

Contenu

[Question](#)

Question

Comment est-ce que je configure l'usurpation d'adresse IP ?

Environnement : Appliance de sécurité Web de Cisco (WSA), toutes les versions d'AsyncOS

Abrégé :

Dans le déploiement traditionnel de proxy l'adresse IP du client est remplacé par celui du serveur de proxy/cache. Tandis que ceci fournit la Sécurité inhérente en masquant l'adresse de l'utilisateur final, applications Web dans certains cas certaines exigent l'accès à l'adresse IP du client de commencement.

En mettant en application la caractéristique de « usurpation d'adresse IP » dans l'appliance de sécurité Web de Cisco (WSA) et en configurant les groupes de service appropriés WCCP sur un périphérique de Cisco IOS, il est possible de présenter l'adresse IP du client aux applications Web au lieu de l'adresse IP de WSA. Le document suivant décrit les étapes nécessaires de configuration pour cette implémentation.

Description :

Pour implémenter la caractéristique de « usurpation d'adresse IP », deux seuls groupes de service WCCP ont dû être créés sur un routeur de Cisco IOS®. Le premier groupe de « Web-cache » WCCP réoriente le HTTP/trafic du port 80 de l'utilisateur au WSA. Des listes spécifiques de contrôle d'accès peuvent être configurées (suivant les indications de l'exemple ci-dessous) pour contrôler quels utilisateurs sont protégés par l'appliance de sécurité Web de Cisco. L'interface utilisateur sur le routeur est configurée pour réorienter le trafic d'arrivée à ce groupe de service WCCP.

Le deuxième groupe de service WCCP doit être défini comme ID de service dynamique (dites l'ID de service 95). De nouveau une liste d'accès est utilisée pour contrôler quels utilisateurs sont protégés (c.-à-d. tenez compte de sauter du système totalement). Pour le trafic web de retour, l'interface extérieure sur le routeur est configurée pour réorienter son trafic d'arrivée au groupe de service WCCP 95.