Activation de l'accès public WAN avec DDNS et le transfert de port

Ce document est un guide pas à pas de la configuration DDNS (de DNS dynamique) et du transfert de port sur les routeurs Cisco Small Business, afin de fournir un accès sécurisé à un serveur Web interne et une caméra vidéo IP à partir du réseau Internet public.

Présentation

Les routeurs Cisco Small Business fournissent une solution réseau de partage Internet avancée pour répondre aux exigences des PME. Plusieurs ordinateurs d'une PME peuvent partager la connexion Internet par l'intermédiaire de connexions avec des ports de commutation intégrés, des commutateurs connectés et des points d'accès sans fil. L'interface WAN 10/100 Ethernet du routeur est directement connectée à la DSL haut débit ou à un modem câble avec un réseau virtuel privé (VPN) et des fonctions de pare-feu.

Toutefois, l'accès aux serveurs du réseau, aux services réseau ou aux caméras de vidéosurveillance IP sur le réseau interne à partir de l'Internet public présente quelques difficultés pour les raisons suivantes :

- L'accès au réseau local interne (LAN) doit être entièrement protégé contre les utilisateurs non autorisés sur l'Internet public par un pare-feu qui empêche les connexions entrantes, à l'exception des accès autorisés à certaines ressources spécifiques du réseau.
- Des adresses IP privées sont affectées aux hôtes du réseau interne, afin de restreindre l'utilisation des adresses IP publiques, dont la disponibilité est limitée. Pour assurer la communication entre les hôtes et l'Internet public, la traduction d'adresses réseau (NAT) doit convertir chaque adresse IP privée en une adresse IP publique.
- La plupart des PME utilisent aujourd'hui des connexions Internet haut débit. La connexion Internet haut débit reçoit une adresse IP publique dynamique affectée par le fournisseur de services. Cette adresse n'est pas statique et peut changer fréquemment.

L'association des fonctions DDNS (DNS dynamique) du routeur avec le transfert de port fournit une solution simple qui permet un accès contrôlé et sécurisé à l'interface WAN du routeur et au réseau interne à partir de l'Internet public.

Principales caractéristiques

DDNS (DNS dynamique)

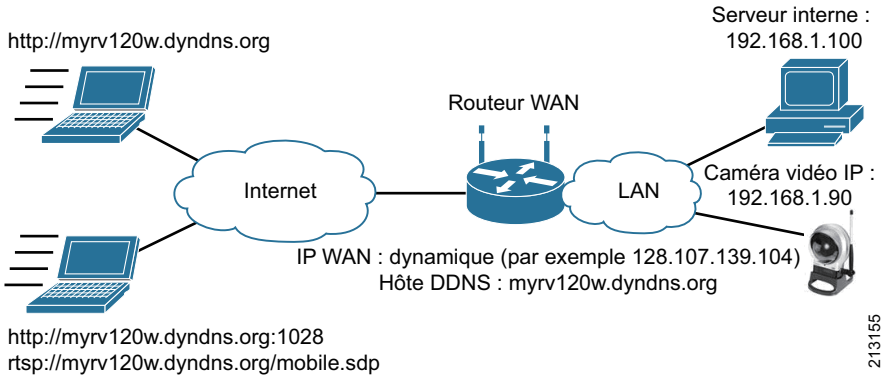
Le service DDNS (DNS dynamique) établit une correspondance entre les noms de domaines Internet et les adresses IP. Contrairement au DNS qui fonctionne uniquement avec des adresses IP statiques, le service DDNS prend en charge les adresses IP dynamiques, notamment celles affectées par un service DHCP. Le service DDNS est une solution appropriée pour les réseaux des PME qui reçoivent des adresses publiques dynamiques à partir d'un fournisseur de services Internet.

Certains fournisseurs de services DDNS, notamment dyndns.com, proposent des services DDNS gratuits. Pour en bénéficier, inscrivez-vous auprès d'un fournisseur de services DDNS, ajoutez le nom de domaine complet (FQDN, Fully Qualified Domain Name) du routeur, et configurez le routeur Cisco afin qu'il mette à jour automatiquement l'adresse IP WAN associée à son nom de domaine complet (FQDN). Vous pouvez maintenant accéder à la ressource réseau et au routeur WAN à l'aide du nom de domaine complet (FQDN), sans connaître l'adresse IP publique actuelle.

