

Prestige 652H/HW

Routeur ADSL sécurisé/LAN sans fil

Guide de prise en main

Version 3.40

Mai 2003



Sommaire

1	Présentation du Prestige	3
2	Matériel	3
2.1	Connexions sur le panneau arrière	4
2.2	Insertion d'une carte de LAN sans fil PCMCIA	5
2.3	Voyants du panneau avant	6
3	Configuration de l'adresse IP de votre ordinateur	7
3.1	Windows 2000/NT/XP.....	8
3.2	Vérification/mise à jour de l'adresse IP de votre ordinateur	9
3.3	Test de la connexion au Prestige	9
4	Configuration de votre Prestige	9
4.1	Accès à votre Prestige via Configurateur Web.....	9
4.2	Boutons courants des commandes d'écrans	11
4.3	Accès Internet à l'aide de l'assistant	11
4.4	Tester votre connexion Internet.....	17
5	Configuration avancée	17
5.1	Configuration du LAN sans fil.....	17
5.2	Configuration de la sécurité LAN sans fil.....	20
5.3	Configuration de l'authentification IEEE 802.1X.....	21
5.4	A propos de la base locale de données utilisateurs et le RADIUS	22
5.5	Aperçu de la traduction d'adresses réseau	24
5.6	Configuration du serveur SUA.....	25
5.7	A propos du Firewall.....	26
5.8	Configuration du Firewall.....	27
5.9	Configuration des adresses d'expéditeur et de destination.....	31
5.10	A propos de VPN.....	32
5.11	Fenêtre sommaire.....	33
5.12	Configuration des règles VPN.....	35
5.13	Visualisation du moniteur SA	40
5.14	perçu de l'UPnP	41
5.15	Configuration de l'UPnP.....	42
6	Dépannage	43

1 Présentation du Prestige

Le routeur ADSL Prestige 652H/HW est le périphérique multifonctions idéal pour la connexion de petits réseaux à Internet via ADSL. Les fonctionnalités clés du Prestige sont les suivantes : firewall, VPN, LAN sans fil, NAT, administration à distance et UPnP. Reportez-vous à votre *Manuel d'utilisation* pour plus de détails sur toutes les fonctionnalités du Prestige.

Vous devez posséder un compte Internet déjà configuré et avoir reçu la plupart des informations suivantes.

INFORMATIONS COMPTE INTERNET	
L'adresse IP du WAN de votre périphérique (si donnée) : _____	
L'adresse IP du serveur DNS (si donnée) : Primaire _____, Secondaire _____	
VPI (Virtual Path Identifier) Identificateur de trajet virtuel : _____	
VCI (Virtual Channel Identifier) Identificateur de voie virtuelle : _____	
Multiplexage (basé sur VC ou LLC) : <input type="checkbox"/> VC <input type="checkbox"/> LLC	
Encapsulation :	
<input type="radio"/> RFC 1483	
<input type="radio"/> ENET ENCAP	Adresse IP de la passerelle de l'encapsulation Ethernet : _____
<input type="radio"/> PPPoA	Nom d'utilisateur : _____ Mot de passe : _____
<input type="radio"/> PPPoE	Nom du service : _____ Nom d'utilisateur : _____ Mot de passe : _____

2 Matériel

2.1 Connexions sur le panneau arrière

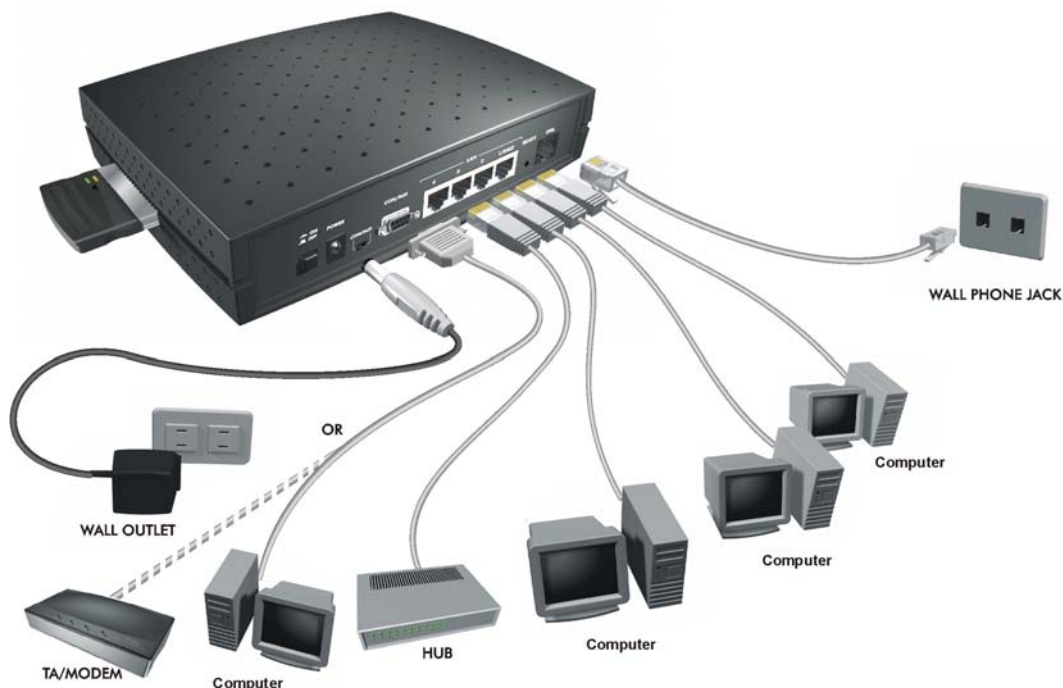


Figure 1 Connexions matérielles du Prestige

Tableau 1 Description du panneau arrière du Prestige

IN ICATION	DESCRIPTION
1. DSL	Connexion à une prise de téléphone à l'aide du câble téléphonique fourni.
2. LAN 1/DMZ-4	Connexion à un ordinateur / un hub externe à l'aide du câble Ethernet. Connexion du port DMZ aux serveurs que vous voulez faire visible de l'extérieur.
3. POWER	Connexion à une source d'alimentation à l'aide du adaptateur secteur approprié (consultez votre <i>manuel d'utilisation</i>).
<p>Une fois les connexions établies, branchez le bloc d'alimentation à la prise et appuyez sur le bouton d'alimentation pour activer le Prestige.</p> <p>Le voyant PWR s'allume. Le voyant SYS clignote pendant les tests système et s'allume en continu si les tests sont réussis. Un voyant LAN s'allume si un port LAN est correctement connecté.</p>	
Interrupteur	Connectez juste ce port si vous souhaitez configurer le Prestige en utilisant le SMT via le

Tableau 1 Description du panneau arrière du Prestige

INDICATION	DESCRIPTION
CON/AUX	<p>port console ou paramétrer une connexion WAN de secours; reportez-vous au <i>Guide d'Utilisateur</i> pour plus de détails.</p> <p>Positionnez cet interrupteur sur "CON" pour utiliser le port CON/AUX comme un port console pour la configuration et la gestion locales du routeur. Connectez un embout du câble console de 9 broches mâle sur le port console du Prestige et l'autre embout sur un port série (COM1, COM2 ou autre port COM) de votre ordinateur. Votre ordinateur doit être équipé d'un logiciel de communication (tel que HyperTerminal) configuré en: émulation de terminal VT100, aucune parité, 8 bits de données, 1 bit d'arrêt, aucun contrôle de flux et vitesse du port de 9600 bps.</p> <p>Positionnez cet interrupteur sur "AUX" pour utiliser le port CON/AUX comme une connexion WAN auxiliaire de secours. Utilisez le convertisseur CON/AUX intégré, avec le câble console pour connecter le port CON/AUX à votre modem ou TA.</p>
RESET	<p>Vous ne devez utiliser ce bouton que si vous avez oublié le mot de passe du Prestige. Il rétablit les paramètres par défaut du Prestige (le mot de passe est 1234, l'adresse IP du LAN 192.168.1.1 etc.; reportez-vous au <i>Manuel d'utilisation</i> pour plus de détails).</p>

2.2 Insertion d'une carte de LAN sans fil PCMCIA

Vous avez besoin d'une carte PCMCIA de LAN sans fil série ZyAIR pour ajouter des fonctionnalités facultatives du LAN sans fil.

1. Eteignez le Prestige.

Ne jamais insérer ou retirer une carte LAN sans fil lorsque le Prestige est en marche.

2. Recherchez l'emplacement portant l'indication **LAN sans fil** sur le Prestige.
3. Avec son connecteur à broches face à l'emplacement et le côté du voyant face vers le haut, glissez la carte du LAN sans fil ZyAIR dans l'emplacement.

Ne jamais forcer, plier ou tordre la carte du LAN sans fil dans l'emplacement.

4. Mettez en marche le Prestige. Le voyant **WLAN** doit s'allumer.

2.3 Voyants du panneau avant



Figure 2 Panneau avant du Prestige

Reportez-vous au tableau suivant pour plus de descriptions détaillées sur les voyants.

Tableau 2 Description des voyants du panneau avant

VOYANT	COULEUR	ÉTAT	DESCRIPTION
PWR	Vert	Allumé	Le Prestige est alimenté.
		Éteint	Le Prestige n'est pas alimenté.
SYS	Vert	Allumé	Le Prestige fonctionne correctement.
		Clignotant	Le Prestige redémarre.
		Éteint	Le système n'est pas prêt ou n'a pas fonctionné correctement.
	Rouge	Allumé	L'alimentation du Prestige est trop basse.
LAN 1/DMZ-4	Vert	Allumé	La connexion Ethernet de 10 Mbps au Prestige fonctionne correctement.
		Clignotant	Le Prestige envoie/reçoit des données.
		Éteint	La connexion Ethernet au Prestige n'atteint pas 10 Mbps.
	Orange	Allumé	La connexion Ethernet de 100 Mbps au Prestige fonctionne correctement.
		Clignotant	Le Prestige envoie/reçoit des données.
		Éteint	La connexion Ethernet au Prestige n'atteint pas 100 Mbps.
WLAN	Vert	Allumé	La liaison sans fil est prête.
		Éteint	La liaison sans fil n'est pas prête ou a échoué.
		Clignotant	Le Prestige envoie/reçoit des données via le WLAN.
	Rouge	Allumé	Il y a un problème avec la carte PCMCIA sans fils

Tableau 2 Description des voyants du panneau avant

VOYANT	COULEUR	ÉTAT	DESCRIPTION
DSL	Vert	Allumé	Le Prestige est parfaitement connecté à un DSLAM.
		Clignotant	Le Prestige initialise la ligne DLS.
		Éteint	La liaison DSL est en panne.
ACT/PPP	Orange	Allumé	Le Prestige est connecter en PPP(PPPOA ou PPPOE)
		Clignotant	Le Prestige envoie/reçoit des données.
		Éteint	Le système est prêt mais n'envoie/ne reçoit pas de données.
	Vert	Clignotant	Le Prestige envoie/reçoit des données.non-PPP
CON/AUX	Verte	Off	Le lien CON/AUX n'est pas prêt,
		On	L'interrupteur CON/AUX est positionné sur CON :mode console.
	Orange	Off	Le lien CON/AUX n'est pas prêt, ou a échoué.
		On	L'interrupteur CON/AUX est positionné sur AUX et le port CON/AUX a une connexion Internet via un modem à numérotation automatique.

