

Routeur de la petite entreprise VoIP : Problèmes avec la connexion aux sites Web sécurisés

Contenu

[Introduction](#)

[Comment est-ce que j'accède à des sites Web sécurisés utilisant le routeur du Cisco Small](#)

[Business VoIP ?](#)

[Informations connexes](#)

[Introduction](#)

Cet article en est un d'une série pour aider à l'installation, au dépannage, et à la maintenance des produits Cisco Small Business.

Q. [Comment est-ce que j'accède à des sites Web sécurisés utilisant le routeur du Cisco Small Business VoIP ?](#)

R.

Remarque: C'est normalement dû à un maximum transmettent le problème d'unité (MTU) et quelques sites sécurisés exigent des ports d'ouverture. Afin d'activer le MTU sur le routeur, terminez-vous les étapes dans ce document.

EnableMTU sur le routeur

Étape 1 :

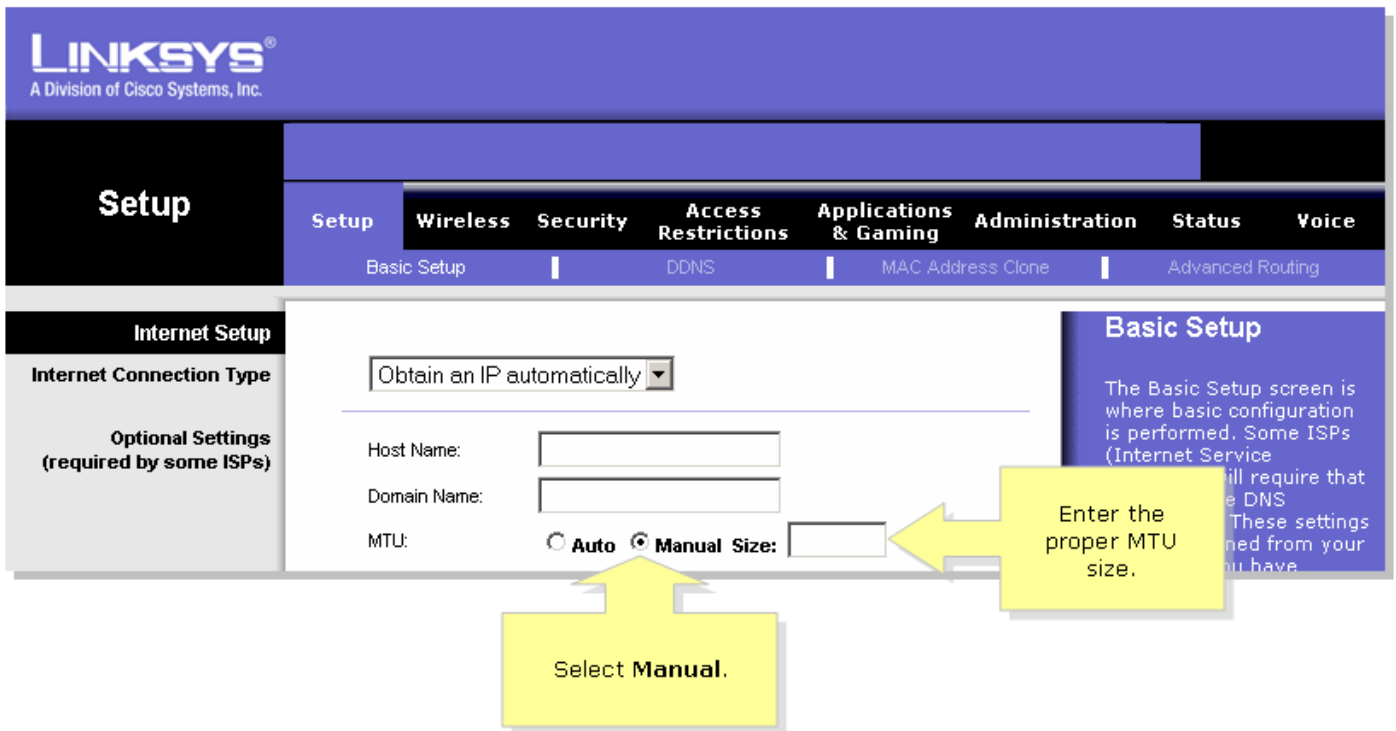
Déterminez la taille appropriée de MTU pour le site Web.

