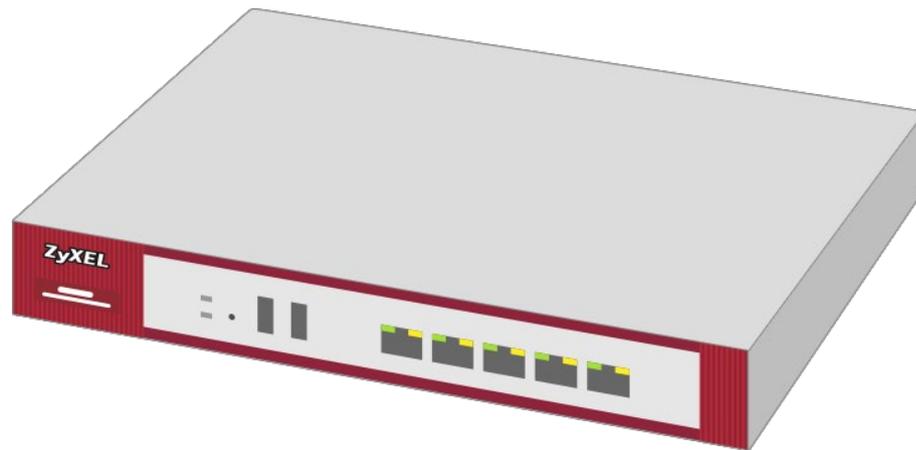


ZYXEL

Your Networking Ally



Bases pour la protection d'un pare-feu

Série pare-feu ZyXel

à partir de la version du firmware 5.35

Knowledge Base KB-3823

Janvier 2023

© ZyXel Corporation

BASES POUR LA PROTECTION D'UN PARE-FEU

Le pare-feu est le premier obstacle pour des pirates sur Internet. Un pare-feu protège le réseau local des accès non autorisés. Il est ainsi partie intégrante de tout concept de sécurité. Mais que se passe-t-il si le pare-feu lui-même est la cible d'attaques de pirates et peut donc devenir une menace potentielle ? Le guide suivant a pour but de fournir des informations sur la manière de limiter les possibilités d'attaque.

POLICY CONTROL

En principe, il faut limiter le nombre d'utilisateurs qui ont accès au pare-feu à aussi peu que possible. Pour garantir cela, il est conseillé de limiter autant que possible les droits d'accès.

Les règles de pare-feu sont créées dans le menu suivant :

[Configuration > Security Policy > Policy Control](#)

Priority	Status	Name	From	To	IPv4 Source	IPv4 Destination	Service	Device	User	Schedule	Action	Log	Profile
6	🔴	gast_block2	any	ZyWALL	any	any	Default_Alb...	any	gast	none	allow	no	
22	🔴	WAN_to_Device	WAN	ZyWALL	Studerus	any	Default_Alb...	any	any	none	allow	log a...	
23	🔴	WAN-Remote_MGMT	WAN	ZyWALL	Studerus	any	Remote_Asb...	any	any	none	allow	log a...	
24	🔴	WAN_to_Device_SSL-2FA	WAN	ZyWALL	Schweiz	any	Remote_SSL...	any	any	none	allow	no	
Default			any	any	any	any	any	any	any	none	deny	log	

La zone ZyWALL joue un rôle particulier. En principe, il est seulement possible de créer des règles vers la zone ZyWALL. Elle contient toutes les adresses d'interface du pare-feu. Par exemple, l'adresse par défaut 192.168.1.1 n'appartient pas à la zone LAN1, mais à la zone ZyWALL.

Priority	Status	Name	From	To	IPv4 Source
6	🔴	gast_block2	any	ZyWALL	any
22	🔴	WAN_to_Device	WAN	ZyWALL	Studerus
23	🔴	WAN-Remote_MGMT	WAN	ZyWALL	Studerus
24	🔴	WAN_to_Device_SSL-2FA	WAN	ZyWALL	Schweiz

Avec les paramètres par défaut, l'accès au pare-feu est largement ouvert. Il convient donc de les limiter davantage.

Restriction des règles « Policy Control »

Les règles de pare-feu peuvent être restreintes sur la base de plusieurs critères. Pour l'accès au pare-feu, 3 critères sont principalement utiles :

1. IPv4 Source (objets d'adresse),
2. service,
3. utilisateur.

Ces éléments sont créés en tant qu'objets.

Objets d'adresse

Il existe en général 3 types d'objets adresse. De quels types s'agit-il ?

1. Adresses IP,
2. adresses FQDN,
3. adresses GeoIP.

Les objets adresses peuvent être rassemblés dans un groupe. Mais il n'est pas possible de mélanger différents types d'adresses.

Configuration > Object > Address > Address > Add :

#	Name	Type	IPv4 Address	Reference
1	ADMIN_LANT	HOST	192.168.1.35	1
2	AD_SERVER	HOST	172.27.2.40	3
3	ALL	SUBNET	0.0.0.0/0	1
4	API	HOST	10.0.0.50	1
5	AP2	HOST	10.0.0.52	1
6	ATP200_06	HOST	217.192.14.86	0
7	Africa	GEOGRAPHY	Africa-All	1
8	Antarctica	GEOGRAPHY	Antarctica-All	1
9	Asia	GEOGRAPHY	Asia-All	1
10	Austria	GEOGRAPHY	Austria-All	1
11	Broadcast	HOST	255.255.255.255	1
12	DMZ_SUBNET	INTERFACE SUBNET	dmz-0.0.0.0/32	3
13	Deutschland	GEOGRAPHY	Germany-All	1
14	Dropbox	RANGE	162.125.0.0-162.125.255.255	1
15	EIMODE_VPN_PROVISIONING_LOCAL	SUBNET	192.168.1.0/24	0
16	EIMODE_VPN_PROVISIONING_REMOTE	SUBNET	0.0.0.0/24	0
17	IGMP	RANGE	224.0.0.0-239.255.255.255	2

1. Adresses IP

Lorsque c'est possible, il convient d'utiliser des adresses IP, car elles sont uniques. Il existe plusieurs types d'adresses IP :

1. Host > Décrit une adresse IP unique
2. Range > Il est possible de saisir n'importe quelle plage, définie par les adresses de début et de fin
3. Subnet > Celui-ci peut être créé en entrant un masque de sous-réseau ou un CIDR (par ex. /24)
4. Interface IP > prend en charge l'adresse IP d'une interface et s'adapte dynamiquement
5. Interface Subnet > prend en charge dynamiquement le Subnet d'une interface
6. Interface Gateway > prend en charge la passerelle d'une interface du type WAN ou général.

