

Filtrage réseau PingOO V3

Sommaire

<u>1. Introduction</u>	1
<u>2. Les profils (ou niveaux de filtrage)</u>	3
<u>2.1. Les profils prédéfinis</u>	3
<u>2.2. Les profils personnalisés</u>	3
<u>2.3. Exemple concret de profil personnalisé : accès web + mail + ftp + messagerie instantanée</u>	4
<u>3. Filtrage simple par classe C</u>	6
<u>4. Filtrage avancé par IP</u>	7
<u>Bookmarks</u>	8

1. Introduction

On retrouve cette fonctionnalité dans PADM section "Sécurité/Filtrage réseau" avec 2 sous-ensembles : "Profils" et "Réseaux".

Cet outil va vous permettre de manipuler simplement des niveaux de filtrage correspondant à des besoins précis, selon des ensembles d'adresses IP (rassemblées en bloc de 254 adresses), et même pour certaines adresses IP précises ! Exemple d'utilisation: si dans une salle vous voulez interdire l'accès internet, sauf pour quelques "personnes" (ou plutôt ordinateurs car le filtrage n'est pas basé sur une authentification utilisateur ; seule l'adresse IP du poste de travail peut être utilisée ici), c'est possible.

Lorsqu'on parle de sécurité réseau, le principe est toujours le même : *par défaut, tout ce qui n'est pas autorisé explicitement est interdit*. C'est le cas ici.

Ici, on ne peut définir le filtrage que dans le sens réseau local vers PingOO V3 et Internet. On ne peut pas modifier les paramètres de filtrage du PingOO pour ce qui vient d'Internet. Le PingOO V3 fait office de "pare-feu" ("firewall") pour protéger les postes du réseau de toute tentative d'intrusion en provenance d'Internet. Vous ne pouvez pas ouvrir d'accès d'Internet vers des machines du réseau local (au travers de "redirection de ports") pour prendre la main sur un poste du réseau depuis une connexion ADSL à la maison par exemple. Pour des raisons de sécurité et pour conserver l'intégrité du réseau protégé par le PingOO, cette fonctionnalité n'a jamais été envisagée sur PingOO V3.

Lorsqu'il est question de "classe C" ici, cela fait référence à un terme spécifique aux réseaux informatiques. Concrètement, le serveur PingOO est en général configuré pour le réseau 192.168.0.0 avec un masque 255.255.0.0 (on parle ici de "classe B" ou de "/16"). On peut décomposer ce réseau en sous-réseaux de type "classe C" (ou "/24" selon la notation CIDR qu'on retrouve dans l'interface) pour leur appliquer des paramètres de filtrage distincts.

On peut donc conseiller de configurer les adresses IP des postes d'un réseau avec cette idée en tête. Ainsi, les postes de la salle 1 pourront être en 192.168.1.x et les postes de la salle 2 en 192.168.2.x Il sera alors possible, simplement, de définir des autorisations d'accès vers l'extérieur pour une salle en quelques clics sans modifier les paramètres de filtrage des postes d'une autre salle informatique.

Dans cette partie de l'interface PADM, on va donc trouver la notation 192.168.X.0/24. Cela correspond concrètement aux adresses IP comprises entre 192.168.X.1 et 192.168.X.254 (sauf pour le 192.168.0.0/24 où cela concernera 192.168.0.2 à 192.168.0.254, l'adresse 192.168.0.1 étant ici réservée pour le serveur PingOO V3 lui-même).

Même si on utilise ici des notations de réseaux en "/24", cela ne veut pas dire que le masque de sous-réseau des postes doit être changé en 255.255.255.0. Celui-ci reste 255.255.0.0 dans tous les cas.

Le classe C 192.168.255.0/24 est un classe C de secours. Si, par mégarde, vous coupez tous les accès, celui-ci permet de se connecter à l'interface pour rétablir des accès "normaux".

Sur les PingOO V3 installés par le CITIC74 pour les établissements scolaires de Haute-Savoie, seuls 20 classes C sont utilisables par défaut (de 192.168.0.0/24 à

Filtrage réseau PingOO V3

192.168.19.0/24). Il est possible de modifier ce paramètre dans la configuration du serveur PingOO (mais ce n'est pas accessible via l'interface PADM => demander aux personnes qui gèrent le serveur PingOO pour augmenter cette valeur et avoir accès à potentiellement 254 classes C différents).

