# Comment bloquer le trafic de messagerie instantanée sur l'appareil de sécurité Web Cisco ?

## Contenu



## Question :

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

### Environnement :

Appareil de sécurité Web Cisco (WSA) exécutant AsyncOS version 7.1.x et ultérieure

**Note: Cet article de la base de connaissances se rapporte à un logiciel qui n'est pas mis à jour ou pris en charge par Cisco. Les informations sont fournies comme courtoisie pour votre commodité. Pour plus d'assistance, communiquez avec le fournisseur du logiciel.**

Le trafic de messagerie instantanée via HTTP peut être bloqué aujourd'hui de la manière suivante :

- Bloquer en définissant les agents utilisateur personnalisés utilisés par les applications de messagerie instantanée.
- Bloquer avec la **catégorie d'URL prédéfinie « Chat and Instant Messaging »**, ou avec une catégorie personnalisée contenant des serveurs de messagerie instantanée (GUI > Gestionnaire de sécurité Web > Stratégies d'accès > Filtrage d'URL)
- Bloquer les applications de messagerie instantanée requises sous le type d'**application** AVC **« Messagerie instantanée »** *(GUI > Gestionnaire de sécurité Web > Politiques d'accès > Applications)*
- Bloquer les ports que les applications de messagerie instantanée utilisent pour effectuer un tunnel via des proxy avec la méthode HTTP CONNECT.
- Ajoutez manuellement des serveurs de messagerie instantanée à la liste noire du Moniteur du trafic de couche 4 pour bloquer l'accès aux destinations de messagerie instantanée les plus courantes, quel que soit le port.

| **MSN Messenger** |
| --- |
| 1. Sous **GUI > Web Security Manager > Access Policies** cliquez sur **des objets**<br>2. Spécifiez ce qui suit sous **Bloquer les types MIME personnalisés** : *application/x-msn-* |

| |
|---|
| *messenger* |
| **Messagerie instantanée Yahoo** |
| 1. Créer une catégorie personnalisée dans **Web Security Manager > Catégories d'URL personnalisées**<br>2. Spécifiez les éléments suivants sous **Sites** : *pager.yahoo.com, shttp.msg.yahoo.com, update.messenger.yahoo.com, update.pager.yahoo.com*<br>3. Définissez cette catégorie personnalisée sur Bloquer. |

| |
|---|
| **AOL Instant Messenger** |
| 1. Créer une catégorie personnalisée dans **Web Security Manager > Catégories d'URL personnalisées**<br>2. Spécifiez les éléments suivants sous **Sites** : *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*<br>3. Définissez cette catégorie personnalisée sur Bloquer. |
| **Chat Google** |
| 1. Créer une catégorie personnalisée dans **Web Security Manager -> Catégories d'URL personnalisées**<br>2. Spécifiez ce qui suit sous **Avancé : Expressions régulières** : *mail\.google\.com/mail/channel*<br>3. Définissez cette catégorie personnalisée sur Bloquer. |
| **Google Chat (méthode alternative)** |
| 1. Créer une catégorie personnalisée dans **Web Security Manager -> Catégories d'URL personnalisées**<br>2. Spécifiez les éléments suivants sous **Sites** : *.chatenabled.mail.google.com, chatenabled.mail.google.com, 216.239.37.125, 72.14.253.125, 72.14.217.189, 209.85.137 125*<br>3. Définissez cette catégorie personnalisée sur Bloquer.<br>**Vous pouvez également bloquer Google Talk en bloquant « User-Agent : Google Talk »** |

Autres liens utiles :

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