Host, Range, Subnet

Les types d'adresse Host, Range et Subnet servent spécialement en tant que IPv4 Source. Si un accès a lieu depuis le WAN, l'adresse IP publique du poste distant est indiquée.

À partir d'un réseau local, ces objets permettent de créer des groupes avec des autorisations différentes.

Interface IP

Cet objet peut être utilisé si l'accès ne doit être possible que sur une adresse IP donnée. Si, par exemple, il y a 2 interfaces WAN, mais qu'un service ne doit être disponible que sur une seule interface, l'IP de l'interface peut être saisie comme destination IPv4 dans la règle de contrôle des politiques.

Interface Subnet

Ce type d'adresse convient si des règles uniformes doivent être créées pour une interface locale (par ex. LAN1).

Passerelle interface

Ce type d'adresse n'est pas pertinent pour l'accès au pare-feu.

2. Objets FQDN

Pour les objets FQDN, il est possible de saisir un nom au lieu d'une adresse IP, par exemple `www.mydomain.com`. Ce type d'entrées convient surtout si un accès a lieu depuis le WAN et le poste distant n'a pas d'adresse IP publique statique. Dans ce cas, un nom DynDNS peut être utilisé à la place de l'adresse IP. Un serveur DNS rapide est nécessaire pour les objets FQDN. Il est également possible d'utiliser des entrées joker, comme `*.mydomain.com`. Ils ne peuvent toutefois pas être utilisés à cette fin.

Adresses Geo IP

Avec GeoIP, il est possible de créer des objets basés sur des pays ou des régions. Le service fait appel à une base de données externe et devrait être régulièrement mis à jour. GeoIP n'offre pas de protection fiable, car il est très facile de manipuler l'adresse d'origine au moyen de services VPN librement disponibles.

Objets de service

Les objets de service permettent de définir les services auxquels l'accès est accordé ou refusé dans les paramètres de contrôle des politiques. Les services peuvent être regroupés. Les services peuvent également être utilisés ailleurs, par exemple dans les Policy Routes et les entrées NAT. Outre les objets de service normaux, il existe quelques objets spéciaux tels que « Wiz_2FA, Wiz_HTTP, Wiz_HTTPS et Wiz_SSLVPN ». Le port de ces services s'adapte automatiquement lorsqu'il est redéfini dans le menu correspondant.

Configuration > Object > Service

#	Name	Content	Reference
1	AH	Protocol=51	2
2	AIM	TCP=5190	0
3	AUTH	TCP=113	0
4	AUTH2FA	TCP=8443	1
5	Any_TCP	TCP/1-65535	0
6	Any_UDP	UDP/1-65535	0
7	BGP	TCP=179	0
8	BONJOUR	UDP=5353	0
9	BOOTP_CLIENT	UDP=68	0
10	BOOTP_SERVER	UDP=67	0
11	CARPWAP-CONTROL	UDP=5246	0
12	CARPWAP-DATA	UDP=5247	0
13	CU_SEENIE_TCP1	TCP=7448	1
14	CU_SEENIE_TCP2	TCP=24032	1
15	CU_SEENIE_UDP1	UDP=7448	1
16	CU_SEENIE_UDP2	UDP=24032	1
17	DHCPv6_CLIENT	UDP=546	1

User

Configuration > Object > User

Il existe différents types d'utilisateurs (user) :

User : admin, peut apporter des modifications à la configuration,

User : limited-admin, peut accéder à la configuration mais ne peut pas la modifier,

User : user, peut s'authentifier par authentification à double facteur (2FA),

User : guest, peut se connecter au pare-feu,

User : ext-user/ext-group-user, s'authentifie sur un serveur externe,

Les « Built-in User » sont des utilisateurs prédéfinis qui ne peuvent pas être supprimés et qui sont destinés à des fins spécifiques.

Les utilisateurs doivent être définis de telle sorte qu'ils ne disposent que des autorisations nécessaires.

Les utilisateurs VPN ou 802.1x, par exemple, sont généralement définis en tant que type d'utilisateur « User ».

Configuration > Object > User/Group > Settings

The screenshot shows the 'User/Group Settings' page for a ZyXEL USG FLEX 100. The page is divided into several sections:

- Miscellaneous Settings:**
 - Allow renewing lease time automatically
 - Enable user idle detection
 - User idle timeout: (1-60 minutes)
- Login Security:**
 - Password must be changed every (days) (1-365 days)
 - Password reset link(FQDN/IP):
 - Enable Password Complexity
 - Complexity requirement:
 - * Minimum password length should be of 8 characters.
 - * Include at least 1 Upper case alphabetic character.
 - * Include at least 1 lower case alphabetic character.
 - * Include at least 1 numeric character.
 - * Include at least 1 special character like @,\$,!,...
- User Logon Settings:**
 - Limit the number of simultaneous logons for administration account
 - Maximum number per administration account: (1-64)
 - Limit the number of simultaneous logons for access account
 - Maximum number per access account: (1-64)
- User IP Lockout Settings:**
 - Enable logon retry limit
 - Maximum retry count: (1-99)
 - Lockout period: (1-65535 minutes)

Securité Login

Définit si les mots de passe doivent être modifiés et dans quel délai, et si une complexité des mots de passe est nécessaire.

Paramètres User Logon

Définit le nombre de fois qu'un utilisateur peut se connecter en même temps. Si la limite est fixée à 1, il peut arriver qu'un administrateur se bloque lui-même.

Paramètres User IP Lockout

Les entrées définissent le nombre de fois qu'une mauvaise saisie du mot de passe est autorisée jusqu'à ce que l'utilisateur soit bloqué pour une période donnée. Ce réglage protège surtout contre les attaques par force brute.

Règles « Policy Control » conseillés

From: WAN To: ZyWALL

Il est vivement recommandé de fermer tous les services qui ne sont pas expressément nécessaires.

