****

**Laboratoire Pare-feu**

**Sécurité des Systèmes Informatiques**

12.10.2011

IL-2012

Brahim Lahlou

Numa Trezzini

1 Introduction 1

2 But 1

3 Mise en œuvre 1

3.1 Règles du pare-feu 1

3.2 Topologie du réseau et équipements 3

3.3 Configuration de l’équipement 4

3.4 Manipulations 5

3.5 Création, application et tests des règles 5

3.5.1 Autorisation du ping 5

3.5.2 Autorisation de DNS 6

3.5.3 Autorisation de http 7

3.5.4 Autorisation du serveur web de la DMZ 8

3.5.5 Autorisation de Telnet 9

3.5.6 Autorisation du partage réseau 10

3.5.7 Autorisation HTTPS 12

4 Conclusion 12

5 Références bibliographiques 13

6 Liste des figures 13

# Introduction

La sécurité sur les réseaux est l’un des principaux soucis des personnes (physiques ou morales). L’une des solutions disponibles aux utilisateurs de réseaux informatiques est le filtrage des transmissions. Un pare-feu est l’un des moyens de contrôle des transmissions les plus efficaces, et donc un outil indispensable à une bonne sécurité d’un réseau. La compréhension du fonctionnement et de la configuration d’un pare-feu devrait ainsi faire partie du bagage de tout informaticien qui se respecte.

Nous allons commencer par présenter le but du rapport, puis la mise en œuvre de l’interface sur laquelle nous allons effectuer nos tests et enfin terminer par une conclusion. La mise en œuvre comprendra la présentation de la topologie réseau sur laquelle nous travaillons et la configuration du matériel et du logiciel, la liste des règles répondant aux besoins de sécurité du réseau et enfin la mise en place desdites règles, avec les réponses aux questions posées.

# But

L’objectif de ce travail est de parfaire nos connaissances en matière de pare-feu, vues aux cours de SSI, par la configuration d’un pare-feu. Nous allons ainsi mettre en place la politique de sécurité d’un réseau privé. La topologie du réseau, présentée plus en détails à la section 3.2, comporte un intranet (LAN), une DeMilitarized Zone (DMZ), internet (WAN) et évidemment un pare-feu. La configuration correcte du pare-feu est le but de ce travail.

# Mise en œuvre

## Règles du pare-feu

Nous avons commencé par lister les règles à appliquer au pare feu. Elles sont basées sur les spécifications suivantes [LAB] :

1. *Les serveurs DNS des postes dans le LAN sont situés sur le WAN. Les services DNS utilisent les ports UDP 53 et TCP 53.*
2. *Laisser passer les PING du LAN au WAN, du LAN à la DMZ et de la DMZ au LAN pour les tests. Le ping utilise le protocole ICMP (ne spécifier aucun type de code dans ICMP).*
3. *Les clients du LAN doivent pouvoir ouvrir des connexions HTTP pour accéder au web. Le protocole HTTP utilise les ports TCP 80 et 8080.*
4. *Le serveur web en DMZ doit être atteignable par le WAN et le LAN et n'utilise que le port 80. Attention: une configuration du NAT supplémentaire doit être effectuée au préalable (traitée ultérieurement dans la manipulation).*
5. *Le serveur de la DMZ peut être commandé à distance par Telnet depuis votre client du LAN uniquement. Le service Telnet utilise le port TCP 23.*
6. *Les clients du LAN doivent pouvoir atteindre un partage réseau dans le WAN (\\eint20\Public par exemple). Le protocole Netbios utilise le port TCP 139 et le protocole microsoft- ds utilise le port TCP 445.*
7. *Les clients du LAN doivent pouvoir consulter les pages web sécurisées hors de la DMZ (par ex. le Webmail de l'école). Le protocole HTTPS utilise le port TCP 443.*
8. *Toute autre action est par défaut refusée.*

**Question 1** *En suivant la méthode vue en classe, établir la table de filtrage avec précision en spécifiant la source et la destination, le type de trafic (TCP/UDP/ICMP) ainsi que les ports sources et destinations et l'action désirée (Accept ou Deny).*