2. Les profils (ou niveaux de filtrage)

2.1. Les profils prédéfinis

Il existe 4 profils prédéfinis non modifiables. Vous pouvez voir la liste des services ouverts/fermés dans la section "Profils" en choisissant le profil concerné dans la liste déroulante.

- ◆ *Sécurité maximum : rien ne passe* : pour isoler un classe C ou un poste du réseau. Ce profil peut être utilisé par des imprimantes par exemple si celles-ci ne doivent même pas avoir à communiquer avec le PingOO. En général, ce profil sera très peu utilisé car l'accès aux ressources du PingOO n'est même pas possible.
- ◆ *Services internes* : les services en local sont ouverts, mais il est impossible de surfer sur internet, ou de sortir du réseau. Ici, on peut donc accéder à l'intranet (interface PADM comprise) mais il ne faut pas que le navigateur web soit configuré pour passer par le proxy, envoyer/recevoir des emails pour les comptes créés sur le PingOO (en utilisant le serveur POP pop.<codeetab>.etab et pour le SMTP mail.<codeetab>.etab), ... Ce profil est également assez peu utilisé car ne permet pas d'accéder à des sites web externes. On peut aussi choisir ce profil pour un équipement réseau type imprimante/photocopieur.
- ◆ *Services internes + internet(proxy)* : en plus de l'accès local, il est possible de surfer sur Internet à condition d'avoir configuré son navigateur web (ou toute autre application nécessitant un accès web) pour utiliser le service proxy présent sur le PingOO V3. Ce profil ne permet pas, par contre, de consulter une boîte email POP/IMAP extérieure au réseau par exemple.
- ◆ *Restrictions minimum* : ce profil ne porte pas forcément bien son nom car il n'autorise pas n'importe quoi comme trafic réseau. Ici, seuls les services prédéfinis (et qu'on peut cocher/décocher dans la partie "Profils" pour des profils sur mesure) vont être ouverts si on choisit ce profil. Les ports "exotiques" (comme le port 2000 ou 4662 ou ...) ne pourront pas passer. **ATTENTION** : ce profil de filtrage permet d'accéder à des sites web externes sans filtrage des sites pornographiques et cie qui est généralement assuré par le PingOO V3. Si vous configurez des adresses IP ou plages d'adresses IP avec ce profil, vous n'avez plus aucune restriction d'accès aux sites en question et vous pouvez donc tomber très facilement sur des images à caractère pornographique notamment. *Ce profil de filtrage est donc à éviter* sauf pour des postes bien précis où un accès sans filtrage des sites web est nécessaire (cas assez rare en principe...).

A l'installation du serveur PingOO, un certain nombre de paramètres par défaut sont définis en terme de filtrage réseau. Les classes C 192.168.0.0/24 et 192.168.18.0/24 sont en "Restrictions minimum", le classe C 192.168.17.0/24 est en "Sécurité maximum". Les autres classes C sont en "Services internes + internet (proxy)". N'utilisez pas des adresses IP en 192.168.0.x sans changer le profil de filtrage si vous ne voulez pas que ces machines puissent accéder à n'importe quel site web sans protection !

2.2. Les profils personnalisés

Si les profils prédéfinis ne vous conviennent pas, vous avez la possibilité de créer votre profil de filtrage sur mesure afin d'autoriser et/ou d'interdire l'accès à certains services. Pour cela, dans la partie "Profils", entrez un nom de profil (évitez tout accent ou caractère spécial) et

cliquez sur "Ajouter un nouveau profil". Il apparaît alors dans le 2ème cadre où vous pouvez le sélectionner via la liste déroulante. Dans le 3ème cadre, vous pouvez alors choisir les accès locaux/externes en cochant les services que vous voulez autoriser. La colonne "Serveur" concerne les accès aux services sur le PingOO lui-même. La colonne "Extérieur" concerne les accès sur des serveurs présents sur Internet.