Services fréquemment utilisés

VPN IPSec (IKEv1, IKEv2, L2TP) :
ESP, IKE, NATT, (L2TP-UDP)

VPN SSL :
Wiz_SSLVPN

L'authentification à double facteur pour VPN :
Wiz_2FA

Un accès à distance via HTTP/HTTPS :
Wiz_HTTP, Wiz_HTTPS

Pour éviter autant que possible les risques de sécurité, une gestion à distance s'effectue idéalement via IPSecVPN. Les adresses sources devraient, si possible, être limitées. Le VPN SSL est déconseillé, car il offre un vecteur d'attaque possible via SSL.

Un accès à distance via HTTPS :
Si un accès à distance via HTTP/HTTPS est nécessaire, l'adresse source doit toujours être limitée à une adresse IP ou à un FQDN. L'utilisation de GeoIP comme adresse source n'est pas sûre et offre un potentiel d'attaque considérable. Pour la gestion HTTPS, il est recommandé d'utiliser un port alternatif.

From: Zone VPN To: ZyWALL (client vers site)

Par défaut, tous les ports sont ouverts. En principe, dans la plupart des cas, très peu de services sont nécessaires. Il s'agit par exemple du DNS et de L2TP-UDP. Pour d'autres services, l'accès doit être bloqué. Si une gestion à distance via VPN client à site est souhaitée, l'accès au pare-feu peut être limité à un utilisateur. Cela ne fonctionne toutefois que si l'utilisateur s'est déjà connecté au pare-feu lors de l'établissement du tunnel.

From: LAN To: ZyWALL

Ici aussi, les droits d'accès doivent être limités. L'accès complet au pare-feu ne devrait être accordé qu'à un LAN de gestion spécial ou à certaines adresses IP d'administrateurs. Pour que certains services fonctionnent correctement, l'accès au pare-feu doit être garanti. Cela concerne par exemple DNS, Multicast, Radius-Auth, NetBIOS, SNMT, SSO, etc. Les accès effectivement nécessaires dépendent fortement de la topologie du réseau et des technologies utilisées.

DÉTECTION ET PRÉVENTION D'ANOMALIE (ADP)

[Configuration](#) > [Security Policy](#) > [ADP](#)

L'ADP offre une protection contre les scans de ports et les comportements réseau inhabituels. Il est recommandé d'activer l'ADP avec le profil par défaut de la zone WAN. Des adaptations individuelles peuvent être apportées au profil en cas de problèmes.

General | Profile | Allow List

General Settings

Enable Anomaly Detection and Prevention

Policies

+ Add | Edit | Remove | Activate | Inactivate | Move

#	Priority	Status	From	Anomaly Profile
1	1	On	WAN	ADP_PROFILE

Page 1 of 1 | Show 50 items | Displaying 1 - 1 of 1

Dans certains cas, ADP peut affecter certains services. Cela concerne surtout la détection d'inondation. Pour cette raison, la protection contre l'inondation peut être désactivée pour certains services, par exemple NAT. Un tel réglage n'est utile qu'en cas de problèmes.

General | Profile | **Allow List**

General Settings

Enable Allow List for Flooding Detection

Rule Summary

+ Add | Edit | Remove | Activate | Inactivate

#	Status	Name	IPv4 Source	IPv4 Destination	Service
1	On	NAT	any	any	NAT

Page 1 of 1 | Show 50 items | Displaying 1 - 1 of 1

GESTION À DISTANCE VIA HTTPS

Certains réglages spécifiques dans les paramètres WWW ont une influence directe sur la sécurité du système.

[Configuration](#) > [System](#) > [WWW](#)

Service Control Login Page

HTTPS

Enable

Server Port:

Authenticate Client Certificates (See [Trusted CAs](#))

Server Certificate:

Redirect HTTP to HTTPS

Admin Service Control

+ Add Edit Remove Move

#	Zone	Address	Action
1	LAN1	LAN1_SUBNET	accept
2	TUNNEL	Remote_Admin_PC	accept
3	WAN	STAG	accept
4	WAN	Public_Remote_Access	accept
5	ALL	ALL	deny
-	ALL	ALL	accept

Page 1 of 1 Show 50 items Displaying 1 - 6 of 6

User Service Control

+ Add Edit Remove Move

#	Zone	Address	Action
-	ALL	ALL	accept

Page 1 of 1 Show 50 items Displaying 1 - 1 of 1

HTTP

Enable

Server Port:

Admin Service Control

+ Add Edit Remove Move

Port serveur

Pour la gestion à distance, il ne faut pas utiliser le port standard 443, car il est toujours scanné en cas d'attaques automatisées. Les ports alternatifs fréquemment utilisés (p. ex. 8443) ne sont pas non plus idéaux.

Rediriger HTTP vers HTTPS

Tous les appels HTTP de l'interface utilisateur graphique sont redirigés vers HTTPS. Attention ! Ce paramètre ne doit pas être activé si l'authentification web est utilisée. Dans tous les autres cas, cette option doit être activée.

Contrôle service admin

Il est possible de définir ici qui peut avoir un accès d'administrateur au pare-feu. Il est conseillé de limiter l'accès à certaines adresses IP. Seules les adresses IP sont autorisées comme objets d'adresse. La dernière règle (ici la règle 5) à créer est la règle ALL/ALL/deny. Lors de la création de la règle, il convient d'être prudent afin de ne pas s'exclure soi-même. C'est pourquoi il faut d'abord créer les règles Accept avant de créer la règle Deny en dernière position.

User Service Control (contrôle service utilisateur)

Dans le « User Service Control », on définit quels clients sont autorisés à s'authentifier sur le pare-feu.

La règle est pertinente pour le SSL-VPN, 2-FA, VPN Configuration Provisioning et WEB-Authentication.

Si cela n'est pas utilisé, une règle deny peut également être définie.

Authenticate Client Certificates

Si l'option « Authenticate Client Certificate » est activée, le client doit s'autoriser avec un certificat valide. Dans le cas contraire, la connexion est refusée. Cela concerne les accès via **HTTPS** et **VPN SSL**. VPN Configuration_Profisioning avec SecuExtender ne fonctionne pas si cette option est activée. Cependant, l'appel de la fenêtre 2FA reste possible sans certificat.