3 Configuration de l'adresse IP de votre ordinateur

Ignorez cette section si votre ordinateur est déjà configuré pour accepter une adresse IP dynamique. Ceci est la valeur par défaut pour la plupart des nouveaux ordinateurs.

Le Prestige est déjà configuré pour assigner à votre ordinateur une adresse IP. Utilisez cette section pour configurer votre ordinateur afin de recevoir une adresse IP ou lui assigner une adresse IP fixe dans la plage 192.168.1.2 à 192.168.1.254 avec un masque de sous-réseau de 255.255.255.0. Ceci est nécessaire pour garantir une communication correcte entre votre ordinateur et le Prestige.

Une carte Ethernet et le protocole TCP/IP doivent être installés sur votre ordinateur. TCP/IP doit déjà être installé sur les ordinateurs utilisant Windows NT/2000/XP, Macintosh OS 7 et les systèmes d'exploitation postérieurs.

3.1 Windows 2000/NT/XP

1. Dans Windows XP, cliquez sur **Démarrer, Panneau de configuration**. Dans Windows 2000/NT, cliquez sur **Démarrer, Paramètres, Panneau de configuration**.
2. Dans Windows XP, cliquez sur **Connexions réseau**.
Dans Windows 2000/NT, cliquez sur **Connexions réseau et accès à distance**.
3. Cliquez avec le bouton droit de la souris sur **Connexion au réseau local** puis cliquez sur **Propriétés**.
4. Sélectionnez **Protocole Internet (TCP/IP)** (dans l'onglet **Général** dans Win XP), puis cliquez sur **Propriétés**.

5. L'écran **Propriétés de protocole Internet (TCP/IP)** s'affiche (l'onglet **Général** dans Windows XP).

- Pour assigner à votre ordinateur une adresse IP dynamique, cliquez sur **Obtenir une adresse IP automatiquement**.

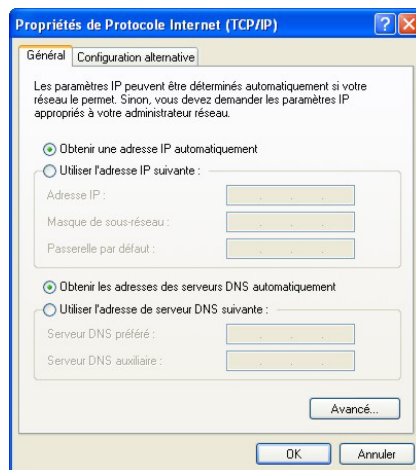
Si vous connaissez les adresse(s) IP du serveur DNS, tapez-les dans les champs **Serveur DNS préféré** et/ou **Serveur DNS auxiliaire**.

- Pour configurer une adresse IP fixe, cliquez sur **Utiliser l'adresse IP suivante** et remplissez les champs **Adresse IP** (choisissez-en une de 192.168.1.2 à 192.168.1.254), **Masque de sous-réseau** (255.255.255.0) et **Passerelle par défaut** (192.168.1.1).

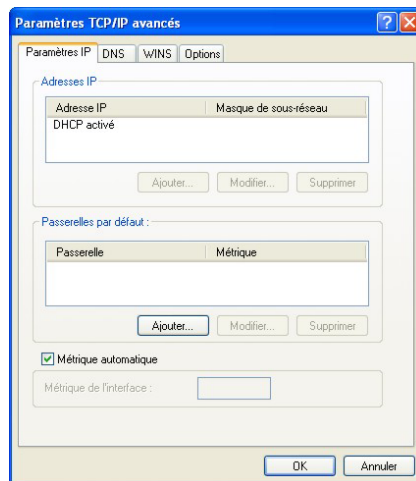
Puis entrez vos adresse(s) IP de serveur(s) DNS dans les champs **Serveur DNS préféré** et/ou **Serveur DNS auxiliaire**.

Si vous disposez de plus de deux serveurs DNS, cliquez sur **Avancé**, l'onglet **DNS** puis configurez-les à l'aide de **Ajouter**.

6. Cliquez sur **Avancé**. Supprimez des passerelles installées auparavant dans l'onglet **Paramètres IP** puis cliquez sur **OK** pour revenir à l'écran **Propriétés de Protocole Internet (TCP/IP)**.



7. Cliquez sur **OK** pour fermer la fenêtre **Propriétés de Protocole Internet (TCP/IP)**.
8. Cliquez sur **OK** pour fermer la fenêtre **Propriétés de Connexion au réseau local**.



3.2 Vérification/mise à jour de l'adresse IP de votre ordinateur

1. Dans l'ordinateur, cliquez sur **Démarrer, (Tous) Programmes, Accessoires** puis **Invite de commandes**.
2. Dans la fenêtre **Invite de commandes**, tapez "ipconfig" puis appuyez sur **ENTRÉE** pour vérifier que l'adresse IP de votre ordinateur soit dans la plage correcte (192.168.1.2 à 192.168.1.254) avec le masque de sous-réseau 255.255.255.0. Ceci est nécessaire à la communication avec le Prestige.

Reportez-vous à votre *Manuel d'utilisation* pour la configuration détaillée des adresses IP dans les autres systèmes d'exploitation des ordinateurs Macintosh et sous Windows.

3.3 Test de la connexion au Prestige

1. Cliquez sur **Démarrer, (Tous) Programmes, Accessoires** puis **Invite de commandes**.
2. Dans la fenêtre **Invite de commandes**, tapez "ping" suivi d'un espace et l'adresse IP du Prestige (192.168.1.1 est la valeur par défaut).
3. Appuyez sur **ENTRÉE** et l'écran suivant s'affiche.

```
C:\>ping 192.168.1.1

Pinging 192.168.1.1 with 32 bytes of data:

Reply from 192.168.1.1: bytes=32 time=10ms TTL=254
Reply from 192.168.1.1: bytes=32 time<10ms TTL=254
Reply from 192.168.1.1: bytes=32 time<10ms TTL=254
Reply from 192.168.1.1: bytes=32 time<10ms TTL=254

Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 10ms, Average = 2ms
```

Votre ordinateur peut désormais communiquer avec le Prestige à l'aide du port LAN.

4 Configuration de votre Prestige

Ce guide de prise en main explique l'utilisation du configurateur Web uniquement. Reportez-vous à votre *manuel d'utilisation* pour plus d'informations d'arrière-plan sur les fonctionnalités du Prestige et la configuration parmi le SMT (System Management Terminal).

4.1 Accès à votre Prestige via Configurateur Web

1. Lancez votre navigateur Web. Entrez "192.168.1.1" comme adresse de site Web.

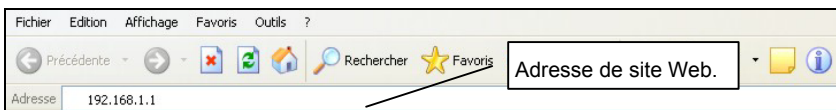


Figure 3 Saisie de l'adresse IP du LAN de Prestige dans Internet Explorer

2. Une fenêtre **Taper un mot de passe réseau** s'affiche. Entrez le nom d'utilisateur ("admin" est la valeur par défaut), mot de passe ("1234" est la valeur par défaut) et cliquez sur **OK**.

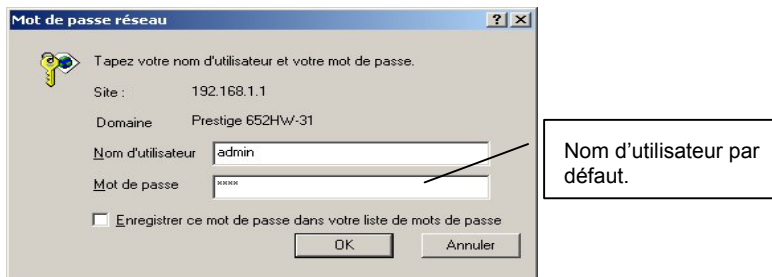


Figure 4 Configurateur Web : Ecran Mot de passe

3. Vous devez maintenant apercevoir l'écran **Plan du site** du configurateur Web.
 - Cliquez sur **Assistant Installation** afin d'afficher une série d'écrans pour une première configuration de votre Prestige.
 - Cliquez sur un lien sous **Configuration avancée** pour configurer les paramètres avancés du Prestige.
 - Cliquez sur un lien sous **Maintenance** pour consulter les statistiques de performance du Prestige, télécharger le microprogramme et sauvegarder, restaurer ou télécharger un fichier de configuration.
 - Cliquez sur **Déconnexion** dans le panneau de navigation après avoir terminé une session d'administration du Prestige.



Figure 5 Configurateur Web : Ecran Plan du site

Le Prestige vous déconnecte automatiquement en cas d'inactivité pendant cinq minutes; appuyez sur ENTRÉE pour vous reconnecter.

4.2 Boutons courants des commandes d'écrans

Le tableau suivant indique les boutons de commandes courants situés sur bon nombre d'écrans du configurateur Web.

Précédent	Cliquez sur Précédent pour retourner à l'écran précédent.
Appliquer	Cliquez sur Appliquer pour enregistrer vos modifications dans le Prestige.
Restaurer/Annuler	Cliquez sur Restaurer ou Annuler pour commencer une nouvelle configuration de cet écran.

4.3 Accès Internet à l'aide de l'assistant

Utilisez les écrans Assistant Installation pour configurer votre système pour les paramètres d'accès Internet et remplir les champs avec les informations du tableau *INFORMATIONS COMPTE INTERNET*.

