

Qu'est ce que NuFace 2.0 ?

Nuface 2.0 est une interface web haut niveau de configuration de pare-feu Netfilter. Écrite en php5, distribuée sous licence gpl v3, elle simplifie la gestion des règles en offrant une vue haut niveau du pare-feu et une aide contextuelle expliquant directement les options de filtrage.

L'utilisation de **Nuface 2.0** permet de réduire les erreurs de manipulations et d'assurer la cohérence des objets. Entièrement traduite en français, l'interface se présente sous la forme de liste agrémentée d'icônes et de couleurs offrant une vue synthétique du jeu de règles.

Travaillant de concert avec NuFW et Nulog, **Nuface 2.0** permet également de gérer des règles d'accès par utilisateur, par application ou par OS. **Nuface 2.0** permet également de voir à partir des journaux affichés par Nulog quelle règle a permis la connexion.

Créez et gérez vos propres règles de sécurité en moins 5 minutes

Les règles d'accès peuvent s'appliquer à une ou plusieurs personnes et être définies de manière temporelle (accès limité par rapport à des tranches horaires) ou hiérarchique.

Nuface 2.0 comprend un nouveau système de fenêtres d'aide permettant d'améliorer la compréhension de chaque manipulation.

Un historique a été ajouté, il améliore la gestion de configuration des règles et permet un gain de temps (utilisation d'anciennes règles). L'interface devient plus réactive avec une diminution des latences, une validation plus rapide et une amélioration des formulaires de saisie.



Nuface 2.0

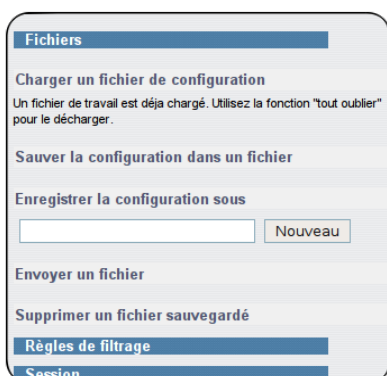
Évolutions technologiques majeures :

- Optimisation des règles
- Diminution des risques de manipulations (grâce à sa nouvelle interface)
- Vérification de la cohérence des règles
- Liens avec Nulog 2.0, outil d'analyse de fichiers journaux (publié sous licence GNU GPLv3)

Amélioration de l'ergonomie :

Les formulaires ont été améliorés, le menu principal utilise maintenant des boutons avec des titres plus explicites :

Version 1.2



Fichiers

Charger un fichier de configuration
Un fichier de travail est déjà chargé. Utilisez la fonction "tout oublier" pour le décharger.

Sauver la configuration dans un fichier

Enregistrer la configuration sous
 Nouveau

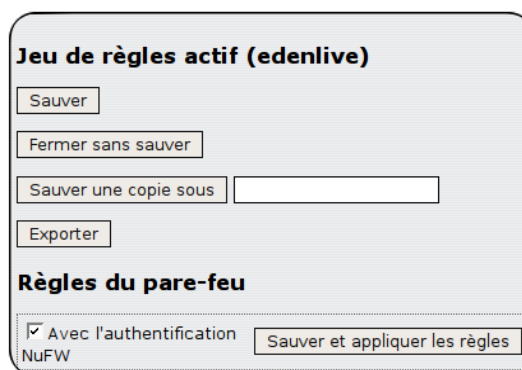
Envoyer un fichier

Supprimer un fichier sauvegardé

Règles de filtrage

Session

Version 2.0



Jeu de règles actif (edenlive)

Sauver

Fermer sans sauver

Sauver une copie sous

Exporter

Règles du pare-feu

Avec l'authentification NuFW

Sauver et appliquer les règles

Menu d'action sur le jeu de règles courant.



Nuface 2.0

L'éditeur d'objet propose une aide contextuelle sur chaque champs :

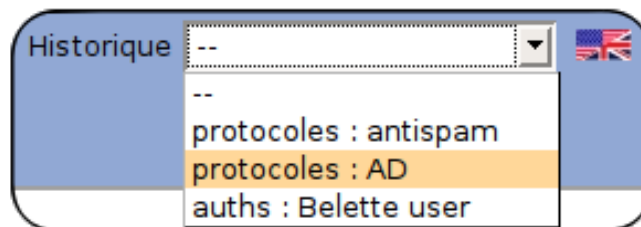
Protocole antispam
Édition de l'élément "TCP 2703" ✖

Champ	Valeur	Nouvelle valeur
type	proto?	
name	TCP 2703	TCP 2703 ?
proto	tcp	tcp ?
dport	2703	
sport		
icmptype		
modified	Mon 19 Fe	
Comment		

Aide de Nuface - proto [X]
On the protocols page, you can set the protocol for each element. Protocol can be defined as TCP, UDP, ICMP, ESP or AH. TCP is the most often used protocol ; UDP is used for many applications with real time needs, such as VoIP, and ICMP is used for sending control and error messages. ESP and AH protocols are only used for IPSEC Virtual Private Networks.
If you choose TCP or UDP, Nuface will let you choose source and destination ports. If you choose ICMP, you will be able to specify an optional ICMP type.

Aide contextuel de l'éditeur de protocole

Nuface 2.0 enregistre l'ensemble des saisies (ACL, protocole, etc) dans un historique situé en haut de la page.



Navigation dans l'historique



Nuface 2.0

ACL :

Une réorganisation de l'éditeur a été faite ainsi qu'un regroupement des champs. Les champs ressources/sujets deviennent source/destination. Les deux icônes du titre peuvent être utilisées pour copier et supprimer une ACL. Enfin les réseaux concernés par l'ACL sont directement visibles sans avoir à cliquer sur un bouton.