Pour qu'un certificat soit considéré comme fiable par le pare-feu, la chaîne de confiance de l'autorité de certification doit être installée. Celle-ci comprend généralement un certificat racine et un certificat intermédiaire. Le pare-feu fait confiance à chaque certificat avec une chaîne de certificats valable ainsi qu'à ses propres certificats auto-signés. Il convient de noter que certains navigateurs refusent systématiquement les certificats auto-signés (actuellement les navigateurs basés sur Firefox). Le certificat client ne doit pas être installé sur le pare-feu.

Configuration > Object > Certificate > Trusted Certificates

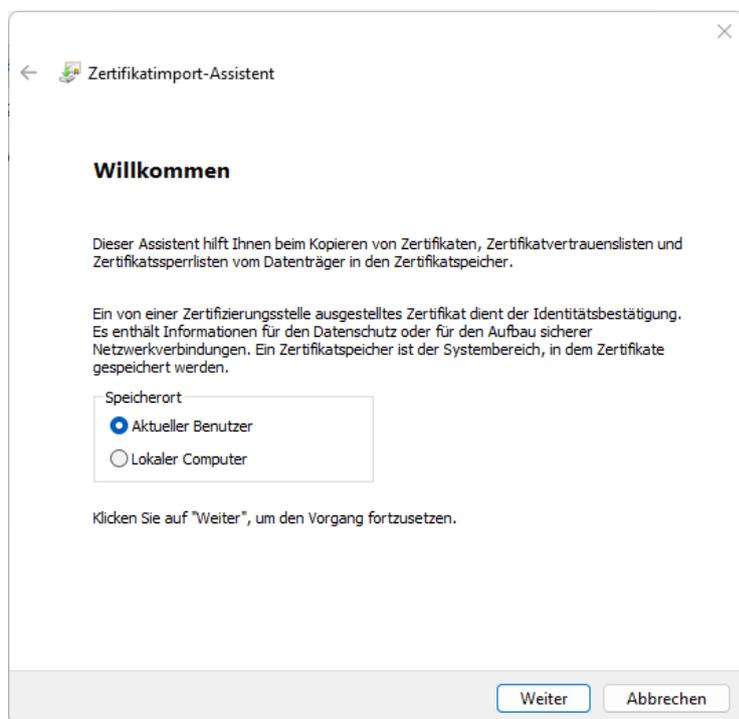
The screenshot shows the 'Trusted Certificates' configuration page in the ZyXEL management interface. The left sidebar contains a navigation menu with categories like CONFIGURATION, Wireless, Network, VPN, BWM, Web Authentication, Security Policy, Security Service, and Object. The main content area has tabs for 'My Certificates' and 'Trusted Certificates'. Below the tabs, there is a 'PKI Storage Space in Use' progress bar showing 17.74% used. A 'Trusted Certificates Setting' table is displayed with the following data:

#	Name	Subject	Issuer	Valid From	Valid To
1	letsencrypt_int...	CN=R3, O=Let's Encrypt, ...	CN=ISRG Root X1, O=Int...	2020-09-04 00:00:00 GMT	2025-09-15 16:00:00 GMT
3	letsencrypt_root	CN=ISRG Root X1, O=Int...	CN=ISRG Root X1, O=Int...	2015-06-04 11:04:38 GMT	2035-06-04 11:04:38 GMT
5	inter_ca_f.der	CN=Nebula Star CA - VV...	CN=ca.cloud.zyxel.com,...	2021-07-14 02:45:43 GMT	2041-07-09 02:45:43 GMT
6	inter_ca_ztp.der	CN=Nebula Star CA - FLE...	CN=ca.cloud.zyxel.com,...	2021-03-29 02:26:05 GMT	2036-03-25 02:26:05 GMT
7	poc-rootca.der	CN=ca.cloud.zyxel.com,...	CN=ca.cloud.zyxel.com,...	2013-05-31 01:53:27 GMT	2033-06-15 01:53:27 GMT
8	secu_manager...	CN=ca.cloudcnm.zyxel,...	CN=ca.cloudcnm.zyxel,...	2017-08-22 02:10:00 GMT	2027-08-20 02:10:00 GMT

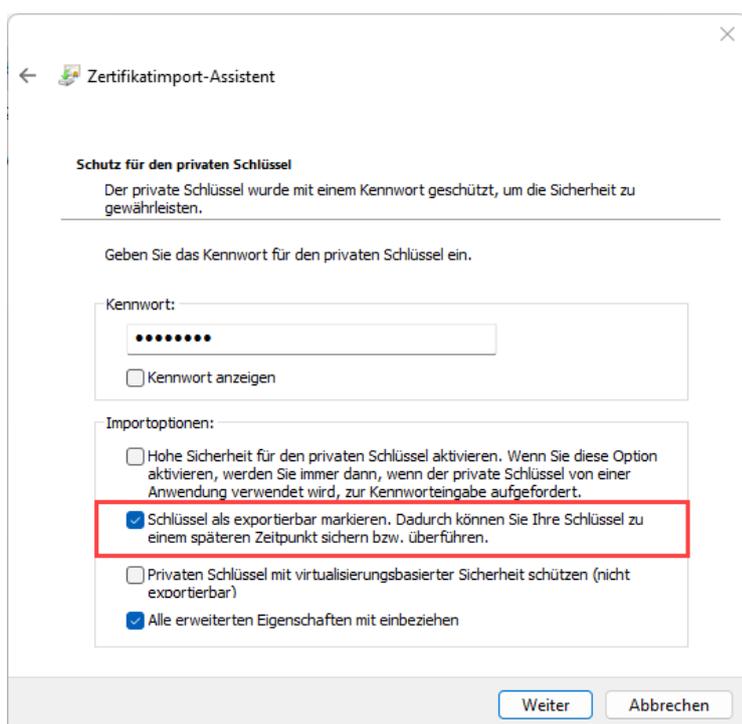
At the bottom of the table, it shows 'Page 1 of 1', 'Show 50 items', and 'Displaying 1 - 8 of 8'.

