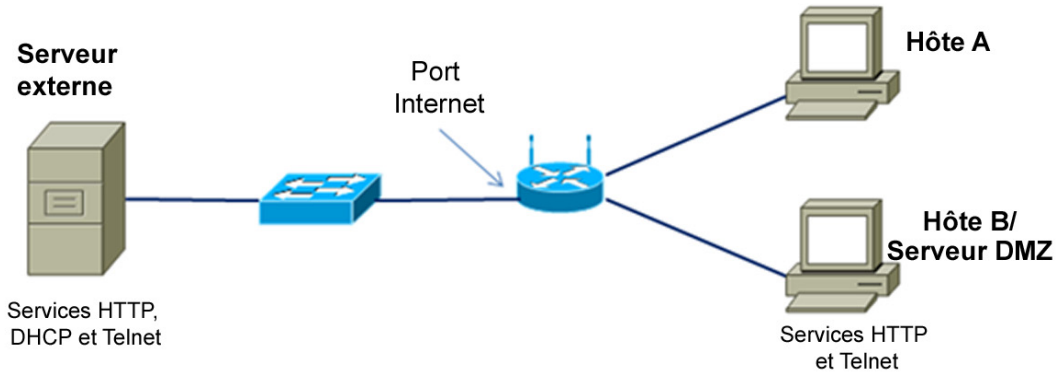
Travaux pratiques 8.4.2 Configuration des stratégies d'accès et des paramètres de la zone démilitarisée (DMZ)



Objectifs

- Se connecter au périphérique multi-fonction et afficher les paramètres de sécurité
- Configurer les stratégies d'accès à Internet à partir de l'adresse IP et de l'application
- Configurer une zone démilitarisée (DMZ) pour un serveur à accès ouvert avec une adresse IP statique
- Configurer la transmission du port pour limiter l'accessibilité du port à HTTP uniquement
- Utiliser les fonctions d'aide du Linksys WRT300N

Contexte / Préparation

Ces travaux pratiques donnent les instructions de configuration des paramètres de sécurité du Linksys WRT300N. Le Linksys est doté d'un pare-feu logiciel visant à protéger les clients internes du réseau local des attaques d'hôtes externes. Les connexions des hôtes internes aux destinations externes peuvent être filtrées à partir de l'adresse IP, du site Web de destination et de l'application. Le Linksys peut également être configuré pour créer une zone démilitarisée (DMZ) en vue de contrôler l'accès à un serveur à partir d'hôtes externes. Ces travaux pratiques sont réalisés par équipes de deux et deux équipes peuvent travailler ensemble pour tester les restrictions d'accès et la fonctionnalité DMZ entre elles. Ces travaux pratiques se divisent en 2 parties :

- Partie 1 : configuration des stratégies d'accès
- Partie 2 : configuration des paramètres de la zone démilitarisée (DMZ)

Ressources requises :

- Le Linksys WRT300N ou un autre périphérique multi-fonction avec la configuration par défaut
- L'ID utilisateur et le mot de passe du périphérique Linksys s'ils sont différents des valeurs par défaut
- Un ordinateur fonctionnant sous Windows XP Professionnel pour accéder à l'interface graphique utilisateur Linksys
- Un PC interne utilisé comme serveur dans la zone démilitarisée (DMZ) avec des serveurs HTTP et Telnet installés (serveur préconfiguré ou CD Discovery Live)

- Un serveur externe pour représenter le fournisseur de services Internet et Internet (avec serveurs DHCP, HTTP et Telnet préconfigurés (vrai serveurs avec des services installés ou le serveur CD Discovery Live)
- Le câblage pour connecter les PC hôtes, le périphérique Linksys WRT300N ou le périphérique multi-fonction, et les commutateurs

Partie 1 : configuration des stratégies d'accès

Étape 1 : création du réseau et configuration des hôtes

a. Connectez les ordinateurs hôtes aux ports du commutateur sur le périphérique multi-fonction comme l'indique le schéma topologique. L'Hôte-A est la console et sert à accéder à l'interface graphique utilisateur du Linksys. L'Hôte-B est à la base une machine test mais devient par la suite le serveur DMZ.

b. Configurez les paramètres IP des deux hôtes à l'aide des connexions réseaux de Windows XP et des propriétés TCP/IP. Vérifiez que l'Hôte-A est configuré comme client DHCP. Attribuez une adresse IP statique à l'Hôte-B dans la portée 192.168.1.x avec un masque de sous-réseau de 255.255.255.0. La passerelle par défaut doit être l'adresse du réseau local interne du périphérique Linksys.