Ces contraintes ont donné lieu à la table de filtrage suivante :

|  |  |  |
| --- | --- | --- |
| **LAN** | **DMZ** | **WAN** |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **IP Source** | **Port Source** | **IP Destination** | **Port Destination** | **Protocole** | **Action** | **Commentaire** |
| No IP | any | Broadcast | any | DHCP | accept | requêtes DHCP des machines sans IP |
| any | any | Broadcast | any | DHCP | accept | réponses aux requêtes DHCP |
| LAN | any | WAN | 53 | UDP | accept | requêtes DNS |
| LAN | any | WAN | 53 | TCP | accept | requêtes DNS |
| LAN | any | WAN | any | ICMP | accept | requêtes PING vers WAN |
| LAN | any | DMZ | any | ICMP | accept | requêtes PING vers DMZ |
| LAN | any | WAN | 80 | TCP | accept | requêtes HTTP |
| LAN | any | WAN | 8080 | TCP | accept | requêtes HTTP |
| LAN | any | DMZ server | 80 | TCP | accept | requêtes serveur WEB |
| LAN client | any | DMZ server | 23 | TCP | accept | requêtes Telnet |
| LAN | any | WAN | 139 | TCP | accept | requêtes NetBios |
| LAN | any | WAN | 445 | TCP | accept | requêtes microsoft-ds |
| LAN | any | WAN | 443 | TCP | accept | requêtes HTTPS |
| LAN | any | any | any | any | deny |  |
| DMZ | any | LAN | any | ICMP | allow | requêtes PING vers LAN |
| DMZ | any | any | any | any | deny |  |
| WAN | any | DMZ server | 80 | TCP | allow | requêtes serveur WEB |
| WAN | any | any | any | any | deny |  |
| any | any | any | any | any | deny |  |

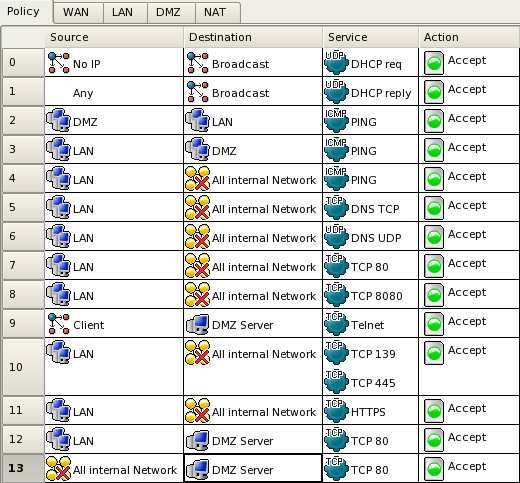


Figure - Tableau final des règles FirewallBuilder. Notons qu’il n’est pas nécessaire de saisir les règles de refus par défaut : FWB s’en occupe de lui-même.

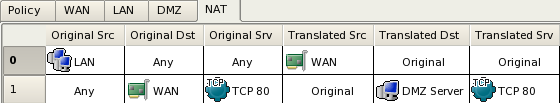


Figure - Règles finales NAT de FirewallBuilder

## Topologie du réseau et équipements

Le réseau sur lequel nous allons travailler se compose de trois entités : un intranet, une DMZ et un pare-feu. L’intranet a comme adresse réseau 192.168.1.0/24 et la DMZ 192.168.2.0/24. L’intranet comporte pour ce laboratoire un client et la DMZ un serveur web [Figure 3].



Figure - Topologie du réseau utilisé [LAB]

Les machines ainsi que le pare-feu sont représentés par une machine virtuelle. Ceci permet de s’affranchir des contraintes matérielles et facilite notre tâche. Même si le réseau est virtuel, les effets restent les mêmes qu’avec des machines physiques séparées. Ainsi, le client de l’intranet est représenté par une machine Damn Small Linux (DSL), le serveur de la DMZ par une machine Gufix et le pare-feu par une machine SLAX. Ces trois machines sont utilisées avec VirtualBox 4.1.6 pour MacOSX et ont été fournies par le professeur.

## Configuration de l’équipement

L’installation des machines est présentée dans le document fourni Installation Virtuelle [IV]. Leur configuration est présentée dans la donnée du laboratoire [LAB].

Les interfaces réseau de la machine SLAX sont configurées pour être liées à la DMZ et l’intranet par les adresses 192.168.2.1 et 192.168.1.1 respectivement. SLAX offre aussi un serveur DHCP à l’intranet.

La machine Gufix est configurée pour offrir un serveur web et un service Telnet.

