Stratégie de contrôle d'accès par défaut sur le routeur VPN CVR100W

Objectif

La stratégie de contrôle d'accès permet à l'utilisateur de décider si les informations du périphérique sont partagées ou non. Cette fonctionnalité peut désactiver la communication entre le réseau local sécurisé et le réseau étendu non sécurisé. Un utilisateur souhaite limiter l'accès via cette stratégie s'il estime que les informations transmises via le WAN ne sont pas sécurisées.

Cet article explique comment configurer la stratégie de contrôle d'accès par défaut sur le routeur VPN CVR100W.

Périphérique applicable

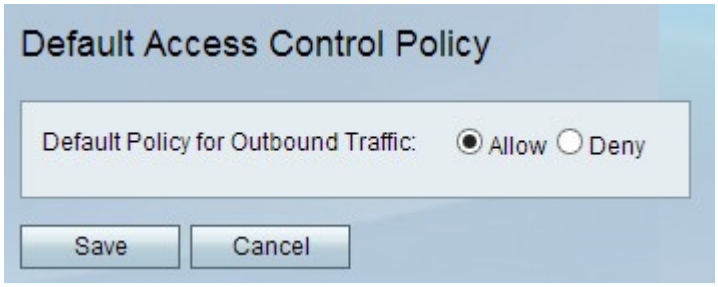
·CVR100W

Version du logiciel

•1.0.1.19

Stratégie de contrôle d'accès par défaut

Étape 1. Connectez-vous à l'utilitaire de configuration Web et choisissez **Firewall > Access Control > Default Access Control Policy**. La page *Stratégie de contrôle d'accès par défaut* s'ouvre :



Étape 2. Choisissez l'une des options suivantes dans le champ *Stratégie par défaut pour le trafic sortant* :

·Allow : permet à toutes les informations de traverser le WAN et de quitter le système si nécessaire. Pour garder les informations moins sécurisées mais plus faciles d'accès, cliquez sur la case d'option **Autoriser**.

·Refuser : refuse que les informations transitent par le port WAN et laisse le système pour conserver les informations sous le niveau de sécurité le plus élevé possible. Les hôtes du port LAN peuvent toujours communiquer même si le port WAN est désactivé. Si vous doutez de la sécurité des informations sortantes, cliquez sur la case d'option **Refuser**.

Étape 4. Click **Save**.