REMARQUE : si l'Hôte-B est déjà un client DHCP, vous pouvez réserver son adresse actuelle et la rendre statique à l'aide de la fonction DHCP Reservation sur l'écran Basic Setup du Linksys.

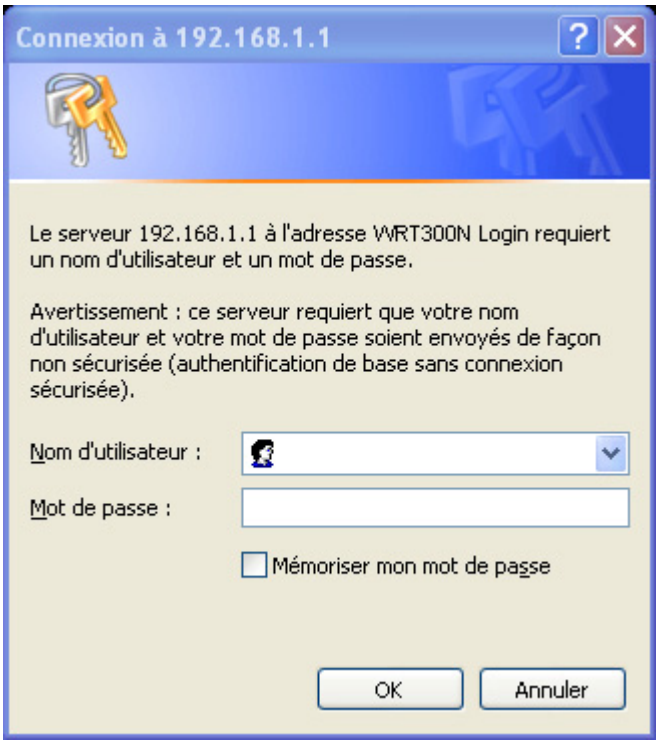
c. Utilisez la commande *ipconfig* pour afficher l'adresse IP, le masque de sous-réseau et la passerelle par défaut de l'Hôte-A et de l'Hôte-B et notez-les dans le tableau. Obtenez l'adresse IP et le masque de sous-réseau du serveur externe de la part du formateur et notez-les dans le tableau.

Hôte	Adresse IP	Masque de sous-réseau	Passerelle par défaut
Hôte-A			
Hôte-B/ Serveur DMZ			
Serveur externe			

Étape 2 : connexion à l'interface utilisateur

a. Pour accéder à l'interface graphique utilisateur basée sur le Web Linksys ou du périphérique multi-fonction, ouvrez un navigateur et entrez l'adresse IP interne par défaut du périphérique, normalement 192.168.1.1.

b. Connectez-vous à l'aide de l'ID d'utilisateur et du mot de passe par défaut ou vérifiez avec le formateur s'ils sont différents.



c. Le périphérique multi-fonction doit être configuré pour obtenir une adresse IP à partir du serveur DHCP externe. L'écran par défaut après la connexion au périphérique multi-fonction est Setup > Basic Setup. Quel est le type de connexion Internet ?

_____

d. Quelle est l'adresse IP du routeur par défaut (interne) et le masque de sous-réseau du périphérique multi-fonction ?

_____

e. Vérifiez que le périphérique multi-fonction a reçu une adresse IP externe à partir du serveur DHCP en cliquant sur l'onglet Statut > Routeur.

f. Quelle est l'adresse IP externe et le masque de sous-réseau du périphérique multi-fonction ?