La machine DSL récupère une adresse IP auprès du serveur DHCP.

**Question 2** *Pour montrer qu’un serveur DHCP est fonctionnel du côté du réseau LAN, faites une capture de la configuration IP de l’interface ethernet grâce à la commande : ifconfig.*

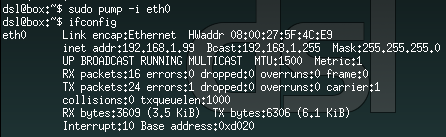


Figure - Capture de la commande ifconfig de la machine DSL après récupération d’une adresse auprès du DHCP

Nous pouvons voir que la machine possède une adresse IP située dans le domaine de l’intranet (192.168.1.99). Comme l’adresse est valide, nous pouvons en conclure que le serveur DHCP a bien fonctionné.

## Manipulations

Pour créer les règles, nous avons utilisé FirewallBuilder (FWB). Pour commencer, nous avons mis en place les règles DHCP, permettant aux machines sans adresse IP d’en demander une et au pare-feu d’y répondre [LAB] :



Figure - Règles FWB autorisant les requêtes DHCP des machines n’ayant pas d’IP et les réponses à ces requêtes

Nous avons ensuite mis en place une règle NAT permettant de cacher la topologie de l’intranet grâce à une translation d’adresses [LAB] :



Figure - Règle NAT de translation d'adresses de la donnée de laboratoire

## Création, application et tests des règles

Dans cette section, nous allons présenter les conditions de la section 3.1

### Autorisation du ping

Le ping doit être autorisé entre l’intranet et la DMZ, la DMZ et l’intranet et l’intranet et le web. Les règles à appliquer sont les suivantes [LAB]:

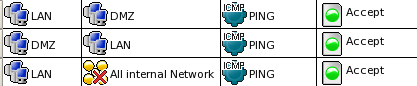


Figure - Règles FWB autorisant le ping entre les zones du réseau privé, ainsi que vers l'extérieur

**Question 3** *Tester ensuite les connections en essayant la commande suivante : sudo ping 195.186.1.111 (IP du DNS de Bluewin) depuis le client pour tester le lien avec le WAN. Faire une capture.*

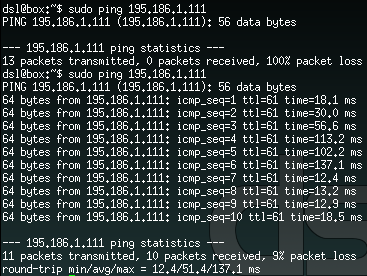


Figure - Résultat de la commande ping depuis la machine DSL vers le DNS de Bluewin. Nous pouvons en constater le bon fonctionnement

La commande ping a également été testée selon le tableau suivant :

|  |  |  |  |
| --- | --- | --- | --- |
| Depuis le serveur web vers (DMZ) | OK/KO | Depuis le client vers (LAN) | OK/KO |
| Interface DMZ | KO | Interface DMZ | OK |
| Interface LAN | OK | Interface LAN | KO |
| Client LAN | OK | Serveur web (DMZ) | OK |
| Serveur WAN | KO | Serveur WAN | OK |

### Autorisation de DNS

Maintenant que le ping est autorisé, nous devons autoriser le DNS pour les clients de l’intranet, afin que ceux-ci puissent résoudre les noms de domaine.

**Question 4** *Si un ping est effectué sur un serveur en utilisant en argument un nom DNS, le client ne pourra pas le résoudre. Le démontrer à l'aide d'une capture (commande sudo ping www.google.tv).*



Figure - tentative de ping de google.tv depuis la machine DSL. Comme la règle DNS n'est pas mise en place, cette requête échoue

Nous en avons déduit les règles suivantes :



Figure - Règles autorisant les clients du LAN à faire des demandes DNS à des serveurs situés dans le web

Une fois que cette règle est appliquée sur la machine SLAX, le résultat de la même commande ping donne le résultat de la [Figure 11].

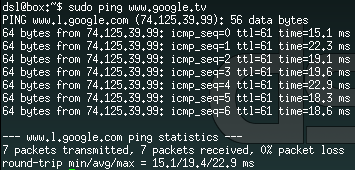


Figure - Après mise en oeuvre de la règle DNS, la même commande qu'à la [Figure 9] fonctionne

### Autorisation de http

**Question 5** *Créer et appliquer la règle adéquate pour que la condition 3 (cf. 2.2.) soit respectée. Tester que la règle soit fonctionnelle en ouvrant une autre fenêtre navigateur pour se connecter à un site web de votre choix*.