Le certificat client avec clé privée est installé sur le client. Voici une installation manuelle sous Windows :

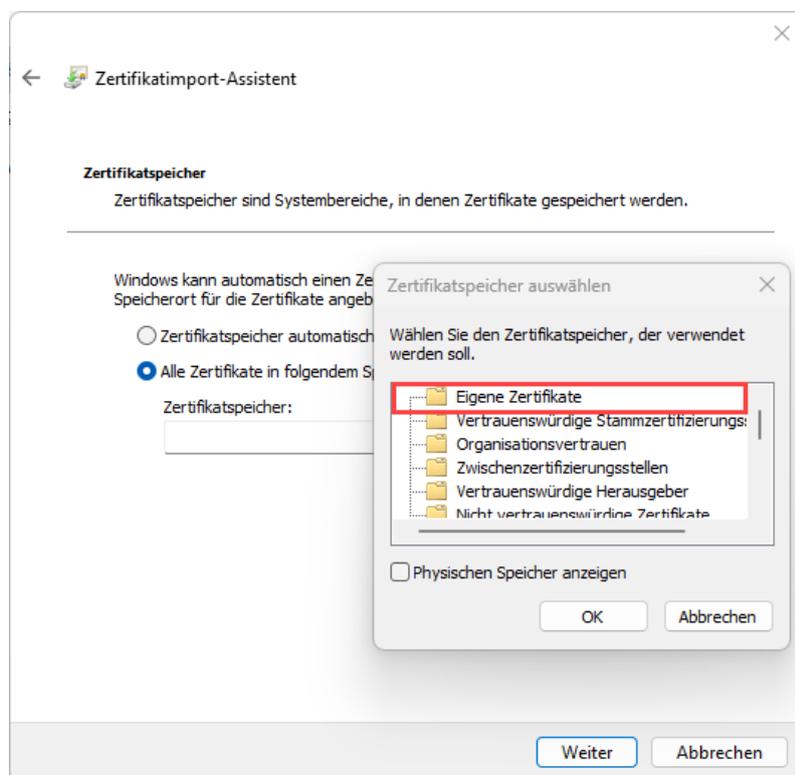
Ouvrir le certificat avec clé privée (PFX ou P12) par un double-clic et l'importer dans l'utilisateur actuel.



Lors de l'importation, veiller à ce que l'option « Marquer les clés comme exportables » soit activée.



L'importation se fait dans le magasin de certificats « Mes certificats ».



SERVICES GESTION À DISTANCE

Configuration > System

Sur le pare-feu, il existe plusieurs services qui ne sont que rarement ou pas du tout utilisés. Ces services peuvent être complètement désactivés.

SSH

Ce service peut être utilisé, par exemple, lorsque des modifications de configuration sont effectuées avec un script automatique. Si SSH n'est pas utilisé régulièrement pour l'administration, le service peut être désactivé. Pour les entrées CLI, la Web Console peut également être utilisée à la place de SSH.



TELNET

N'est pas nécessaire dans la plupart des cas et peut être désactivé.

FTP

Le FTP permet par exemple d'actualiser le firmware ou de télécharger des fichiers de configuration. Le FTP doit être activé si HA-Pro est utilisé. Si ce n'est pas le cas, FTP peut être désactivé. Si le service est utilisé de manière sporadique, il peut être activé temporairement en cas de besoin.

SNMP

Ce service est nécessaire pour la surveillance du réseau et est requis pour des solutions comme par ex : PRTG. Si aucune surveillance du réseau n'est effectuée, le service peut être désactivé.

ZON

Permet l'échange d'informations avec des appareils voisins (modèle, nom, firmware, adresse MAC, adresse IP) via LLDP ainsi qu'avec le logiciel ZON de Zyxel sur le même LAN. Le service n'est pas nécessaire pour le fonctionnement normal.

VPN

IPSec-VPN

Site à site

Lors de l'utilisation de tunnels site à site, une adresse de passerelle d'égal à égal doit être saisie dans la mesure du possible. Si l'autre partie a une adresse IP dynamique, il est également possible d'utiliser un nom DynDNS. Il est également possible d'utiliser un nom DynDNS si l'autre partie se trouve derrière un NAT/CG-NAT. Il est alors important que la connexion soit établie depuis le côté opposé et que le service DynDNS synchronise l'adresse IP publique.

Pour l'authentification, un certificat est préférable à un PSK. Il faut tenir compte des points suivants :

1. Le certificat utilisé peut être un « Self-Signed Certificate », mais doit être déposé sous « Trusted Certificates » du côté opposé.
2. Un certificat propre est créé des deux côtés.
3. Le type d'ID locale est extrait du certificat et doit être enregistré de manière identique en tant que Peer ID du côté opposé.
4. La recommandation pour la durée de vie SA maximale est de 86400 secondes dans la passerelle VPN et de 14400 secondes dans la connexion VPN.
5. Les paramètres suivants sont recommandés au minimum pour le cryptage VPN : AES256 / SHA256 / DH15. Ceci aussi bien dans la passerelle VPN que dans la connexion VPN.
6. Le protocole d'authentification étendu est également possible pour les tunnels site à site. Toutefois, l'utilisateur inscrit n'est pas connecté au pare-feu lors de l'établissement de la connexion.

Edit VPN Gateway VTI_CAB_HOME

Show Advanced Settings Create New Object

General Settings

Enable
VPN Gateway Name: MyIkeV2_GATEWAY

IKE Version

IKEV1
 IKEV2

Gateway Settings

My Address

Interface: Gateway Static -- 217.192.14.85/255.255.255.192
 Domain Name / IPv4

Peer Gateway Address

Static Address Primary: me.selfhost.eu
Secondary: 0.0.0.0
 Fall back to Primary Peer Gateway when possible
Fall Back Check Interval: 300 (60-86400 seconds)
 Dynamic Address

Authentication

Pre-Shared Key
 unmasked
 Certificate VTI (See My Certificates)

Advance

Local ID Type: IPv4
Content: 217.192.14.85
Peer ID Type: DNS
Content: me.selfhost.eu

Phase 1 Settings

SA Life Time: 86400 (180 - 3000000 Seconds)

Advance

Proposal

#	Encryption	Authentication
1	AES256	SHA256

Key Group: DH19

Extended Authentication Protocol

Enable Extended Authentication Protocol
Allowed Auth Method: mschapv2
 Server Mode
AAA Method: default
Allowed User: S2S-VPN
 Client Mode
User Name :
Password:

OK Cancel

VPN client vers site

Pour les VPN client à site, IKEv2 avec certificat et Extended Authentication Protocol est recommandé.

