

RADIUS PFSENSE

Nouvel objet - Groupe

Créer dans : learn.local/Users

Nom du groupe :
pfsense-adm

Nom de groupe (antérieur à Windows 2000) :
pfsense-adm

Étendue du groupe

☐ Domaine local

☒ Globale

☐ Universelle

Type de groupe

☒ Sécurité

☐ Distribution

OK Annuler

Propriétés de : pfsense-adm

Général Membres Membre de Géré par

Membres :

Nom	Dossier Services de domaine Active Directory
Lucas Muller	learn.local/Lyon/Informatique

Ajouter... Supprimer

OK Annuler Appliquer

```
PS C:\Windows\system32> netsh nps show registeredserver

Inscription du serveur :
-----
Statut = Enregistré

Ok.

PS C:\Windows\system32>
```

Serveur NPS (Network Policy Server)

Fichier Action Affichage ?



- NPS (Local)
 - Clients et serveurs RADIUS
 - Clients RADIUS
 - Groupes de serveurs RADIUS distants
 - Stratégies
 - Stratégies de demande de connexion
 - Stratégies réseau
 - Gestion
 - Gestion des modèles
 - Secrets partagés
 - Clients RADIUS
 - Serveurs RADIUS distants
 - Filtres IP

Clients RADIUS



Les clients RADIUS vous permettent de spécifier les serveurs d'accès réseau qui fournissent l'accès à votre réseau.

Nom convivial Adresse IP Fabricant du

Nouveau client RADIUS

Paramètres Avancé

☒ Activer ce client RADIUS

☐ Sélectionner un modèle existant :

Nom et adresse

Nom convivial :

FW1

Adresse (IP ou DNS) :

10.1.1.9

Vérifier...

Secret partagé

Sélectionnez un modèle de secrets partagés existant :

Aucun

Pour taper manuellement un secret partagé, cliquez sur Manuel. Pour générer automatiquement un secret partagé, cliquez sur Générer. Vous devez configurer le client RADIUS avec le même secret partagé entré ici. Les secrets partagés respectent la casse.

☒ Manuel

☐ Générer

Secret partagé :

.....

Confirmez le secret partagé :

.....

OK



Annuler



Spécifier les conditions

Spécifiez les conditions qui déterminent si cette stratégie réseau est évaluée pour une demande de connexion. Au minimum, une condition est nécessaire.

Conditions :

Condition	Valeur
 Type d'authentification	PAP
 Groupes d'utilisateurs	LEARN\pfsense-adm

Description de la condition :

La condition Groupes d'utilisateurs spécifie que l'utilisateur qui tente d'établir la connexion doit appartenir à l'un des groupes sélectionnés.

[Ajouter...](#)[Modifier...](#)[Supprimer](#)[Précédent](#)[Suivant](#)[Terminer](#)[Annuler](#)

Server Settings

Descriptive name

rad

Type

RADIUS

RADIUS Server Settings

Protocol

PAP

Hostname or IP address

10.1.1.1

Shared Secret

.....

Services offered

Authentication and Accounting

Authentication port

1812

Accounting port

1813

Authentication Timeout

5

This value controls how long, in seconds, that the RADIUS server may take to respond to an access request. NOTE: If using an interactive two-factor authentication system, increase this timeout and enter a token.

RADIUS NAS IP Attribute

LAN - 10.1.1.9

Enter the IP to use for the "NAS-IP-Address" attribute during RADIUS Access-Requests. Please note that this choice won't change the interface used for contacting the RADIUS server.

UsersGroupsSettingsAuthentication Servers

Settings

Session timeout

10

Time in minutes to expire idle management sessions. The default is 4 hours (240 minutes). Enter 0 to never expire!

Authentication Server

rad

Password Hash Algorithm

bcrypt -- Blowfish-based crypt

Selects which algorithm the firewall will use when creating hashes for local user passwords. The most secure option is currently bcrypt. Some users may prefer SHA-512-based crypt hashes for compatibility.

Shell Authentication

☐ Use Authentication Server for Shell Authentication

If RADIUS or LDAP server is selected it is used for console and SSH authentication. Otherwise, the Local Database is used. To allow logins with RADIUS credentials, equivalent local users with the expected privileges must be created first. To allow logins with LDAP credentials, Shell Authentication Group DN must be specified on the LDAP server configuration.

Auth Refresh Time

Time in seconds to cache authentication results. The default is 30 seconds, maximum 3600 (one hour). Shorter times result in more frequent authentication server queries.

Save

Save & Test

Propriétés de pfsense-adm

Vue d'ensembleConditionsContraintesParamètres

Nom de la stratégie :

pfsense-adm

État de la stratégie

Si la stratégie est activée, le serveur NPS l'évalue lors de l'autorisation. Si elle est désactivée, le serveur NPS ne l'évalue pas.

☒ Stratégie activée

Autorisation d'accès

Si la demande de connexion répond aux conditions et contraintes de la stratégie réseau, celle-ci peut soit accorder l'accès, soit le refuser. [Qu'est-ce qu'une autorisation d'accès ?](#)

☒ Accorder l'accès. Accorder l'accès si la demande de connexion correspond à cette stratégie.