Pour autoriser les clients de l’intranet à naviguer sur internet (HTTP non sécurisé), nous avons créé la règle suivante :



Figure - Règle autorisant les clients de l'intranet à faire des requêtes HTTP sur le web



Figure - Après application de la règle permettant HTTP, nous pouvons accéder à internet depuis la machine DSL, ce qui n'était pas possible auparavant

### Autorisation du serveur web de la DMZ

**Question 6** *Créer et appliquer la règle adéquate pour que la condition 4 soit respectée.*

Nous devons ici autoriser la DMZ à accepter les demandes http destinées au serveur web qu’elle contient. Pour que cette étape fonctionne, nous avons dû configurer la machine SLAX pour qu’elle redirige les requêtes arrivant sur le port 80. Les règles suivantes ont été écrites :



Figure - Règles autorisant les requêtes HTTP auprès du serveur de la DMZ



Figure - Règle NAT de translation d'adresses redirigeant les requêtes HTTP au serveur web de la DMZ

Le résultat de l’application des règles permet les accès suivants :

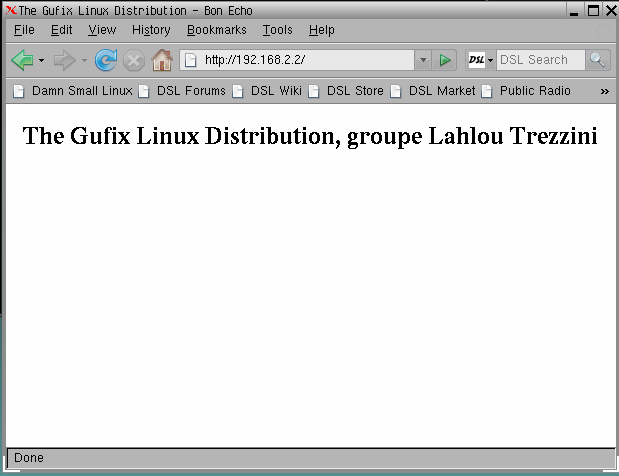


Figure - Un client de l'intranet peut accéder au serveur web de la DMZ. Il s'agit ici du navigateur de la machine DSL

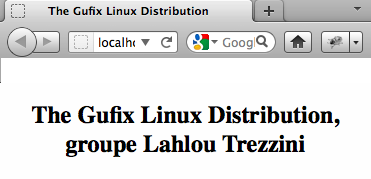


Figure - Le serveur DMZ est accessible depuis le WAN, soit la machine hôte, ici

### Autorisation de Telnet

**Question 7** *Créer et appliquer la règle adéquate pour que la condition 5 soit respectée. Tester avec la commande : telnet 192.168.2.2. Faire une capture. Expliquer l'utilité de telnet sur un serveur. Un autre protocole applicatif serait-il préférable? Pourquoi? A quoi faut-il particulièrement faire attention lors de l'écriture des règles du pare-feu pour ce type de connexion?*

Nous devons autoriser un service Telnet entre l’intranet et le serveur web de la DMZ. Pour ce faire, la règle suivante a été mise en place :



Figure - Cette règle autorise les clients de l'intranet à commander le serveur web de la DMZ grâce à Telnet

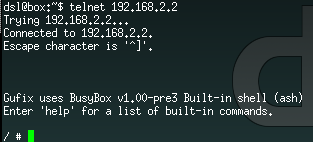


Figure - Le Telnet entre le client de l'intranet (DSL) et le serveur web de la DMZ

L’utilisation de Telnet permet d’avoir accès au serveur à distance pour pouvoir le contrôler. Cependant, l’utilisation de Telnet pose un problème de sécurité, car le protocole n’est pas sûr. Il conviendrait mieux d’utiliser un protocole tel que SSH, permettant un contrôle des accès plus poussé que Telnet. Nous devons également faire particulièrement attention à n’autoriser que les machines possédant les droits à utiliser le service Telnet.

