Contenu

Introduction

La caractéristique de Seveur mandataire d'authentification permet à des utilisateurs pour ouvrir une session à un réseau ou accéder à l'Internet par l'intermédiaire du HTTP, avec leur accès spécifique profile automatiquement récupéré et appliqué à partir d'un serveur TACACS+ ou de RAYON. Les profils utilisateurs sont en activité seulement quand il y a du trafic actif des utilisateurs authentifiés.

Cette configuration est conçue pour évoquer le navigateur Web sur 10.1.1.1 et pour le viser chez 10.17.17.17. Puisque le client vpn est configuré pour passer par le point final 10.31.1.111 de tunnel pour obtenir au réseau 10.17.17.x, le tunnel d'IPSec est construit et le PC obtient l'adresse IP hors du groupe RTP-POOL (puisque la configuration de mode est exécutée). L'authentification est alors demandée par le routeur de Cisco 3640. Après que l'utilisateur écrive un nom d'utilisateur et mot de passe (enregistré sur le serveur TACACS+ à 10.14.14.3), la liste d'accès passée vers le bas du serveur obtient ajouté à la liste d'accès 118.

Conditions préalables

Conditions requises

Avant de tenter cette configuration, assurez-vous que vous répondez à ces exigences :

- Le Client VPN Cisco est configuré pour établir un tunnel d'IPSec avec le routeur de Cisco 3640.
- Le serveur TACACS+ est configuré pour le Seveur mandataire d'authentification. Voyez les informations relatives