

Liste des zones

Nom de la zone	Interface du FW et VLAN	Adresse ou plage d'adr.	Equipmt réalisant le routage	Adresse routage
Internet	eth0		Pare-feu	11.22.33.45
DMZ In	eth1:0	11.22.33.40/30	Pare-feu	11.22.33.43
DMZ In Admin	eth1:1	192.168.1.0/24	Pare-feu	192.168.1.1
DMZ Out Proxy	eth2	192.168.2.2	Pare-feu	192.168.2.1
Base de données	eth3	192.168.3.2	Pare-feu	192.168.3.1
Mails	eth4	192.168.4.2	Pare-feu	192.168.4.1
Authentification	eth5	192.168.5.0/24	Pare-feu	192.168.5.1
Serveurs métier admin	eth6:0	192.168.60.2	Pare-feu	192.168.60.1
Serveurs métier 1	eth6:1	192.168.61.2	Pare-feu	192.168.61.1
Serveurs métier 2	eth6:2	192.168.62.2	Pare-feu	192.168.62.1
Serveurs métier 3	eth6:3	192.168.63.2	Pare-feu	192.168.63.1
Serveurs Fichiers/impression	eth6:4	192.168.64.2	Pare-feu	192.168.64.1
Postes de travail Admin	eth7:0	192.168.70.0/24	Pare-feu	192.168.70.1
Postes de travail métier 1	eth7:1	192.168.71.0/24	Pare-feu	192.168.71.1
Postes de travail métier 2	eth7:2	192.168.72.0/24	Pare-feu	192.168.72.1
Postes de travail métier 3	eth7:3	192.168.73.0/24	Pare-feu	192.168.73.1
Postes de travail VIP	eth7:4	192.168.74.0/24	Pare-feu	192.168.74.1
Postes de travail DSI	eth7:5	192.168.75.0/24	Pare-feu	192.168.75.1
Impression	eth7:6	192.168.76.0/24	Pare-feu	192.168.76.1

Configuration réseau pour les salles de réunion

Certains utilisateurs de l'entreprise ne sont pas toujours connectés au même point d'accès sur le réseau, mais ils doivent néanmoins conserver leur contexte de connexion quelle que soit leur localisation. Qu'ils aient un bureau tournant ou qu'ils soient dans une salle de réunion, ils doivent être affectés dans le même VLAN et donc disposer des mêmes règles de filtrage, afin d'avoir accès à leurs données et leurs services métier. Affecter un VLAN à un port physique de commutateur ne permet pas de répondre à ce besoin. Cela implique de configurer sur les équipements réseau la fonction d'authentification réseau 802.1x.

Avec 802.1x, lorsque le poste d'un utilisateur se connecte sur un port physique, le switch lui envoie une demande d'authentification. Le switch relaie l'authentification aux serveurs Radius, qui lui-même se repose sur l'Active Directory pour valider l'authentification. L'authentification peut se faire soit avec un mot de passe, soit par certificat client (ce qui est recommandé, car plus robuste).

En plus de relayer la validité de l'authentification, le serveur Radius peut transmettre en attribut de sa réponse le groupe dans lequel figure le poste de l'utilisateur. En fonction de ce groupe, le switch peut positionner le port sur lequel il est connecté dans le VLAN qui correspond à sa zone réseau. Comme la configuration du VLAN dépend de l'authentification du poste et non de l'attribution fixe d'un VLAN à un port physique, la configuration réseau suit l'utilisateur partout où il va dans l'entreprise !