### Autorisation du partage réseau

**Question 8** *Créer et appliquer la règle adéquate pour que la condition 6 soit respectée.*

Nous devons autoriser les accès au partage réseau grâce aux protocoles Netbios (port 139) et microsoft-ds (port 445). Voici la règle que nous avons écrite :



Figure - Cette règle autorise les clients de l'intranet à se connecter via Netbios ou Microsoft-ds

Suite à cette configuration, il nous est possible d’accéder au partage réseau de l’école :

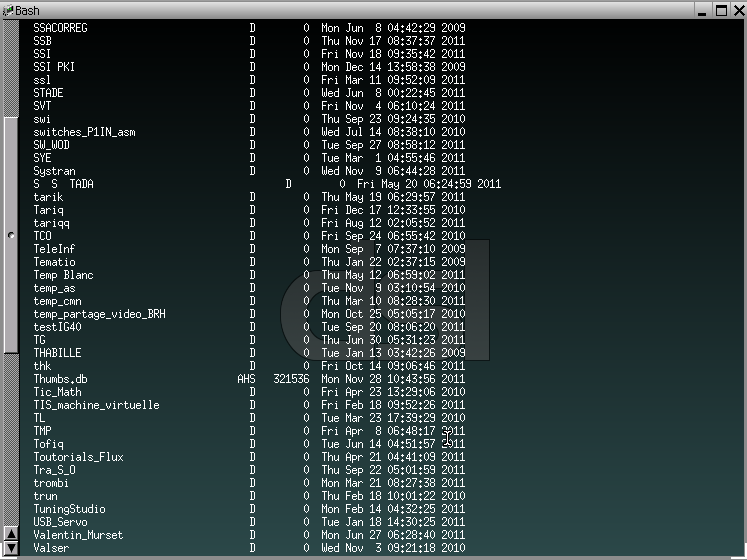


Figure - Capture de la commande ls effectuée dans le dossier partagé Public du serveur eint20 depuis la machine DSL

Comparons cette liste avec celle obtenue par l’accès habituel dont nous disposons :

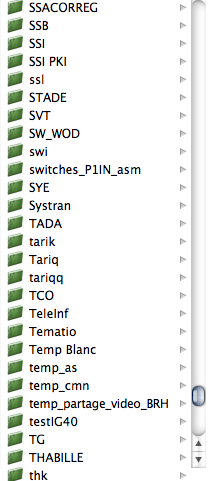


Figure - Capture du contenu du dossier partagé Public du serveur eint20 depuis un accès que nous savons fonctionnel. Nous pouvons voir que les dossiers sont identiques à ceux de la [Figure 21]

### Autorisation HTTPS

**Question 9** *Créer et appliquer la règle adéquate pour que la condition 7 soit respectée. Tester l’accès avec le site https://webmail.heig-vd.ch/ et effectuer une capture d'écran. Attention, Dillo supporte mal les certificats, utiliser Firefox !*

Pour finir les règles demandées à ce laboratoire, nous devons autoriser les connexions HTTPS (port 443) depuis l’intranet vers le web. La règle résultante est la suivante :



Figure - Cette règle autorise les clients du LAN d'accéder à des pages HTTPS

Nous pouvons voir que l’accès à un site sécurisé fonctionne :

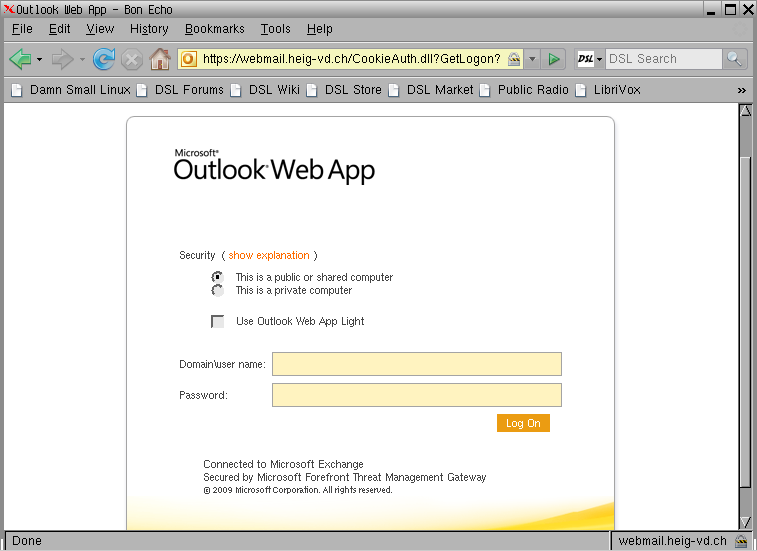


Figure - Accès à la page HTTPS du webmail de la HEIG. Avant application de la règle HTTPS, nous ne pouvions pas accéder à cette page