☐ Refuser l'accès. Refuser l'accès si la demande de connexion correspond à cette stratégie.

☐ Ignorer les propriétés de numérotation des comptes d'utilisateurs.

Si la demande de connexion répond aux conditions et contraintes de cette stratégie réseau, et si la stratégie accorde l'accès, l'autorisation est basée uniquement sur la stratégie réseau ; les propriétés de numérotation des comptes d'utilisateurs ne sont pas évaluées.

Méthode de connexion réseau

Sélectionnez le type de serveur d'accès réseau qui envoie la demande de connexion au serveur NPS. Vous pouvez sélectionner une valeur dans Type de serveur d'accès réseau ou bien Spécifique au fournisseur, mais ces paramètres ne sont pas obligatoires. Si votre serveur d'accès réseau est un commutateur d'authentification ou un point d'accès sans fil 802.1X, sélectionnez Non spécifié.

☒ Type de serveur d'accès réseau :

Non spécifié

☐ Spécifique au fournisseur :

10

OK

Annuler

Appliquer

Propriétés de pfsense-adm

Vue d'ensemble



Conditions

Contraintes

Paramètres

Configurez les conditions de cette stratégie réseau.

Si la demande de connexion répond aux conditions, le serveur NPS utilise cette stratégie pour autoriser la demande de connexion. Si la demande de connexion ne répond pas aux conditions, le serveur NPS ignore cette stratégie et en évalue d'autres. Si des stratégies supplémentaires seraient configurées.

Condition	Valeur
 Groupes d'utilisateurs	LEARN\pfsense-adm
 Type d'authentification	PAP

Propriétés de pfsense-adm

Vue d'ensemble

Conditions

Contraintes

Paramètres

Configurez les paramètres de cette stratégie réseau.

Si la demande de connexion répond aux conditions et contraintes, et si la stratégie accorde l'accès, les paramètres sont appliqués.


Paramètres :


Attributs RADIUS


Standard


☒ Spécifiques au fournisseur

Routage et accès à distance

 Liaisons multiples et protocole BAP (Bandwidth Allocation Protocol)

 Filtres IP

 Chiffrement

 Paramètres IP

Pour envoyer des attributs supplémentaires aux clients RADIUS, sélectionnez un attribut RADIUS standard, puis cliquez sur Modifier. Si vous ne configurez pas d'attribut, celui-ci n'est pas envoyé aux clients RADIUS. Consultez la documentation de votre client RADIUS pour connaître les attributs nécessaires.

Attributs :

Nom	Valeur
Class	pfsense-adm
Framed-Protocol	PPP
Service-Type	Framed

Ajouter...

Modifier...

Supprimer

```
FreeBSD/amd64 (pfSense.learn.local) (ttyv0)

VMware Virtual Machine - Netgate Device ID: eebaecaaf8f3f41f7818

*** Welcome to pfSense 2.7.1-RELEASE (amd64) on pfSense ***

WAN (wan)      -> le1      ->
LAN (lan)      -> le0      -> v4: 10.1.1.9/24

0) Logout (SSH only)          9) pfTop
1) Assign Interfaces          10) Filter Logs
2) Set interface(s) IP address 11) Restart webConfigurator
3) Reset webConfigurator password 12) PHP shell + pfSense tools
4) Reset to factory defaults    13) Update from console
5) Reboot system              14) Enable Secure Shell (sshd)
6) Halt system                15) Restore recent configuration
7) Ping host                  16) Restart PHP-FPM
8) Shell

Enter an option:
Message from syslogd@pfSense at Jun 19 08:59:31 ...
php-fpm[3961]: /index.php: Successful login for user 'Administrateur' from: 10.1.
1.102 (RADIUS/rad)
█
```

VPN avec RADIUS

Confirmer les sélections d'installation

SERVEUR DE DESTINATION
DC1.learn.local

Avant de commencer

Type d'installation

Sélection du serveur

Rôles de serveurs

Fonctionnalités

AD LDS

Confirmation

Résultats

Pour installer les rôles, services de rôle ou fonctionnalités suivants sur le serveur sélectionné, cliquez sur Installer.

☐ Redémarrer automatiquement le serveur de destination, si nécessaire

Il se peut que des fonctionnalités facultatives (comme des outils d'administration) soient affichées sur cette page, car elles ont été sélectionnées automatiquement. Si vous ne voulez pas installer ces fonctionnalités facultatives, cliquez sur Précédent pour désactiver leurs cases à cocher.

Outils d'administration de serveur distant

Outils d'administration de rôles

Outils AD DS et AD LDS

AD LDS Snap-Ins and Command-Line Tools

Services AD LDS (Active Directory Lightweight Directory Services)

[Exporter les paramètres de configuration](#)[Spécifier un autre chemin d'accès source](#)

< Précédent

Suivant >

Installer

Annuler