1. Dans l'écran **Plan du site**, cliquez sur **Assistant Installation** pour afficher le premier écran de l'assistant.

Assistant Installation- Paramètres du fournisseur de services Internet pour l'accès à Internet

Mode Routing ▾

Encapsulation ENET ENCAP ▾

Multiplex LLC ▾

Identification du circuit virtuel

VPI 8

VCI 35

Suivant

Figure 6 Ecran 1 de l'assistant

Dans la zone de liste déroulante **Mode**, sélectionnez **Routing** (par défaut) si votre ISP permet à plusieurs ordinateurs de partager un compte Internet. Sinon, sélectionnez **Bridge**.

Sélectionnez le type d'encapsulation utilisé par votre ISP dans la zone de liste déroulante **Encapsulation**. Les choix varient selon ce que vous sélectionnez dans le champ **Mode**.

Sélectionnez la méthode de multiplexage utilisée par votre ISP dans la zone de liste déroulante **Multiplex**.

Entrez les numéros corrects du VPI (Virtual Path Identifier) et du VCI (Virtual Channel Identifier) fournis par votre ISP dans les champs **VPI** et **VCI**. Il se peut que ces champs soient déjà configurés.

Cliquez sur **Suivant**.

2. Le deuxième écran de l'assistant varie selon le mode et le type d'encapsulation utilisés. Tous les écrans affichés sont en mode routage. Configurez les champs et cliquez sur **Suivant** pour continuer.

Assistant Installation - Paramètres du fournisseur de services Internet pour l'accès à Internet

Nom du service

Nom d'utilisateur

Mot de passe

Adresse IP

Obtenir automatiquement une adresse IP

Adresse IP fixe

Connexion

Connexion sur demande : Délai d'inactivité max. sec.

Reconnexion automatique

NAT (Traduction d'adresses réseau)

Si votre ISP donne le nom de votre fournisseur de services PPPoE, entrez-le dans le champ **Nom du service**.

Entrez le nom d'utilisateur et le mot de passe *exactement* comme ils ont été assignés par votre ISP.

Sélectionnez **Obtenir automatiquement une adresse IP** si vous possédez une adresse IP dynamique; sinon, sélectionnez **Adresse IP fixe** et tapez l'adresse IP assigné par votre ISP dans la zone de texte ci-dessous.

Sélectionnez **Connexion sur demande** lorsque que vous ne voulez pas que la connexion soit permanente et spécifiez un délai d'inactivité (en secondes) dans le champ **Délai d'inactivité max.**

Figure 7 Connexion Internet avec PPPoE

Sélectionnez **Reconnexion automatique** lorsque vous voulez que votre connexion soit permanente. Le Prestige essaiera de rétablir automatiquement la connexion en cas de déconnexion.

Dans la zone de liste déroulante **NAT (Traduction d'adresses réseau)**, sélectionnez **Uniquement SUA**, **Tout** ou **Sans**. Reportez-vous à la section *Traduction d'adresses réseau* pour plus d'informations.

Assistant Installation - Paramètres du fournisseur de services Internet pour l'accès à Internet

Adresse IP

NAT (Traduction d'adresses réseau)

Entrez l'adresse IP fournie par votre ISP dans le champ **Adresse IP**.

Le champ Adresse IP n'est pas disponible pour le mode pont.

Reportez-vous à la *figure 7* pour une description du champ **NAT(Traduction d'adresses réseau)**.

Figure 8 Connexion Internet avec RFC 1483

Assistant Installation- Paramètres du fournisseur de services Internet pour l'accès à Internet

Adresse IP

Obtenir automatiquement une adresse IP
 Adresse IP fixe

Adresse IP
 Masque de sous-réseau
 Passerelle ENET ENCAP

NAT (Traduction d'adresses réseau)

Uniquement SUA ▼

Précédent Suivant

Dans le champ **Passerelle ENET ENCAP**, entrez l'adresse IP de la passerelle fournie par votre ISP.

Reportez-vous à la *figure 7* pour d'autres descriptions de champs.

Figure 9 Connexion Internet avec ENET ENCAP

Assistant Installation- Paramètres du fournisseur de services Internet pour l'accès à Internet

Nom d'utilisateur

Mot de passe

Adresse IP

Obtenir automatiquement une adresse IP
 Adresse IP fixe

Connexion

Connexion sur demande : Délai d'inactivité max. sec.
 Reconnexion automatique

NAT (Traduction d'adresses réseau)

Uniquement SUA ▼

Précédent Suivant

Reportez-vous à la *figure 7* pour les descriptions de champs.

Les champs Adresse IP et NAT (Traduction d'adresses réseau) ne sont pas disponibles pour le mode Bridge.

Figure 10 Connexion Internet avec PPPoA

3. Vérifiez les paramètres dans l'écran affiché ensuite. Pour changer les informations du LAN sur le Prestige, cliquez sur **Modifier la configuration LAN**. Sinon, cliquez sur **Enregistrer les paramètres** pour enregistrer la configuration et passez à l'étape 5.

Assistant Installation- Paramètres du fournisseur de services Internet pour l'accès à Internet

Informations WAN
Mode: **Routing**
Encapsulation: **ENET ENCAP**
Multiplexage: **LLC**
VPI/VCI: **8/35**
Adresse IP: **Obtenir automatiquement une adresse IP**
NAT (Traduction d'adresses réseau): **Uniquement SUA**

Informations LAN
Adresse IP: **192.168.1.1**
Masque IP: **255.255.255.0**
DHCP: **Activé**
Adresse IP de début client: **192.168.1.33**
Taille du groupe d'adresses IP client: **32**

Modifier la configuration LAN

Enregistrer les paramètres

Figure 11 Ecran 3 de l'assistant

4. Si vous voulez changer les paramètres LAN de votre Prestige, cliquez sur **Modifier la configuration LAN** pour afficher l'écran tel qu'il apparaît ensuite.

Assistant Installation- Paramètres du fournisseur de services Internet pour l'accès à Internet

Adresse IP LAN	<input type="text" value="192.168.1.1"/>
Masque de sous-réseau LAN	<input type="text" value="255.255.255.0"/>
DHCP	
Serveur DHCP	<input type="text" value="Activé"/>
Début du groupe d'adresses IP	<input type="text" value="192.168.1.33"/>
Taille du groupe d'adresses IP client	<input type="text" value="32"/>
Serveur DNS primaire	<input type="text" value="0.0.0.0"/>
Serveur DNS secondaire	<input type="text" value="0.0.0.0"/>

Entrez l'adresse IP de votre Prestige en notation décimale séparée par des points dans le champ **Adresse IP LAN**. Par exemple, 192.168.1.1 (paramètres par défaut).

Si vous changez l'adresse IP LAN du Prestige, vous devez utiliser la nouvelle adresse IP si vous voulez accéder de nouveau au configurateur Web.

Figure 12 Assistant : Configuration LAN

Entrez un masque de sous-réseau en notation décimale séparée par des points dans le champ **Masque de sous-réseau LAN**.

Dans la zone de liste déroulante **Serveur DHCP**, sélectionnez **Activé** pour permettre à votre Prestige d'assigner des adresses IP, une passerelle par défaut IP et des serveurs DNS aux systèmes informatiques qui prennent en charge le client DHCP. Sélectionnez **Désactivé** pour désactiver le serveur DHCP.

Lors de l'utilisation du serveur DHCP, définissez les éléments suivants :

Spécifiez la première des adresses contiguës du groupe d'adresses IP dans le champ **Début du groupe d'adresse IP**.

Spécifiez la taille ou le décompte du groupe d'adresses IP dans le champ **Taille du groupe d'adresses IP client**.

Entrez les adresse(s) IP des serveur(s) DNS dans les champs **Serveur DNS primaire** et/ou **Serveur DNS secondaire**.

5. Le Prestige teste automatiquement la connexion aux ordinateur(s) connectés aux ports LAN. Pour tester la connexion entre le Prestige et l'ISP, cliquez sur **Démarrer le diagnostic**. Sinon, cliquez sur **Revenir au Menu principal** pour retourner à l'écran **Plan du site**.

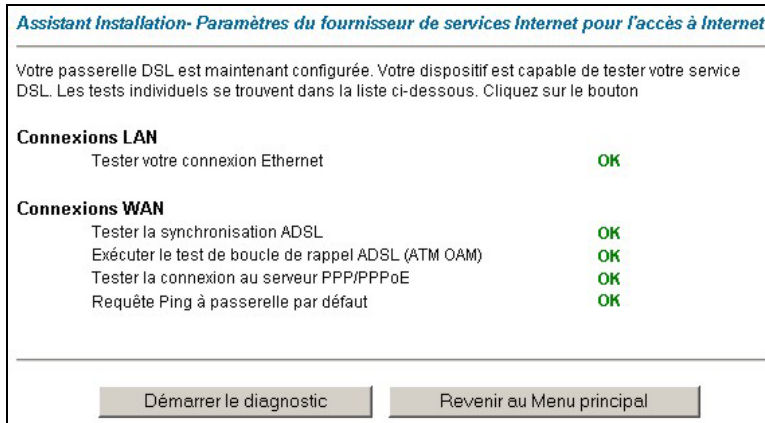


Figure 13 Ecran 4 de l'assistant

4.4 Tester votre connexion Internet

Lancez votre navigateur Web et allez à www.zyxel.com. L'accès Internet ne représente que le début. Reportez-vous au *Manuel d'utilisation* pour de plus amples informations sur la gamme complète des fonctionnalités du Prestige. Si vous ne pouvez pas accéder à Internet, ouvrez à nouveau le configurateur pour confirmer que les paramètres Internet configurés dans l'Assistant Installation sont corrects.

5 Configuration avancée

Cette section décrit la configuration de certains paramètres avancés du Prestige.

5.1 Configuration du LAN sans fil

Un LAN sans fil (WLAN) offre un système flexible de communications de données que vous pouvez utiliser pour accéder à différents services (Internet, E-mail, services de l'imprimante, etc.) sur le réseau câblé sans infrastructure supplémentaire de câblage réseau onéreuse. En effet, un environnement de LAN sans fil vous permet de rester connecté au réseau câblé tout en vous déplaçant dans la zone desservie.

L'écran WLAN est disponible seulement si une carte WLAN est installée.

Pour configurer des paramètres sans fil, cliquez sur **Configuration avancée**, **LAN sans fil** puis cliquez sur la liaison **Sans fil**.

Figure 14 LAN sans fil : Sans fil

Le tableau suivant décrit les champs dans cet écran.

