

Présentation

Le serveur 'Kwartz' dispose de fonctionnalités permettant de gérer les flux réseau entrant (qui proviennent de l'Internet : WAN) et à destination des divers services s'exécutant sur le serveur ou sur les postes du réseau local (LAN) mais aussi les flux sortant du serveur vers l'Internet : c'est-à-dire ceux provenant de l'un des services hébergés par le serveur 'Kwartz' (proxy, messagerie, etc.) ou de tout ou partie des postes du réseau local (LAN). Parmi ces fonctionnalités on trouve :

- La gestion des flux par l'intermédiaire du pare-feu (services usuels et autres services).
- La redirection de ports.
- La gestion du trafic entre deux réseaux.
- Les règles d'accès à l'Internet.

Il est essentiel pour le gestionnaire du réseau de bien comprendre le fonctionnement de ces composants.

Nous détaillerons ci-dessous certains de ces services et donnerons quelques exemples à suivre (et d'autres qui doivent être évités car potentiellement dangereux...).

N'oubliez pas que votre fonction de PRTICE/PRNUM vous donne certaines responsabilités (qui vous sont déléguées par votre chef d'établissement) et que vis-à-vis de la loi et des usages d'Internet qui s'effectuent sur votre réseau, vous êtes le premier garant de la sécurité de votre serveur et des postes de votre réseau local.

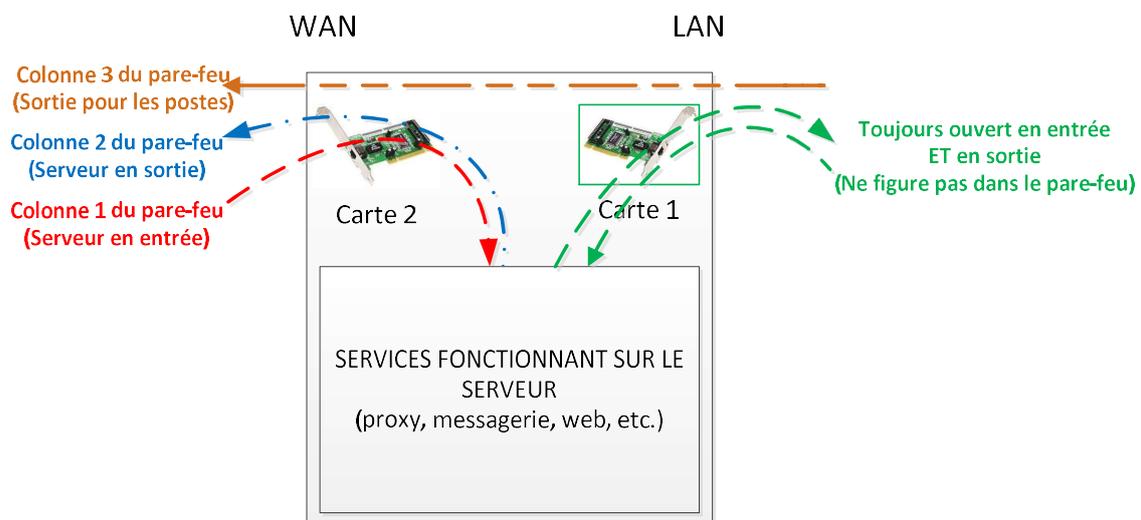
Remarques importantes concernant l'ouverture des ports du pare-feu (services usuels et autres).

a) Organisation

Dans l'option « Pare-feu » du menu « Sécurité » de 'Kwartz~Control', le pare-feu s'organise en 3 colonnes dont les 2 premières correspondent à la carte réseau 2 (réseau étendu : WAN) et dont la dernière correspond à la carte réseau 1 (réseau local : LAN).

| | | | |
|---------|------------------------|-----------|----------------------|
| Service | pour le serveur KWARTZ | | pour tous les postes |
| | en entrée | en sortie | en sortie |

L'organisation est donnée ci-dessous :



b) Concernant la carte 1 du serveur (LAN).

| Services usuels: | | | |
|------------------|------------------------|-----------|----------------------|
| Service | pour le serveur KWARTZ | | pour tous les postes |
| | en entrée | en sortie | en sortie |

Cette carte permet au serveur de dialoguer avec les équipements installés sur le réseau local (et inversement).

Au niveau du pare-feu, aucune action sur la carte réseau 1 n'est nécessaire pour que les postes du réseau local accèdent aux divers services proposés par le serveur 'Kwartz' car tous les ports disponibles en écoute (donc les services proposés) sur le serveur sont accessibles depuis le réseau local.