_____

Étape 3 : affichage des paramètres du pare-feu du périphérique multi-fonction

a. Le Linksys WRT300N est doté d'un pare-feu de base qui fait appel à la traduction d'adresses de réseau (NAT). De plus, il offre une fonctionnalité de pare-feu supplémentaire à l'aide de l'inspection dynamique de paquets (IDP) permettant de détecter et de bloquer du trafic non demandé à partir d'Internet.

b. Sur l'écran principal, cliquez sur l'onglet **Security** pour afficher l'état des éléments **Firewall** et **Internet Filter**. Quel est l'état de la protection du pare-feu de l'inspection dynamique de paquets ?

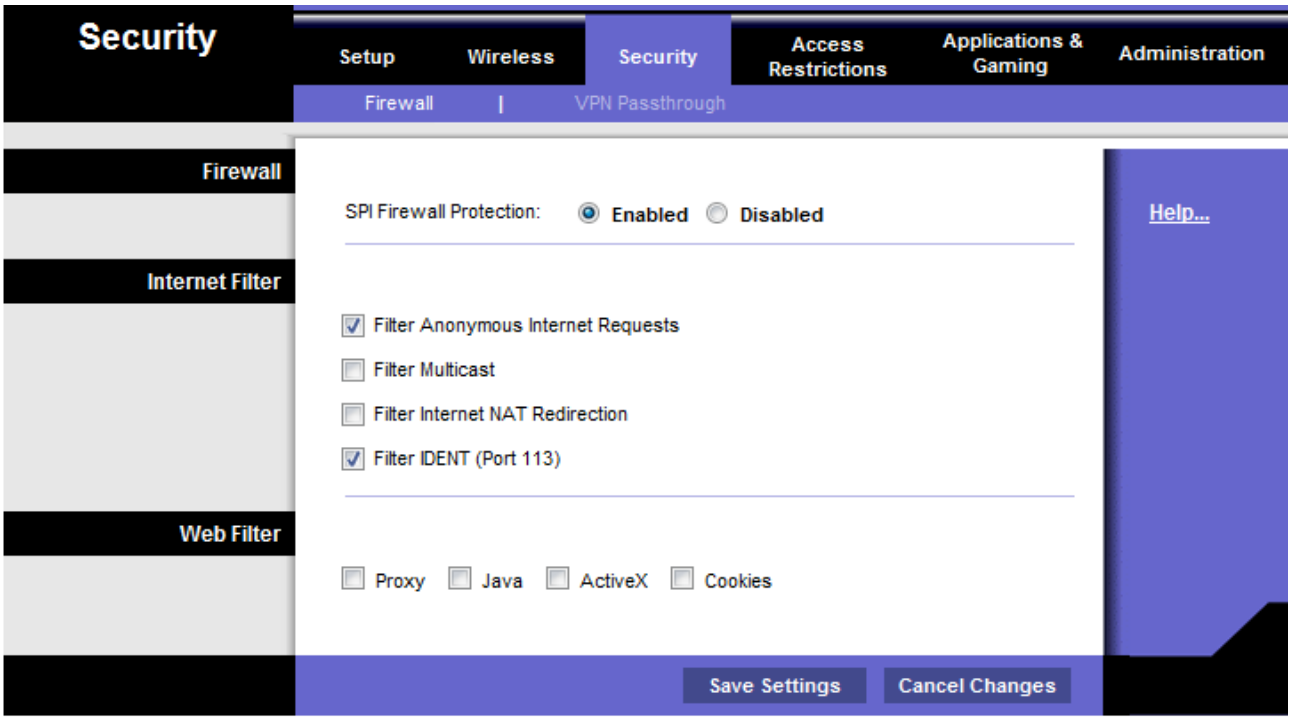
_____

c. Quelles cases à cocher **Internet Filter** sont activées ?"

_____

d. Cliquez sur **Help** pour en savoir plus sur ces paramètres. Quels avantages le filtrage IDENT offre-t-il ?