Dans la connexion VPN, Configuration Payload est obligatoire.

Edit VPN Connection RemoteAccess_Wiz

Show Advanced Settings Create New Object ▼

Application scenario

- Site-to-site
- Site-to-site with Dynamic Peer
- Remote Access (Server Role)
- Remote Access (Client Role)
- VPN Tunnel Interface

VPN Gateway: RemoteAccess_Wi Gateway 0.0.0.0, 0.0.0.0

Policy

Local Policy: LAN1_SUBNET INTERFACE SUBNET, 192.168.111.0/24

▼ Advance

Configuration Payload

- Enable Configuration Payload
- IP Address Pool: RemoteAccess_Wi RANGE, 192.168.51.1-192.168.51.250 ⓘ
- First DNS Server (Optional): 192.168.111.1
- Second DNS Server (Optional):
- First WINS Server (Optional):
- Second WINS Server (Optional):
- Allow Traffic Through WAN Zone

Phase 2 Setting

SA Life Time: 28800 (180 - 3000000 Seconds)

▼ Advance

Related Settings

Zone: IPSec_VPN ⓘ

▼ Advance

Après l'établissement de la connexion, le client est connecté au pare-feu avec l'utilisateur. Pour un éventuel accès admin au pare-feu, l'utilisateur admin correspondant peut donc être enregistré dans le Policy Control.

VPN L2TP

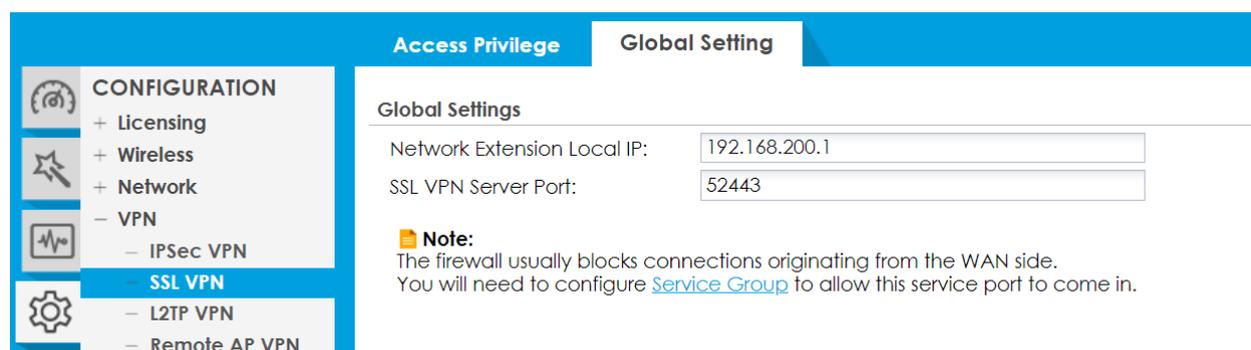
Il est déconseillé d'utiliser le VPN L2TP. IKEv2 peut être utilisé à la place.

VPN SSL

En raison des performances et des éventuels problèmes de sécurité, le VPN SSL n'est pas recommandé. Toutefois, comme il est souvent utilisé en raison de sa facilité de configuration, il convient de tenir compte des points suivants :

Configuration > VPN > SSL VPN > Global Setting

L'utilisation d'un port séparé pour SSL VPN est obligatoire. Le port 443 ne doit en aucun cas être utilisé.



The screenshot displays the configuration page for SSL VPN. On the left, a navigation menu is visible with the following items: CONFIGURATION, + Licensing, + Wireless, + Network, - VPN, - IPsec VPN, - SSL VPN (highlighted), - L2TP VPN, and - Remote AP VPN. The main content area is titled 'Global Settings' and contains two input fields: 'Network Extension Local IP' with the value '192.168.200.1' and 'SSL VPN Server Port' with the value '52443'. Below these fields, a note is displayed: 'Note: The firewall usually blocks connections originating from the WAN side. You will need to configure [Service Group](#) to allow this service port to come in.'

La sécurité est considérablement renforcée par l'utilisation d'un certificat pour l'authentification. La configuration est décrite sous « Gestion à distance via HTTPS > Authenticate Client Certificate ».

Dans le Policy Control, il est conseillé de limiter l'IP source pour l'accès du WAN au ZyWALL pour le service Wiz_SSLVPN. Au moins sur une GeoIP, mieux sur un FQDN ou une adresse IP.

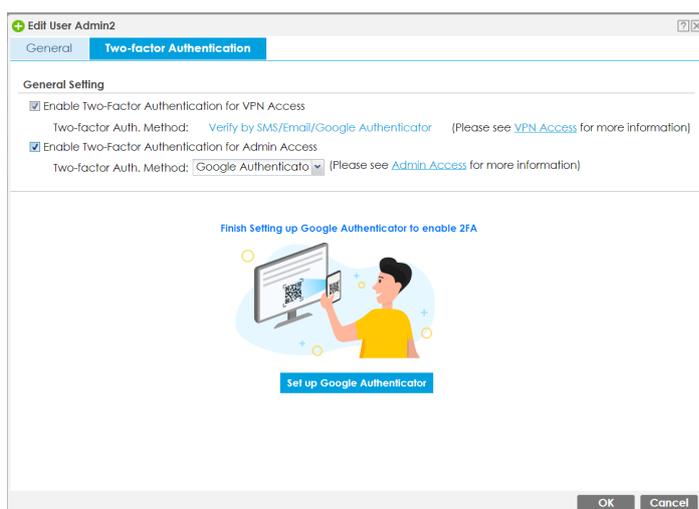
Il est également possible de limiter l'accès de l'administrateur au pare-feu depuis la zone SSL-VPN à l'utilisateur admin. Cela est possible car l'utilisateur se connecte déjà au pare-feu lors de l'établissement du tunnel.

Les utilisateurs normaux n'ont pas besoin d'accéder au pare-feu depuis la zone SSL-VPN. Il suffit d'autoriser ici les services typiques tels que DNS.