Nouveaux champs de filtrage :

- Système d'exploitation
- Utilisateur authentifié
- Période de temps
- Log
- Message de log

Maintenant, il est possible de loguer ou non les connexions avec un message personnalisé. Vous pouvez également limiter la fréquence de message de log (par exemple, limiter les logs icmp à 5/secondes)

Version 1.2

[1] HTTPS for teachers

[HTTPS][Teachers =>Internet]

Réseaux auxquels appartient l'acl

Nom [HTTPS for teach]

Protocole [HTTPS]

Période [--]

Application [--]

Sujet [Teachers]

Ressource [Internet]

Decision [accept]

Modifié [Wed 24 Oct 2007]

Groupe [Teachers] [Activé]

Commentaire

Appliquer

Supprimer

Version 2.0

édite FORWARD ACL #2 (Tue 12 Feb 2008)

Nom [autoriser websurf depuis intranet ou vpn auth ver]

Groupe [default]

Commentaire

Paramètres réseaux

Source [Intra_VPN] Nouveau

Destination [Internet]

Protocole [websurf] Nouveau

I/FW

Auth [--] Nouveau

Périodicité [--] Nouveau

Durée [--] Nouveau

OS [--] Nouveau

Application [--] Nouveau

Action

Décision [accept]

Log [Limité : Log illimité]

Message de log [web intranet vpn. -]

Sauver

Réseaux de l'ACL

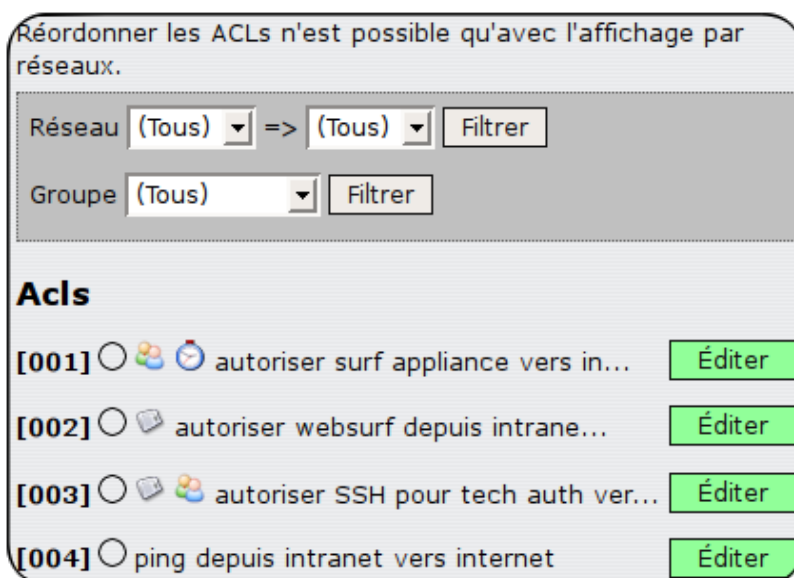
ETH0-ETH0

Éditeur d'ACL avec champs groupés et réordonnés



Nuface 2.0

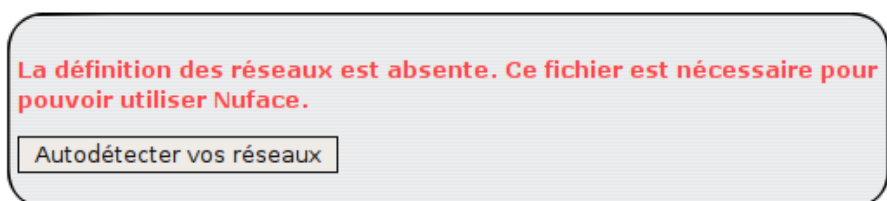
Les listes d'ACLs locales et de filtrages contiennent à présent des icônes permettant de voir les options de chaque ACL : règles authentifiantes NuFW, règles de temps (période ou durée) et journalisation.



Liste d'ACL avec les icônes associées
(authentification, temps et journalisation)

Auto-configuration :

Lorsque le fichier de description du réseau était manquant (desc.xml) Nuface 1.2 demandait systématiquement l'écriture manuellement de ce fichier. **Nuface 2.0** dispose d'un programme d'auto-détection (gendesc), celui-ci détecte les interfaces réseaux, routes et la passerelle par défaut.




Nuface 2.0 propose la détection de votre configuration



Nuface 2.0

Cohérence :

Nuface 2.0 vérifie désormais la cohérence des objets au chargement du jeu de règles mais aussi après chaque changement. Ainsi les erreurs sont directement détectées et ne bloquent pas l'enregistrement du jeu de règles. Le fichier de description des réseaux (desc.xml) est également vérifié par le script checkdesc.

 *Impossible de créer le nouvel élément : Incohérence dans Élément "127.0.0.1" (#3, type "ipv4") : Adresse IPv4 locale ("127.0.0.1") interdite !*

*Message d'erreur lors de la création d'un élément IPv4 invalide
(le réseau 127.0.0.0/8 est interdit)*

Autres changements :

- **Nuface 2.0** peut être utilisé sur une passerelle avec une seule interface
- Passage à la licence GNU GPLv3
- **Nuface 2.0** demande l'utilisation de PHP5 pour l'utilisation des exceptions PHP
- Utilisation de gettext pour la traduction
- Optimisation du fichier de configuration (config.php) : il ne contient que la configuration (changements par rapport à la configuration par défaut)

INL

101/103, Bvd MacDonald

75019 Paris - France

Tel +33 (0) 1 44 89 46 35

www.inl.fr



Nuface 2.0