¿Cómo bloquear el tráfico de la Mensajería inmediata (IM) en el dispositivo de seguridad de la red de Cisco?

Contenido

Pregunta:

¿Cómo bloquear el tráfico o IM de la Mensajería inmediata (IM) charla en el dispositivo de seguridad de la red de Cisco?

Entorno:

Versión 7.1.x y posterior de AsyncOS del dispositivo de seguridad de la red de Cisco que se ejecuta (WSA)

Nota: Este artículo sobre Knowledge Base se refiere al software que no es mantenido ni es soportado por Cisco. La información se proporciona como cortesía para su conveniencia. Para la asistencia adicional, entre en contacto por favor al proveedor de software.

El tráfico inmediato de Messaing (IM) sobre el HTTP se puede bloquear hoy de las siguientes maneras:

- Bloque definiendo los agentes de usuario de encargo usados por las aplicaciones IM.
- Bloque con la **"charla y la categoría predefinida inmediata de la Mensajería" URL**, o con una categoría de encargo que contiene los servidores IM (GUI > administrador de seguridad > políticas de acceso > Filtrado de URL de la red)
- Bloquee las aplicaciones requeridas IM bajo **"Mensajería inmediata" AVC Application type (Tipo de aplicación)** *(GUI > administrador de seguridad > las políticas de acceso > las aplicaciones de la red)*
- Bloquee los puertos que el uso de las aplicaciones IM de hacer un túnel con los proxys con el HTTP CONECTA el método.
- Agregue manualmente los servidores IM en la lista del negro del control de tráfico L4 para bloquear el acceso a los destinos populares IM con independencia del puerto.

MSN Messenger
1. Bajo el **GUI > el administrador de seguridad > las políticas de acceso de la red** hacen clic en los **objetos** 2. Especifique los **tipos MIME de encargo del bloque** inferior siguiente: *application/x-msn-*

messenger
Mensajería instantánea de Yahoo
1. Cree una categoría de encargo en el **administrador de seguridad de la red > las categorías de encargo URL** 2. Especifique los **sitios** inferiores siguientes: *pager.yahoo.com, shttp.msg.yahoo.com, update.messenger.yahoo.com, update.pager.yahoo.com* 3. Fije esta categoría de encargo para bloquear.

AOL Instant Messenger
1. Cree una categoría de encargo en el **administrador de seguridad de la red > las categorías de encargo URL** 2. Especifique los **sitios** inferiores siguientes: *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. Fije esta categoría de encargo para bloquear.
Google Chat
1. Cree una categoría de encargo en el **administrador de seguridad de la red - > las categorías de encargo URL** 2. Especifique el **avanzado** inferior siguiente**: Expresiones normales**: *correo \ .google \ .com/correo/canal* 3. Fije esta categoría de encargo para bloquear.
Google Chat (Método alternativo)
1. Cree una categoría de encargo en el **administrador de seguridad de la red - > las categorías de encargo URL** 2. Especifique los **sitios** inferiores siguientes: *.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. Fije esta categoría de encargo para bloquear. **Usted puede también bloquear Google Talk bloqueando el “agente de usuario: Google Talk”**

Otros links útiles:

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