indifférenciée.

Chaque routeur a un niveau de priorité. Le routeur ayant le niveau de priorité le plus fort est automatiquement désigné comme étant le maître. Lors d’une panne sur le routeur maître, les routeurs sont configurés pour désigner un nouveau maître selon les niveaux de priorité définis. Ainsi, l’équipement qui envoie les données n’a pas à choisir à quel routeur il les transmet, puisque les données sont automatiquement envoyées au routeur qui a le rôle de maître.

**5 - ) VLAN :**

Dans notre architecture on distingue plusieurs services qui travaillent ensemble, il faut donc pour s’y retrouver créer des réseau local virtuel (VLAN) pour éviter que tous les flux de données soient visibles de tous.

Maintenant qu’on sait à quoi sert le VLAN, on peut l’utiliser en fonction de nos besoins. On peut lister les différents VLANs qu’on aura besoin :

VLAN n°2 pour le service Production qui concerne Métier

VLAN n°10 pour le service Recettes qui concerne M.O.A

VLAN n°20 pour le développeur

On crée le VLAN sur le switch puis on attribue ce VLAN sur les ports souhaités. Par exemple le port du switch qui est branché au PC est configuré pour être dans le VLAN et entre chaque switch on a mis en place un Bridge qui va faire passer certain VLAN et bloquer d’autre

