Comment bloquer le trafic de messagerie instantanée (IM) sur l'appliance de sécurité Web de Cisco ?

Contenu

Question :

Comment bloquer le trafic ou IM de messagerie instantanée (IM) conversation sur l'appliance de sécurité Web de Cisco ?

Environnement :

Appliance de sécurité Web de Cisco (WSA) exécutant la version 7.1.x et ultérieures d'AsyncOS

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.

Le trafic instantané de Messaing (IM) au-dessus du HTTP peut être bloqué aujourd'hui des manières suivantes :

- Bloc en définissant les agents d'utilisateur faits sur commande utilisés par les applications IM.
- Le bloc avec la **« conversation et la messagerie instantanée » a prédéfini la catégorie URL**, ou avec une catégorie faite sur commande contenant les serveurs IM (GUI > gestionnaire de sécurité Web > stratégies > Filtrage URL d'Access)
- Bloquez les applications IM requises sous le **type d'application AVC de « messagerie instantanée »** *(GUI > gestionnaire de sécurité Web > stratégies > applications d'Access)*
- Bloquez les ports que l'utilisation des applications IM de percer un tunnel par des proxys avec le HTTP CONNECTENT la méthode.
- Ajoutez manuellement les serveurs IM dans la liste de noir de moniteur du trafic L4 pour bloquer l'accès aux destinations IM populaires indépendamment du port.

MSN Messenger
1. Sous le **GUI > le gestionnaire de sécurité Web > les stratégies d'Access** cliquent sur en fonction des **objets** 2. Spécifiez les **types MIME faits sur commande de bloc** de dessous suivant : *application/x-msn-messenger*
Instant Messenger de Yahoo

1. Créez une catégorie faite sur commande dans le **gestionnaire de sécurité Web > des catégories faites sur commande URL**
2. Spécifiez les **sites** de dessous suivants : *pager.yahoo.com, shttp.msg.yahoo.com, update.messenger.yahoo.com, update.pager.yahoo.com*
3. Placez cette catégorie faite sur commande pour bloquer.

AOL Instant Messenger

1. Créez une catégorie faite sur commande dans le **gestionnaire de sécurité Web > des catégories faites sur commande URL**
2. Spécifiez les **sites** de dessous suivants : *login.oscar.aol.com, login.messaging.aol.com, 64.12.161.153, 64.12.161.185, 64.12.200.89, kdc.gkdc.uas.aol.com, 205.188.0.0/16*
3. Placez cette catégorie faite sur commande pour bloquer.

Google Chat

1. Créez une catégorie faite sur commande dans le **gestionnaire de sécurité Web - > des catégories faites sur commande URL**
2. Spécifiez l'**avancé** de dessous suivant **: Expressions régulières** : *messagerie* \ *.google* \ *.com/messagerie/canal*
3. Placez cette catégorie faite sur commande pour bloquer.

Google Chat (autre méthode)

1. Créez une catégorie faite sur commande dans le **gestionnaire de sécurité Web - > des catégories faites sur commande URL**
2. Spécifiez les **sites** de dessous suivants : *.chatenabled.mail.google.com, chatenabled.mail.google.com, 216.239.37.125, 72.14.253.125, 72.14.217.189, 209.85.137.125*
3. Placez cette catégorie faite sur commande pour bloquer.

Vous pouvez également bloquer Google Talk en bloquant le « Utilisateur-agent : Google Talk »

D'autres liens utiles :

http://csshyamsundar.wordpress.com/2007/03/07/blocking-google-talk-in-your-organization/
http://support.microsoft.com/kb/925120/en-us