_____



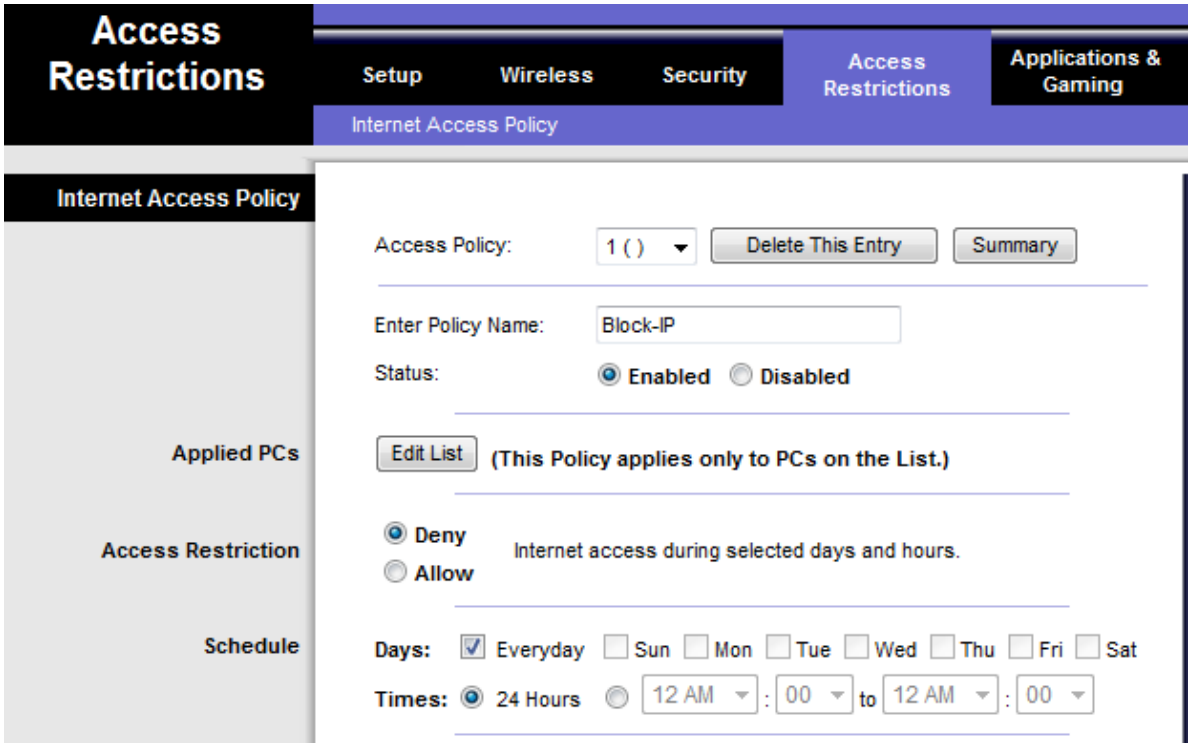
Étape 4 : configuration des restrictions d'accès à Internet à partir de l'adresse IP

Dans les travaux pratiques 7.3.5, vous avez vu que les fonctions de sécurité sans fil peuvent servir à contrôler les ordinateurs clients sans fil qui peuvent avoir accès au périphérique multi-fonction, à partir de leur adresse MAC. Cela empêche les ordinateurs externes non autorisés de se connecter au point d'accès sans fil et d'avoir accès au réseau local interne et à Internet.