**Configuration d’un VLAN sur un switch :**

Nous allons prendre l'exemple du VLAN n°1

SwitchX# configure terminal

SwitchX(config)# vlan 2

SwitchX(config-vlan)# name Production

SwitchX(config-vlan)#end

## 

## 

## **Attribution d’un port dans un VLAN :**

SwitchX# configure terminal

SwitchX(config)# interface fastethernet 0/1

SwitchX(config-if)# switchport access vlan 2

SwitchX(config-if)# end

SwitchX# show vlan

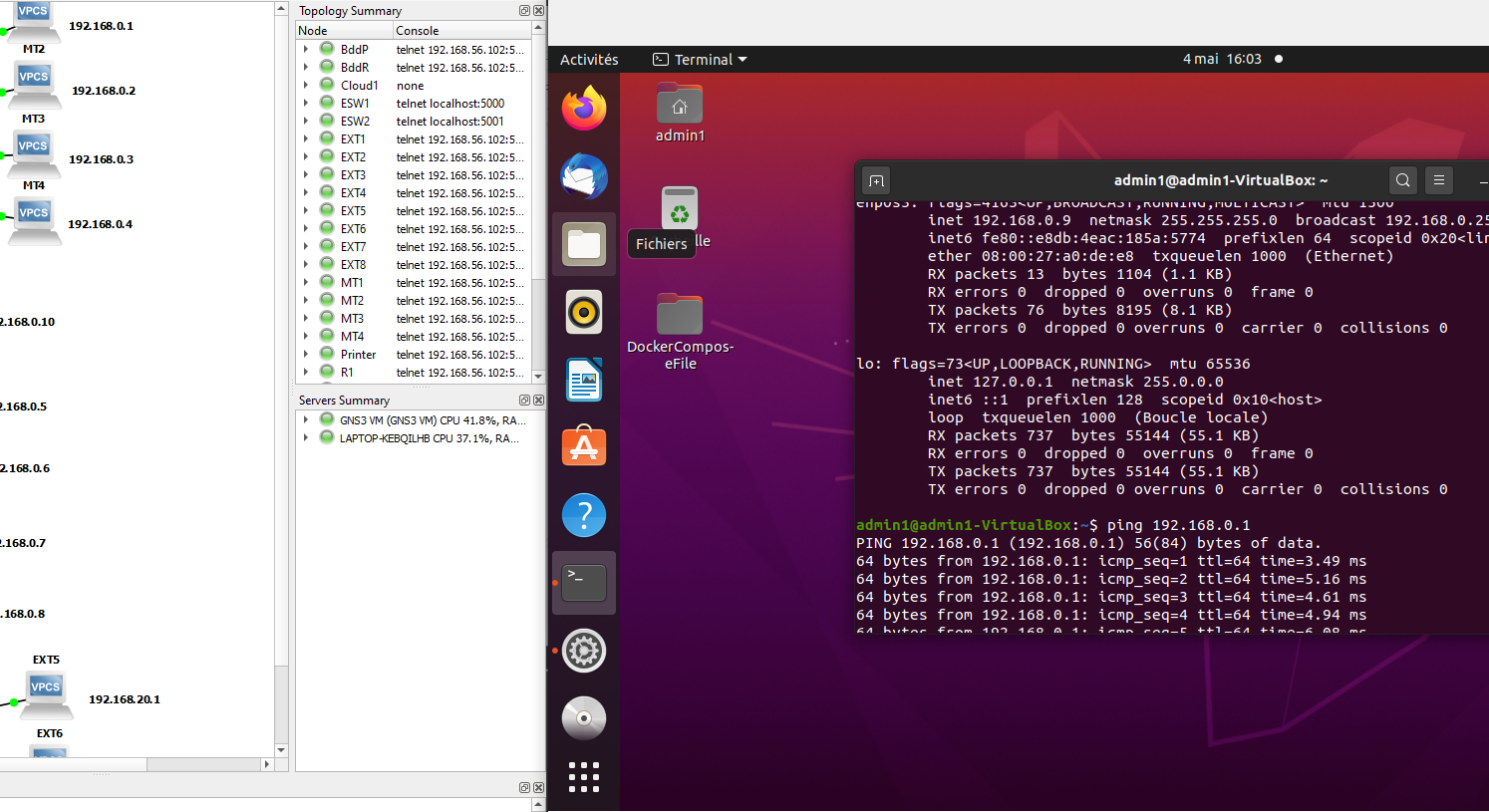
VLAN Name Status Ports

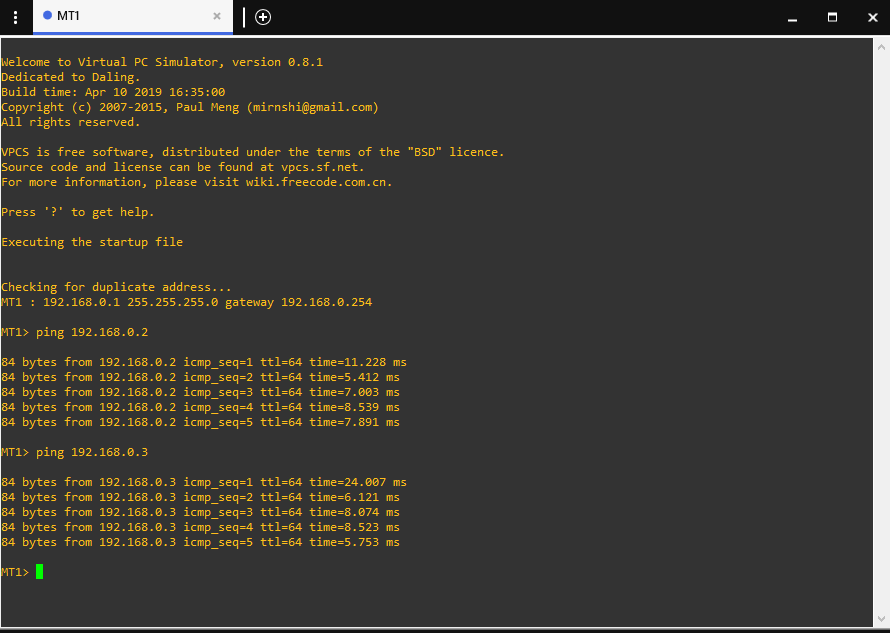
---- -------------------------------- --------- ----------------------

1 default active Fa0/2

2 Production active Fa0/1

VII.) Démo : traçage de paquets avec routage/filtrage fonctionnel





VIII.) Problème rencontré.

Liste non exhaustive des problèmes rencontrés lors de ce projet :

* Virtualbox : soucis de stabilité (plantage régulier et non explicable des VM)
* GNS3 : le versioning et la licence qu’on a du craquer car non fonctionnel en Free-to-use
* firewall : fait planter GNS3
* Routeur : commande qui ne fonctionne pas (pourtant présente dans la doc constructeur)
* Switch : commande qui ne fonctionne pas (pourtant présente dans la doc constructeur)

IX.) Annexe

Doc & Ressource consulté:

* <https://www.comparitech.com/net-admin/how-to-establish-a-honeypot-on-your-network/>
* [https://fr.wikipedia.org/wiki/Réseau\_local\_virtuel](https://fr.wikipedia.org/wiki/R%C3%A9seau_local_virtuel)
* [https://fr.wikipedia.org/wiki/Zone\_démilitarisée\_(informatique)](https://fr.wikipedia.org/wiki/Zone_d%C3%A9militaris%C3%A9e_(informatique))
* <https://www.fortinet.com/fr/resources/cyberglossary/what-is-dmz>