

Premiers Pas avec le serveur SLIS

1.0

CARMI INTERNET DE L'ACADÉMIE DE GRENOBLE

Table des matières



| | |
|---|-----------|
| I - Le serveur SLIS | 5 |
| A. Gestion des sous réseaux..... | 6 |
| B. Filtrage web..... | 9 |
| C. Pare-feu..... | 12 |
| 1. Du réseau local vers Internet..... | 13 |
| 2. Autoriser un service dans la DMZ..... | 16 |
| 3. Autoriser un droit d'accès sur la DMZ..... | 19 |
| D. Sauvegarde et restauration..... | 20 |

Le serveur SLIS

| | |
|----------------------------|----|
| Gestion des sous réseaux | 6 |
| Filtrage web | 9 |
| Pare-feu | 12 |
| Sauvegarde et restauration | 20 |

Vous accédez à l'interface d'administration de votre serveur SLIS en vous connectant via un butineur internet à l'adresse suivante :

`https://<nom-de-domaine>:1098`

D'une station du réseau local, vous pourrez aussi utiliser l'URL :

`https://172.16.0.1:1098`

Lors de l'installation du SLIS, une fiche de paramètres vous a été remise (voir exemple ci-dessous). Cette fiche contient l'URL de l'interface d'administration et les identifiants permettant de s'y connecter.

Dans le cas où les coordonnées de l'administrateur n'auraient pas été renseignées à l'installation, elles vous seront demandées à la première connexion.

Remarque : Si vous souhaitez changer le mot de passe du compte "admin", il faut vous reporter à la documentation "*Premiers Pas avec le serveur LCS¹*".

```
PARAMETRES DU SLIS: clg-test
-----
SITE
Code: carmi1
Nom: CARM1 Internet
Ville: Echirrolles, 38

SLIS:
Version: 4.1dkw1
Fop: AMPLIVIA_ADSL
Type routeur: 33
Reseau niveau INTERNET (vers routeur):
Adresse IP: 10.239.32.66
Adresse Nat: 193.54.150.128
Masque: 255.255.255.248
IP routeur: 10.239.32.65
Reseau niveau INTRANET (vers le LAN):
Adresse IP: 172.16.0.1
Masque: 255.255.0.0
Nom de domaine: clg-test.ac-grenoble.fr

INTERFACE D'ADMINISTRATION LOCALE:
URL de l'interface d'administration:
https:// clg-test.ac-grenoble.fr:1098
Utilisateur pour se connecter à l'interface:
Utilisateur: admin
Mot de passe: QSZAhYKS

-----
http://slis.ac-grenoble.fr
```

Fiche de paramètres du SLIS

Après authentification, vous aboutissez sur la page d'accueil de l'interface d'administration du SLIS (voir ci-dessous).



Page d'accueil de l'interface d'administration du SLIS

Le menu de gauche vous permet d'accéder aux différentes fonctionnalités du SLIS. Les voyants verts de bas de page indiquent les services activés.

A. Gestion des sous réseaux

Principe de base

Cette option permet de gérer l'activation ou la désactivation des accès à l'internet des machines situées sur le réseau local.

Chaque machine du réseau appartient à un sous-réseau en fonction de l'adresse IP qui lui est attribuée.

Vous trouverez sur le site "Assistance Technique aux AIPRT" les *préconisations académiques pour le plan d'adressage du réseau local*² des établissements secondaires de l'académie de Grenoble.



Exemple

Dans un établissement, les machines de la salle 104 auront une adresse IP attribuée dans la plage du sous-réseau 172.16.104.1 à 172.16.104.254. Les horaires d'accès à l'Internet des machines de celle salle pourront être gérés indépendamment de ceux des autres salles.

Il pourra être intéressant d'affecter à un même sous-réseau toutes les machines réservées aux professeurs, quelle que soit la salle d'appartenance. On pourra ainsi gérer le filtrage web et les horaires d'accès de ces machines indépendamment de celles réservées aux élèves.

L'accès à la gestion des sous-réseaux se fait par la commande :
Sécurité → Accès → Accès par sous-réseaux

2 - <ftp://ftp.ac-grenoble.fr/assistance.logicielle/intranet.pdf>

| Status | Nom | Adresses des sous-réseaux | Horaire |
|---|--|-------------------------------|---|
| <input checked="" type="checkbox"/>  |  Salle 101 élèves | 172.16.101.1 à 172.16.101.254 |  |
| <input type="checkbox"/>  |  2 | 172.16.102.1 à 172.16.102.254 |  |
| <input type="checkbox"/>  |  Salle 103 élèves | 172.16.103.1 à 172.16.103.254 |  |
| <input type="checkbox"/>  |  Salle 104 élèves | 172.16.104.1 à 172.16.104.254 |  |

Sous-réseau : tableau

Modification des noms des sous-réseaux

Nous conseillons en tout premier lieu de nommer chacun des sous-réseaux utilisés. Pour cela, cliquer sur le bouton "Renommer" à gauche du nom du sous-réseau, saisir le nom du sous-réseau et valider avec le bouton "Modifier".