Tableau 3 LAN sans fil : Sans fil

INDICATION	DESCRIPTION
ESSID	(Extended Service Set IDentity) L'ESSID est un nom unique pour identifier le Prestige dans le LAN sans fil. Tous les clients sans fil s'associant à un point d'accès (le Prestige) doivent posséder le même ESSID. Entrez un nom descriptif (jusqu'à 32 caractères ASCII 7 bits imprimables).
ESSID caché	Sélectionnez Oui pour masquer l'ESSID afin qu'un client sans fil ne puisse pas obtenir l'ESSID grâce à une recherche passive. Sélectionnez Non pour afficher l'ESSID afin qu'un client sans fil puisse obtenir l'ESSID grâce à une recherche passive.

Tableau 3 LAN sans fil : Sans fil

INDICATION	DESCRIPTION
Canal ID	<p>La plage de fréquences radio utilisée par les appareils sans fil IEEE 802.11b est appelée un canal. Définissez la fréquence/le canal de fonctionnement selon votre région spécifique.</p> <p>Sélectionnez un canal dans la zone de liste déroulante. Les PA (points d'accès) adjacents, avec des zones desservies chevauchantes, doivent utiliser des canaux différents pour réduire la diaphonie. Ceci se produit lorsque les signaux radio d'autres points d'accès chevauchent et interfèrent avec un autre facteur susceptible d'affecter la performance.</p>
Seuil RTS/CTS	<p>Sélectionnez cette option pour permettre au seuil RTS (Request To Send) Demande d'émission/CTS (Clear To Send) Prêt à émettre de réduire les collisions. Entrez une valeur entre 0 et 2432. La valeur par défaut est 2432.</p> <p>La demande d'émission est le seuil (nombre d'octets) pour permettre l'établissement de liaison RTS/CTS. Les données avec une taille de trame supérieure à cette valeur effectuent l'établissement de liaison RTS/CTS. La définition de cet attribut pour qu'il soit supérieur à la taille maximum de MSDU (MAC Service Data Unit) désactive l'établissement de liaison RTS/CTS.</p>
Seuil de fragmentation	<p>Le seuil de fragmentation est la taille du fragment de données maximum pouvant être envoyée.</p>
Encryptage WEP	<p>WEP (Wired Equivalent Privacy) crypte les trames de données avant de les transmettre sur le réseau sans fil.</p> <p>Sélectionner Désactiver permet la communication entre tous les ordinateurs sans fil et les points d'accès sans cryptage de données.</p> <p>Sélectionnez WEP 64 bits ou WEP 128 bits puis configurez les clés dans les champs fournis pour activer le cryptage des données.</p>
Clé 1 à clé 4	<p>Les clés WEP sont utilisées pour crypter les données. Le Prestige et les clients sans fil doivent utiliser la même clé WEP pour la transmission des données.</p> <p>Si vous choisissez WEP 64 bits, entrez 5 caractères (chaîne ASCII) ou 10 caractères hexadécimaux ("0-9", "A-F").</p> <p>Si vous choisissez WEP 128 bits, entrez 13 caractères (chaîne ASCII) ou 26 caractères hexadécimaux ("0-9", "A-F").</p> <p>Ne sélectionnez qu'une clé à activer n'importe quand.</p>

Les clients sans fil et le Prestige doivent utiliser le même ESSID, la même identification de canal et clé de cryptage WEP (si WEP est activé) pour une communication sans fil.

5.2 Configuration de la sécurité LAN sans fil

Pour une sécurité supplémentaire, configurez votre Prestige de sorte à vérifier l'adresse MAC de l'appareil du client sans fil avec une liste d'adresses MAC autorisées ou refusées.

Pour configurer la liste des adresses MAC pour le LAN sans fil, cliquez sur **Configuration avancée** dans le panneau de navigation, **Sans fil** puis cliquez sur la liaison **Filtre MAC**.

LAN sans fil- Filtre MAC

Activer

Action

Adresse MAC	
<input type="text" value="00:00:00:00:00:00"/>	<input type="text" value="00:00:00:00:00:00"/>
<input type="text" value="00:00:00:00:00:00"/>	<input type="text" value="00:00:00:00:00:00"/>
<input type="text" value="00:00:00:00:00:00"/>	<input type="text" value="00:00:00:00:00:00"/>
<input type="text" value="00:00:00:00:00:00"/>	<input type="text" value="00:00:00:00:00:00"/>
<input type="text" value="00:00:00:00:00:00"/>	<input type="text" value="00:00:00:00:00:00"/>
<input type="text" value="00:00:00:00:00:00"/>	<input type="text" value="00:00:00:00:00:00"/>
<input type="text" value="00:00:00:00:00:00"/>	<input type="text" value="00:00:00:00:00:00"/>
<input type="text" value="00:00:00:00:00:00"/>	<input type="text" value="00:00:00:00:00:00"/>
<input type="text" value="00:00:00:00:00:00"/>	<input type="text" value="00:00:00:00:00:00"/>
<input type="text" value="00:00:00:00:00:00"/>	<input type="text" value="00:00:00:00:00:00"/>
<input type="text" value="00:00:00:00:00:00"/>	<input type="text" value="00:00:00:00:00:00"/>
<input type="text" value="00:00:00:00:00:00"/>	<input type="text" value="00:00:00:00:00:00"/>
<input type="text" value="00:00:00:00:00:00"/>	<input type="text" value="00:00:00:00:00:00"/>
<input type="text" value="00:00:00:00:00:00"/>	<input type="text" value="00:00:00:00:00:00"/>
<input type="text" value="00:00:00:00:00:00"/>	<input type="text" value="00:00:00:00:00:00"/>
<input type="text" value="00:00:00:00:00:00"/>	<input type="text" value="00:00:00:00:00:00"/>

Figure 15 LAN sans fil : Filtre Adresse MAC

Le tableau suivant décrit les champs dans cet écran.

Tableau 4 LAN sans fil : Filtre d'adresses MAC

CHAMP	DESCRIPTION
Activer	Sélectionnez Oui dans la zone de liste déroulante pour permettre le filtrage des adresses MAC.
Action	Définissez l'action du filtre pour la liste des adresses MAC dans le tableau Adresse MAC . Sélectionnez Refuser l'association pour bloquer l'accès au routeur ; les adresses MAC non listées auront l'accès autorisé au routeur. Sélectionnez Autoriser l'association pour permettre l'accès au routeur ; les adresses MAC non listées auront l'accès refusé au routeur.
Adresse MAC	Entrez la liste des adresses MAC dans ce tableau.

5.3 Configuration de l'authentification IEEE 802.1X

Vous pouvez paramétrer le Prestige et votre réseau pour identifier un client sans fil avant que le client sans fil puisse communiquer avec le Prestige et le réseau câblé auquel le Prestige est connecté. Votre Prestige supporte le standard IEEE 802.1x qui fonctionne avec IEEE 802.11 pour améliorer l'authentification d'utilisateur.

Pour changer les paramètres de l'authentification de votre Prestige, cliquez sur

LAN sans fil → 802.1x , La fenêtre s'ouvre, comme indiqué.

Figure 16 Authentification 802.1X du LAN sans fil

Le tableau suivant décrit les champs de cette fenêtre.

Tableau 5 Authentification 802.1X du LAN sans fil

ETIQUETTE	DESCRIPTION
Activer	<p>Sélectionnez Authentification requise, acces non autorisé, aucune Authentification requise à partir de la zone de liste déroulante.</p> <p>Sélectionnez Authentification requise pour identifier tous les clients sans fil avant qu'il puisse accéder au réseau câblé.</p> <p>Sélectionnez ,aucune Authentification requise pour permettre à tous les clients sans fil d'accéder à votre réseau sans fil sans authentification.</p> <p>Sélectionnez accès non autorisé pour interdire tous les clients sans fil d'accéder à votre réseau câblé.</p>
Période de ré-authentification	<p>Précisez l'intervalle de temps entre lequel l'authentification du serveur RADIUS vérifie les utilisateurs sans fil connectés au réseau.</p> <p>Ce champ est activé seulement si vous sélectionnez le contrôle d'authentification en Auto.</p>
Bases de données d'authentification	<p>Ce champ n'est activé que lorsque vous sélectionnez Authentification requise dans le champ Contrôle de port sans fil.</p> <p>Sélectionnez Base de données des utilisateurs locale uniquement pour que le Prestige vérifie juste la base de données des utilisateurs intégrée au Prestige pour le nom d'utilisateur et le mot de passe d'un client.</p> <p>Sélectionnez Uniquement RADIUS pour que le Prestige vérifie juste la base de données des utilisateurs sur le serveur RADIUS spécifié.</p> <p>Sélectionnez BD locale d'abord puis RADIUS pour que le Prestige vérifie d'abord la base de données des utilisateurs du Prestige pour le nom d'utilisateur et le mot de passe d'un client. Si aucune correspondance n'est trouvée, la base de données des utilisateurs sur le serveur RADIUS spécifié est alors vérifiée.</p> <p>Sélectionnez RADIUS d'abord puis BD locale pour que le Prestige vérifie d'abord la base de données des utilisateurs sur le serveur RADIUS spécifié pour le nom d'utilisateur et le mot de passe d'un client. Si aucune correspondance n'est trouvée, la base de données des utilisateurs sur le Prestige est alors vérifiée.</p>

5.4 A propos de la base locale de données utilisateurs et le RADIUS

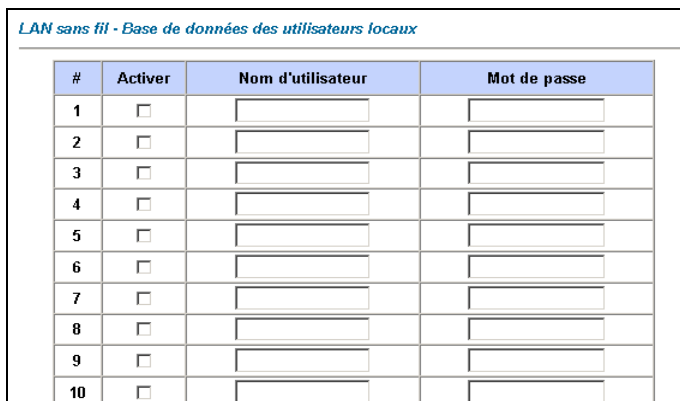
Le EAP est un protocole d'authentification destiné d'origine à parcourir la trame PPP (Point-to-Point Protocol) afin de supporter les multiples types de l'authentification d'utilisateur. Le RADIUS est basé sur un modèle client-seveur qui supporte l'authentification, l'autorisation et la répartition. Le point d'accès (Prestige) est le client et le serveur RADIUS. Le RADIUS est un simple échange

de paquets sur lequel votre Prestige agit comme des messages différés entre le client sans fil et le serveur RADIUS du réseau. Afin d'assurer la sécurité du réseau, le point d'accès et le serveur RADIUS utilisent une clé secrète partagée, laquelle est un mot de passe, que tous les deux connaissent. La clé n'est pas envoyée via le réseau. En plus de la clé partagée, l'information échangée du mot de passe est aussi cryptée pour protéger le réseau de l'accès non autorisé. En utilisant le EAP pour interagir avec un serveur RADIUS compatible EAP, le point d'accès aide un client sans fil et un serveur RADIUS de réaliser l'authentification mutuelle.

