Contenu

Introduction

Ce document décrit un problème qui est produit sur l'appliance de sécurité Web de Cisco (WSA) quand l'avertissement, l'accusé de réception, ou les pages de la notification d'utilisateur final (EUN) n'affichent pas correctement pour des demandes explicites HTTPS. Un contournement pour ce problème est également fourni.

Conditions préalables

Conditions requises

Les informations dans ce document supposent cela :

- Les adresses de proxy WSA sont déployées en mode explicite.
- Les demandes HTTPS ou sont bloquées, averti, ou exigez l'accusé de réception d'utilisateur.

Composants utilisés

Les informations dans ce document sont basées sur Cisco WSA.

Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est opérationnel, assurez-vous que vous comprenez l'effet potentiel de toute commande.

Problème

L'avertissement, l'accusé de réception, ou les pages EUN n'affichent pas correctement pour des demandes explicites HTTPS. Le navigateur affiche une page inachevée de notification, ou elle n'affiche pas la page du tout et affiche à la place une page d'erreur.

Il y a plusieurs questions qui entourent ces pages quand vous utilisez des demandes explicites HTTPS. Quand vous configurez votre navigateur pour utiliser un proxy, le trafic HTTPS est dirigé

vers le WSA au-dessus du HTTP. Cette demande est formatée comme HTTPS au-dessus de HTTP.

Il y a deux problèmes connus avec les navigateurs qui ne manipulent pas correctement les réponses de HTTP que le WSA renvoie pour des demandes explicites HTTPS. Quand une demande explicite HTTPS est bloquée, averti, ou exige l'accusé de réception d'utilisateur, le WSA renvoie code d'état 403. Dans cette réponse, le WSA inclut le contenu de notification qui devrait normalement être rendu sur l'écran de sorte qu'il soit visualisable. Cependant, dans certains cas, le navigateur ne peut pas comprendre la réponse dans le contenu retourné.
C'est le comportement du navigateur qui est observé :

- Quand la version 6 (IE6) d'Internet Explorer et quelques versions d'IE7 sont utilisées, ces demandes ne rendent pas le plein contenu de la réponse HTML. Le navigateur honore seulement les octets premiers (le contenu dans le premier paquet) et ignore le repos. En pareil cas, vous voyez une page inachevée qui affiche seulement quelques caractères. Remarque: Si c'est le cas, Cisco recommande que vous rétrécissiez la page par défaut de notification de la réponse WSA. Pour plus d'informations sur la façon éditer votre page EUN, référez-vous à la section **éditante de pages de notification d'IronPort du guide utilisateur WSA**.
- Quand IE8 et plus nouvelles versions de version 3 de Mozilla Firefox sont utilisés, le programme de lecture ignore complètement la réponse que le WSA la renvoie et masque avec sa propre page d'erreur. Ce comportement du navigateur défait le but de la notification 403 et entraîne l'interruption avec la configuration.

Solution

Cette section décrit le processus qui se produit quand le déchiffrement HTTPS est activé sur le WSA. Comme contournement au problème précédemment décrit, utilisez les informations fournies afin de s'assurer que votre système est configuré en conséquence.

Voici un exemple de la circulation quand une demande explicite HTTPS est envoyée :

- Quand le déchiffrement HTTPS est activé, le WSA valide d'abord la demande contre les stratégies de déchiffrement.

- Si la demande est marquée pour la **FONCTION ÉMULATION**, alors on permet le trafic (aucun avertissement ou EUN).

- Si la demande est marquée en tant que **DÉCHIFFRÉ**, alors la demande est validée contre les stratégies d'Access. Dans ce cas, si la stratégie d'Access est configurée afin d'**AVERTIR** ou **BLOQUER**, puis la page EUN affiche correctement. Malheureusement, parce que accusé de réception que l'utilisateur doit naviguer vers la page de HTTP et reconnaître, qui exige la navigation par le proxy et puis au site HTTPS.

- Le WSA se souvient l'adresse IP de client et n'exige pas un autre accusé de réception jusqu'à ce que le temporisateur expire.