Création de sous-réseaux

Si les adresses IP des machines de votre établissement ne sont pas incluses dans les plages apparaissant dans la liste, vous pourrez créer les plages nécessaires. Dans la liste déroulante, choisir l'action "Créer un nouveau sous-réseau, puis cliquer sur le bouton "Valider". Renseigner alors "Réseau", "Masque de réseau" et "Nom" puis cliquer sur "Création".

Exemple pour créer le sous-réseau Salle T1 ayant pour plage 172.16.201.1 à 172.16.201.254

- réseau = 172.16.201.1
- masque de réseau = 255.255.255.0
- nom = Salle T1

Suppression de sous-réseaux

Si certaines plages sont inutiles pour votre établissement, vous pourrez les supprimer.

- 1- Sélectionner les sous-réseaux à supprimer. Astuce : si le nombre de sous-réseaux à supprimer est important, sélectionner les sous-réseaux à conserver puis cliquer sur "Inverser la sélection".
- 2- Choisir l'action "Remove the selected subnets" puis cliquer sur Valider.

Basculer d'une activation automatique (programmée) à une activation manuelle ou inversement

- 1- Sélectionner le(s) sous-réseau(x) à basculer.
- 2- Choisir l'action "Passer les sous-réseaux sélectionnés en état manuel" ou "Passer les sous-réseaux sélectionnés en état automatique" puis valider.

Activer ou désactiver un sous-réseau (mode manuel)

Lorsqu'un sous-réseau est en mode d'activation manuel, il est possible de basculer son état (activé/désactivé) de deux façons :

- soit en cliquant sur le bouton "Status" Vert/Rouge.
- soit par sélection puis choix de l'action et enfin validation.

Programmation horaire de l'activation d'un sous-réseau

Pour accéder à la modification de la programmation de l'activation d'un sous-réseau, cliquer sur le bouton "Horaire" correspondant à ce sous-réseau.

Dans la nouvelle page qui apparaît, placer la souris -sans cliquer- sur l'icône "poubelle" d'un des jours de la semaine. L'info-bulle vous indiquera les horaires programmés par défaut pour cette journée.

Pour modifier ces horaires, commencer par les supprimer. Puis sélectionner les horaires souhaités d'activation dans les listes déroulantes ("Activé de ... à ...") et valider avec OK.

Il est aussi possible de recopier les horaires d'un autre jour de la semaine. Pour cela, sélectionner le jour à partir duquel vous souhaitez faire la copie, puis cliquer sur "Copier".

Cliquer sur le lien "Continuer" pour valider les modifications et revenir à la page principale d'administration des sous-réseaux.

Programmation horaires sous-réseaux

B. Filtrage web

Obligation légale

La législation rend obligatoire la mise en place de dispositifs informatiques pour éviter le plus possible l'accès des mineurs à des sites à caractère pornographique, racistes ou violents. Le SLIS répond à cette obligation en mettant en place un filtrage. Ce filtrage, bien qu'imparfait, correspond à l'état de l'art actuel. Il est basé sur *les listes de filtrage de l'université de Toulouse*³ qui sont soutenues par le ministère.

Principe de base

Le filtrage sur le SLIS repose sur un ensemble de bases de filtrage. Ces bases indiquent des sites à autoriser ou interdire. Ces bases sont utilisées dans des règles de filtrage qui indiquent pour les différents sous-réseaux quelles sont les bases à autoriser ou interdire.



Conseil : Modifications

La configuration par défaut correspond aux recommandations académiques. Ne

3 - <http://cri.univ-tlse1.fr/blacklists/>

modifiez cette configuration qu'en connaissance de cause. Si vous modifiez la configuration, vérifiez bien à chaque étape de vos modifications que tout fonctionne, et revenez en arrière en cas d'erreur.

Si vous rencontrez des problèmes, entrez en communication avec l'assistance académique.

Présentation des règles de filtrage

Via le menu de l'interface, vous pouvez accéder à la configuration des règles :

Sécurité → Filtrage web → Édition des règles de filtrage

La liste des règles présentes vous est affichée. Au départ, vous n'avez qu'une règle, la règle par défaut. Vous pouvez ajouter des règles pour certains sous réseaux (pour limiter l'accès aux sites de streaming dans une salle libre service par exemple)

En cliquant sur une règle, vous accédez à sa configuration comme ci-dessous.



Règles de filtrage du SLIS

L'ordre des bases de filtrage dans une règle est important. Elles sont lues du haut vers le bas jusqu'à ce que l'une d'elles s'applique. Les petites flèches à droite d'une base servent à la faire monter ou descendre dans la liste.

Pour modifier une règle, il faut commencer par supprimer la base finale "Laisser_passer - all". Vous modifiez ensuite la règle. Une fois que les modifications sont terminées, vous rajoutez la règle "Laisser_passer - all" qui doit être la dernière règle.

N'oubliez pas de valider vos modifications.