Étape 2 :

Accédez à la page de configuration Web du routeur. Pour des instructions, cliquez [ici](#).

Étape 3 :

Quand la page basée sur le WEB de l'installation du routeur paraît, placez le **MTU au manuel** et écrivez la valeur appropriée de MTU dans le **champ de taille**.



Remarque: Ce sont les tailles recommandées de MTU pour le DSL et la connexion du câble :

Connexion du câble : 1500

Connexion DSL de PPPoE : 1492

Étape 4 :

Clic **Save Settings**.

Remarque: Si ceci ne fonctionnait pas, des ports ouverts sur le routeur. Pour des instructions, terminez-vous les étapes dans la section suivante.

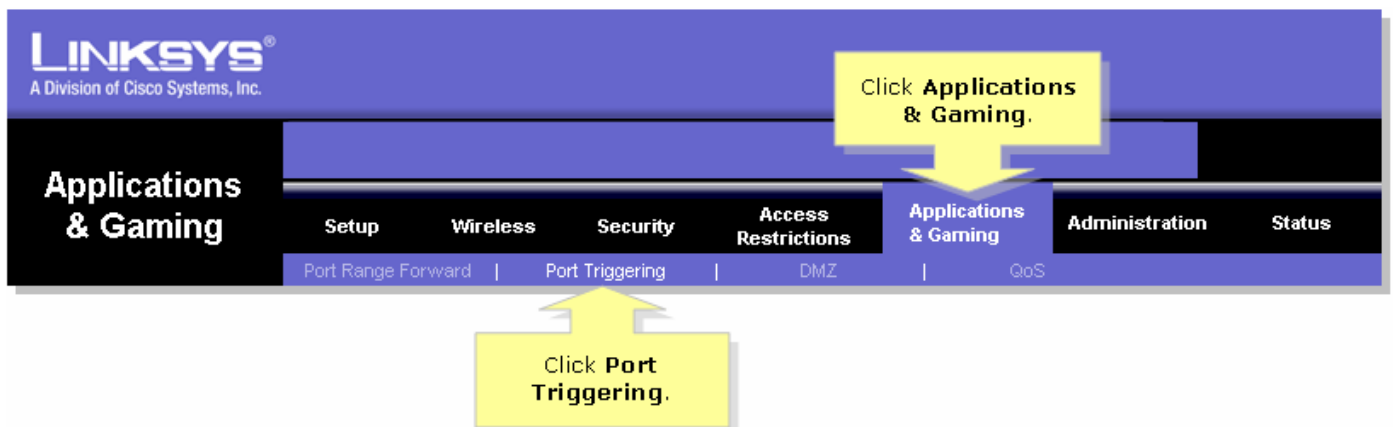
Ports ouverts pour les sites sécurisés

Étape 1 :

Accédez à la page de configuration Web du routeur. Pour des instructions, cliquez [ici](#).

Étape 2 :

Quand la page basée sur le WEB de l'installation du routeur paraît, cliquez sur les **applications et le déclenchement d'onglet Gaming > de port**.



Étape 3 :

Sous l'application, le type « https » et dans les domaines de connexion sortante déclenchée et de connexion entrante transférée, et le type "443" (le port utilisé par des https).

LINKSYS
A Division of Cisco Systems, Inc.

Applications & Gaming

Setup | Wireless | Security | Access Restrictions | **Applications & Gaming** | Administration | Status | Voice

Port Range Forwarding | Port Triggering | DMZ | QoS

Port Triggering

Under **Application**, enter "https" then under **Triggered** and **Forwarded Range**, enter "443" on both fields.

Application	Triggered Range		Forwarded Range	
	Start Port	End Port	Start port	End Port
https	443	to 443	443	to 443
		to		to
		to		to
		to		to
		to		to
		to		to
		to		to
		to		to
		to		to
		to		to
		to		to

Port Triggering

Port triggering will forward port based on the incoming port specified. Check with your software application to find out what is necessary to enter in these fields.

To add a server using forwarding:

1. Enter an Application name of the service you want to forward.
2. Enter the Trigger Range for Start and End of the services to trigger forwarding.
3. Enter the Forwarded Range for Start and End of the service you want to forward.

[More...](#)

Save Settings **Cancel Changes**

CISCO SYSTEMS

Étape 4 :

Clic **Save Settings**.

Informations connexes

- [Support et documentation techniques - Cisco Systems](#)