Come bloccare il traffico di messaggistica istantanea (IM) su Cisco Web Security Appliance?

Sommario

Domanda:

Come bloccare il traffico di messaggistica immediata (IM) o la chat IM su Cisco Web Security Appliance?

Ambiente:

Cisco Web Security Appliance (WSA) con AsyncOS versione 7.1.x e successive

Nota: Questo articolo della Knowledge Base fa riferimento a software che non è gestito o supportato da Cisco. Le informazioni vengono fornite per comodità dell'utente. Per ulteriore assistenza, contattare il fornitore del software.

Il traffico di messaggistica istantanea (IM) su HTTP può essere bloccato oggi nei modi seguenti:

- Blocca definendo agenti utente personalizzati utilizzati dalle applicazioni di messaggistica immediata.
- Blocca con la **categoria URL predefinita "Chat e Messaggistica immediata"** o con una categoria personalizzata contenente server di messaggistica immediata (GUI > Web Security Manager > Criteri di accesso > Filtro URL)
- Bloccare le applicazioni IM richieste in **"Messaggistica immediata"** *(GUI > Web Security Manager > Criteri di accesso > Applicazioni).*
- Blocca le porte utilizzate dalle applicazioni di messaggistica istantanea per eseguire il tunneling dei proxy con il metodo CONNECT HTTP.
- Aggiungere manualmente i server di messaggistica istantanea nella lista nera di L4 Traffic Monitor per bloccare l'accesso alle destinazioni di messaggistica istantanea più comuni indipendentemente dalla porta.

MSN Messenger
1. In **GUI > Web Security Manager > Criteri di accesso** fare clic sugli **oggetti** 2. Specificare quanto segue in **Tipi MIME personalizzati blocco**: *application/x-msn-messenger*
Yahoo Instant Messenger

1. Creare una categoria personalizzata in **Web Security Manager > Categorie URL personalizzate**
2. Specificare quanto segue in **Siti**: *pager.yahoo.com, shttp.msg.yahoo.com, update.messenger.yahoo.com, update.pager.yahoo.com*
3. Impostare questa categoria personalizzata su Blocca.

AOL Instant Messenger

1. Creare una categoria personalizzata in **Web Security Manager > Categorie URL personalizzate**
2. Specificare quanto segue in **Siti**: *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. Impostare questa categoria personalizzata su Blocca.

Chat di Google

1. Creare una categoria personalizzata in **Web Security Manager -> Categorie URL personalizzate**
2. Specificare quanto segue in **Avanzate: Espressioni regolari**: *posta\.google\.com/posta/canale*
3. Impostare questa categoria personalizzata su Blocca.

Google Chat (metodo alternativo)

1. Creare una categoria personalizzata in **Web Security Manager -> Categorie URL personalizzate**
2. Specificare quanto segue in **Siti**: *.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. Impostare questa categoria personalizzata su Blocca.

Puoi anche bloccare Google Talk bloccando "Agente-Utente: Google Talk"

Altri collegamenti utili:

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