Présentation des bases de filtrage

Les règles de filtrage reposent sur les bases de filtrage. Vous pouvez utiliser des bases de filtrage personnalisées. Cette opération doit être menée avec précaution.

Une mauvaise configuration de vos bases de filtrage risque de bloquer la configuration du SLIS et de vous interdire tout accès à l'Internet pour l'ensemble de l'établissement. En cas de problème, contactez l'assistance académique.

Les bases de filtrage pré-installées du SLIS sont mises à jour toutes les nuits à partir des listes de l'université de Toulouse. Elles ne peuvent pas être modifiées localement.

Vous pouvez créer des bases de filtrage personnalisées. Elles pourront servir pour autoriser certains sites (elles seront utilisée en "laisser passer" dans une règle) ou

pour interdire certains sites (utilisation en "bloquer" dans une règle.)

Pour accéder à la création d'une base personnalisée via le menu :

Sécurité → Filtrage web → Édition des bases de filtrage

Vous aurez alors la possibilité d'éditer vos bases personnelles où d'en créer de nouvelles.

En fin de création ou d'édition d'une base, ne pas oublier de cliquer sur le bouton "Appliquer les modifications".

Création ou édition d'une base de filtrage personnalisée

Une base de filtrage comprend trois parties :

- Une liste d'URL, c'est à dire une liste de pages web. A cet endroit, on va interdire des pages spécifiques mais pas tout un domaine.
- Une liste de domaines. Ici, ce sont des domaines complets de l'Internet que vous spécifiez. Attention de ne pas être trop restrictif.
- Une liste d'expression régulière. **Sauf si vous savez exactement ce que sont les expressions régulières, ne les utilisez pas.** La mauvaise utilisation des expressions régulières est l'une des principales cause de dysfonctionnement des serveurs SLIS.

Soyez bien attentif à ne pas mélanger les URLs et les domaines.



Exemple : Méthode simple pour personnaliser une règle

1- Créer 2 bases personnalisées (voir "Présentation des bases de filtrage") :

- une base appelée par exemple "Autorisations", dans laquelle on listera tout ce que l'on souhaite laisser passer (contenus normalement bloqués par les bases pré-installées),
- une base appelée par exemple "Interdictions", dans laquelle on listera tout ce que l'on souhaite interdire en plus du filtrage par défaut.

2- Modifier ensuite la "Règle par défaut" (voir "Présentation des règles de filtrage") :

- supprimer la base "all" en cliquant sur l'icône poubelle à gauche,
- ajouter la base "Autorisations" avec la consigne "Laisser_passer" et la positionner en haut de la liste (utiliser les flèches vers le haut),
- ajouter la base "Interdictions" avec la consigne "Bloquer" (en bas de la liste),
- remettre en place la base "all" avec la consigne "Laisser_passer" (en bas de la liste),
- appliquer les modifications en cliquant sur le bouton correspondant et attendre le message de confirmation "Changements pris en compte" avant de tester ces modifications.

Enrichissement des bases nationales

Afin d'améliorer les performances et la qualité du filtrage, un retour d'information est nécessaire. Il permet de supprimer de la liste des sites injustement filtrés et d'ajouter dans chaque catégorie de nouveaux sites découverts par les administrateurs et les utilisateurs.

Le ministère a mis en place *une page destinée à la mise à jour de ces sites*.⁴

Un ensemble de moteurs logiciels analysera la page soumise et une vérification visuelle aura lieu si besoin avant l'incorporation du site dans les listes.

La participation de chacun, par l'intermédiaire de ce dispositif, permettra d'obtenir une liste de plus en plus performante.