- ◆ Messagerie: pour envoyer et recevoir vos emails => POP/POPs/IMAP/IMAPs/SMTP => ports 110, 995, 143, 993, 25
- ◆ Accès distant (SSH): => SSH, telnet => ports 22, 23
- ◆ Transfert de fichiers par FTP: => ports 20, 21, 989, 990
- ◆ Partages Windows: ("Serveur" uniquement) => ports 137, 138, 139
- ◆ Messageries instantanées: MSN, ICQ, AIM, yahoo messenger => ports 1863, 4000, 5190, 5050
- ◆ Authentification LDAP: si vous avez besoin d'accéder à une base LDAP (peut être utile pour un carnet d'adresses) => ports 389, 636
- ◆ Accès à Internet avec filtrage: ("Serveur" uniquement) => port 3128 pour l'accès au proxy du PingOO
- ◆ Accès à Internet sans filtrage: ("Extérieur" uniquement) => port 80, 443
- ◆ Ping: pour faire un test basique de communication réseau => protocole ICMP
- ◆ Sites web internes: ("Serveur" uniquement) => port 80, 443 du PingOO lui-même
- ◆ Impression: ("Serveur" uniquement) => port 631
- ◆ Ports supplémentaires: surtout utile côté "Extérieur" pour autoriser des accès nécessitant une ouverture sur des ports particuliers avec l'extérieur

Pour faire un profil sur mesure, cochez simplement les services à autoriser et validez. Il faudra ensuite bien sûr appliquer ce profil aux adresses IP ou plages d'adresses IP qui nous intéressent (voir chapitres suivants).

Pour spécifier des ports supplémentaires dans un profil personnalisé (on ne peut pas le faire pour les profils prédéfinis) :

- ◆ il faut en 1er lieu cocher la case "Ports supplémentaires" (en général sur la colonne "Extérieur") dans le profil qu'on est en train de modifier et "Valider"
- ◆ ensuite, donner la liste des ports séparés par des virgules, exemples: *4662,4663*. A noter que les protocoles UDP et TCP seront ouverts pour ces ports. A noter également qu'on ne peut pas définir un ensemble de ports (de 6000 à 6005, il faut indiquer "6000,6001,6002,6003,6004,6005" etc.)
- ◆ enfin, cliquer sur "Mettre à jour cette liste" pour valider ces modifications.

Les ports supplémentaires qu'on peut indiquer seront repris dans tous les profils personnalisés où la case "Ports supplémentaires" est cochée. On ne peut pas avoir des listes de ports supplémentaires différentes d'un profil à un autre.

Et enfin, vous pouvez supprimer un profil que vous avez créé. Dans ce cas, toutes les classes C et IP ayant ce profil passeront automatiquement au filtrage le plus sécuritaire: "Sécurité maximum : rien ne passe".

2.3. Exemple concret de profil personnalisé : accès web + mail + ftp + messagerie instantanée

Ce profil qui pourrait être considéré comme le plus utile pour pas mal d'établissements utilisant un PingOO V3 n'existe pas par défaut. Voilà une bonne occasion de se pencher sur

l'interface PADM pour y remédier.

On va ici ajouter 5 ports supplémentaires qui peuvent se révéler utiles : ports 1935, 554 et 1755 qui sont utilisés pour la diffusion de certains contenus multimédia (utilisant les protocoles "mms:" et "rtsp:") et les ports 3478 et 9000 qu'on a repérés comme étant utilisés sur une communication MSN avec webcam.

Donc, voilà simplement de façon synthétique les manipulations à faire dans l'interface pour créer ce profil :

- ◆ Interface PADM, login avec un compte ayant droit à la gestion du filtrage réseau (ex : master)
- ◆ section "Sécurité/Filtrage réseau", sous-section "Profils"
- ◆ on rentre le nom de profil "internet-mail-ftp-webcam" et clic sur "Ajouter un profil"
- ◆ on sélectionne ce profil dans la liste déroulante
- ◆ on coche dans la colonne "Serveur" toutes les autorisations sauf "Ports supplémentaires" (inutile)
- ◆ dans la colonne "Extérieur", on coche "Messagerie", "Transfert de fichiers par FTP", "Messageries instantanées", "Ports supplémentaires" et on clique sur "Valider"
- ◆ dans le champ "Liste de ports", on indique cela : 1935,554,1755,3478,9000 et on clique sur "Mettre à jour cette liste"

Le profil sur mesure est prêt à l'emploi. Il pourra être appliqué aux adresses IP qui nous intéressent.

Une documentation dans ce sens avait été rédigée pour l'accès aux ressources ENS : voir http://tice.edres74.net/article.php3?id_article=340.