Le périphérique multi-fonction peut aussi contrôler les utilisateurs internes qui peuvent quitter Internet à partir du réseau local. Vous pouvez créer une stratégie d'accès à Internet pour refuser ou autoriser certains ordinateurs internes spécifiques à accéder à Internet à partir de l'adresse IP, de l'adresse MAC et d'autres critères.

a. Sur l'écran principal du périphérique multi-fonction, cliquez sur l'onglet **Access Restrictions** pour définir la stratégie **Access Policy 1**.

b. Entrez **Blocage-IP** comme nom de stratégie. Sélectionnez **Enabled** pour activer la stratégie, puis sélectionnez **Deny** pour empêcher l'accès à Internet à partir d'une adresse IP spécifiée.



c. Cliquez sur le bouton **Edit List** et entrez l'adresse IP de l'Hôte-B. Cliquez sur **Save Settings**, puis sur **Close**. Cliquez sur **Save Settings** pour enregistrer la stratégie d'accès Internet 1 – Blocage IP.

d. Testez la stratégie en tentant d'accéder au serveur Web externe à partir de l'Hôte-B. Ouvrez un navigateur et entrez l'adresse IP du serveur externe dans la zone d'adresse. Pouvez-vous accéder au serveur ? _____

e. Changez le statut de la stratégie Blocage-IP en **Disabled** et cliquez sur **Save Settings**. Pouvez-vous accéder au serveur maintenant ? _____

f. De quelles autres manières les stratégies d'accès peuvent-elles être utilisées pour bloquer l'accès à Internet ?

_____

Étape 5 : configuration d'une stratégie d'accès à Internet à partir d'une application

Vous pouvez créer une stratégie d'accès à Internet pour bloquer des ordinateurs spécifiques afin de les empêcher d'utiliser certaines applications Internet ou protocoles.

a. Sur l'écran principal de l'interface graphique utilisateur Linksys, cliquez sur l'onglet Access Restrictions pour définir une stratégie d'accès à Internet.

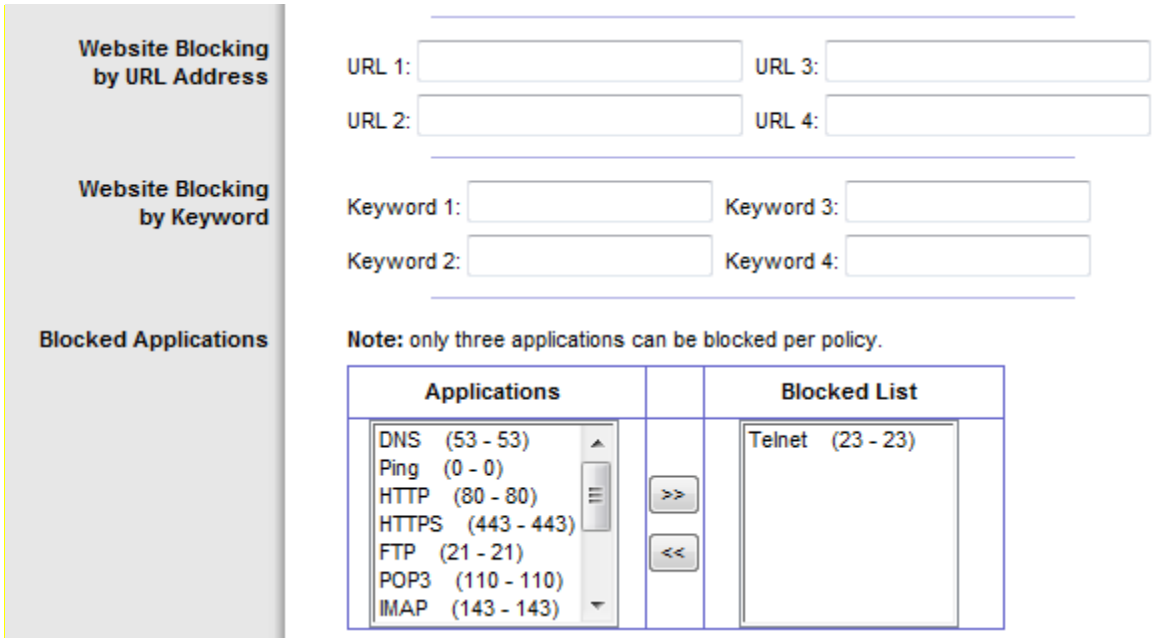
b. Entrez Blocage-Telnet comme nom de stratégie. Sélectionnez Enabled pour activer la stratégie, puis cliquez sur Allow pour permettre un accès Internet à partir d'une adresse IP spécifiée, pour autant qu'il ne s'agisse pas de l'une des applications bloquées.

c. Cliquez sur le bouton Edit List et entrez l'adresse IP de l'Hôte-B. Cliquez sur Save Settings, puis sur Close.