C. Pare-feu

Rôle d'un pare-feu

Principaux flux réseau

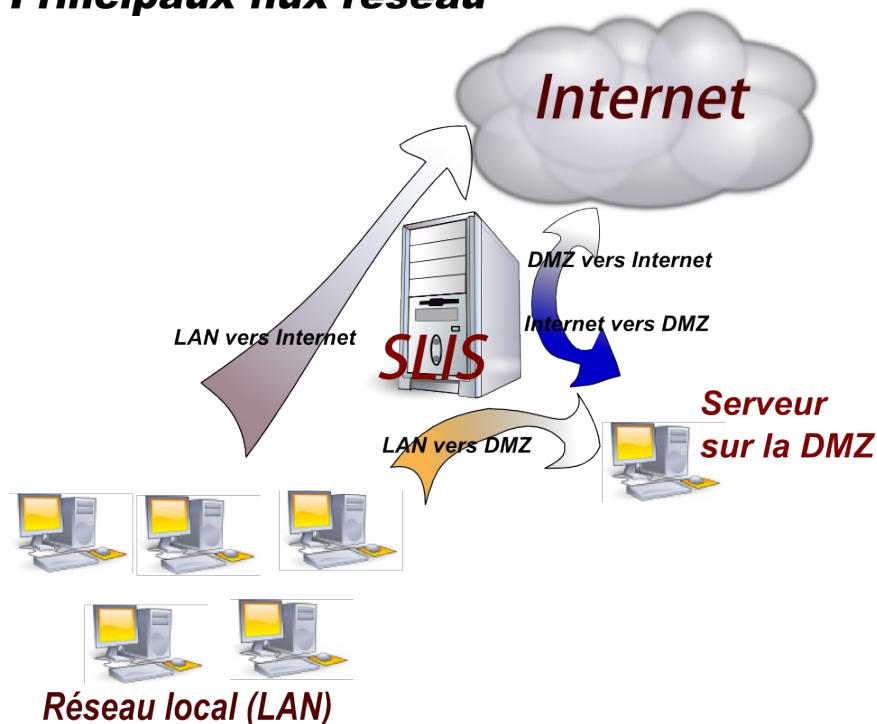


Schéma de principe du pare feu

Un pare-feu a pour fonction de réguler le trafic entre deux réseaux ou plus. Il sert à accepter ou rejeter un flux, ou éventuellement le rediriger.

Sur le slis, le pare-feu régule le trafic entre trois zones :

- la zone WAN ("Wan Area Network" : Internet, quoi...),
- la zone LAN ("Local Area Network" : chez vous bien au chaud),
- la zone DMZ ("Demilitarized Zone" : une zone semi-publique pour vos serveurs),

La gestion des flux sur le SLIS s'intéresse principalement (mais pas exclusivement) :

- aux flux de votre réseau local vers internet (à quoi les machines du réseau

4 - <http://aiedu.education.fr/>

local ont elles accès sur internet),

- aux flux du réseau local vers la DMZ (quel service la DMZ propose t'elle au réseau local),
- au flux de l'internet vers la DMZ (quels services l'établissement scolaire propose-t'il sur internet),
- aux flux de la DMZ vers internet (quels sont les services sur internet dont les ordinateurs de la DMZ ont besoin ?).

Cas d'usage

Nous allons distinguer quelques cas d'usage courant et présenter la façon dont on procède pour répondre à ces demandes :

- Autoriser un service du réseau local vers l'internet,
- Fournir un service sur une machine à partir de votre zone démilitarisée.

1. Du réseau local vers Internet

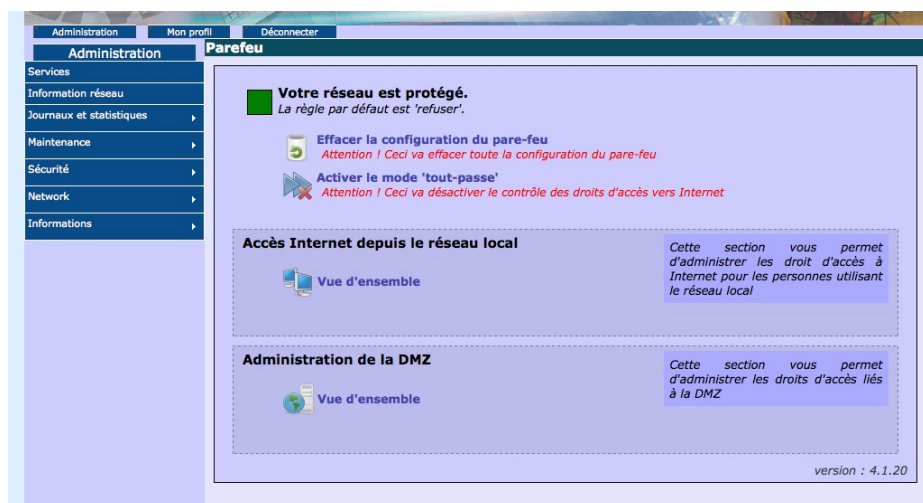
Comment autoriser MSN sur une plage d'adresse ?

Dans votre réseau d'établissement, l'accès aux messageries instantanées n'est pas autorisé par défaut. Mais voilà, les assistants de langue utilisent ces outils pour rester en contact avec leurs proches et ils souhaiteraient pouvoir les utiliser. Pour cela, il va vous falloir autoriser cet outil. Le pare-feu du SLIS vous permet de ne l'autoriser que depuis certains postes pour peu que vous ayez défini vos sous-réseaux correctement au sein de l'établissement.

Supposons que vous souhaitiez autoriser cet accès dans la salle des professeurs, où les assistants de langue utilisent les ordinateurs, et que cette salle corresponde au sous-réseau 172.16.101.0/24

Il vous faut d'abord ouvrir la page d'accueil du pare feu en y accédant par le menu du SLIS.

Sécurité -> Pare-feu -> Pare-feu



Page d'accueil du pare-feu

Votre configuration concerne la gestion de l'accès internet depuis le réseau local. Vous allez donc cliquer sur "Vue d'ensemble" de la partie "Accès internet depuis le réseau local". Vous obtenez alors la page d'accueil du pare-feu qui a l'apparence suivante.

Parefeu - Stations de travail

Accès depuis le réseau local (règle par défaut : 'refuser')
 Vous pouvez autoriser certains usages d'Internet comme le ftp, le chat, ...