Pour identifier les utilisateurs sans fil sans interaction sur un serveur RADIUS du réseau, vous pouvez stocker localement les profiles des utilisateurs.

Le Prestige vérifie premièrement la base locale de données utilisateurs, puis il utilise la base de données utilisateurs sur le serveur RADIUS pour identifier les clients sans fil. Pour changer la liste locale des utilisateurs de votre Prestige, cliquez sur **LAN SANS FIL**, puis sur l'onglet **Utilisateur local de la base de données**.

Si vous activez l'authentification EAP, vous devez préciser la base locale de données utilisateurs ou le serveur externe pour l'authentification de l'utilisateur distant. Pour paramétrer la base locale de données utilisateurs de votre Prestige, cliquez sur **LAN sans fil → Base de données des utilisateurs locaux**.



#	Activer	Nom d'utilisateur	Mot de passe
1	<input type="checkbox"/>		
2	<input type="checkbox"/>		
3	<input type="checkbox"/>		
4	<input type="checkbox"/>		
5	<input type="checkbox"/>		
6	<input type="checkbox"/>		
7	<input type="checkbox"/>		
8	<input type="checkbox"/>		
9	<input type="checkbox"/>		
10	<input type="checkbox"/>		

Figure 17 Base de données des utilisateurs locaux

Pour paramétrer le serveur RADIUS de votre Prestige, cliquez sur **LAN sans fil → RADIUS**

LAN sans fil - RADIUS

Serveur d'authentification

Activer

Adresse du serveur IP

Numéro du port

Code secret partagé

Serveur de gestion de comptes

Activer

Adresse du serveur IP

Numéro du port

Code secret partagé

Figure 18 RADIUS

5.5 Aperçu de la traduction d'adresses réseau

NAT (Network Address Translation - NAT, RFC 1631) est la traduction de l'adresse IP d'un hôte dans un paquet. Par exemple, l'adresse source d'un paquet sortant, utilisée à l'intérieur d'un seul réseau, devient une adresse IP différente connue dans un autre réseau.

Si vous possédez une seule adresse IP publique, sélectionnez **Uniquement SUA** dans l'écran **NAT-Mode** (voir *Figure 16*). Si vous disposez de plusieurs adresses IP publiques, vous pouvez utiliser tous les types de mises en correspondance (reportez-vous au *manuel d'utilisateur* pour plus de détails).

NAT prend en charge cinq types de mises en correspondance IP/port. Ce sont :

1. **Une adresse sur une** : Le mode Une adresse sur une permet de faire correspondre une adresse IP locale avec une adresse IP globale. Notez que les numéros de ports ne changent pas pour un type de mise en correspondance NAT Une adresse sur une.
2. **Plusieurs adresses sur une** : Le mode Plusieurs adresses sur une permet de faire correspondre plusieurs adresses IP locales avec une adresse IP globale.
3. **Plusieurs adresses sur plusieurs partagées** : Le mode Plusieurs adresses sur plusieurs partagées permet de faire correspondre plusieurs adresses IP locales avec des adresses IP globales partagées.
4. **Plusieurs adresses sur plusieurs univoques** : Le mode Plusieurs adresses sur plusieurs univoques permet de faire correspondre une adresse IP locale avec des adresses IP globales uniques.

5. **Serveur** : Ce type vous permet de spécifier des serveurs intérieurs de différents services derrière le NAT accessibles au monde extérieur.

5.6 Configuration du serveur SUA

Une table de correspondance du serveur SUA est une liste des serveurs (derrière NAT sur le LAN) intérieurs, par exemple, Web ou FTP, que vous pouvez montrer au monde extérieur même si SUA fait apparaître l'ensemble de votre réseau intérieur comme un ordinateur unique au monde extérieur.

1. Dans le menu principal, cliquez sur **Configuration avancée** puis sur **NAT** pour afficher l'écran **NAT - Mode**. Sélectionnez **Uniquement SUA**.



NAT - Mode

Traduction d'adresses réseau (NAT)

Sans

Uniquement SUA [Modifier les détails](#)

Tout [Modifier les détails](#)

Appliquer

Figure 19 NAT: Mode

2. Cliquez sur Modifier les détails.

NAT - Modifier table de correspondance du serveur SUA/NAT

	N° de port de début	N° de port de fin	Adresse IP
1	Tous les ports	Tous les ports	0.0.0.0
2	0	0	0.0.0.0
3	0	0	0.0.0.0
4	0	0	0.0.0.0
5	0	0	0.0.0.0
6	0	0	0.0.0.0
7	0	0	0.0.0.0
8	0	0	0.0.0.0
9	0	0	0.0.0.0
10	0	0	0.0.0.0
11	0	0	0.0.0.0
12	0	0	0.0.0.0

Enregistrer Annuler

Figure 20 Serveur SUA/NAT

Le tableau suivant décrit les champs dans cet écran.

Tableau 6 Serveur SUA/NAT

INDICATION	DESCRIPTION
N° de port de début	Tapez un numéro de port dans ce champ. Pour router uniquement un port, tapez à nouveau le numéro du port dans le champ Port de fin . Pour router une série de ports, tapez le numéro du port de début ici et le numéro de port de fin dans le champ Port de fin .
N° de port de fin	Tapez un numéro de port dans ce champ. Pour router uniquement un port, tapez le numéro du port dans le champ Port de début ci-dessus puis tapez-le à nouveau dans ce champ. Pour router une série de ports, tapez le numéro du dernier port dans une série qui commence par le numéro de port dans le champ Port de début .
Adresse IP	Entrez l'adresse IP du serveur intérieur ici.

5.7 A propos du Firewall

Le firewall du Prestige est un firewall stateful inspection et il est destiné pour protéger contre les attaques DoS (Denial of Service) lorsqu'il est activé. Le but de Prestige est de permettre à un LAN (Local Area Network) privé de rester en sécurité pendant les connexions à l'Internet. Le Prestige peut être utilisé pour empêcher le vol, la destruction et la modification des données, aussi bien le

journal d'événements qui peut être important pour la sécurité de votre réseau. Le Prestige a aussi la fonction du filtrage de paquets.

Une fois activé, le firewall autorise tout le trafic vers l'Internet qui provient du LAN, et bloque tout le trafic vers le LAN qui provient de l'Internet. Autrement dit, le Prestige:

Permettra toutes les sessions en provenance du LAN vers le WAN
Bloquera toutes les sessions en provenance du WAN vers le LAN

Les règles **LAN-to-WAN** sont les règles du firewall de réseau local vers l'Internet. Par défaut, c'est de faire suivre tout le trafic de votre réseau local vers l'Internet.

La figure suivante illustre une application de firewall du Prestige.

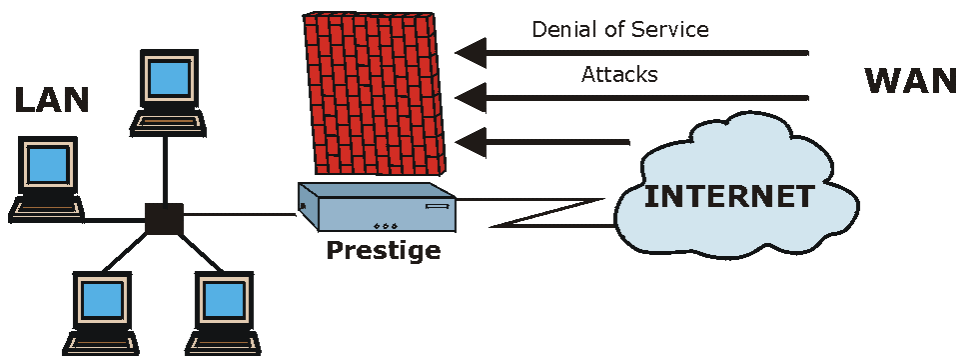


Figure 21 Application de firewall du Prestige

5.8 Configuration du Firewall

Cliquez sur **AVANCE** et puis sur **FIREWALL** pour ouvrir la fenêtre **Config**. Validez (ou activez) le firewall en cochant la case **Activer le Firewall** comme indiqué dans la fenêtre suivante.

Coupe-feu - Configuration - Config

Coupe-feu activé

Le coupe-feu protège contre les attaques DoS (Denial of Service) lorsqu'il est activé. Les tables de polices par défaut

1. autorisent toutes les sessions depuis le réseau local vers Internet et
2. refusent toutes les sessions depuis Internet vers le réseau local

Vous pouvez définir des règles de polices supplémentaires ou modifier des règles existantes ; effectuez l'opération avec précaution.

1. Table de règles LAN-Internet
2. Table de règles Internet-LAN

ATTENTION : Si l'option "Coupe-feu activé" n'est pas cochée, toutes les polices de sécurité du coupe-feu existant et les fonctions du coupe-feu seront désactivées.

Figure 20 Activer le Firewall

De Menu Principale cliquez sur **Configuration avancée** puis **Firewall** et pour ouvrir la fenêtre **Sommaire des règles** pour LAN vers WAN ou WAN vers LAN vous aurez la fenêtre suivante.