3. Filtrage simple par classe C

Dans la page "Réseaux", deux sections distinctes :

- ◆ la première en haut, pour ajouter un nouvel accès à un classe C encore non défini.
- ◆ l'autre affiche les différents classe C ainsi que leur niveau de filtrage. Les classes C non affichés n'ont aucun accès.

Pour ajouter un classe C, choisissez le dans l'ascenseur de sélection, spécifiez son niveau de filtrage, puis validez. Ce nouveau filtre est enregistré, mais pas effectif tout de suite. C'est le cas pour toute les modifications qu'on fait dans l'interface, cela pour permettre de modifier plusieurs filtres avant de les activer sur le système, et aussi pour vous permettre de vérifier vos filtres: évitez par exemple de choisir le niveau de filtrage "rouge" ("Sécurité maximum") pour votre machine depuis laquelle vous êtes en train d'administrer le PingOO sinon vous ne pourrez plus accéder à l'interface !

Pour modifier un profil de filtrage pour chaque classe C, il suffit de choisir dans la liste déroulante en face de chaque sous-réseau le profil qu'on désire appliquer (parmi ceux créés par défaut et ceux qu'on a créés sur mesure) et de valider le changement avec le bouton "Valider" correspondant.

Si la liste déroulante des profils pour un classe C apparaît grisée, c'est qu'un filtrage spécifique pour une ou plusieurs adresses IP de ce classe C a été défini (voir chapitre suivant).

Si la configuration du système est différente de celle affichée, un bouton apparaît vous signalant qu'il faut activer ces filtres sur le système. Normalement c'est rapide, quelques secondes, si ça prend plus d'une minute, alors vous vous êtes sûrement trompé dans vos filtres et n'avez plus accès à l'interface depuis ce poste client ! Vous pouvez donc effectuer de nombreuses opérations sur le filtrage réseau et les activer seulement à la fin des manipulations. Et il ne faut donc pas oublier de valider les changements effectués par le bouton prévu à cet effet.

La liste: descriptions des colonnes :

classe C	voir explication au début de cette documentation. A noter : la couleur correspond au niveau de filtrage si c'est un profil prédéfini qui est appliqué
niveau	le profil de filtrage choisi, avec possibilité de le changer. Apparaît grisé (et donc non modifiable) s'il existe des IP de ce classe C qui ont un filtrage spécifique.
icone verte/rouge	si rouge, le classe C a des IP avec un niveau de filtrage différent !
bouton détails	pour voir et définir les niveaux de filtrage pour des adresses IP précises
bouton valider	pour valider si vous avez changé le niveau de filtrage d'un classe C
bouton supprimer	pour supprimer ce classe C, c'est à dire couper tout accès sur cette plage d'adresses IP

4. Filtrage avancé par IP

Cliquez sur le *détails* d'une classe C. Par défaut, toutes les IP de cette classe C (de 1 à 255) auront comme filtre celui choisi dans la plage d'adresse IP principale. Ce niveau de filtrage est modifiable dans le premier cadre.

Le 2ème cadre permet d'ajouter une IP avec un autre filtre.

Le 3ème cadre affiche les IP ayant un filtre spécifique, que vous pouvez modifier. Cochez "supprimer" pour supprimer ce filtre spécifique à cette IP, qui aura alors à nouveau le filtre par défaut de la classe C.

Exemple: vous avez une salle, classe C 192.168.5.0/24, avec le niveau de filtrage "Services internes" (voir description des niveaux de filtrage). Mais vous voulez que le PC du professeur/formateur/etc ait accès à Internet pendant que les élèves travaillent. Pour cela configurez le poste du professeur/formateur avec une IP fixe en 192.168.5.2, puis dans l'interface ajoutez l'IP 192.168.5.2 avec le niveau "Services internes + internet (proxy)" par exemple (ou le profil sur mesure expliqué plus haut). N'oubliez pas d'activer les filtres sur le système via la page principale et le bouton prévu à cet effet !

A partir du moment où on spécifie un paramétrage de filtrage réseau pour une ou plusieurs adresses IP d'une classe C, le profil appliqué à la classe C dans son ensemble n'est plus modifiable (la liste déroulante correspondant à la classe C apparaît grisée quand on est dans la page de sélection des filtres pour les différentes classes C). Si on veut pouvoir modifier à nouveau le profil appliqué à la classe C dans son ensemble, il faut supprimer toute autorisation particulière.

Bookmarks

Document généré avec les cri-doctools