Transfert de port

Le transfert de port ouvre un port TCP ou UDP spécifique sur un serveur derrière le pare-feu du routeur, afin d'autoriser le transfert de tout le trafic entrant sur ce port vers le serveur spécifié. Cette fonctionnalité autorise les connexions entre les hôtes et les services externes au sein d'un réseau local (LAN) privé.

Figure 1 Schéma du réseau DDNS et du transfert de port



Produits proposés

- Routeur pare-feu VPN Cisco RV120W Wireless-N (Les écrans de configuration de l'interface utilisateur graphique de ce routeur sont présentés dans ce document à titre d'exemple.)
- Pare-feu de sécurité réseau Cisco RV220W Wireless-N
- Routeurs Cisco RV042, RV082, RV016, RVL200, WRVS4400N, RVS4000 et WRV210 pour PME

Conseils de conception

Adresse IP WAN : deux types d'adresses IP WAN seront fournis par l'ISP, avec affectation dynamique ou affectation statique. Pour les adresses IP statiques, l'utilisateur peut tout simplement utiliser l'adresse IP avec le transfert de port pour réaliser les objectifs ci-dessus sans utiliser DDNS.

DDNS : un compte doit être ouvert auprès d'un fournisseur de services DDNS tel que dyndns.com ou tzo.com. Au sein du compte, plusieurs entrées hôtes DDNS sont créées. L'administrateur doit créer un nom d'hôte DDNS pour l'adresse IP WAN du routeur. Le routeur met à jour l'entrée DDNS immédiatement par l'intermédiaire de HTTP, chaque fois que l'adresse IP change.

Transfert de port : il est important de connaître les ports de services utilisés par le serveur. Les ports de services communs, notamment le service Web ou le service de messagerie, sont prédéfinis sur le routeur afin de simplifier la configuration. Tout service personnalisé peut également être créé en se basant sur le numéro de port TCP ou UDP associé. Le transfert de port simplifie la configuration lorsque vous ne déployez pas le même service sur plusieurs serveurs.

Adresse IP LAN : nous vous recommandons de configurer le serveur interne ou la caméra IP qui utilise le transfert de port avec une adresse IP statique locale, au lieu d'obtenir l'adresse DHCP à partir du routeur. L'utilisation de l'adresse DHCP invalide la règle de transfert de port la prochaine fois que l'adresse IP change sur le périphérique interne. L'adresse IP statique configurée sur l'hôte directement ne doit pas se situer dans la même plage que le pool d'adresses DHCP.

Schéma du réseau

La Figure 1 fournit un exemple d'implémentation de DDNS et du transfert de port à l'aide d'un routeur Cisco Small Business.

Le routeur WAN reçoit son adresse dynamiquement, et le pare-feu et la traduction des adresses réseau (NAT) sont activés par défaut. Dans cet exemple, le routeur WAN est accessible par l'intermédiaire de son nom de domaine complet (FQDN) : myrv120w.dyndns.org. Pour cela, l'entrée d'hôte DDNS *myrv120w.dyndns.org* est mappée sur l'adresse IP dynamique de l'interface WAN du routeur.

Le transfert de port doit être configuré comme suit :

- Transférez le port 80 sur le port 80 du serveur Web sur le réseau local (LAN) interne (192.168.1.100).
- Transférez le port 1028 sur le port 80 d'une caméra vidéo IP 192.168.1.90.
- Transférez le protocole RTSP sur le port RTSP de la caméra vidéo.

Avec cette configuration, les ordinateurs distants et les périphériques mobiles peuvent accéder aux services internes à l'aide des navigateurs et des applications Web à partir de l'Internet public.

Configuration du service DDNS et du transfert de port sur les routeurs Cisco Small Business

Liste de contrôle de préconfiguration

Connectez le câble Ethernet entre le port WAN du routeur RV et le port Ethernet du modem DSL ou du modem câble. Mettez le routeur RV sous tension, puis connectez les ordinateurs, les serveurs et les caméras vidéo internes au commutateur LAN ou aux ports de commutation du routeur RV. Reportez-vous au document Cisco Small Business Conseils avancés relatif à la connexion d'un routeur et d'un commutateur avec les réseaux locaux virtuels (VLAN) et les jonctions, pour achever la configuration des paramètres du réseau local (LAN).

