

Activer la protection Web pour le filtrage des URL sur les routeurs VPN RV016 et RV082

Objectif

Cisco ProtectLink Web est une mesure de sécurité qui bloque le spam, le contenu indésirable et les logiciels espions. Cela est utile lorsque vous utilisez Internet. Avant que votre navigateur ne visite une URL, Cisco ProtectLink Web vérifie le site Web et bloque toute menace pour la sécurité.

L'une des fonctionnalités de Cisco ProtectLink Web est qu'un utilisateur peut créer une liste d'URL approuvées. La protection Web pour les URL est une fonctionnalité qui permet de bloquer l'accès aux sites Web en fonction de catégories prédéfinies. Cet article explique comment configurer la protection Web pour l'URL sur les routeurs VPN RV082.

Périphériques pertinents

- RV082

Version du logiciel

- v 4.2.2.08

Filtre URL

Remarque : avant de commencer la configuration, assurez-vous que l'accès ProtectLink est activé sur le périphérique. Suivez les étapes mentionnées dans le document ProtectLink Web Registration and Activation on the RV082 VPN Routers pour activer ProtectLink.

Étape 1. Connectez-vous à l'utilitaire de configuration Web et choisissez Cisco ProtectLink Web > Web Protection. La page Web Protection s'ouvre :

Web Protection

Enable URL Filtering

Enable Web Reputation

URL Filtering

URL Categories	Business Hours	Leisure Hours	Instances Blocked
+ Adult	<input type="checkbox"/>	<input type="checkbox"/>	
+ Business	<input type="checkbox"/>	<input type="checkbox"/>	
+ Computers/Bandwidth	<input type="checkbox"/>	<input type="checkbox"/>	
+ Computers/Harmful	<input type="checkbox"/>	<input type="checkbox"/>	
+ Computers/Communication	<input type="checkbox"/>	<input type="checkbox"/>	
+ General	<input type="checkbox"/>	<input type="checkbox"/>	
+ Social	<input type="checkbox"/>	<input type="checkbox"/>	

Étape 2. Cochez la case Enable URL Filtering pour activer le filtrage des URL.

Étape 3. Cochez la case Business Hours des catégories et sous-catégories que vous souhaitez bloquer pendant les heures d'ouverture. Pour afficher les sous-catégories, cliquez sur le bouton + en regard d'une catégorie. Les heures d'ouverture sont définies dans la section Paramètres des heures d'ouverture.

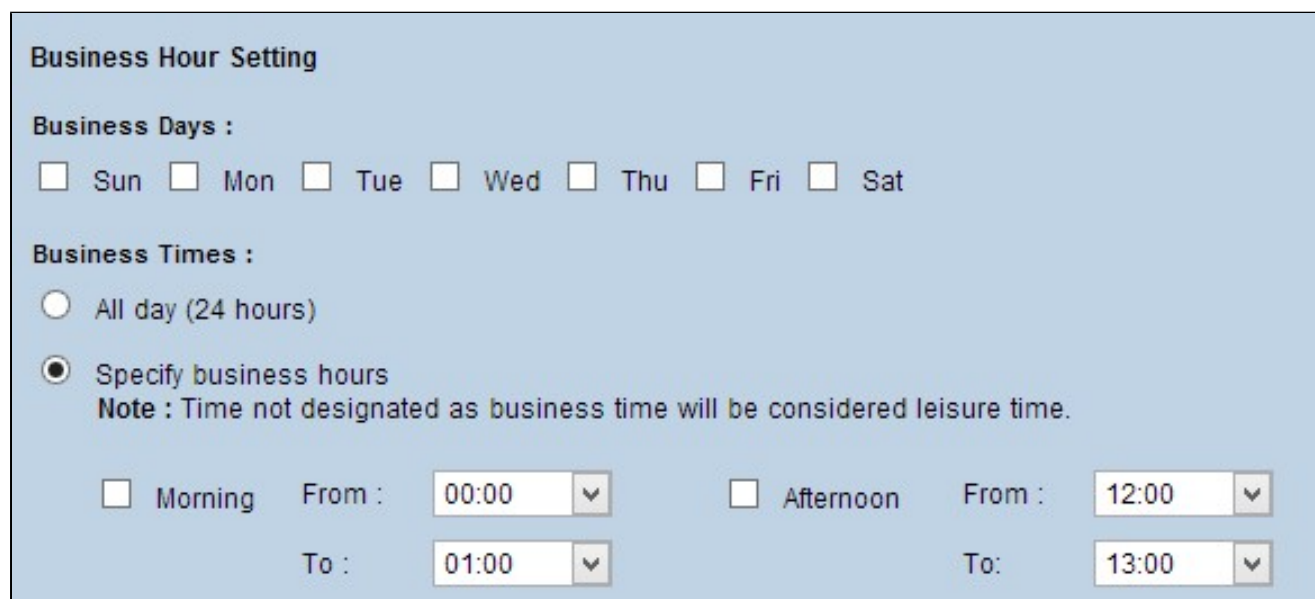
Étape 4. Cochez la case Leisure Hours des catégories et sous-catégories que vous souhaitez bloquer pendant les heures de loisir. Les heures de loisir sont définies comme n'importe quelle heure en dehors des heures d'ouverture spécifiées.

Étape 5. Cliquez sur Save pour enregistrer les modifications ou sur Cancel pour annuler les modifications.