Cette colonne concernera donc « TOUS LES POSTES » ou « UN POSTE PARTICULIER » du réseau local pour un accès DIRECT vers l'Internet et donc sans aucun filtrage du(des) port(s) concerné(s).

On comprend donc qu'il n'est absolument pas recommandé d'ouvrir les ports http (port 80) et https (port 443) pour tout ou partie des postes du réseau et qu'il faudra plutôt utiliser les règles d'accès Internet afin d'obtenir l'effet désiré...).

c) Concernant la carte 2 du serveur (WAN).

1) **En sortie pour le serveur.**

| Services usuels: | | | |
|------------------|------------------------|-----------|----------------------|
| Service | pour le serveur KWARTZ | | pour tous les postes |
| | en entrée | en sortie | en sortie |
| | | | |

Cela **concerne uniquement les services et applicatifs s'exécutant sur le serveur 'Kwartz' et qui demandent un accès vers l'Internet** sur un port ou plusieurs ports spécifiques (messagerie, Proxy pour l'accès http, https, etc.).

2) **En entrée sur le serveur.**

| Services usuels: | | | |
|------------------|------------------------|-----------|----------------------|
| Service | pour le serveur KWARTZ | | pour tous les postes |
| | en entrée | en sortie | en sortie |
| | | | |

Cela **concerne uniquement l'accès aux services s'exécutant sur le serveur 'Kwartz' et qui devront être accessibles depuis l'Internet.**

Nota 1 :

Il ne sert à rien d'ouvrir un port spécifique en entrée sur le serveur si aucun service fonctionnant sur le serveur n'est en écoute sur ce port.

De même, il est inutile d'ouvrir un port en entrée sur le serveur si vous effectuez une redirection de port.

Nota 2 :

Il est possible d'installer plus de 2 cartes réseau dans le serveur mais nous n'aborderons pas ce cas dans ce document.

Le pare-feu : Les services usuels.

L'interface 'Kwartz~control' dispose d'un grand nombre de services qui peuvent être mis à la disposition des usagers du réseau local (LAN) mais aussi à disposition des usagers externes (WAN).

Dans ce dernier cas le gestionnaire du réseau devra être très attentif aux accès qu'il va autoriser.

Les services usuels sont présentés ci-dessous :

| Services usuels: | | | |
|--|------------------------|-----------------|----------------------|
| Service | pour le serveur KWARTZ | | pour tous les postes |
| | en entrée | en sortie | en sortie |
| Ping | ● | toujours ouvert | ● |
| Web, pages internet (http, https) | non autorisé | ● | non autorisé |
| Extranet KWARTZ non sécurisé (http) | ● | ● | ● |
| Extranet KWARTZ sécurisé (https) | ● | ● | ● |
| Transfert de fichier (ftp) | ● | ● | ● |
| Réception de courrier (pop-3, imap) | ● | ● | ● |
| Réception de courrier sécurisée (pop3s, imaps) | ● | ● | ● |
| MSN / Windows Live Messenger | non disponible | non autorisé | ● |
| Forum (nntp) | non disponible | non autorisé | ● |
| Partage de fichiers (smb) | ● | ● | ● |
| Annuaire LDAP | non autorisé | ● | ● |
| Connexion sécurisée à distance(ssh) | non autorisé | ● | ● |
| KWARTZ~Control | ● | ● | ● |
| Console KMC | ● | ● | ● |
| Connexion réseau privé virtuel(pptp) | ● | non autorisé | ● |
| Maintenance IRIS (ssh) | ● | non autorisé | non autorisé |

[Modifier ...](#)

Les services sont associés à un ou plusieurs ports et/ou à un ou plusieurs protocoles particuliers. Le tableau ci-dessous donne la correspondance pour certains services usuels du pare-feu.

| Service | Protocole et/ou port(s) associé(s) |
|---------------------------------------|--|
| Ping | Protocole ICMP |
| Web, pages internet (http, https) | Port 80/TCP protocole HTTP, Port 443/TCP protocole HTTPS |
| Extranet Kwartz non sécurisé (http) | Port 8080/TCP protocole HTTP |
| Extranet sécurisé (https) | Port 4443/TCP protocole HTTPS |
| Transfert de fichiers (ftp) | Ports 20/TCP, Port 21/TCP protocole FTP |
| Réception de courrier (pop3, Imap) | Port 110/TCP protocole POP3, Port 143/TCP protocole IMAP |
| Réception de courrier (pop3s, imaps) | Port 995/TCP protocole POP3S, Port 993/TCP protocole IMAPS |
| Forum (nntp) | Ports 119/TCP protocole NNTP |
| Partage de fichiers (smb) | Ports 137/UDP, 138/UDP, 139/TCP, 445/TCP protocole SMB |
| Annuaire LDAP | Port 389/TCP protocole LDAP |
| Connexion sécurisée à distance (ssh) | Port 22/TCP protocole SSH |
| KWARTZ~Control | Port 9999/TCP protocole HTTPS |
| Console KMC | Port 4443/TCP protocole HTTPS |
| Connexion réseau privé virtuel (pptp) | Port 1723 – TCP – Protocoles GRE, PPTP |
| Maintenance Iris (ssh) | Port 22/TCP pour une adresse IP spécifique |