Vérifiez que les ordinateurs et les serveurs locaux protégés par le pare-feu du routeur RV peuvent communiquer entre eux et avec le routeur. Vérifiez que le serveur Web interne a l'adresse IP 192.168.1.100, et définissez l'adresse IP statique 192.168.1.90 pour la caméra vidéo IP WVC210. Reportez-vous au document *IP Video Surveillance Smart Setup Guide* pour obtenir des instructions sur la configuration de l'adresse IP de la caméra vidéo IP WVC210.

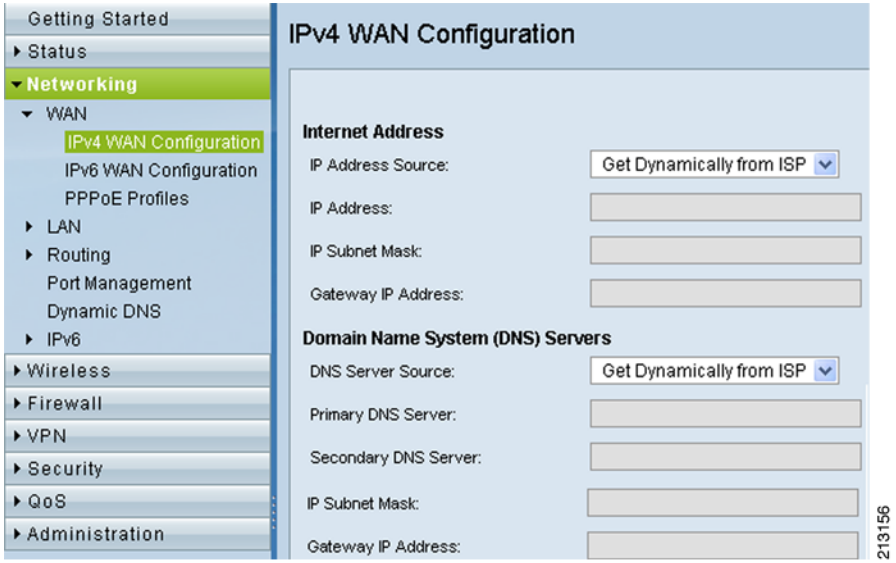
Configuration de l'accès au réseau étendu (WAN)

Le paramètre WAN par défaut du routeur RV est configuré pour obtenir son adresse IP dynamiquement de l'ISP. Le pare-feu et la traduction d'adresses réseau NAT sont également activés par défaut. Aucune configuration supplémentaire n'est requise pour activer l'accès WAN de base.

Étape 1 Accédez à **Networking > WAN > IPv4 WAN Configuration**, et vérifiez que la source d'adresse Internet et les serveurs DNS sont définis sur la valeur **Get Dynamically from ISP.**

Remarque Si l'adresse est attribuée de manière statique par l'ISP, définissez la source d'adresse IP sur la valeur Use Static IP Address, et entrez l'adresse IP spécifique, ainsi que les informations du routeur par défaut et du masque de sous-réseau fournies par l'ISP.

Figure 2 Vérification de la configuration WAN



Étape 2 Accédez à **Status > System Summary** et, dans la section **WAN information (IPv4)**, vérifiez que le routeur reçoit son adresse IP, le masque de sous-réseau, la passerelle et les informations DNS à partir de l'ISP, et que la traduction d'adresses de réseau (NAT) est activée.

Configuration des paramètres DDNS

Dans cette section, nous allons créer l'entrée DDNS *myrv120w.dyndns.org* pour le routeur WAN, et configurer ce dernier afin qu'il mette à jour cette entrée DDNS automatiquement avec son adresse IP WAN actuelle à chaque changement.