Quels sont les autres protocoles et les autres applications Internet qui peuvent être bloqués ?

_____

d. Sélectionnez l'application **Telnet** dans la liste des applications qui peuvent être bloquées, puis cliquez sur la double flèche vers la droite pour l'ajouter à la liste **Blocked List**. Cliquez sur **Save Settings**.



e. Testez la stratégie en ouvrant une invite de commandes à l'aide de **Démarrer > Tous les programmes > Accessoires > Invite de commandes**.

f. Envoyez une requête ping à l'adresse IP du serveur externe à partir de l'Hôte-B à l'aide de la **commande ping**.

Pouvez-vous utiliser une commande ping sur le serveur ? _____

g. Envoyez une requête Telnet à l'adresse IP du serveur externe à partir de l'Hôte-B à l'aide de la commande telnet A.B.C.D (où A.B.C.D est l'adresse IP du serveur).

Pouvez-vous utiliser une commande telnet sur le serveur ? _____

REMARQUE : si vous n'avez pas l'intention de faire la deuxième partie de ces travaux pratiques aujourd'hui et que d'autres participants utilisent le matériel après vous, passez à l'Étape 3 de la Partie 2 et restaurez le périphérique multi-fonction à ses paramètres par défaut.

Partie 2 : configuration d'une zone démilitarisée (DMZ) sur le périphérique multi-fonction

Étape 1 : configuration d'une zone démilitarisée (DMZ) simple

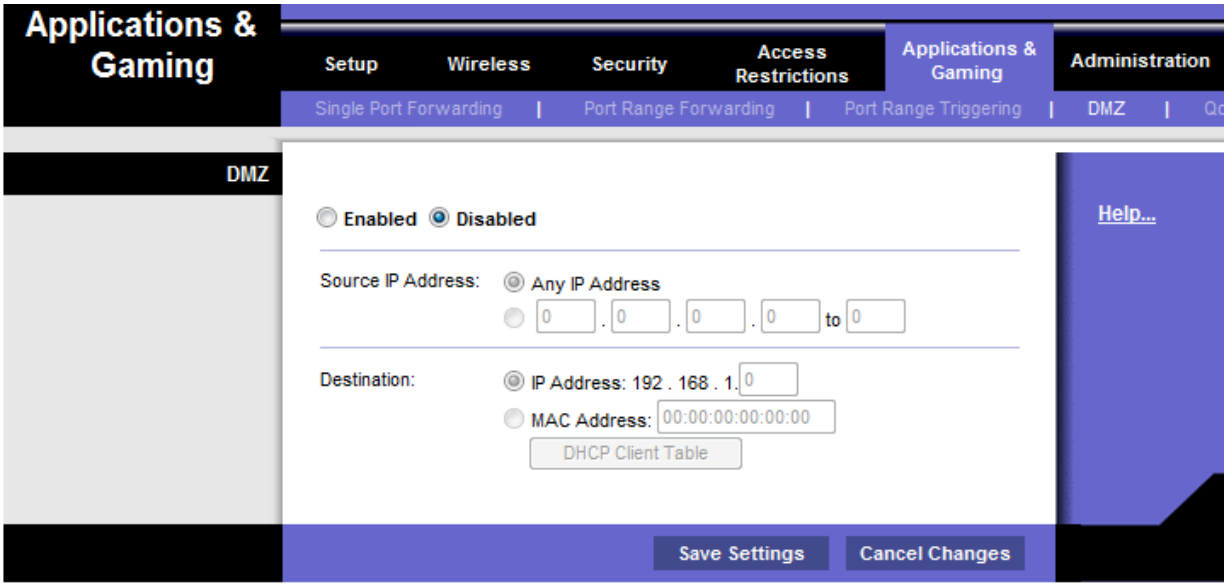
Il est parfois nécessaire d'autoriser l'accès à un ordinateur à partir d'Internet tout en protégeant les autres ordinateurs du réseau local interne. Pour ce faire, vous pouvez configurer une zone démilitarisée (DMZ) qui vous permet d'ouvrir l'accès aux ports et aux services qui s'exécutent sur le serveur indiqué. Toutes les requêtes réalisées pour des services vers l'adresse extérieure du périphérique multi-fonction seront redirigées vers le serveur spécifié.

