Comment bloquez-vous des applications inconnues sur l'appliance de sécurité Web de Cisco ?

Contenu

Question

Comment bloquez-vous des applications inconnues sur l'appliance de sécurité Web de Cisco ?

Remarque: Cet article de la base de connaissances met en référence le logiciel qui n'est pas mis à jour ou est pris en charge par Cisco. Les informations sont données comme courtoisie pour votre commodité. Pour davantage d'assistance, contactez s'il vous plaît le fournisseur de logiciels.

1. La première défense est d'employer des chaînes « d'agent d'utilisateur » pour bloquer de telles applications. Puisque nous ne connaissons pas tous les utilisateur-agents pour des ces application, vous devrez les rechercher sur les liens ci-dessous.
   Nous pouvons ajouter le « Utilisateur-agent » sous le ***gestionnaire de sécurité Web > les stratégies d'Access > les protocoles et le*** <for de la colonne d'***agents d'utilisateur le*** policy> prié d'accès.--**>** ajoutez la chaîne d'agent d'utilisateur sous ***« les agents d'utilisateur faits sur commande de bloc : »*** (un par la ligne).

2. Si les contrôles de visibilité d'application (AVC) sont activés *(sous GUI > Services de sécurité > réputation et Anti-malware de Web)*, alors nous pouvons bloquer accès basé sur sur des types d'application comme des proxys, partage de fichier, des utilitaires d'Internet. Nous pouvons faire ceci dans le cadre du ***gestionnaire de sécurité Web > des stratégies d'Access > <for de colonne de « applications » le policy> prié d'accès***.
3. Si l'agent d'utilisateur n'existe pas, vous pouvez tenter d'ajouter le type MIME (exemple *:* applications de torrents de bit).
   Nous pouvons ajouter des types « MIME » *sous le <for de colonne de* ***gestionnaire de sécurité Web*** *>* ***de stratégies*** *>* ***d'objets d'accès au Web le*** *policy> prié d'accès.------>* ajoutez dans l'objet/pantomime saisissent **« la** section des **types MIME faits sur commande de bloc** comme application/x-bittorrent (un par la ligne).

4. Assurez-vous que les catégories comme la manière d'éviter de filtre, des activités illégales sont bloquées dans des stratégies d'accès. Si quelques applications utilisent l'URLs connu ou les adresses IP pour leurs connexions, alors nous pouvons bloquer leurs catégories assocaited URL de prédéfinis ou les configurer dans une catégorie faite sur commande bloquée URL utilisant leur adresse IP, FQDN, ou une expression régulière appariant les domaines. Nous pouvons faire ceci *dans le cadre du* ***gestionnaire de sécurité Web > des***

stratégies d'Access > colonne ***« de catégories URL »***.

5. Quelques applications peuvent utiliser le HTTP CONNECTENT la méthode pour se connecter à différents ports. Laissez seulement su que les ports ou les ports de particularité requis dans votre environnement dans le HTTP CONNECTENT des domaines de configuration de ports.
   Le HTTP CONNECT peut être configuré *sous le* ***gestionnaire de sécurité Web > les stratégies d'Access > les protocoles et le*** *<for de la colonne d'****agents d'utilisateur le*** *policy> exigé d'accès*.--**> les** ports permis Add sous le **« HTTP CONNECTENT des ports : "**

6. Pour des applications où vous savez seulement des adresses IP de destination étant accédées à, vous pouvez employer la caractéristique de moniteur du trafic L4 pour bloquer l'accès pour l'adresse IP intéressée. Nous pouvons ajouter la destination IPS *sous le* ***gestionnaire de sécurité Web >*** *le* ***moniteur du trafic L4 >*** *des* ***adresses suspectées supplémentaires de malware.***

Si vous êtes inconscient dont le type d'agent » ou « de pantomime » de « utilisateur est utilisé par certaines applications, alors vous pouvez faire l'un ou l'autre du suivant pour trouver ces informations :

- Exécutez une capture de paquet avec WireShark (éthéré) sur l'ordinateur et le filtre de client pour le protocole de « HTTP ».
- Exécutez la capture sur WSA (sous la capture de « support et d'aide » **>** « de paquet »), filtré sur l'adresse IP du client.

Liste d'agents d'utilisateur :
==========
http://www.user-agents.org/

Liste de types MIME :
==========
http://www.webmaster-toolkit.com/mime-types.shtml

http://www.microsoft.com/technet/isa/2004/plan/commonapplicationsignatures.mspx