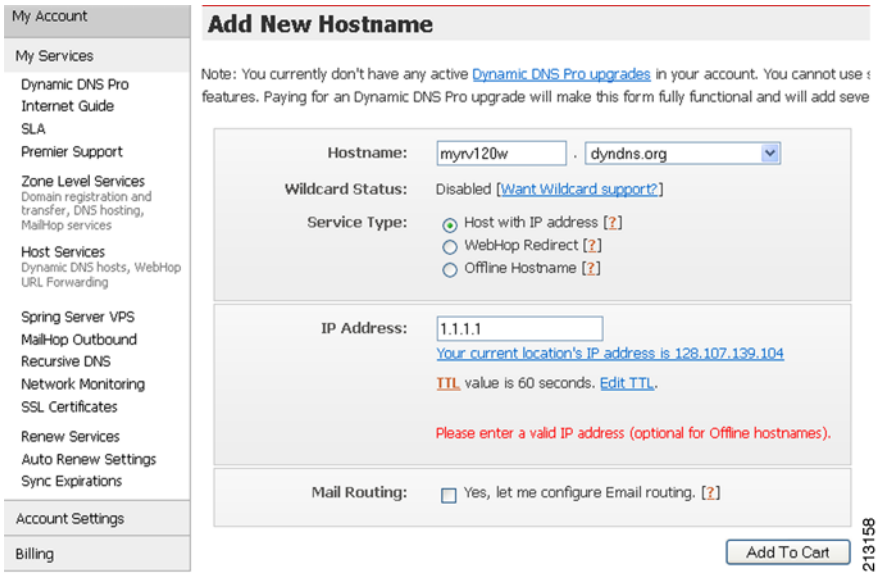
Étape 1 Configurez le compte DDNS.

1. Si vous ne disposez pas d'un compte DDNS, accédez à www.dyndns.com pour demander un compte DDNS.

Une adresse électronique valide est requise pour activer le compte. Le service de base est gratuit.

2. Lorsque le compte est approuvé et activé, connectez-vous et accédez à **My Services > My Hosts**. Cliquez sur **Add Host Service** pour créer un nom d'hôte pour le routeur RV.

Figure 3 Ajout d'un nouveau nom d'hôte sur le site Web dyndns.com



Dans cet exemple, le nom d'hôte myrv120w.dyndns.org est créé pour le routeur RV.

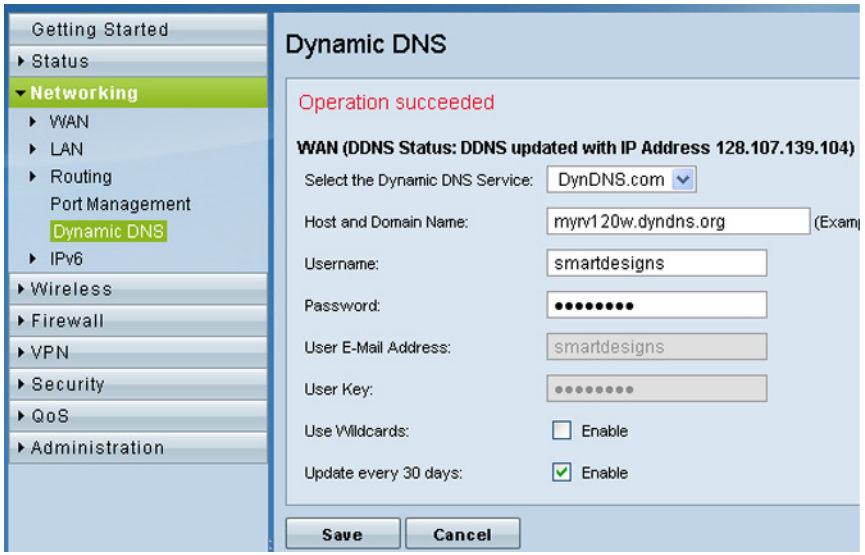
3. Saisissez une adresse IP quelconque, par exemple 1.1.1.1 pour le moment, et cliquez sur **Add to Cart** pour terminer la configuration.

Étape 2 Configurez le routeur Cisco.

1. Connectez-vous au routeur RV et accédez à **Networking > Dynamic DNS** pour sélectionner *DynDNS.com* pour le service DDNS.
2. Saisissez *myrv120w.dyndns.org* pour le nom de l'hôte et le nom du domaine, puis saisissez le nom d'utilisateur et le mot de passe de votre compte dyndns.com.
3. Cochez la case **Update every 30 days** pour configurer le routeur afin qu'il mette à jour les informations de l'hôte sur DynDNS.com et conserve l'activation de l'abonnement après la période d'essai de 30 jours.
4. Cliquez sur **Save** afin que le routeur mette à jour immédiatement l'entrée DDNS en ligne avec son adresse IP WAN actuelle.