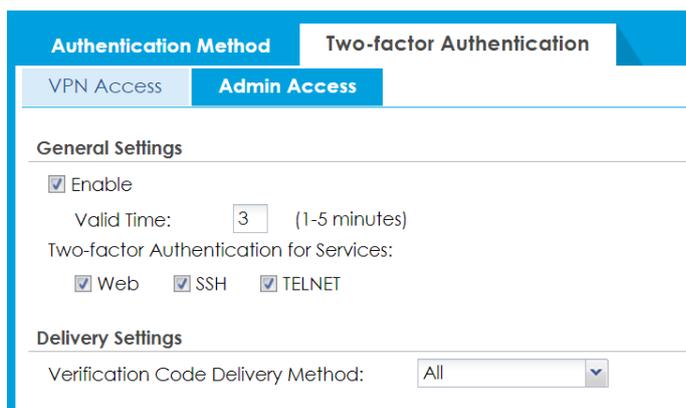
AUTHENTIFICATION À DOUBLE FACTEUR

Une authentification à double facteur (2FA) est recommandée pour Admin Access, de préférence avec Google Authenticator.

La configuration pour 2FA doit être effectuée séparément pour chaque utilisateur. La méthode Google Authenticator est recommandée. Il convient de noter que les utilisateurs pour lesquels 2FA n'est pas configuré peuvent continuer à se connecter sans authentification supplémentaire. C'est pourquoi 2FA n'offre qu'une protection limitée.



[Configuration](#) > [Object](#) > [Auth. Method](#) > [Two-factor Authentication](#) > [Admin Access](#)



Configuration > Object > Auth. Method > Two-factor Authentication > VPN Access

2FA peut également être activé pour l'accès VPN.

Un port spécifique est toujours utilisé pour l'authentification (objet Wiz_2FA).

Il existe également différentes méthodes pour envoyer un lien. En fin de compte, toutes les méthodes appellent un lien vers l'interface utilisateur web.

Comme l'interface web doit être accessible depuis le WAN pour 2FA, il existe ici aussi un risque d'attaque potentiel. C'est pourquoi cette fonction doit être utilisée avec prudence

The screenshot shows the configuration page for Two-factor Authentication under VPN Access. The left sidebar contains a navigation menu with categories like CONFIGURATION, Licensing, Wireless, Network, VPN, BWM, Web Authentication, Security Policy, Security Service, Object, and Auth. Method. The main content area is titled 'Authentication Method' and 'Two-factor Authentication'. It has two tabs: 'VPN Access' (selected) and 'Admin Access'. Under 'General Settings', there is an 'Enable' checkbox, a 'Valid Time' of 3 minutes, and checkboxes for 'Two-factor Authentication for Services' including SSL VPN Access, IPsec VPN Access, and L2TP/IPsec VPN Access. The 'User/Group' section shows a list of 'Selectable User/Group Objects' (any, ldap-users, ad-users) and 'Selected User/Group Objects' (radius-users, admin, cab). The 'Delivery Settings' section includes 'Deliver Authorize Link Method' (SMS, Email, Google Authenticator), 'Authorize Link URL Address' (https, User-Defined, my.domain.com), and 'Authorized Port' (8008). A message template is provided for the default message.

Note

- 1.The Default Message must use alphanumeric characters.
- 2.The Multilingual file must be in UTF-8 format and named '2FA-msg.txt'.
- 3.The Default Message and the Multilingual file must contain a <url> tag. You can also use <user>/<host>/<time> variables to display dynamic information.
- 4.The Default Message and the Multilingual file do not support HTML tags such as
, <i>, and so on.

ALERT LOGS

Pour certaines options, il peut avoir du sens de paramétrer un Alert Log qui déclenche tout de suite une alerte e-mail lors d'un évènement choisi. Cette fonction s'avère utile par exemple si un administrateur se connecte, notamment pour des pare-feux surveillés à intervalles irréguliers.

[Configuration > Log & Report > Log Settings](#)

✎ Edit log Category Setting - System log

E-mail Server 1

Active

Mail Server: (Outgoing SMTP Server Name or IP Address)

Mail Server Port: TLS Security STARTTLS Authenticate Server

Mail Subject:

Send From: (E-Mail Address)

Send Log to: (E-Mail Address)

Send Alerts to: (E-Mail Address)

Sending Log: ▼

Day for Sending Log: ▼

Time for Sending Log: ⌚

SMTP Authentication

User Name:

Password:

Retype to Confirm:

Active Log and Alert

Log Category+	System Log			E-mail Server 1		E-mail Server 2	
	disable	normal	debug	normal	alert	normal	alert
<input checked="" type="checkbox"/> Authenticate	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
- User	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
- PKI	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
- Account	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
- Auth. Policy	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
- Web Authentication	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
- Authentication Server	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
- ...	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

MISES À JOUR DE FIRMWARE AUTOMATIQUES

Il faut toujours veiller à ce que le firmware du pare-feu soit à jour. Les mises à jour peuvent être effectuées manuellement sur les systèmes qui sont gérés activement. Cependant, dans la réalité, il arrive souvent que cela soit négligé et que les pare-feux présentant des failles de sécurité connues ne soient pas mis à jour pendant une longue période.

En particulier dans les environnements de ce type, il est recommandé d'activer les mises à jour automatiques.

Maintenance > File Manager > Firmware Management

The screenshot displays the ZyXEL web interface for Firmware Management. The left sidebar shows the 'MAINTENANCE' menu with options like 'File Manager', 'Diagnostics', 'Packet Flow Explore', and 'Shutdown/Reboot'. The main content area has three tabs: 'Configuration File', 'Firmware Management' (selected), and 'Shell Script'. Under 'Firmware Management', there is a 'Firmware Status' section with a table:

#	Status	Model
1	Running	ATP200
2	Standby	ATP200

Below the table, there is a 'Cloud Firmware Information' section with a 'Note' and a 'Check Now' button. The 'Auto Update' section is highlighted with a red box, showing the following options:

- Auto Update ⓘ
 - Daily: 2 (Hour)
 - Weekly: Sunday (Day), 0 (Hour)
 - Auto Reboot

At the bottom, the 'Firmware Upgrade Service Status' section shows 'Service Status: Activated'.