a. L'Hôte-B fera office de serveur DMZ et il devra exécuter les serveurs HTTP et Telnet. Vérifiez que l'Hôte-B a une adresse IP statique ou si l'Hôte-B est un client DHCP, vous pouvez réserver son adresse actuelle et la rendre statique à l'aide de la fonction **DHCP Reservation** sur l'écran **Basic Setup** du périphérique Linksys.

b. Sur l'écran principal de l'interface graphique utilisateur Linksys, cliquez sur l'onglet **Applications & Gaming**, puis cliquez sur **DMZ**.

c. Cliquez sur **Help** pour en savoir plus sur la zone démilitarisée (DMZ). Pour quelles autres raisons voudriez-vous configurer un hôte sur la zone démilitarisée (DMZ) ?

_____



d. La fonction DMZ est désactivée par défaut. Sélectionnez **Enabled** pour activer la zone démilitarisée (DMZ). Laissez l'adresse **Source IP Address** sélectionnée en tant que **Any IP Address**, puis entrez l'adresse IP de l'Hôte-B dans **Destination IP Address**. Cliquez sur **Save Settings**, puis sur **Continue** lors de l'invite.

e. Testez l'accès de base au serveur DMZ en exécutant une commande ping à partir du serveur externe vers l'adresse extérieure du périphérique multi-fonction. Utilisez la commande **ping –a** pour vérifier que c'est le serveur DMZ qui répond et non le périphérique multi-fonction. Pouvez-vous utiliser une commande ping sur le serveur DMZ ?

_____

f. Testez l'accès HTTP sur le serveur DMZ en ouvrant un navigateur sur le serveur externe et en pointant vers l'adresse IP externe du périphérique multi-fonction. Essayez la même chose à partir d'un navigateur sur l'Hôte-A vers l'Hôte-B à l'aide des adresses internes.

Pouvez-vous accéder à la page Web ? _____

g. Testez l'accès Telnet en ouvrant une invite de commandes comme décrit à l'Étape 5. Utilisez une commande Telnet vers l'adresse IP extérieure du périphérique multi-fonction à l'aide de la commande **telnet** *A.B.C.D* (où A.B.C.D est l'adresse extérieure du périphérique multi-fonction).