# Conclusion

Pour accomplir ce travail, nous avons, à partir de conditions imposées, créé et mis en place une politique de sécurité pour un pare-feu. Nous avons du prendre en compte la topologie du réseau à sécuriser et les règles susmentionnées. Pour commencer, nous avons défini les règles de la même manière que présentée aux cours, puis nous les avons mises en place grâce à FirewallBuilder et les machines virtuelles fournies.

L’un des grands challenges de ce travail a été premièrement de définir les règles correctes pour les spécifications. Ensuite, nous avons dû faire particulièrement attention à contraindre correctement les adresses sources et destinations, car il peut s’agir de l’origine de failles de sécurité importantes.

# Références bibliographiques

* [LAB] : VALLAT Gilles-Etienne et al. , *Laboratoire SSI Pare-feu - Donnée v2.5*, 14.11.2011, HEIG-VD
* [IV] : VALLAT Gilles-Etienne et al. , *Laboratoire SSI Pare-feu – Installation virtuelle v2.5*, 14.11.2011, HEIG-VD

# Liste des figures

Figure 1 - Tableau final des règles FirewallBuilder. Notons qu’il n’est pas nécessaire de saisir les règles de refus par défaut : FWB s’en occupe de lui-même. 3

Figure 2 - Règles finales NAT de FirewallBuilder 3

Figure 3 - Topologie du réseau utilisé [LAB] 4

Figure 4 - Capture de la commande ifconfig de la machine DSL après récupération d’une adresse auprès du DHCP 5

Figure 5 - Règles FWB autorisant les requêtes DHCP des machines n’ayant pas d’IP et les réponses à ces requêtes 5

Figure 6 - Règle NAT de translation d'adresses de la donnée de laboratoire 5

Figure 7 - Règles FWB autorisant le ping entre les zones du réseau privé, ainsi que vers l'extérieur 5

Figure 8 - Résultat de la commande ping depuis la machine DSL vers le DNS de Bluewin. Nous pouvons en constater le bon fonctionnement 6

Figure 9 - tentative de ping de google.tv depuis la machine DSL. Comme la règle DNS n'est pas mise en place, cette requête échoue 6

Figure 10 - Règles autorisant les clients du LAN à faire des demandes DNS à des serveurs situés dans le web 7

Figure 11 - Après mise en oeuvre de la règle DNS, la même commande qu'à la [Figure 9] fonctionne 7

Figure 12 - Règle autorisant les clients de l'intranet à faire des requêtes HTTP sur le web 7

Figure 13 - Après application de la règle permettant HTTP, nous pouvons accéder à internet depuis la machine DSL, ce qui n'était pas possible auparavant 8

Figure 14 - Règles autorisant les requêtes HTTP auprès du serveur de la DMZ 8

Figure 15 - Règle NAT de translation d'adresses redirigeant les requêtes HTTP au serveur web de la DMZ 8

Figure 16 - Un client de l'intranet peut accéder au serveur web de la DMZ. Il s'agit ici du navigateur de la machine DSL 9

Figure 17 - Le serveur DMZ est accessible depuis le WAN, soit la machine hôte, ici 9

Figure 18 - Cette règle autorise les clients de l'intranet à commander le serveur web de la DMZ grâce à Telnet 10

Figure 19 - Le Telnet entre le client de l'intranet (DSL) et le serveur web de la DMZ 10

Figure 20 - Cette règle autorise les clients de l'intranet à se connecter via Netbios ou Microsoft-ds 10

Figure 21 - Capture de la commande ls effectuée dans le dossier partagé Public du serveur eint20 depuis la machine DSL 11

Figure 22 - Capture du contenu du dossier partagé Public du serveur eint20 depuis un accès que nous savons fonctionnel. Nous pouvons voir que les dossiers sont identiques à ceux de la [Figure 21] 11

Figure 23 - Cette règle autorise les clients du LAN d'accéder à des pages HTTPS 12

Figure 24 - Accès à la page HTTPS du webmail de la HEIG. Avant application de la règle HTTPS, nous ne pouvions pas accéder à cette page 12