

# Wie wird Instant Messaging (IM)-Datenverkehr auf der Cisco Web Security Appliance blockiert?

## Inhalt

[Frage:](#)

[Umgebung:](#)

## Frage:

Wie kann Instant Messaging (IM)-Datenverkehr oder IM-Chat auf der Cisco Web Security Appliance blockiert werden?

## Umgebung:

Cisco Web Security Appliance (WSA) mit AsyncOS Version 7.1.x und höher

**Hinweis:** Dieser Knowledge Base-Artikel bezieht sich auf Software, die nicht von Cisco verwaltet oder unterstützt wird. Die Informationen werden Ihnen zu Ihrer Zufriedenheit zur Verfügung gestellt. Wenden Sie sich für weitere Unterstützung an den Softwareanbieter.

Instant Messaging (IM)-Datenverkehr über HTTP kann heute auf folgende Weise blockiert werden:

- Blockierung durch die Definition benutzerdefinierter Benutzeragenten, die von den IM-Anwendungen verwendet werden.
- Blockierung mit der **vordefinierten URL-Kategorie "Chat und Instant Messaging"** oder mit einer benutzerdefinierten Kategorie, die IM-Server enthält (GUI > Web Security Manager > Zugriffsrichtlinien > URL-Filterung)
- Blockieren Sie die erforderlichen IM-Anwendungen unter **"Instant Messaging" AVC-Anwendungstyp** (GUI > Web Security Manager > Zugriffsrichtlinien > Anwendungen)
- Blockiert Ports, die IM-Anwendungen verwenden, um Proxys über die HTTP CONNECT-Methode zu durchlaufen.
- Manuelles Hinzufügen von IM-Servern zur Blacklist der L4 Traffic Monitor, um den Zugriff auf beliebige IM-Ziele zu blockieren, unabhängig vom Port.

<b>MSN Messenger</b>
1. Klicken Sie unter <b>GUI &gt; Websicherheits-Manager &gt; Zugriffsrichtlinien</b> auf <b>Objekte</b> .
2. Geben Sie unter <b>Benutzerdefinierte MIME-Typen sperren</b> Folgendes an: <i>Anwendung/x-msn-Messenger</i>
<b>Yahoo Instant Messenger</b>
1. Erstellen einer benutzerdefinierten Kategorie in <b>Websicherheits-Manager &gt; Benutzerdefinierte URL-Kategorien</b>

2. Geben Sie unter **Standorte** Folgendes an: *pager.yahoo.com, shttp.msg.yahoo.com, update.messenger.yahoo.com, update.pager.yahoo.com*
3. Legen Sie diese benutzerdefinierte Kategorie auf Block fest.

#### **AOL Instant Messenger**

1. Erstellen einer benutzerdefinierten Kategorie in **Websicherheits-Manager > Benutzerdefinierte URL-Kategorien**
2. Geben Sie unter **Standorte** Folgendes an: *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, 20 5. 188.0.0/16*
3. Legen Sie diese benutzerdefinierte Kategorie auf Block fest.

#### **Google-Chat**

1. Erstellen einer benutzerdefinierten Kategorie in **Web Security Manager -> Benutzerdefinierte URL-Kategorien**
2. Geben Sie unter **Erweitert** Folgendes an: **Reguläre Ausdrücke:**  
*mail.google.com/mail/channel*
3. Legen Sie diese benutzerdefinierte Kategorie auf Block fest.

#### **Google Chat (Alternative Methode)**

1. Erstellen einer benutzerdefinierten Kategorie in **Web Security Manager -> Benutzerdefinierte URL-Kategorien**
2. Geben Sie unter **Standorte** Folgendes an: *.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. Legen Sie diese benutzerdefinierte Kategorie auf Block fest.

**Sie können Google Talk auch blockieren, indem Sie "User Agent: Google Talk"**

Weitere nützliche Links:

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