La page de configuration de DDNS affiche les messages suivants : *Operation succeeded* et *WAN (DDNS Status: DDNS updated with IP address 128.107.139.104)*.

Figure 4 Page de configuration DDNS



Remarque Pour que les paramètres DDNS entrent en vigueur immédiatement, le routeur doit avoir une connexion Internet active. Vous pouvez également vous connecter à dyndns.com pour vérifier que l'entrée de l'hôte comporte une adresse IP mise à jour récemment.

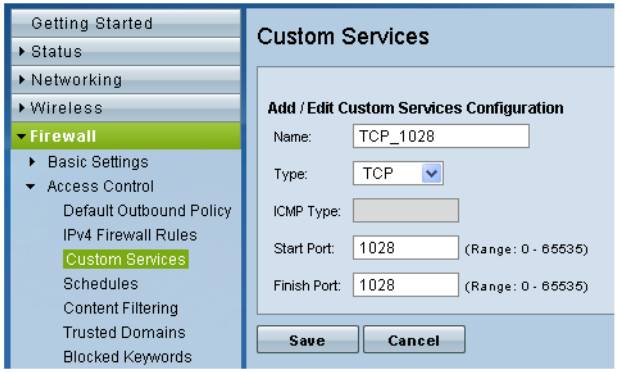
Configuration du transfert de port

Dans cette section, vous allez configurer le transfert de port pour le serveur Web interne 192.168.1.100, et une caméra vidéo IP interne avec l'adresse IP 192.168.1.90. Les utilisateurs de l'Internet public peuvent alors accéder au serveur Web en utilisant http://myrv120w.dyndns.org, et accéder à la page Web de la caméra vidéo IP à l'aide de http://myrv120w.dyndns.org:1028, ou au flux RTSP de la caméra vidéo IP directement à l'aide de rtsp://myrv120w.dyndns.org/mobile.sdp.

Étape 1 Créez un service à utiliser pour le transfert de port.

1. Accédez à **Firewall > Access Control > Custom Service**.
2. Cliquez sur **Add** pour créer un service pour le port 1028 TCP.
3. Saisissez le nom TCP_1028, spécifiez le type TCP, et configurez les ports de départ et de fin sur la valeur 1028.

Figure 5 Écran Custom Services



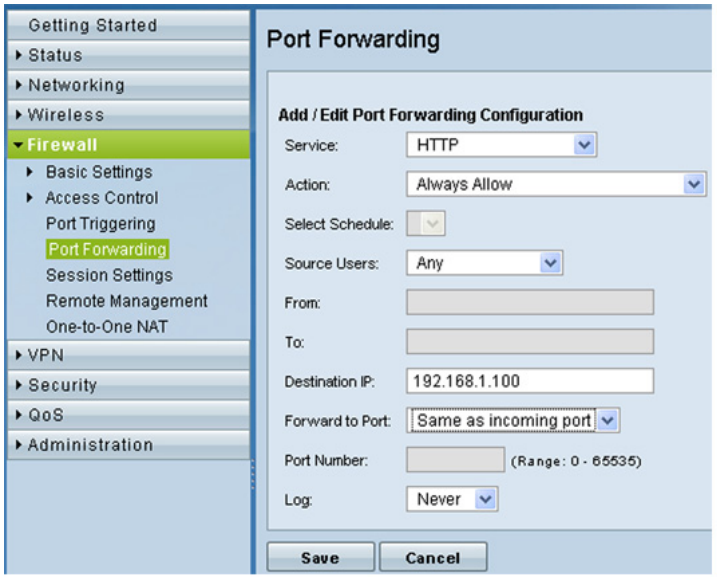
Étape 2 Ajoutez la première règle de transfert de port pour l'accès au serveur Web interne.

Après avoir créé cette règle, le trafic HTTP (port 80 TCP) est redirigé vers le port HTTP pour le serveur Web interne (192.168.1.100).

1. Accédez à **Firewall > Port Forwarding** et cliquez sur **Add**.
2. Sélectionnez **HTTP in Service,** définissez l'action sur la valeur **Always Allow**, et sélectionnez **Any** dans la liste de sélection déroulante Source Users.
3. Saisissez l'adresse IP du serveur Web interne (*192.168.1.100)* pour l'IP de destination.
4. Sélectionnez **Same as incoming port** pour le transfert vers le port, puis cliquez sur **Save**.