- Retourner à la page d'accueil du pare-feu
- Modifier la planification horaire des sous-réseaux
- Changer la règle par défaut en acceptant toutes les connexions non listées
 Quand la règle par défaut est 'accepter', toutes les connexions non listées ci-dessous seront acceptées.
- Autoriser un nouveau droit d'accès à Internet

Liste des accès autorisés
 Ceci correspond aux services sur Internet auxquels les stations de travail ont accès.

| Description | Nom du schéma | Source | Destination | Action | état | modifier / supprimer | Priorité |
|---|---------------|-----------|-------------|--------------------------------|------|----------------------|----------|
| Interdire les flux dns vers Internet ne passant pas par le slis | dns | 0.0.0.0/0 | 0.0.0.0/0 | Toujours refuser | | Règle obligatoire | |
| Autoriser le transfert de fichiers (ftp) vers Internet | ftp | 0.0.0.0/0 | 0.0.0.0/0 | Selon la planification horaire | | Règle activable | |
| Autoriser les connexions https vers Internet | https | 0.0.0.0/0 | 0.0.0.0/0 | Selon la planification horaire | | Règle activable | |
| Autoriser la consultation des annuaires LDAP | ldap | 0.0.0.0/0 | 0.0.0.0/0 | Selon la planification horaire | | Règle activable | |

Page d'accueil de la partie "Accès à internet depuis le réseau local"

Dans cette page, vous pouvez distinguer une première partie avec les actions que vous pouvez accomplir :

- Retourner à la page d'accueil du pare-feu
- Modifier la programmation horaire des sous-réseaux (renvoie vers le menu de la gestion des sous-réseaux)
- Passer votre pare-feu en mode "tout passe", ce qui peut être utile pour faire des tests mais est fortement déconseillé en fonctionnement normal
- Et enfin la création d'un nouveau droit d'accès. C'est cette option qui nous intéresse pour notre exemple.

Dans la seconde partie de la page, vous avez l'ensemble des paramètres de configuration de votre pare-feu pour l'accès à internet depuis le réseau local. Cette liste contient trois types de règles différentes :

- Les règles obligatoires. Ce sont des règles décidées au niveau académique, qui sont indispensables au bon fonctionnement du SLIS. Elles sont présentes pour information, surlignées en gris, mais vous ne pouvez pas agir dessus.
- Les règles prédéfinies. Elles sont mises en place par défaut. Dans le cadre de la politique locale de l'établissement, vous pouvez décider de les désactiver. Soyez attentifs aux conséquences. Elles sont sur fond bleu.
- Enfin, tout en bas, vous trouverez les règles personnalisées. Elles sont sur fond blanc.

C'est justement une de ces règles personnalisées que nous allons rajouter. Vous allez donc cliquer sur "Autoriser un nouveau droit d'accès à l'internet".

Cela vous conduira à une nouvelle page.

Parefeu - Stations de travail Autoriser un nouvel accès sortant vers Internet

Autoriser un nouvel accès sortant vers Internet

Donner une description courte :
 Autoriser l'accès à MSN depuis la salle des professeurs 1

Choisissez un schéma :

- Transférer des fichiers (ftp)
- Transférer des fichiers (sftp) vers LCS
- Messagerie instantanée (msn, yahoo, jabber, icq, irc) 2
- Consultation par envoi de messages pop(imap(s))
- Lire les nouvelles par nntp/nntp(s)
- Utiliser un service web mandataire (proxy)
- Accéder au Web (http et https)
- Accéder au Web (seulement http)
- Accéder au Web (seulement https)
- Lire les flux audio/vidéo (rstp, h323)

+ Créer
 Modifier
 Supprimer

Autoriser l'accès depuis :

Tout le réseau local

Une adresse ou un réseau spécifique 172.16.101.0/24 3 par ex. 172.16.1.0/24 ou 172.16.0.34

Autoriser l'accès vers :

Tout Internet 4

Une adresse ou un réseau spécifique [] par ex. 193.54.149.12

Cible :

Cible : Selon la planification horaire 5

Annuler 6 Valider

Nouveau droit d'accès du réseau local vers Internet

Vous allez maintenant procéder en 6 étapes :

1. Donner un nom à votre règle de pare-feu. C'est celui qui apparaîtra dans votre liste sur la page d'accueil et vous renseignera sur la règle. Autant être précis. On va donc choisir "autoriser l'accès à MSN depuis la salle des profs"
2. Choisir le schéma. Les schémas sont les différents types de services auxquels vous souhaitez pouvoir accéder. Un certain nombre de schémas sont prédéfinis et vous ne devriez pas avoir besoin de nouveau schéma. Si c'était le cas, il faudrait vous référer à la documentation de référence ou contacter l'assistance académique. Ici, le schéma qui nous intéresse est celui de "Messagerie instantanée" que nous cochons donc.
3. La zone suivante nous demande le réseau qui doit avoir accès à ce service. Il ne s'agit pas de tout le réseau local. Nous cochons donc la case "depuis une adresse ou un réseau spécifique" et nous indiquons le sous-réseau de la salle des professeurs : 172.16.101.0/24
4. L'accès doit bien se faire vers tout internet par contre. Nous laissons cochée la case "Tout internet".
5. La cible de la règle est "Selon la planification horaire". La règle sera acceptée pendant les plages horaires d'activation définies pour le sous-réseau de la salle des professeurs.
6. Il ne reste plus qu'à valider.