Nota :

Le protocole NTP (service de temps sur le port 123/UDP) n'est pas visible dans cette liste mais est ouvert en sortie par défaut. Nous conseillons d'utiliser, pour les équipements du réseau, la synchronisation horaire avec le serveur (script 'logon.bat').

On distingue plusieurs colonnes :

a) Pour le serveur : en entrée.

Cette colonne concerne la carte réseau 2 du serveur 'Kwartz' (qui permet l'accès depuis l'Internet : WAN).

L'activation des services dans cette colonne permet de mettre à disposition des usagers de l'Internet un ou plusieurs services fonctionnant SUR le serveur 'Kwartz'.

Nous allons détailler les différents services usuels proposés pour l'accès au serveur depuis l'Internet.

| Option proposée par le serveur 'Kwartz' | Remarques concernant l'activation. |
|---|---|
| Ping | L'activation de cette option permet à un usager de l'Internet de tester si le serveur est joignable depuis le réseau étendu (WAN). <u>Il est déconseillé d'activer cette option</u> qui est très souvent utilisée par les pirates informatiques pour tester la présence d'une machine depuis l'Internet. |
| Extranet 'Kwartz' non sécurisé (http) | Si cette option est active, elle met à disposition des usagers de l'Internet le service http (fonctionnant sur le port 8080/TCP) du serveur qui permet d'accéder aux <u>sites web stockés sur le serveur 'Kwartz'</u> (Extranet). Les propriétés de l'option « Services web » du menu « Services » de 'Kwartz~Control' permettent de paramétrer ce type d'accès. |
| Extranet 'Kwartz' sécurisé (https) | Si cette option est active, elle met à disposition des usagers de l'Internet le service https (fonctionnant sur le port 8443/TCP) du serveur qui permet d'accéder de manière sécurisée (transmission chiffrée) aux <u>sites web stockés sur le serveur 'Kwartz'</u> . On utilisera ce type d'accès à partir du moment où l'on transmettra des données confidentielles au travers du réseau (page d'authentification par compte et mot de passe par exemple). Les propriétés de l'option « Services web » du menu « Services » de 'Kwartz~Control' permettent de paramétrer ce type d'accès. |
| Transfert de fichiers (ftp) | Si cette option est active, elle permettra aux usagers de l'Internet d'accéder aux fichiers stockés sur le serveur (du moins, ceux qui sont autorisés à l'utilisateur). <u>Nous déconseillons l'ouverture de ce service</u> car il demande une authentification qui circulera 'en clair' sur le réseau. Nous vous conseillons d'utiliser 'Owncloud' ou un client 'WebDAV' (https) pour déposer/récupérer des fichiers de votre espace de stockage sur le serveur 'Kwartz'. Ce service utilise les ports standards 20 et 21/TCP. |

