Utilisant le GREP pour filtrer les logs d'accès

Contenu

Question :

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

Comment est-ce que je peux rechercher l'accès ouvre une session l'appliance de série S ?

De l'interface de ligne de commande de l'appliance de sécurité Web de Cisco, vous pouvez utiliser la commande de **grep** de filtrer les logs d'accès et de déterminer ce qui est bloqué. Voici un exemple pour prouver à tout qu'est bloqué :

TestS650.wsa.com () **> grep**

Logs actuellement configurés :
1. type de « accesslogs » : « Access se connecte » la récupération : Balayage de FTP
<… >
18. type de « welcomeack_logs » : « Logs d'accusé de réception d'écran de bienvenue »
Récupération : Balayage de FTP

Introduisez le nombre du log que vous souhaitez au grep.
[] **> 1**

Écrivez l'expression régulière au grep.
[] **> BLOCK_**

Voulez-vous que cette recherche soit-elle ne distinguant pas majuscules et minuscules ? [Y] **> n**

Voulez-vous suivre les logs ? [N] **> n**

Voulez-vous paginer la sortie ? [N] **> n**

(des entrées seront affichées)

Pour la question d'expression régulière, vous pouvez écrire **BLOCK_** (sans devis) pour prouver à chaque demande que WSA a bloqué. (Avertissant : cette liste peut être très longue).

Vous pouvez également écrire des parties d'URL de site si vous voulez afficher de longues entrées d'accès liées à un site spécifique. Par exemple - Écrire le **windowsupdate** pour l'expression régulière t'affichera toutes les entrées de journal d'accès contenant l'URL de Windows

Update de windowsupdate.microsoft.com.

Obtenant un peu plus avancé, si vous vouliez afficher les entrées de journal d'accès pour un site avec le windowsupdate dans l'URL, qui ont été également bloquées, vous pourriez utiliser l'expression régulière **windowsupdate.*BLOCK_**.