Voilà, la nouvelle règle est en place et prête à l'emploi.

2. Autoriser un service dans la DMZ



Définition : Zone démilitarisée (DMZ)

La DMZ est une zone intermédiaire entre le réseau internet et votre réseau local. Les machines hébergées sur la DMZ sont accessibles de l'internet. En tant que telles, elles sont considérées comme peu sûres et sont donc séparées du réseau

local. Cependant, elles ne sont pas directement sur Internet. Le pare-feu du SLIS les protège des éventuelles tentatives d'attaque en provenance d'internet.

Fournir un service accessible depuis internet

Nous allons considérer que vous avez installé une machine fabuleuse qui permet de faire le café à partir d'internet. Cette machine a besoin pour fonctionner d'écouter sur le port 2345. Pour pouvoir se mettre à jour et offrir de nouvelles façons de préparer le café à ses utilisateurs, elle a aussi besoin d'accéder au site FTP du fabricant, qui fonctionne sur le port 21.

Il va donc falloir :

- Indiquer au pare feu qu'un nouveau serveur est sur la DMZ.
- Lui indiquer quel service il fournit au monde entier et au LAN.
- Lui indiquer quelle fonctionnalité d'internet cette machine va utiliser.

Commençons par déclarer ce nouveau serveur au pare-feu du SLIS. Pour cela, de la page d'accueil du pare-feu, vous allez ouvrir cette fois la vue d'ensemble de "l'administration de la DMZ" et non pas de l'accès internet depuis le réseau local. Vous accéderez alors à une page qui déclare toutes vos machines sur la DMZ.



Page d'accueil de la partie DMZ du pare feu

Cette page vous propose de revenir au menu d'accueil ou de déclarer une nouvelle machine. Elle vous fournit par ailleurs la liste des machines déjà existantes sur la DMZ. Par défaut, sur un SLIS fraîchement installé, vous ne verrez que le LCS. Cette ligne grisée et le petit icône avec un cadenas vous indique que cette machine est prédéfinie au niveau académique et que vous ne pouvez ni la supprimer, ni la désactiver. Elle est en effet indispensable au bon fonctionnement de votre SLIS.

Nous allons donc cliquer sur l'ajout d'une nouvelle machine en DMZ.

Nouvel hôte sur la DMZ

Cette page est assez simple à remplir. Il faut donner :

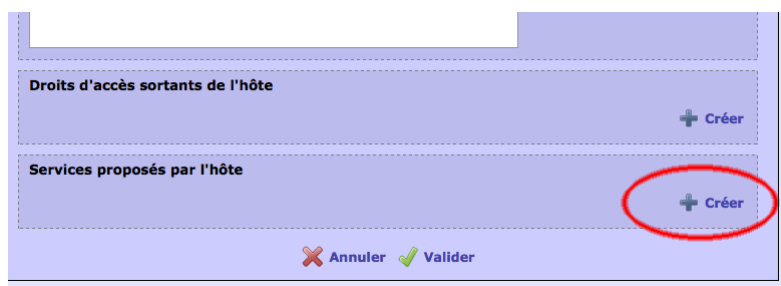
1. le nom de l'hôte. Autant que possible, cela doit correspondre à son nom au sens réseau du terme. Nous indiquerons ici "cafe".

2. l'adresse IP. Cette adresse étant sur la DMZ, dans une configuration standard, elle est sur le réseau 192.168.234.0/24. Pour les établissements de l'académie de Grenoble, vous trouverez les préconisations d'adressage et l'indication des IP réservées sur le document "*Adressage IP pour l'intranet et la DMZ des réseaux Pédagogiques*"⁵ du site "Assistance Technique aux AIPRT". Dans notre exemple, nous choisissons l'IP 192.168.234.100
3. une description la plus complète possible de la machine.
4. Puis Valider.

En cliquant sur la validation, la machine est créée et la page est rechargée, avec cette fois deux zones supplémentaires :

- Les droits d'accès sortant de la machine
- Les services proposés par la machine

Dans notre exemple, la machine fournit un service de contrôle du café. Il va falloir configurer un service en cliquant sur le bouton " + Créer " pour ajouter un service.