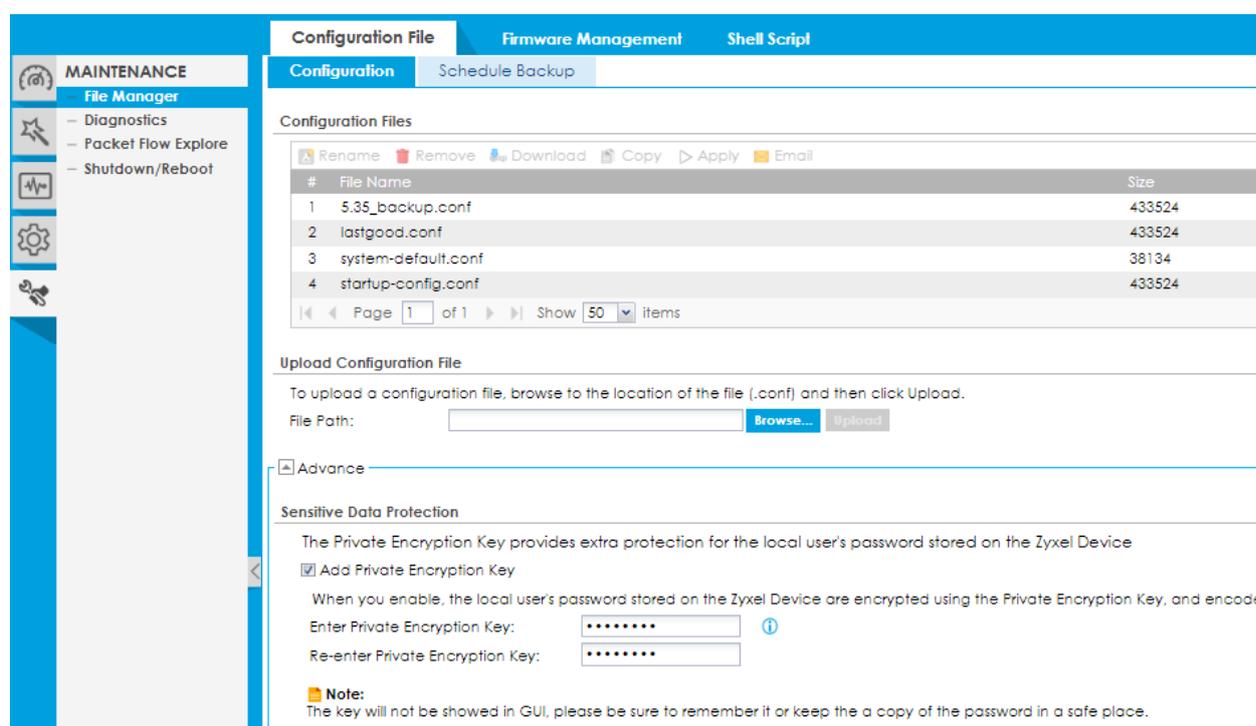
PROTECTION DES DONNÉES SENSIBLES

À partir de la version 5.35 du firmware, les mots de passe peuvent être cryptés avec une clé propre au lieu de l'algorithme par défaut.

Cette fonction protège également contre la lecture des mots de passe des utilisateurs dans les fichiers de configuration à l'aide d'outils de piratage.

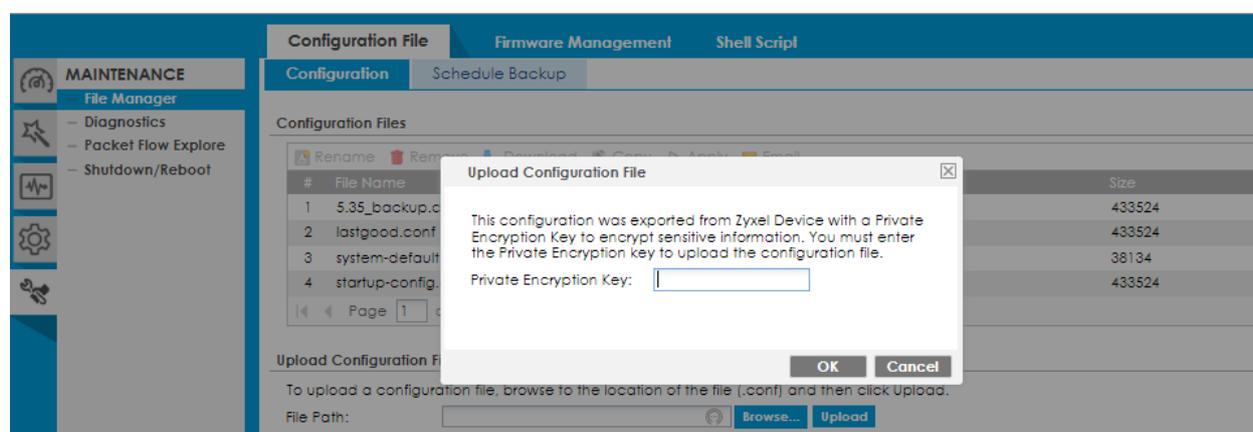
Les autres mots de passe continuent d'utiliser la méthode par défaut.

Maintenance > File Manager > Configuration File > Configuration > Sensitive Data Protection



The screenshot shows the 'Sensitive Data Protection' section in the ZyXEL web interface. The 'Add Private Encryption Key' checkbox is checked. Below it, the text reads: 'When you enable, the local user's password stored on the Zyxel Device are encrypted using the Private Encryption Key, and encode'. There are two input fields for the key, both containing asterisks. A note at the bottom states: 'The key will not be showed in GUI, please be sure to remember it or keep the a copy of the password in a safe place.'

Si le fichier est réimporté sur un pare-feu. Cela n'est possible qu'avec la clé correspondante.



The screenshot shows a dialog box titled 'Upload Configuration File' overlaid on the web interface. The dialog box contains the text: 'This configuration was exported from Zyxel Device with a Private Encryption Key to encrypt sensitive information. You must enter the Private Encryption key to upload the configuration file.' and a 'Private Encryption Key:' input field. There are 'OK' and 'Cancel' buttons at the bottom of the dialog box.