| | |
|--|---|
| Réception de courrier pop-3, Imap) | L'activation de cette option permet à un usager de l'Internet d'utiliser le service de réception de courriers (Pop-3 : port 110/TCP et/ou Imap ; port 143/TCP) s'exécutant sur le serveur 'Kwartz' (lecture des messages stockés sur le serveur). <u>Nous vous déconseillons d'ouvrir ce service.</u> |
| Réception de courrier sécurisée (pop3s, imaps) | L'activation de cette option permet à un usager de l'Internet d'utiliser le service de réception de courriers (Pop3s : port 995/TCP et/ou Imaps ; port 993/TCP) s'exécutant sur le serveur 'Kwartz'. <u>Nous vous déconseillons d'ouvrir ce service</u> (Utilisez plutôt Owncloud). |
| Partage de fichiers (smb) | L'activation de cette option permet de mettre à disposition des utilisateurs du Wan les partages réseau Microsoft du serveur (dont le partage 'ProgRW' accessible à tous en lecture/écriture et sans restriction). <u>Nous vous déconseillons d'ouvrir ce service.</u> |
| Annuaire LDAP | <u>L'annuaire est un service d'authentification qui ne doit être accessible que sur le réseau local</u> (port 389/TCP et port 3268/TCP pour Active directory). <u>Il est très fortement déconseillé d'activer ce service.</u> |
| 'Kwartz~Control' | L'activation de cette option permet à un usager de l'Internet de s'authentifier de manière sécurisée (https sur le port 9999/TCP) afin d'accéder à l'interface de gestion du serveur. Cette option permet à la PRTICE de pouvoir gérer le serveur à distance. Cette option est active par défaut et le mot de passe utilisé doit être complexe. Une alerte de sécurité apparaîtra si le certificat du serveur 'Kwartz' est autosigné (non validé par une autorité de certification externe). |
| Console 'KMC' | L'activation de cette option permet à un usager de l'Internet de s'authentifier de manière sécurisée (https sur le port 4443) afin d'accéder à l'interface de gestion des tablettes de l'établissement. Cette option est active par défaut si le module 'KMC' a été acquis. Une alerte de sécurité apparaîtra si le certificat du serveur 'Kwartz' est autosigné. (non validé par une autorité de certification externe). |
| Connexion réseau virtuel (pptp) | Cette option permet à un poste de l'Internet (après authentification sécurisée de l'usager) d'établir un tunnel sécurisé pour accéder au réseau de l'établissement. Cette option ne doit être active que si vous utilisez cette fonctionnalité. |
| Maintenance Iris (ssh) | Cette option permet à l'éditeur de la solution 'Kwartz' d'établir une connexion sécurisée avec votre serveur. Cette connexion sécurisée est utilisée dans le cadre des maintenances et mises à jour pouvant intervenir. <u>Cette option doit toujours être active.</u> |

b) Pour le serveur : en sortie.

Cette colonne concerne la carte réseau 2 du serveur qui permet l'accès à l'Internet pour les services s'exécutant sur le serveur 'Kwartz'.

L'activation des services dans cette colonne permet au serveur 'Kwartz' de se connecter sur des services externes disponibles sur l'Internet.

Nous allons détailler les différents services usuels proposés pour l'accès du serveur vers l'Internet.

| Option proposée par le serveur 'Kwartz' | Remarques concernant l'activation. |
|---|--|
| Ping | Par défaut, le serveur peut effectuer un 'ping' sur les machines du Wan. |
| Web, pages internet (http, https) | Cette option, <u>qui doit être active</u> , permet au service Proxy exécuté par le serveur 'Kwartz' de transmettre les demandes des postes du LAN pour les accès Internet en http (port 80/TCP) et https (port 443/TCP). |
| Extranet 'Kwartz' non sécurisé (http) | Le serveur Kwartz peut-il effectuer des requêtes http (port 8080/TCP) ? |
| Extranet 'Kwartz' sécurisé (https) | Le serveur Kwartz peut-il effectuer des requêtes https (port 4443/TCP) ? |
| Transfert de fichiers (ftp) | Le serveur 'Kwartz' peut-il effectuer des requêtes FTP (port 20 et 21/TCP) sur les machines du WAN ? |

| | |
|--|--|
| Réception de courrier pop-3, Imap) | Le serveur 'Kwartz' peut-il se connecter à un serveur de l'Internet pop3 (port 110) et/ou Imap (port 143) afin de rapatrier les courriers externes de ses utilisateurs ? Cette option sera dépendante de votre configuration. Dans la majorité des cas cette option sera désactivée. |
| Réception de courrier sécurisée (pop3s, imaps) | Le serveur peut-il se connecter à un serveur de l'Internet pop3s (port 995) et/ou Imaps (port 993) afin de rapatrier le courrier externe de ses utilisateurs ? Cette option sera dépendante de votre configuration. Dans la majorité des cas cette option sera désactivée. |
| Partage de fichiers (smb) | L'activation de cette option permet au serveur 'Kwartz' d'accéder aux partages réseau Microsoft des machines du Wan. Dans la majorité des cas cette option sera désactivée. |
| Annuaire LDAP | L'activation de ce service permet au serveur 'Kwartz' de se connecter à des annuaires externes sur les ports 389/TCP et 3268/TCP pour Active directory. Dans la majorité des cas, cette option sera désactivée. |
| Connexion sécurisée à distance (ssh) | Permet au serveur 'Kwartz' de se connecter en ssh (port 22/TCP) sur des serveurs externes. Par exemple, l'option « Assistance à distance » de 'Kwartz~Control' permet de gérer cela. Dans la majorité des cas cette option sera activée. |
| 'Kwartz~Control' | Permet au serveur 'Kwartz' de se connecter en https sur le port 9999/TCP sur d'autres services 'Kwartz~Control' disponibles sur l'Internet. Dans la majorité des cas cette option sera désactivée. |
| Console 'KMC' | Permet au serveur 'Kwartz' de se connecter en https sur le port 4443/TCP sur d'autres services 'Kwartz~KMC' disponibles sur l'Internet. Dans la majorité des cas cette option sera désactivée. |
| Connexion réseau virtuel (pptp) | Cette option permet au serveur 'Kwartz' d'établir un tunnel sécurisé pour accéder à un poste du WAN. Utilisez l'option par défaut pour ce service. |