Création d'un nouveau service pour l'hôte

Il va maintenant falloir définir le service. Sur cette page, vous devrez renseigner :

1. Le nom du service, par exemple "Contrôleur de café".
2. La source des requêtes. Votre service peut répondre à des requêtes internet ou à des requêtes provenant du réseau local. Dans notre cas, il faudra procéder en deux étapes. La première fois, nous créons le service depuis internet. Le réseau source sera 0.0.0.0/0, ce qui signifie que tout internet a accès à ce service.
3. Le port source. Une requête sur internet a un port source et un port de destination. Il est extrêmement rare que le port source soit fixé. On laisse donc la valeur par défaut : "all".
4. Le protocole. La plupart du temps, il s'agit du protocole tcp.
5. Le port d'écoute. C'est ce port qui est associé au service que nous utiliserons. Ici, il s'agit du port 2345.
6. Le NAT. Les requêtes venant d'internet ne connaissent à priori que votre SLIS. Il faut donc que le SLIS les intercepte et les renvoie vers le serveur idoine sur la DMZ. Cette fonctionnalité des pare-feu s'appelle le NAT (Network Address Translation). Il faut donc ici choisir "oui" pour le NAT.
7. Le port sur lequel le SLIS écoute peut être différent du port sur lequel le serveur écoute. Par défaut, sauf besoin particulier, nous mettons ici le même port.
8. Et enfin, on valide tout cela.

Parefeu - DMZ

Déclarer/modifier un nouveau service fourni par l'hôte : 'cafe'

Donner une description courte :
 1

Autoriser la source :
 depuis le réseau local :
 depuis Internet : 2

Choisissez le(s) port(s) source(s) :
 Le(s) port(s) source(s) : 3

Choisissez le protocole :
 tcp 4
 udp
 tcp + udp
 icmp (11,0,3,8)

Choisissez le port d'écoute :
 Le port d'écoute : 5

Adresse et port 'natté' :
 Voulez-vous 'natter' l'adresse et le port depuis le SLIS : Yes 6
 No
 Le port d'écoute pour le slis : 7

8

Définition d'un service dans la DMZ

Nous allons ensuite définir le même service pour le LAN. Nous procéderons exactement de la même façon à quelques petits détails près.

Dans "Services proposés par l'hôte", cliquer une nouvelle fois sur " + Créer".

- Le nom du service peut être identique ou un peu différent. On peut par exemple le nommer "contrôleur de café (LAN)".
- Le réseau source doit être le LAN. On peut indiquer comme réseau 172.16.0.0/16
- On peut "natter" de la même façon que pour le service internet.

Au final, vous devez alors avoir une configuration de ce type qui s'affiche.

Modifier l'hôte

Nom
 Un nom court pour identifier l'hôte

adresse IP :
 Mettre l'adresse Ip de l'hôte

Description

Droits d'accès sortants de l'hôte + Créer

Services proposés par l'hôte + Créer

| Description | Réseau source | Adresse source | état | Modifier/Supprimer |
|------------------|---------------|----------------|------|--------------------|
| Contrôle de café | wan | 0.0.0.0/0 | ✓ | |
| Contrôle de café | lan | 172.16.0.0/16 | ✓ | |

✗ Annuler ✓ Valider

État des services proposés

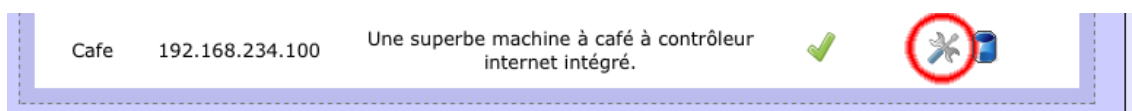
3. Autoriser un droit d'accès sur la DMZ

Le FTP des mises à jour.

Votre machine à café est fabriquée par "Neslonguo, le café des gogos". Vous savez que régulièrement, de nouveaux firmwares sont proposés et des mises à jour de sécurité aussi, afin de ne pas vous faire perdre la main sur cet outil indispensable à tout pédagogue qui se respecte.

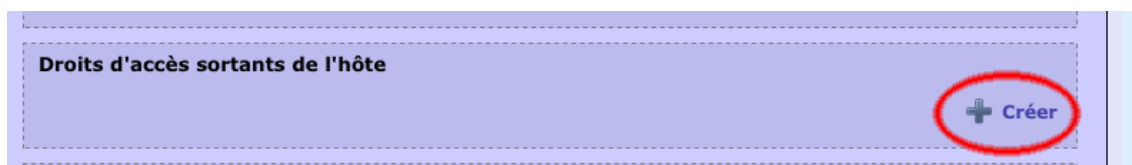
La mise à jour utilise le protocole FTP et se fait sur le site ftp.neslonguo.com

L'accès à internet n'est pas ouvert par défaut pour les machines de la DMZ. Il va falloir fournir à votre machine le droit d'accéder à ce site en FTP. La démarche sera sensiblement la même que pour fournir un accès à une machine du réseau local. Vous allez d'abord accéder à la page d'accueil de la DMZ. Dans la liste des hôtes hébergés, vous allez cliquer sur la modification de la machine cafe (c'est à dire sur l'icône avec les petits outils).



Accès en modification à la machine "cafe"

Dans la page dédiée à cette machine, vous avez une liste (vide pour l'instant) des droits d'accès sortant. Nous allons en créer un. Vous cliquerez donc sur le bouton de création.