Une règle doit apparaître dans le récapitulatif.

Figure 6 Écran Port Forwarding



Remarque Lors de la définition des règles, la source fait référence aux utilisateurs de l'Internet public, et la destination fait référence au réseau local (LAN) interne de l'entreprise.

Étape 3 Répétez la procédure décrite à l'étape 2 pour créer la deuxième règle d'affichage de la page Web de la caméra vidéo IP.

Après avoir créé cette règle, le trafic TCP vers le port TCP 1028 est redirigé vers le port HTTP pour le serveur interne 192.168.1.90.

1. Pour cette règle, sélectionnez **TCP_1028** dans la section Service.
2. Modifiez l'action sur la valeur **Always Allow**, et sélectionnez **Any** dans la liste de sélection déroulante Source Users.
3. Saisissez l'adresse IP de la caméra (192.168.1.90), sélectionnez **Specify Port** dans la liste déroulante Forward to Port, entrez le numéro de port 80 et cliquez sur **Save**.

Étape 4 Répétez la procédure décrite à l'étape 2 pour créer la troisième règle de transfert du service RTSP : TCP vers le même port sur la caméra vidéo IP (192.168.1.90).

Après avoir terminé cette étape, l'ensemble des trois règles doit s'afficher, comme dans la Figure 7.

Figure 7 Entrées de transfert de port

Validation de la configuration

Étape 1 À partir d'un ordinateur ou d'un ordinateur portable client connecté à l'Internet public, dirigez le navigateur Web vers http://myrv120w.dyndns.org.

Le navigateur Web doit afficher le contenu du site Web interne.

Étape 2 À partir d'un ordinateur ou d'un ordinateur portable client connecté à l'Internet public, dirigez le navigateur Web vers http://myrv120w.dyndns.org:1028.

Le navigateur Web doit afficher la page Web et le flux vidéo de la caméra vidéo IP WVC210 IP.

Figure 8 Vérification du transfert de port TCP

Étape 3 À partir d'un smartphone ou d'un ordinateur portable connecté à l'Internet public, lancez un lecteur multimédia tel que le lecteur VLC sur l'ordinateur pour afficher le flux RTSP directement à partir de la caméra vidéo IP WVC en utilisant le lien RTSP://myrv120w.dyndns.org/mobile.sdp.

Remarque Pour vérifier le transfert RTSP, le flux vidéo mobile doit être déjà activé sur la caméra vidéo IP WVC210.

Figure 9 Vérification du transfert RSTP

Autres fonctionnalités associées

Zone démilitarisée

Le routeur Cisco RV prend également en charge une option de zone démilitarisée (DMZ). Une zone DMZ est un sous-réseau accessible à partir de l'Internet public, mais elle réside derrière le pare-feu. La fonction DMZ redirige les paquets destinés à une adresse IP de port WAN spécifique vers une adresse IP particulière du réseau local (LAN).

Les règles du pare-feu peuvent être configurées pour permettre l'accès aux services et aux ports spécifiques de la zone démilitarisée (DMZ) à partir du réseau local (LAN) ou de l'Internet public. Dans le cas d'une attaque éventuelle de l'un ou l'autre des nœuds DMZ, le réseau local n'est pas nécessairement affecté. La zone DMZ peut également être utilisée avec DDNS dans un scénario selon lequel un serveur unique offrant plusieurs services sur le réseau Small Business doit être accessible à partir de l'Internet public.

Translation d'adresses réseau (NAT) un-à-un

Le routeur Cisco RV prend également en charge la translation d'adresses réseau (NAT) un-à-un qui permet aux systèmes situés derrière un pare-feu avec une adresse IP privée d'apparaître comme s'ils utilisaient des adresses IP publiques. La translation d'adresses réseau (NAT) un-à-un peut être utilisée lorsque l'ISP fournit un pool d'adresses IP publiques statiques. Elle mappe l'adresse privée de chaque serveur derrière le pare-feu à une adresse IP publique unique. Cette solution est simple lorsque l'entreprise dispose d'une connexion haut débit de type T1 ou professionnelle. Le coût de ces services est en général plus élevé. Toutefois, la translation d'adresses réseau (NAT) un-à-un est nécessaire lorsque plusieurs serveurs utilisent le même port, notamment lorsque plusieurs serveurs Web accèdent au port 80.