c) Pour tous les postes

Cette colonne concerne la carte réseau 1 du serveur 'Kwartz' et permet la communication de TOUT OU PARTIE DES POSTES du réseau local avec l'extérieur (WAN).

L'activation des services dans cette colonne permet à l'ensemble des postes du réseau local (LAN) de se connecter directement sur des services externes disponibles sur l'Internet.

Nous allons détailler les différents services usuels proposés pour l'accès du serveur vers l'Internet.

| Option proposée par le serveur 'Kwartz' | Remarques concernant l'activation. |
|--|---|
| Ping | Les postes du réseau local peuvent-ils effectuer un 'ping' sur les postes du WAN ? |
| Extranet 'Kwartz' non sécurisé (http) | L'ensemble des postes du réseau local (LAN) peuvent-ils effectuer des requêtes http sur le port 8080/TCP ? |
| Extranet Kwartz sécurisé (https) | L'ensemble des postes du réseau local (LAN) peuvent-ils effectuer des requêtes https sur le port 8443/TCP ? |
| Transfert de fichiers (ftp) | L'ensemble des postes du réseau local (LAN) peuvent-ils effectuer des requêtes FTP (port 20 et 21/TCP) sur les machines du WAN ? <u>Nous déconseillons d'utiliser ce protocole qui n'est pas sécurisé.</u> |
| Réception de courrier pop-3, Imap) | L'ensemble des postes du réseau local (LAN) peuvent-ils se connecter à un serveur de messagerie de l'Internet en pop3 (port 110) et/ou Imap (port 143) afin de rapatrier du courrier externe ? Cette option sera dépendante de votre configuration. En cas d'activation, il sera probablement nécessaire d'activer le port SMTP 25/TCP afin que ces postes puissent aussi envoyer du courrier sans passer par l'intermédiaire du serveur 'Kwartz'. <u>Ces protocoles ne sont pas forcément sécurisés.</u> |
| Réception de courrier sécurisée (pop3s, imaps) | L'ensemble des postes du réseau local (LAN) peuvent-ils se connecter de manière sécurisée à un serveur de messagerie de l'Internet en pop3s (port 995/TCP) et/ou Imap (port 993/TCP) afin de rapatrier du courrier externe ? Cette option sera dépendante de votre configuration. En cas d'activation, il sera probablement nécessaire d'activer les ports SMTPS 465/TCP (SSL) et/ou 587/TCP (TLS) afin que ces postes puissent aussi envoyer de manière sécurisée du courrier sans passer par l'intermédiaire du serveur Kwartz. |

| | |
|--------------------------------------|---|
| MSM / Windows Live Messenger | L'activation de cette option permet à l'ensemble des postes du réseau d'accéder aux services MSM/Messenger situés sur l'Internet. <u>En général, cette option est désactivée.</u> |
| Forum (nntp) | Cette option permet à l'ensemble des postes du réseau local de se connecter aux serveurs de news (nntp sur le port 119/TCP et/ou 563/TCP) de l'Internet. Cette option est désactivée par défaut. |
| Partage de fichiers (smb) | L'activation de cette option permet à l'ensemble des postes du réseau local (LAN) d'accéder aux partages réseau 'Microsoft' des machines du Wan. <u>Nous vous déconseillons d'ouvrir ce service.</u> |
| Annuaire LDAP | L'activation de ce service permet à l'ensemble des postes du réseau local (LAN) de se connecter à des annuaires LDAP ou active directory du WAN (sur les ports 389/TCP et 3268/TCP pour Active directory). Cette option est généralement désactivée. |
| Connexion sécurisée à distance (ssh) | Permet à l'ensemble des postes du réseau local (LAN) de se connecter en ssh (port 22/TCP) sur des serveurs externes. Cette option est généralement désactivée. |
| 'Kwartz~Control' | Cette option permet à l'ensemble des postes du réseau local (LAN) de se connecter en https sur le port 9999/TCP sur l'interface 'Kwartz~Control' des serveurs disponibles sur l'Internet. Cette option est généralement désactivée. |
| Console 'KMC' | Permet à l'ensemble des postes du réseau local (LAN) de se connecter en https sur le port 4443/TCP sur d'autres services 'KMC' disponibles sur l'Internet. Cette option est généralement désactivée. |
| Connexion réseau virtuel (pptp) | Cette option permet à l'ensemble des postes du réseau local (LAN) d'établir un tunnel sécurisé PPTP pour accéder à un poste de l'Internet. Cette option est généralement désactivée. |

Le pare-feu : Les autres services

Cette rubrique vous permet de créer vos propres règles d'accès.