Création d'un droit d'accès sortant sur la DMZ

pour configurer ce service, voici les étapes :

1. On donne un nom au droit d'accès sortant. Ici, ce sera l'accès au serveur de mise à jour.
2. On choisit le schéma. Parmi les schémas prédéfinis, on trouve "Transférer des fichiers (ftp)". On choisit donc ce schéma.

- 3. Le droit d'accès sortant est vers internet et non pas vers le réseau local. Il faut accéder au serveur ftp.neslonguo.com. Comme on ne connaît pas l'IP de ce serveur, on indique 0.0.0.0/0 dans l'adresse autorisée, ce qui autorise le FTP vers tout internet. Il serait préférable de ne l'autoriser que vers un seul serveur. ATTENTION, ce doit toujours être une adresse IP ou un réseau IP, jamais un nom DNS.
- 4. On autorise ce droit d'accès selon la planification horaire.
- 5. On valide.

Page de création d'un droit sortant de la DMZ

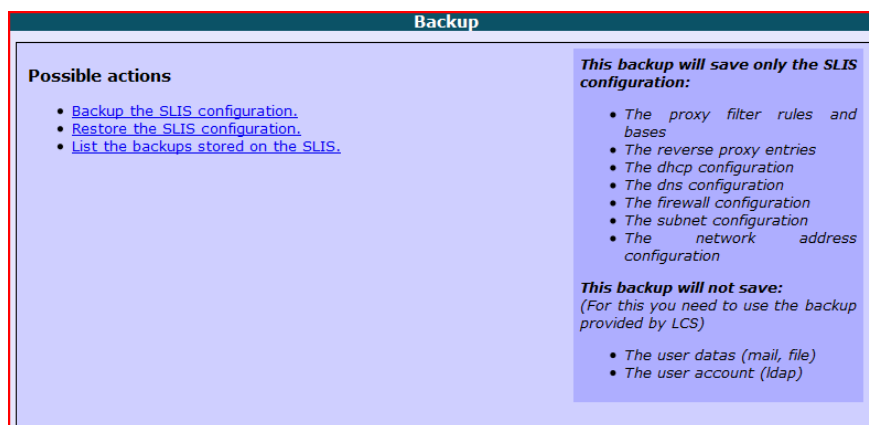
Après la validation, vous êtes redirigés vers la fiche du serveur, et les droits d'accès sortant ont été mis à jour.

| Droits d'accès sortants de l'hôte | | | | | |
|-------------------------------------|-------------------|--------------|--------------------------------|------|--------------------|
| Description | Type de ressource | Réseau cible | Action | état | Modifier/Supprimer |
| Accès en FTP au site de mise à jour | ftp | 0.0.0.0/0 | Selon la planification horaire | ✓ | |

Liste des droits d'accès sortant

D. Sauvegarde et restauration

Sauvegarde



Page de Sauvegarde

Nous vous conseillons de créer une sauvegarde à chaque fois que des modifications de paramétrage sont effectuées.

Cette fonction sauvegarde uniquement la configuration du SLIS (voir détails sur la page "Backup" de l'interface).

Les données du serveur LCS ne seront donc pas sauvegardées (configuration, comptes des utilisateurs, mels, données des utilisateurs, ...).

La fonction est accessible dans l'interface d'administration par le menu :

Administration → Backup → Backup the SLIS configuration.

Deux possibilités sont offertes :

1. soit télécharger le fichier de sauvegarde à partir du SLIS (par exemple sur la station à partir de laquelle vous faites la sauvegarde ou encore sur un support amovible qui y est connecté).
2. soit enregistrer le fichier de sauvegarde sur le SLIS. Dans ce cas, la sauvegarde sera accessible par les équipes de support académiques. Si le SLIS n'est pas équipé de 2 disques durs en raid, il faudra doubler cette opération avec une sauvegarde par téléchargement du fichier (cas n°1).

Une fois le choix effectué, démarrer la sauvegarde en cliquant sur le bouton "Launch the backup".

Dans le cas N°1, la fenêtre proposant l'enregistrement du fichier apparaîtra quelques instants après.

Dans le cas N°2, la sauvegarde sera terminée dès l'apparition du message "Backup is done".

Restauration

La fonction est accessible dans l'interface d'administration par le menu :

Administration → Backup → Restore the SLIS configuration.

Deux possibilités sont offertes pour effectuer la restauration :

1. soit à partir d'un fichier enregistré situé hors du SLIS
2. soit à partir d'un fichier enregistré sur le SLIS

Dans les 2 cas, il faudra effectuer le choix du fichier (le nom des fichiers de sauvegarde contient toujours la date et l'heure de sauvegarde), puis lancer la restauration en cliquant sur "Launch the restoration".

La restauration sera terminée après l'apparition du message "Restoration is done". Comme indiqué, vous devrez redémarrer le SLIS.

Pour cela :

onglet Administration → Maintenance → Arrêt/Redémarrage → Redémarrer uniquement le serveur SLIS. Valider enfin par OK.



Attention

Ne jamais restaurer une sauvegarde générée à partir d'une version V1.x, V2.x ou V3.x.