Paramètres des heures ouvrables

Faites défiler la page jusqu'à la section Paramètres des heures d'ouverture de la page Protection Web, où vous pouvez déterminer quelles heures sont considérées comme des heures d'ouverture et quelles heures sont considérées comme des heures de loisir. Toute heure non prise en compte des heures d'ouverture sera considérée comme des heures de loisirs.

Étape 1. Dans le champ Jours ouvrables, sélectionnez les jours auxquels vous souhaitez appliquer les filtres d'URL des heures ouvrables.



The screenshot shows a configuration panel titled "Business Hour Setting". It contains two main sections: "Business Days" and "Business Times".

Business Days : A row of seven checkboxes labeled Sun, Mon, Tue, Wed, Thu, Fri, and Sat, all of which are currently unchecked.

Business Times : This section has two radio button options: "All day (24 hours)" (unchecked) and "Specify business hours" (checked). Below the "Specify business hours" option is a note: "Note : Time not designated as business time will be considered leisure time."

Under the "Specify business hours" section, there are two columns of settings. The first column is for "Morning" (checkbox unchecked) and includes "From : 00:00" and "To : 01:00" dropdown menus. The second column is for "Afternoon" (checkbox unchecked) and includes "From : 12:00" and "To : 13:00" dropdown menus.

Étape 2. Dans le champ Business Times, cliquez sur la case d'option correspondant à la méthode que vous souhaitez utiliser pour déterminer les heures d'ouverture. Les options disponibles sont les suivantes :

- Toute la journée (24 heures) — Appliquer le filtrage des heures ouvrables pour toute la journée.
- Spécifier les heures d'ouverture — Définissez manuellement la période pour laquelle le filtrage des heures d'ouverture s'applique.

Étape 3. Si l'option Spécifier les heures d'ouverture est sélectionnée, cochez la case Matin et choisissez les heures de début et de fin dans les listes déroulantes pour spécifier les heures d'ouverture le matin. Cochez la case Afternoon et choisissez les heures de début et de fin dans les listes déroulantes pour spécifier les heures d'ouverture de l'après-midi.

Étape 4. Cliquez sur Save pour enregistrer les modifications ou sur Cancel pour annuler les modifications.

Réputation Web

La réputation de sites Web vous aide à prévenir les menaces contre les sites Web potentiellement malveillants. Il vérifie les sites Web à partir de la base de données Cisco ProtectLink Web Security.

Étape 1. Cochez la case Enable Web Reputation pour activer la réputation Web.

Web Protection

Enable URL Filtering

Enable Web Reputation

URL Filtering

URL Categories	Business Hours	Leisure Hours	Instances Blocked
+ Adult	<input type="checkbox"/>	<input type="checkbox"/>	
+ Business	<input type="checkbox"/>	<input type="checkbox"/>	
+ Computers/Bandwidth	<input type="checkbox"/>	<input type="checkbox"/>	
+ Computers/Harmful	<input type="checkbox"/>	<input type="checkbox"/>	
+ Computers/Communication	<input type="checkbox"/>	<input type="checkbox"/>	
+ General	<input type="checkbox"/>	<input type="checkbox"/>	
+ Social	<input type="checkbox"/>	<input type="checkbox"/>	

Reset Counters

Étape 2. Faites défiler jusqu'au champ Réputation Web et cliquez sur la case d'option du niveau de sécurité approprié.

Web Reputation

Security level :

High Blocks a greater number of Web threats but increases the risk of false positives.

Medium Blocks most Web threats and does not create too many false positives. This is the recommended setting.

Low Blocks fewer Web threats but reduces the risk of false positives.

- Élevé - Cette option bloque un nombre plus élevé de sites Web potentiellement malveillants, mais présente également une incidence plus élevée de faux positifs (sites légitimes classés comme malveillants).
- Moyen - Cette option bloque la plupart des sites Web potentiellement malveillants et présente une incidence plus faible de faux positifs. Le paramètre recommandé est Medium.
- Faible - Cette option bloque moins de sites Web potentiellement malveillants et réduit

donc le risque de faux positifs.

Étape 3. Cliquez sur Save pour enregistrer les modifications ou sur Cancel pour annuler les modifications.

Contrôle de débordement d'URL

Dans le champ Contrôle de débordement d'URL, vous pouvez déterminer l'action à entreprendre lorsqu'il y a plus de demandes d'URL que le service ne peut traiter.

Étape 1. Sélectionnez la case d'option correspondant à l'action que ProtectLink doit effectuer en cas de dépassement de capacité. Les options disponibles sont les suivantes :

- Bloquer temporairement les requêtes d'URL : ce paramètre est recommandé et par défaut. Il bloque toutes les requêtes d'URL jusqu'à ce qu'elles soient traitées.
- Contourner temporairement la vérification des URL demandées — Cette option permet de transmettre toutes les demandes sans vérification. Ce paramètre n'est pas recommandé.



The image shows a dialog box titled "URL Overflow Control" with a light blue background. It contains two radio button options. The first option, "Temporarily block URL requests(This is the recommended setting)", is selected with a black dot. The second option, "Temporarily bypass Cisco ProtectLink URL Filtering for requested URLs", is unselected with a white dot. At the bottom of the dialog, there are two buttons: "Save" and "Cancel".

Étape 2. Cliquez sur Save pour enregistrer les modifications ou sur Cancel pour annuler les modifications.

À propos de cette traduction

Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.