Nous vous mettons en garde concernant la création de ces règles car il est facile de créer des règles qui peuvent être potentiellement dangereuses pour votre serveur/réseau (ouverture de port en entrée sur le serveur) ou des règles qui ne correspondent pas à la législation en vigueur (Sécurité des mineurs : filtrage d'accès, obligation de garder les traces des connexions, etc.).

Pour pouvoir créer de manière efficace une règle personnalisée, il vous faudra vous poser les questions suivantes :

- « Qu'est-ce que je veux faire exactement ? ».
- « Quelle est(sont) la(les) machine(s) du réseau local concernée(s) ? ».
- « Le serveur 'Kwartz' est-il aussi concerné par cette action ? ».
- « Quelle méthode vais-je utiliser afin de pouvoir exploiter le service envisagé ? »
- « Cette méthode va mettre en œuvre une communication réseau :
 - Quel(s) sera(seront) le(s) émetteur(s)/initiateur(s) de la communication ?
 - Quel sera le récepteur de la communication ?
 - Quels seront les ports de communication et protocoles concernés pour l'émetteur (et quelquefois du récepteur) ? »

Remarque importante

Il ne faut absolument pas ouvrir tous les ports et tous les protocoles pour un ou plusieurs postes du réseau local.

Afin de donner accès à certains services du web pour un poste ou pour un usager spécifique, on utilisera l'option « Accès à Internet » du menu « Sécurité » de 'Kwartz~Control' (profil des postes, profil des utilisateurs).

Cette possibilité d'ouverture complète devra être utilisée uniquement dans le cadre de tests particuliers (mise au point d'une règle par exemple) mais devra être supprimée (ou désactivée) dès que possible.

N'oubliez jamais que vous n'êtes pas seul sur Internet et que si vous pouvez accéder à des machines/services du Net, les usagers du Net peuvent aussi potentiellement accéder à votre serveur et vos postes.

Quelques exemples :

- a) Je veux que l'ensemble des postes de mon réseau local (postes professeurs) puisse se connecter au serveur 'Pronote' figurant sur le DMZ (patte N° 4 du boîtier 'Fortinet').
- 1) Pour cela, un professeur doit pouvoir se connecter sur l'un des postes du réseau local (LAN).
=> Tous les postes sont potentiellement concernés (colonne 3 active)
 - 2) Le serveur 'Kwartz' n'est pas concerné par cette action car aucun service du serveur 'Kwartz' n'accède au serveur Pronotes.
=> Colonne 2 non active.
 - 3) Le professeur va utiliser un logiciel (client Pronote) pour pouvoir se connecter au serveur Pronote.
 - 4) Le client Pronote se connecte sur le port 49300/TCP (par défaut) du serveur 'Pronote' (j'ai consulté la documentation technique pour savoir cela...).
=> Port 49300 en TCP.
- La réciproque n'est pas vraie : le serveur Pronote ne se connecte pas sur le serveur Kwartz (Il n'existe pas d'applicatif utilisant le port 49300 sur le serveur : ce port n'est pas en écoute sur le serveur).
=> Colonne 1 non active.

Je vais créer la règle qui permettra aux postes du réseau local d'accéder à mon serveur Pronote en DMZ.