Pouvez-vous utiliser une commande telnet sur le serveur ? _____

Étape 2 : configuration d'un hôte avec transmission à port simple

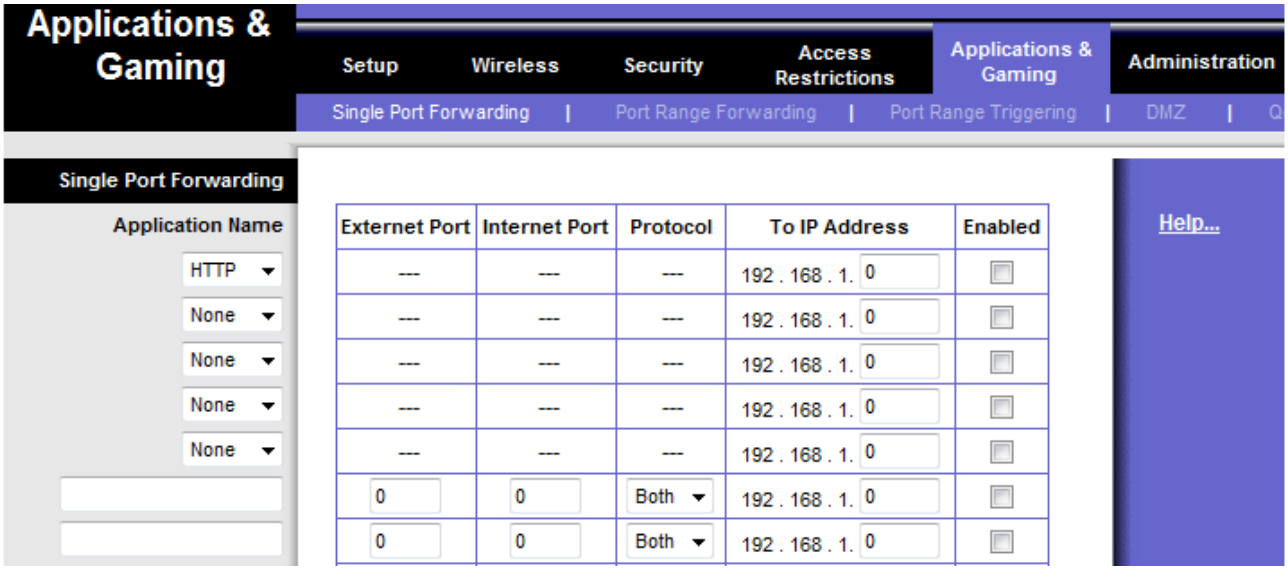
La configuration d'hôte DMZ basique à l'Étape 6 vous permet d'ouvrir l'accès à tous les ports et à tous les services s'exécutant sur le serveur, comme HTTP, FTP et Telnet. Si un hôte doit servir à une fonction particulière, comme des services FTP ou Web, l'accès doit être limité au type de services fournis. La transmission de port simple peut être utilisée pour cela et est plus sécurisée qu'une zone démilitarisée (DMZ) de base, car elle ouvre uniquement les ports nécessaires. Avant de réaliser cette étape, désactivez les paramètres de la zone démilitarisée (DMZ) pour l'étape 1.

L'Hôte-B est le serveur sur lequel des ports sont transmis mais dont l'accès est uniquement limité au protocole HTTP (Web).

a. Sur l'écran principal, cliquez sur l'onglet **Applications & Gaming**, puis cliquez sur **Single Port Forwarding** pour préciser les applications et les numéros des ports.

b. Cliquez sur le menu déroulant de la première entrée sous **Application Name** et sélectionnez **HTTP**. Il s'agit du port 80 du protocole du serveur Web.

c. Dans le premier champ **To IP Address**, entrez l'adresse IP de l'Hôte-B et sélectionnez **Enabled**. Cliquez sur **Save Settings**.



d. Testez l'accès HTTP sur l'hôte DMZ en ouvrant un navigateur sur le serveur externe et en pointant vers l'adresse IP extérieure du périphérique multi-fonction. Essayez la même chose à partir d'un navigateur sur l'Hôte-A vers l'Hôte-B.

Pouvez-vous accéder à la page Web ? _____

e. Testez l'accès Telnet en ouvrant une invite de commandes comme décrit à l'Étape 5. Essayez d'utiliser une commande Telnet vers l'adresse IP extérieure du périphérique multi-fonction à l'aide de la commande **telnet** *A.B.C.D* (où A.B.C.D est l'adresse extérieure du périphérique multi-fonction).

Pouvez-vous utiliser une commande telnet sur le serveur ?

_____

Étape 3 : rétablir les paramètres par défaut du périphérique multi-fonction

a. Pour rétablir les paramètres d'usine par défaut du Linksys, cliquez sur l'onglet **Administration > Factory Defaults**.

b. Cliquez sur le bouton **Restore Factory Defaults**. Toutes les entrées ou toutes les modifications apportées aux paramètres seront perdues.

REMARQUE : les paramètres actuels peuvent être enregistrés et rétablis plus tard avec l'onglet **Administration > Management** et les boutons **Backup Configuration** et **Restore Configuration**.