

¿Cómo se bloquea el tráfico de mensajería instantánea (IM) en el dispositivo Cisco Web Security?

Contenido

[Pregunta:](#)

[Entorno:](#)

Pregunta:

¿Cómo se bloquea el tráfico de mensajería instantánea (IM) o el chat de mensajería instantánea en el dispositivo Cisco Web Security?

Entorno:

Dispositivo de seguridad Cisco Web Security Appliance (WSA) que ejecuta AsyncOS versión 7.1.x y posterior

Nota: Este artículo sobre Base de conocimiento hace referencia a software que no es mantenido ni soportado por Cisco. La información se proporciona como cortesía para su conveniencia. Para obtener asistencia adicional, comuníquese con el proveedor de software.

El tráfico de mensajería instantánea (IM) a través de HTTP se puede bloquear hoy de las siguientes maneras:

- Bloquear mediante la definición de agentes de usuario personalizados que utilizan las aplicaciones de IM.
- Bloquear con la "**categoría de URL predefinida de Chat y Mensajería Instantánea**", o con una categoría personalizada que contenga servidores de mensajería instantánea (GUI > Administrador de seguridad web > Políticas de acceso > Filtrado de URL)
- Bloquee las aplicaciones de mensajería instantánea necesarias en el tipo de aplicación "**Mensajería instantánea**" AVC (GUI > Administrador de seguridad web > Políticas de acceso > Aplicaciones)
- Bloquee los puertos que las aplicaciones de IM utilizan para tunelizar a través de proxies con el método HTTP CONNECT.
- Agregue manualmente los servidores IM a la lista negra del monitor de tráfico L4 para bloquear el acceso a destinos de IM populares independientemente del puerto.

MSN Messenger
1. En GUI > Web Security Manager > Access Policies haga clic en objetos
2. Especifique lo siguiente en Bloquear tipos MIME personalizados: <i>application/x-msn-</i>

messenger

Yahoo Instant Messenger

1. Crear una categoría personalizada en **Web Security Manager > Categorías de URL personalizadas**
2. Especifique lo siguiente en **Sitios**: *pager.yahoo.com, shttp.msg.yahoo.com, update.messenger.yahoo.com, update.pager.yahoo.com*
3. Establezca esta categoría personalizada en Block (Bloquear).

AOL Instant Messenger

1. Crear una categoría personalizada en **Web Security Manager > Categorías de URL personalizadas**
2. Especifique lo siguiente en **Sitios**: *login.oscar.aol.com, login.messages.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. Establezca esta categoría personalizada en Block (Bloquear).

Chat de Google

1. Crear una categoría personalizada en **Web Security Manager -> Categorías de URL personalizadas**
2. Especifique lo siguiente en **Avanzado: Expresiones normales**:
mail.google.com/mail/channel
3. Establezca esta categoría personalizada en Block (Bloquear).

Google Chat (método alternativo)

1. Crear una categoría personalizada en **Web Security Manager -> Categorías de URL personalizadas**
2. Especifique lo siguiente en **Sitios**: *.chatenenabled.mail.google.com, chatencapabilities.mail.google.com, 216.239.37.125, 72.14.253.125, 72.14.217.189, 209.85.137.0, 125*
3. Establezca esta categoría personalizada en Block (Bloquear).

También puede bloquear Google Talk bloqueando "User-Agent: Google Talk"

Otros enlaces útiles:

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