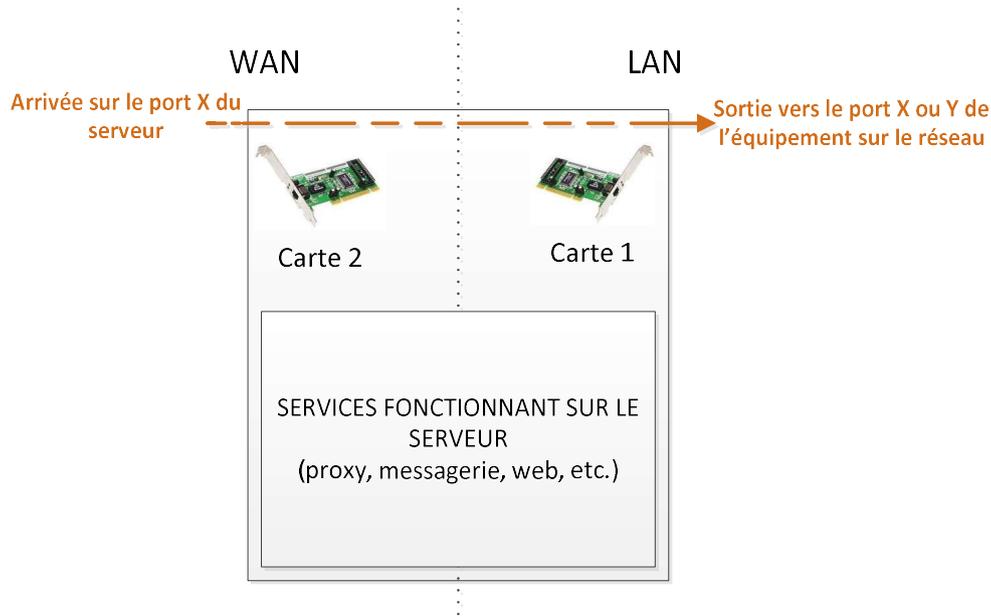
The screenshot shows the configuration for a service named 'Accès SRV Pronote'. The protocol is set to 'tcp' and the port is '49300'. The 'Ouvrir ce service en sortie' section is configured to allow traffic from 'toute adresse IP' to 'toute adresse IP' for 'tous les postes'. Red arrows and text annotations explain the configuration: '1-Cela concerne l'ensemble des postes du réseau' points to the 'Pour' dropdown; '2-Ni le serveur, ni les postes externes ne sont concernés' points to the 'Depuis' dropdown; '3-4-Client Pronote en TCP sur le port 49300' points to the 'Port' field; and 'On donne un nom EXPLICITE à la règle' points to the 'Nom' field.

| | | | | | | |
|-------------------|---|-----|-------|---|---|---|
| Accès SRV Pronote | ● | tcp | 49300 | ● | ● | ● |
|-------------------|---|-----|-------|---|---|---|

- b) Je désire que le poste du documentaliste puisse bénéficier des services externes 'e-sidoc' (duplication des bases BCDI) installés sur son poste.
- 1) Cela ne concerne que le poste du documentaliste.
=> Colonne 3 pour le documentaliste (l'adresse IP de son poste). Les autres colonnes ne seront pas concernées.
 - 2) La documentation technique mentionne que pour exploiter ces services le poste concerné doit accéder à des ressources de l'Internet par :
 - L'ensemble des ports 1024 à 1028/TCP.
⇒ Il faudra créer une règle pour le poste du documentaliste qui permettra la sortie en TCP sur les ports 1024 à 1028.
- | | | | | | | |
|-------------------|---|-----|-----------|---|---|-----------------------------------|
| e-sidoc 1024-1028 | ● | tcp | 1024:1028 | ● | ● | ● (IP du poste du documentaliste) |
|-------------------|---|-----|-----------|---|---|-----------------------------------|
- Le port de connexion 990/TCP devra être utilisé pour le transfert FTPS depuis le poste concerné.
⇒ Il faudra créer une règle pour le poste du documentaliste (colonne 3) qui permettra la sortie en TCP sur le port 990/TCP.
- | | | | | | | |
|-------------------|---|-----|-----|---|---|-----------------------------------|
| e-sidoc transfert | ● | tcp | 990 | ● | ● | ● (IP du poste du documentaliste) |
|-------------------|---|-----|-----|---|---|-----------------------------------|
- Une connexion web sur les ports 80/TCP et 443/TCP devra aussi être possible à partir du poste concerné.
⇒ Ici les accès sur les ports 80/TCP et 443/TCP s'effectuent déjà pour tous les postes du réseau par l'intermédiaire du service proxy du serveur 'Kwartz'. Il faudra donc s'assurer que le système du poste du documentaliste utilise bien le serveur proxy du serveur 'Kwartz' sur le port 3128.
On s'assurera ensuite que le service 'e-sidoc' est fonctionnel sur le poste du documentaliste en activant l'application.

La redirection des ports

La redirection de ports permet de rendre disponible à partir d'Internet un service s'exécutant sur un poste du réseau local. Le schéma ci-dessous illustre cette fonctionnalité.



Remarque importante :

Il est impératif de ne pas utiliser un port d'entrée qui est déjà utilisé par un service s'exécutant sur le serveur 'Kwartz' (80, 8080, 443, 4443, 9000 : serveur 'BCDI', etc.).

Il est recommandé de prêter une attention particulière lors de la création d'une redirection car une mauvaise configuration peut potentiellement mettre en danger la machine cible (voire le réseau local).

Un exemple de redirection.