Coupe-feu - LAN vers WAN- Sommaire des règles

L'action par défaut pour les paquets ne correspondant pas aux règles suivantes:

Journal d'autorisation par défaut

No.	IP source	IP de destination	Service	Action	Journal
1					
2					
3					
4					
5					
6					
7					
8					
9					
10					

Réorganiser les règles: Déplacer le numéro de la règle vers le numéro

Tableau 7 Écran Récapitulatif

ETIQUETTE	DESCRIPTION
L'action par défaut pour les paquets ne correspondent pas aux règles	Utilisez les options pour sélectionner si Bloquer (supprimer) ou Autoriser (permettre le passage de) les paquets qui se déplacent dans la direction sélectionnée
Journal d'autorisation par défaut	Cochez cette case pour créer un log (quand l'action citée ci-dessus est engagée) des paquets qui se déplacent dans la direction sélectionnée et ne correspondent à aucune des règles citées au-dessous.
Les champs suivants en lecture seule résumant les règles que vous avez créé pour appliquer au trafic circulant dans la direction sélectionnée des paquets. Les règles de firewall que vous configurez (résumées ci-dessous) prennent la priorité sur les configurations des actions générales de firewall citées ci-dessus.	
No.	C'est le numéro de règle de votre firewall. Le classement de vos règles est important car les règles sont appliquées à tour de rôle. Le champ Déplacer ci-dessous vous permet de rénuméroter vos règles.
Adresse de source	Cette zone de liste déroulante affiche les adresses sources ou les plages des adresses auxquelles cette règle de firewall s'applique. Veuillez noter qu'un champ vide de l'adresse source ou de destination est équivalent à Any .
Adresse de destination	Cette zone de liste déroulante affiche les adresses de destination ou les plages des adresses auxquelles cette règle de firewall s'applique. Veuillez noter qu'un champ vide de l'adresse source ou de destination est équivalent à Any .
Type de service	Cette zone de liste déroulante affiche les services auxquels cette règle de firewall s'applique. Veuillez noter qu'un champ vide du type de services est équivalent à Any .
Action	C'est l'action spécifiée pour cette règle-là, soit Bloquer , soit Autoriser . Notez que Bloquer signifie que le firewall supprime discrètement le paquet.
Journal	Ce champ vous affiche si un journal est créé pour les paquets qui correspondent à la règle (Match), ne correspondent pas à la règle (Not Match), tous les deux (Both) ou aucun journal n'est créé (None).
Réorganiser les règles	Sélectionnez le numéro de règle de votre firewall pour lequel vous voulez établir un classement. Cliquez sur Déplacer pour déplacer la règle vers le numéro que vous avez tapé. Le classement de vos règles est important car elles sont appliquées par ordre de leur numérotation.
vers le numéro	Choisissez le nombre que vous voulez déplacer la règle à.
Déplacer	Le déplacement de la règle

Suivez ces instructions pour créer une nouvelle règle.

1. Dans l'écran récapitulatif, cliquez sur un numéro, L'écran d'édition règle s'ouvre.
2. Dans la zone de texte **Services disponibles**, sélectionnez les services que vous voulez. Configurez les ports personnalisés pour les services non prédéfinis par le Prestige en

cliquant sur les boutons **Ajouter** ou **Editer** au-dessous de **Port personnalisé**. Pour une liste complète des numéros de ports et de services, visitez le site web de l'IANA (Internet Assigned Number Authority)..

3. Configurez **Adresse de source** et **Adresse de destination** pour la règle

Figure 21 Création/Édition d'une règle de firewall

Le tableau suivant décrit les champs de cette fenêtre.

Tableau 8 Création/Édition d'une règle de firewall

ETIQUETTE	DESCRIPTION
Adresse de source	Cliquez sur Ajouter source pour ajouter une nouvelle adresse, sur Editer source pour éditer une adresse existante ou sur Supprimer source pour supprimer une adresse. Reportez-vous au chapitre suivant pour plus d'informations sur l'ajout et l'édition des adresses sources..

Tableau 8 Création/Édition d'une règle de firewall

ETIQUETTE	DESCRIPTION
Adresse de destination	Cliquez sur Ajouter dest pour ajouter une nouvelle adresse, sur Editer dest pour éditer une adresse existante ou sur Supprimer dest pour supprimer une adresse. Reportez-vous au chapitre suivant pour l'ajout et l'édition des adresses de destination.
Services Services disponibles/sélectionnés	Mettez en surbrillance un service dans la liste Services disponibles à gauche, puis cliquez sur >> pour l'ajouter à la liste de Services sélectionnés à droite. Pour déplacer un service, mettez le en surbrillance dans la liste Services sélectionnés à droite, puis cliquez sur <<.
Modifier le service disponible	Cliquez sur ce bouton pour actualiser cette fenêtre que vous utilisez pour configurer un nouveau service personnalisé qui ne se situe pas dans la liste de services prédéfinis.
Action pour les paquets correspondants	Que les paquets qui correspondent à cette règle soient bloqués ou autorisés? Faites votre choix dans la zone de liste déroulante. Notez que Block signifie que le firewall supprime discrètement le paquet.
Log	Cochez cette case pour les paquets qui correspondent à cette règle.
Alerte	Cochez la case Alerte pour déterminer que cette règle-là génère une alerte lorsque la règle est adaptée.
Supprimer	Sélectionnez un service personnalisé (indiqué par une “*”) dans la liste Services disponibles et cliquez sur ce bouton pour déplacer le service.

5.9 Configuration des adresses d'expéditeur et de destination

Pour ajouter une nouvelle adresse d'expéditeur ou de destination, cliquez sur **Ajouter source** ou **Ajouter dest** dans l'écran suivant. Pour éditer une adresse existante d'expéditeur ou de destination, sélectionnez-en dans la case et cliquez sur **Editer source** ou **Editer dest** dans l'écran suivant. L'une ou l'autre action affiche la fenêtre suivante.

Coupe-feu - LAN vers WAN- Config IP de la règle

Type d'adresse:

Adresse IP de début:

Adresse IP de fin:

Masque de sous-réseau:

Figure 22 Ajouter/Editer les adresses d'expéditeur et de destination

Le tableau suivant décrit les champs de cette fenêtre.

Tableau 9 Ajouter/Editer les adresses d'expéditeur et de destination

ETIQUETTE	DESCRIPTION
Type d'adresse	Voulez-vous que votre règle soit appliqué aux paquets avec une adresse IP particulière (unique), une plage des adresses IP (par ex., de 192.168.1.10 à 192.169.1.50), un sous-réseau ou aucune adresse IP? Sélectionnez une option dans la zone de liste déroulante.
Adresse IP du début	Entrez ici l'adresse IP unique ou l'adresse IP de début dans une plage.
Adresse IP de la fin	Entrez ici l'adresse de fin dans une plage.
Masque de sous-réseau	Entrez ici le masque de sous-réseau, si applicable.

5.10 A propos de VPN

Un VPN (Virtual Private Network) fournit des communications sécurisées entre les sites sans les frais pour les lignes spécialisées site-à-site. Un VPN sécurisé est une combinaison de tunnel, de cryptage, d'authentification, d'accès contrôlé et de technologies/services de vérification, utilisée pour l'acheminement du trafic sur Internet ou sur n'importe quel autre réseau manquant de sécurité qui utilisent l'ensemble de protocoles TCP/IP pour la communication.

La figure suivante fournit un exemple d'une application de VPN.

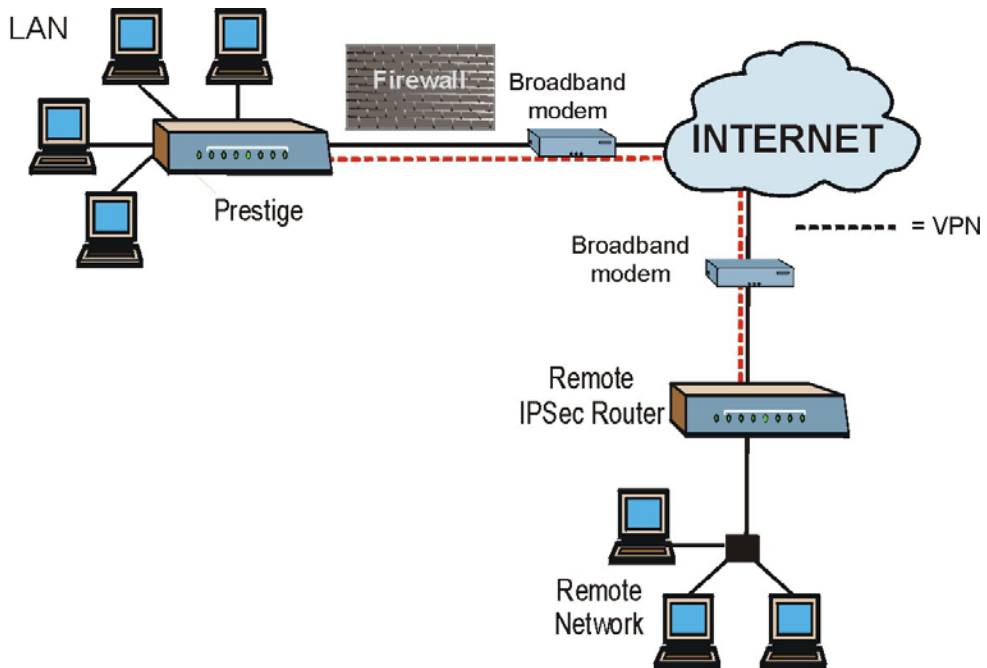


Figure 23 Application de VPN

5.11 Fenêtre sommaire

Les adresses IP locales et distantes doivent être statiques.

Cliquez sur **Configuration AVANCE** → **VPN** → **Configuration** pour ouvrir la fenêtre **Sommaire**. C'est un menu en lecture seule de vos règles IPSec (tunnels).

Editez ou créez une règle IPSec en cliquant sur le numéro de règle pour configurer les sous-menus associés

VPN - Sommaire

No.	Nom	Activer	Adresse locale	Adresse du nœud distant	Encap.	Algorithme IPSec	IP de la passerelle autorisée
1							
2							
3							
4							
5							
6							
7							
8							
9							
10							

Précédent

Figure 24 Sommaire de VPN

Le tableau suivant décrit les champs de cette fenêtre.

Tableau 10 Sommaire de VPN

ETIQUETTE	DESCRIPTION
No	Le nombre indice de règle VPN
Nom	Ce champ affiche le nom d'identification pour cette règle VPN.
Activer	Ce champ affiche laquelle des règles VPN est active ou inactive. Yes signifie que cette règle VPN est active. No signifie que cette règle VPN n'est pas active.
Adresse locale	<p>C'est la(les) adresse(s) IP d'ordinateur(s) sur votre réseau local derrière votre Prestige.</p> <p>La même adresse IP (statique) est affichée deux fois lorsque le champ Type d'adresse locale dans l'écran Configure-IKE (ou Manual) est configuré en Single Address.</p> <p>Les adresses IP de début et de fin (statiques), dans l'ensemble des stations sont affichées lorsque le champ Type d'adresse locale dans l'écran Configure-IKE (ou Manual) est configuré en Range Address.</p> <p>Une adresse IP (statique) et un masque de sous-réseau est affiché lorsque le champ Type d'adresse locale dans l'écran Configure-IKE (ou Manual) est configuré en Subnet Address.</p>

Tableau 10 Sommaire de VPN

ETIQUETTE	DESCRIPTION
Adresse distante	<p>C'est la(les) adresse(s) IP d'ordinateur(s) sur le réseau distant derrière un routeur distant IPSec.</p> <p>Ce champ affiche N/A lorsque le champ Adresse du pont sécurisé affiche 0.0.0.0. Dans ce cas, seulement le routeur distant IPSec peut lancer le VPN.</p> <p>La même adresse IP (statique) est affichée deux fois lorsque le champ Type d'adresse distante dans l'écran Configure-IKE (ou Manual) est configuré en Single Address.</p> <p>Les adresses IP de début et de fin (statiques), dans l'ensemble des stations sont affichées lorsque le champ Type d'adresse distante dans l'écran Configure-IKE (ou Manual) est configuré en Range Address.</p> <p>Une adresse IP (statique) et un masque de sous-réseau sont affichés lorsque le champ Type d'adresse distante dans l'écran Configure-IKE (ou Manual) est configuré en Subnet Address.</p>
Encap.	Ce champ affiche le mode Tunnel ou Transport (La sélection par défaut est "Tunnel").
Algorithme IPSec	<p>Ce champ affiche les protocoles de sécurité utilisés pour un SA.</p> <p>Tous les deux AH et ESP augmentent les conditions de traitement de Prestige et le temps d'attente de communications (délai).</p>
Adresse IP de la passerelle distant	C'est l'adresse IP WAN statique ou l'URL du routeur distant IPSec. Ce champ affiche 0.0.0.0 lorsque vous configurez le champ Adresse du pont sécurisé dans l'écran Configure-IKE en 0.0.0.0 .