M. Dupont, professeur de technologie, me demande de mettre en place un accès à partir d'Internet à un applicatif Web d'un serveur du réseau local qui permet le pilotage d'un équipement industriel. Cette application demande une authentification avant accès.

Cet accès est déjà opérationnel à partir du réseau local mais pas à partir d'Internet.

Cet applicatif utilise le protocole https sur le port standard (443/TCP).

Cet accès ne concerne que l'enseignant et permettra la préparation des travaux des élèves.

Dans ce cas de figure, il faudra :

- S'assurer que le service utilisable sur le poste soit suffisamment sécurisé pour être exposé sur le Net : mise à jour du système, des applicatifs installés, de l'antivirus, un pare-feu n'autorisant que les accès entrants nécessaires, etc., mot de passe d'accès au service.
- Etre certain que les accès depuis le Net s'effectueront uniquement à partir du poste personnel de l'enseignant (adresse IP qui ne changera pas).
- Se demander quel sera le port d'entrée à utiliser au niveau du serveur et vers quel port d'entrée rediriger au niveau de l'équipement sur le réseau local.

Suivant ce qui a été dit ci-dessus, j'ai effectué les opérations suivantes :

- a) Sur le poste du réseau local (LAN) qui sera exposé sur l'Internet.
 - Mise à jour du système (et vérification du bon fonctionnement).
 - Mise à jour des applicatifs installés (et vérification du bon fonctionnement).
 - Mise à jour (et vérification du bon fonctionnement) des mises à jour antivirales.
 - Ouverture en entrée du port 443 dans le pare-feu (et suppression des règles d'entrée en ouverture inutiles).
 - Vérification que le mot de passe d'accès à l'applicatif utilise un mot de passe fort (exemple : 8 caractères minimum, 1 majuscule minimum, 1 minuscule minimum, 1 chiffre minimum, 1 symbole minimum).
 - J'ai relevé l'adresse IP du poste (qui doit être une adresse réservée allouée par le serveur : poste client). Ici 172.16.254.200.
- b) Sur le poste du professeur (à son domicile).
 - J'ai récupéré l'adresse IP publique fixe du poste de l'enseignant. Ici 194.195.196.198.

c) Sur le serveur 'Kwartz'.

- J'ai vérifié que le port 443 n'est pas utilisé. Cela n'est pas le cas car le service Web sécurisé du serveur 'Kwartz' l'utilise (port 4443 avec redirection vers le port 443 pour les accès à Owncloud, horde3, sites web, etc.).

J'ai donc choisi le port d'entrée 3333 qui est supérieur à 1024 (ports standards du système) et qui n'est pas utilisé par le serveur.

- J'ai mis en place la redirection suivante :

Redirection d'un port

Nom explicite pour la redirection

Redirection de port

Nom : Dupont-Mach. Outil

Désactiver cette redirection

Protocole utilisé

Protocole : tcp

Port d'entrée sur le serveur

Port : 3333

Adresse du poste externe

Depuis : uniquement cette adresse 194.195.196.198

Port d'entrée sur l'équipement du LAN

Vers le port : 443

Adresse IP locale sur l'équipement du LAN

du poste : 172.16.254.200

[Besoin d'aide?](#)

| Redirection de port: 1 port(s) redirigé(s) | | | | | | |
|--|-------|-----------|------|-----------------|----------------|------|
| Service | Actif | Protocole | Port | Depuis | Redirigé vers | |
| | | | | | Poste | Port |
| Dupont-Mach. Outil | ● | tcp | 3333 | 194.195.196.198 | 172.16.254.200 | 443 |

- Le professeur testera la bonne connexion à partir de son domicile.

Le trafic entre deux réseaux

Nous n'évoquerons pas cette fonctionnalité dans ce document car cela concerne essentiellement des configurations matérielles comportant plus de 2 (ou 3) cartes réseau (ce qui n'est pas la majorité des cas). Si vous disposez d'une telle configuration, nous vous conseillons de vous rapprocher de votre Baip afin de configurer cette fonctionnalité suivant vos besoins.

Les accès Internet

Un prochain document portera sur les accès Internet à partir des équipements du réseau local afin de ne pas surcharger ce document. Nous vous conseillons de vérifier régulièrement la présence de nouveaux documents techniques sur notre site web : <https://webdaip.ac-lille.fr> rubrique « SI et numérique » / « Fiches techniques »..

Conclusion

Nous espérons que ce document vous aura permis de mieux appréhender la configuration des accès à l'Internet de votre serveur.

Vous pouvez laisser vos commentaires et questions sur notre forum : <https://forums-daip.ac-lille.fr>.