5.12 Configuration des règles VPN

Cliquez sur le numéro de règle pour éditer les règles VPN.

VPN - IKE

Configuration IPSec

Activer Connexion fixe

Nom

Mode clé IPSec

Mode de négociation

Local:

Type d'adresse locale

Adresse IP de départ

Fin/Masque de sous réseau

Nœud distant:

Type d'adresse distante

Adresse IP de départ

Fin/Masque de sous réseau

Type ID local

Contenu

Mon adresse IP

Type d'ID nœud distant

Contenu

Adresse IP de la passerelle autorisée

Mode d'encapsulation

Protocole de sécurité

Protocole VPN

Clé pré-partagée

VPN - Configuration

Algorithme d'authentification

Figure 25 IKE VPN

Le tableau suivant décrit les champs de cette fenêtre.

Tableau 11 IKE VPN

ETIQUETTE	DESCRIPTION
Activer	Cochez cette case pour activer ce tunnel VPN. Cette option détermine si une règle VPN est appliquée avant qu'un paquet traverse le firewall.
Connexion Fixe	Sélectionnez soit Yes soit No dans la zone de liste déroulante. Sélectionnez Yes pour faire que le Prestige réinitialise automatiquement le SA après que la durée de vie de SA arrive au bout de son délai, même s'il n'y a aucun trafic. Le routeur distant IPSec doit aussi resté activé en ordre que cette caractéristique fonctionne.
Nom	Tapez jusqu'à 32 caractères pour identifier cette règle VPN. Vous pouvez utiliser n'importe quel caractère, incuant les espaces, mais le Prestige élimine les espaces à droite.
Gestion de clé	Sélectionnez IKE ou Manual Key dans la zone de liste déroulante. Le IKE fournit plus de protection, donc il est en général recommandé. Le Manual Key est une option utile pour le dépannage.
Mode négociation	Sélectionnez Main ou Aggressive dans la zone de liste déroulante. Les multiples connexions SA via une passerelle sécurisée doivent avoir le même mode de négociation.
Local	Les adresses IP locales doivent être statiques et correspondre aux adresses IP distantes configurées dans le routeur distant IPSec. Les deux SA actifs peuvent avoir la même adresse IP locale ou distante, mais pas les deux. Vous pouvez configurer les multiples SA entre les mêmes adresses IP locales et distantes, aussi longtemps que seulement un soit actif en tout temps.
Type d'adresse	Utilisez le menu déroulant pour choisir Single Address , Range Address , ou Subnet Address . Sélectionnez Single Address pour une adresse IP unique. Sélectionnez Range Address pour une plage spécifique des adresses IP. Sélectionnez Subnet Address pour préciser les adresses IP sur un réseau par leur masque de sous-réseau.
Adresse IP de départ	Lorsque le champ Type d'adresse est configuré en Single Address , entrez une adresse IP (statique) sur le LAN derrière votre Prestige. Lorsque le champ Type d'adresse est configuré en Range Address , entrez l'adresse IP de début (statique), dans un ensemble de stations sur votre LAN derrière votre Prestige. Lorsque le champ Type d'adresse est configuré en Subnet Address , c'est une adresse IP (statique) sur le LAN derrière votre Prestige.
Fin/Masque de sous-réseau	Lorsque le champ Type d'adresse est configuré en Single Address , ce champ est N/A. Lorsque le champ Type d'adresse est configuré en Range Address , entrez l'adresse IP de fin (statique), dans un ensemble de stations sur votre LAN derrière votre Prestige. Lorsque le champ Type d'adresse est configuré en Subnet Address , c'est un masque de sous-réseau sur le LAN derrière votre Prestige.

Tableau 11 IKE VPN

ETIQUETTE	DESCRIPTION
Distant	<p>Les adresses IP distantes doivent être statiques et correspondre aux adresses IP locales configurées dans le routeur distant IPSec. Les champs distants ne sont pas appliqués lorsque le champ Adresse du pont sécurisé est configuré en 0.0.0.0. Dans ce cas, seulement le routeur distant IPSec peut lancer le VPN.</p> <p>Les deux SA actifs ne peuvent pas avoir la(les) même(s) adresse(s) IP locale(s) et distante(s). Les deux SA actifs peuvent avoir la même adresse IP locale ou distante, mais pas les deux. Vous pouvez configurer les multiples SA entre les mêmes adresses IP locales et distantes, aussi longtemps que seulement un soit actif en tout temps.</p>
Type d'adresse	<p>Utilisez le menu déroulant pour choisir Single Address, Range Address, ou Subnet Address. Sélectionnez Single Address avec une adresse IP unique. Sélectionnez Range Address pour une plage spécifique des adresses IP. Sélectionnez Subnet Address pour préciser les adresses IP sur un réseau par leur masque de sous-réseau.</p>
Adresse IP de départ	<p>Lorsque le champ Type d'adresse est configuré en Single Address, entrez une adresse IP (statique) sur le réseau derrière le routeur distant IPSec. Lorsque le champ Type d'adresse est configuré en Range Address, entrez l'adresse IP de début (statique), dans l'ensemble de stations sur le réseau derrière le routeur distant IPSec. Lorsque le champ Type d'adresse est configuré en Subnet Address, entrez une adresse IP (statique) sur le réseau derrière le routeur distant IPSec.</p>
Fin/Masque de sous-réseau	<p>Lorsque le champ Type d'adresse est configuré en Single Address, ce champ est N/A. Lorsque le champ Type d'adresse est configuré en Range Address, entrez l'adresse IP de fin (statique), dans l'ensemble de stations sur le réseau derrière le routeur distant IPSec. Lorsque le champ Type d'adresse est configuré en Subnet Address, entrez un masque de sous-réseau sur le réseau derrière le routeur distant IPSec.</p>
Type ID local	<p>Sélectionnez IP pour identifier ce Prestige par son adresse IP. Sélectionnez DNS pour identifier ce Prestige par un nom de domaine. Sélectionnez E-mail pour identifier ce Prestige par une adresse e-mail.</p>
Contenu	<p>Lorsque vous sélectionnez IP dans le champ Type ID local, tapez l'adresse IP de votre ordinateur ou laissez le champ vide pour avoir le Prestige qu'il utilise automatiquement sa propre adresse IP.</p> <p>Lorsque vous sélectionnez DNS dans le champ Type ID local, tapez un nom de domaine (jusqu'à 31 caractères) par lequel ce Prestige sera identifié.</p> <p>Lorsque vous sélectionnez E-mail dans le champ Type ID local, tapez une adresse e-mail (jusqu'à 31 caractères) par laquelle ce Prestige sera identifié.</p> <p>Le nom de domaine ou l'adresse e-mail que vous utilisez dans le champ Contenu sont utilisés seulement pour l'identification et non pas besoin d'avoir un nom de domaine ou une adresse e-mail réels.</p>

Tableau 11 IKE VPN

ETIQUETTE	DESCRIPTION
Mon adresse IP	<p>Entrez l'adresse IP WAN de votre Prestige. Le Prestige utilise son adresse IP WAN actuelle (statique ou dynamique) dans l'établissement du tunnel VPN si vous laissez ce champ en 0.0.0.0.</p> <p>Le tunnel VPN doit être reconstruit, si cette adresse IP change.</p>
Type ID d'homologues	<p>Sélectionnez IP pour identifier le routeur distant IPSec par son adresse IP. Sélectionnez DNS pour identifier le routeur distant IPSec par un nom de domaine. Sélectionnez E-mail pour identifier la routeur distant IPSec par une adresse e-mail.</p>
Contenu	<p>Lorsque vous sélectionnez IP dans le champ Type ID d'homologues, tapez l'adresse IP de la station avec laquelle vous allez créer la connexion VPN, ou laissez ce champ vide pour que le Prestige utilise automatiquement l'adresse dans le champ Pont sécurisé.</p> <p>Lorsque vous sélectionnez DNS dans le champ Type ID d'homologues, tapez un nom de domaine (jusqu'à 31 caractères) pour identifier le routeur distant IPSec.</p> <p>Lorsque vous sélectionnez E-mail dans le champ Type ID d'homologues, tapez une adresse e-mail (jusqu'à 31 caractères) pour identifier le routeur distant IPSec.</p> <p>Le nom de domaine ou l'adresse e-mail que vous utilisez dans le champ Contenu sont utilisés seulement pour l'identification et non pas besoin d'avoir un nom de domaine ou une adresse e-mail réels. Le nom de domaine aussi ne doit pas correspondre à l'adresse IP du routeur distant ou à celui-ci que vous configurez dans le champ Adresse du pont sécurisé ci-dessous.</p>
Adresse de la passerelle VPN distante	<p>Tapez l'adresse IP WAN ou l'URL (jusqu'à 31 caractères) du routeur IPSec avec qui vous créez la connexion VPN. Paramétrez ce champ en 0.0.0.0 si le routeur distant IPSec a une adresse IP WAN dynamique (le champ Gestion de clé doit être paramétré en IKE).</p>
Mode d'encapsulation	<p>Sélectionnez le mode Tunnel ou le mode Transport dans la zone de liste déroulante.</p>
ESP	<p>Sélectionnez l'ESP si vous voulez utiliser l'ESP (Encapsulation Security Payload). Le protocole ESP (RFC 2406) fournit le cryptage aussi bien que la plupart des services offerts par AH. Si vous sélectionnez l'ESP ici, vous devez sélectionner les options dans les champs Algorithme d'encryptage et Algorithme d'authentification (décrits ci-dessous).</p>

Tableau 11 IKE VPN

ETIQUETTE	DESCRIPTION
Algorithme d'encryptage	Sélectionnez DES , 3DES ou NULL dans la zone de liste déroulante. Lorsque le DES est utilisé pour les communications des données, l'émetteur et le récepteur doivent connaître tous les deux la même clé secrète qui peut être utilisée pour crypter et décrire le message ou générer et vérifier un code d'authentification du message. L'algorithme de cryptage DES utilise une clé de 56-bit. Le triple DES (3DES) est une variation de DES qui utilise une clé de 168-bit. En conséquence, le 3DES est plus sécurisé que le DES . Il demande aussi plus de puissance pour le traitement, entraînant le temps d'attente et la baisse du débit. Sélectionnez NULL pour paramétrer un tunnel sans le cryptage. Lorsque vous sélectionnez NULL , vous n'entrez pas une clé de cryptage.
Algorithme d'authentification	Sélectionnez SHA1 ou MD5 dans la zone de liste déroulante. Le MD5 (Message Digest 5) et le SHA1 (Secure Hash Algorithm) sont les algorithmes dispersés utilisés pour identifier les données du paquet. L'algorithme SHA1 est en général considéré comme plus puissant que le MD5 , mais il plus lent. Sélectionnez MD5 pour la sécurité minimale et SHA-1 pour la sécurité maximale.
AH	Sélectionnez AH si vous voulez utiliser l'AH (Authentication Header Protocol). Le protocole AH (RFC 2402) était destiné pour l'intégrité, l'authentification, l'intégrité sequentiel (réinsération de résistance), et non-répudiation, mais pas pour la confidentialité, pour laquelle l'ESP était destiné. Si vous sélectionnez AH ici, vous devez sélectionner les options dans le champ Algorithme d'authentification (décrit ci-dessous).
Algorithme d'authentification	Sélectionnez SHA1 ou MD5 dans la zone de liste déroulante. Le MD5 (Message Digest 5) et le SHA1 (Secure Hash Algorithm) sont les algorithmes dispersés utilisés pour identifier les données du paquet. L'algorithme SHA1 est en général considéré comme plus puissant que le MD5 , mais plus lent. Sélectionnez MD5 pour la sécurité minimale et SHA-1 pour la sécurité maximale.
Clé pré-partagée	Tapez votre clé pré-partagée dans ce champ. Une clé pré-prépartagée identifie un correspondant pendant une phase 1 de négociation IKE. Elle est appelée "pré-partagée" parce que vous devez la partager avec l'autre partie avant que vous puissiez communiquer avec elle via une connexion sécurisée. Les multiples SA qui se connectent via une passerelle sécurisée, doivent avoir la même clé pré-partagée.
Avancé	Cliquez sur Avancé pour configurer les paramètres plus détaillés de la gestion de votre clé IKE.

5.13 Visualisation du moniteur SA

Une Association de sécurité (SA) est un groupe des paramètres de sécurité relatif à un tunnel VPN spécifique. Cet écran affiche les connexions VPN actives. Utilisez **Actualiser** pour afficher les connexions VPN actives. Cet écran est en lecture seul.

Dans le programme de configuration par web, cliquez sur **AVANCE→VPN** et sur l'onglet **Surveillance** pour visualiser les Associations de sécurité (SA).

VPN - Surveillance SA

No.	Nom	Encapsulation	Algorithme IPSec	Déconnecter
1	Paris	Tunnel	ESP DES--SHA1	<input type="radio"/>
2	-	-	-	<input type="radio"/>
3	-	-	-	<input type="radio"/>
4	-	-	-	<input type="radio"/>
5	-	-	-	<input type="radio"/>
6	-	-	-	<input type="radio"/>
7	-	-	-	<input type="radio"/>
8	-	-	-	<input type="radio"/>
9	-	-	-	<input type="radio"/>
10	-	-	-	<input type="radio"/>

Précédent Appliquer Actualiser

Figure 26 Surveillance

Lorsqu'il y a du trafic sortant, mais pas du trafic entrant, le SA arrive automatiquement au bout de son délai dans deux minutes. Un tunnel sans trafic sortant ou entrant est "au repos" et n'arrive pas au bout de son délai jusqu'à ce que la période de durée de vie de SA n'expire pas.

5.14 perçu de l'UPnP

Universal Plug and Play (UPnP) est une norme de réseau ouverte répartie qui utilise TCP/IP pour une connectivité réseau simple de nœuds distants entre des périphériques. Un périphérique UPnP peut dynamiquement entrer dans un réseau, obtenir une adresse IP, transférer ses fonctionnalités et apprendre d'autres périphériques du réseau. A son tour, un périphérique peut quitter un réseau discrètement et automatiquement lorsqu'il n'est plus utilisé.

Tous les périphériques activés par UPnP peuvent communiquer librement entre eux sans configuration supplémentaire. Désactivez UPnP si ceci n'est pas votre intention.

Windows ME et Windows XP prennent en charge UPnP. Reportez-vous au site Web de Microsoft pour plus d'informations sur d'autres systèmes d'exploitation de Microsoft.

S'assurer d'appliquer le correctif de sécurité UPnP de Microsoft avant d'activer la fonctionnalité UPnP. Se reporter au site Web de Microsoft.

5.15 Configuration de l'UPnP

Cliquez sur **Configuration avancée** puis sur **UPnP** pour afficher l'écran **UPnP**.

The screenshot shows a configuration window titled "UPnP". It contains three unchecked checkboxes:

- Activer le service UPnP (Universal Plug and Play)
- Permettre aux utilisateurs de modifier la configuration à travers le UPnP
- Permettre au UPnP de traverser le coupe-feu

 At the bottom of the window, there are two buttons: "Appliquer" and "Annuler".

Figure 29 UPnP

Le tableau suivant décrit les champs dans cet écran.

Tableau 12 UPnP

CHAMP	DESCRIPTION
Activer le service UPnP (Universal Plug and Play)	Cochez cette case pour activer UPnP. Gardez à l'esprit que n'importe qui peut utiliser une application UPnP pour afficher l'écran de connexion du configurateur sans taper l'adresse IP du Prestige (bien que vous devez toujours taper le mot de passe pour accéder au configurateur Web).
Permettre aux utilisateurs de modifier la configuration à travers le UPnP	Cochez cette case pour permettre aux applications activées par UPnP de configurer automatiquement le Prestige de sorte qu'elles puissent communiquer via le Prestige, par exemple en utilisant NAT Transversal. Les applications UPnP réservent automatiquement un port de routage NAT afin de communiquer avec un autre périphérique activé par UPnP ; cela vous évite de configurer manuellement le routage des ports pour l'application activée par UPnP.
Permettre au UPnP de passer à travers de Firewall	Cochez cette case pour créer une règle qui permet l'acheminement des ports 1900 et 80. Cette case cochée crée aussi une règle de firewall dynamique chaque fois qu'un port d'acheminement de NAT est réservé à l'UPnP. Ce paramètre reste actif jusqu'à ce que vous désactiviez l'UPnP ou décochez cette case. Décochez cette case pour avoir le firewall qui bloque tous les paquets de l'application de UPnP (par exemple, paquets MSN) à la place de créer une règle de firewall pour eux.

6 Dépannage

Tableau 13 Dépannage

PROBLÈME	ACTION CORRECTIVE
Aucun des voyants ne s'allume lorsque vous activez le Prestige.	<p>Vérifiez que l'adaptateur secteur correct soit bien connecté au Prestige et branché à une source d'alimentation appropriée. Vérifiez toutes les connexions de câbles.</p> <p>Si les voyants ne s'allument pas, il s'agit probablement d'un problème matériel. Dans ce cas, contactez votre revendeur local.</p>
Impossible d'accéder au Prestige depuis le LAN.	<p>Vérifiez la connexion des câbles entre le Prestige et votre ordinateur ou concentrateur. Reportez-vous à la section Matériel pour plus de détails.</p> <p>Envoyez une requête Ping au Prestige depuis un ordinateur de LAN. Assurez-vous que la carte réseau Ethernet de votre ordinateur soit installée et fonctionne correctement.</p>
Impossible d'envoyer la requête ping vers tout ordinateur du LAN	<p>Si les voyants du LAN sont tous éteints, vérifiez la connexion des câbles entre le Prestige et vos ordinateurs sur le LAN.</p> <p>Vérifiez que l'adresse IP, le masque de sous-réseau du Prestige et les ordinateurs sur le LAN se trouvent dans la même plage d'adresses IP.</p>
Impossible d'envoyer la requête ping vers tout ordinateur du WLAN	<p>Assurez-vous que la carte sans fil soit correctement insérée dans le Prestige et que le voyant WLAN soit allumé.</p> <p>Assurez-vous que la carte sans fil sur le client sans fil fonctionne correctement.</p> <p>Vérifiez que le Prestige et les client(s) sans fil utilisent le même ESSID, canal et clés WEP (si le cryptage WEP est activé).</p>
Impossible d'obtenir une adresse IP WAN auprès de l'ISP	<p>Vérifiez vos paramètres de l'encapsulation, du multiplexage et VPI/VCI (référez-vous à la section 4.3).</p> <p>Vous avez besoin d'un nom d'utilisateur et d'un mot de passe si vous utilisez l'encapsulation PPPoE ou PPPoA. Assurez-vous que vous avez correctement entré le Nom de service (Encapsulation PPPoE uniquement), le Nom d'utilisateur et le Mot de passe (le nom d'utilisateur et le mot de passe sont les cas sensible). Référez-vous à la section 4.3 pour plus d'information.</p> <p>L'adresse IP WAN est fournie une fois que l'ISP a vérifié l'adresse MAC, l'hôte et l'identification de l'utilisateur. Découvrez la méthode de vérification utilisée par votre ISP et configurez les champs correspondants.</p> <p>Si l'ISP vérifie l'identification de l'utilisateur, vérifiez votre type de service, nom d'utilisateur et mot de passe dans l'écran WAN.</p>
Impossible d'accéder à Internet.	<p>Vérifiez les paramètres de la connexion Internet dans l'écran WAN.</p> <p>Assurez-vous d'avoir entré le nom d'utilisateur et mot de passe corrects.</p> <p>Vérifiez que le Prestige et les client(s) sans fil utilisent le même ESSID, canal et clés WEP (si le cryptage WEP est activé).</p>