Interested in learning more about security?

SANS Institute
InfoSec Reading Room

This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

Choosing corporate level instant messaging system and implementing audit controls

Instant messaging (IM) is an efficient way of real-time communication that enables message, file and presence transfer over the Internet. Business can benefit from IM as it is a cost-effective alternative for teleconferences by reducing phone call bills, need for meeting rooms and travel. IM systems can be hosted inside a corporate network or hosted off-site. In this paper we present criteria for choosing a suitable IM system and show how to implement reliable audit controls for the IM system using Snort rules.

Copyright SANS Institute
Author Retains Full Rights

AD

Choosing corporate level instant messaging system and implementing audit controls

GIAC (GSNA) Gold Certification

Author: Mikko Niemelä, mikko@silverskin.fi
Advisor: Tim Proffitt

Accepted: 2010

Abstract

Instant messaging (IM) is an efficient way of real-time communication that enables message, file and presence transfer over the Internet. Business can benefit from IM as it is a cost-effective alternative for teleconferences by reducing phone call bills, need for meeting rooms and travel. IM systems can be hosted inside a corporate network or hosted off-site. In this paper we present criteria for choosing a suitable IM system and show how to implement reliable audit controls for the IM system using Snort rules.

© 2010 SANS Institute, Author retains full rights.

1. Introduction

Instant messaging system (IM) is a type of communications service over the Internet that enables users to exchange messages and presence status. Instant messaging systems are split in to two groups: public instant messaging systems and corporate-grade instant messaging systems. The most popular public systems are AOL Instant Messenger, ICQ, MSN Messenger, and Yahoo! Instant Messenger. Corporate-grade leaders are Microsoft Office Live Communications, IBM Lotus Sametime, Skype for business and Jabber. (Amman, Mohammad; van Oorschot, P.C, 2005)

Everybody is familiar with e-mail these days and it is sometimes used for real-time messaging as well. The most obvious day-to-day email hazard is time-wasting. Spam is a growing irritation that wastes bandwidth on corporate networks. (Company, & Miller, 2003) Compared with e-mail instant messaging provides faster and spam-free communication channel with presence status.

Instant messaging systems are already implemented in some organizations. For other corporations, IM is seen as just another way that people avoid work and possibly steal corporate information. IM can be considered as a risk to corporate networks since new data disclosures are reported monthly and public instant messaging systems tend to have major vulnerabilities. (Bankes, Hatter, Fernández, & Cole, 2002) By implementing commercial-grade instant messaging system these risks can be mitigated and controlled.

This paper is split into business and technical aspect. In the second section the business aspect of choosing instant messaging system is discussed. More technical details about detecting instant messaging activity and implementing audit controls are discussed in section three. Section three will additionally demonstrate how to detect IM activity with Snort – a popular packet sniffer and intrusion detection system.

Mikko Niemelä, mikko@silverskin.fi

© 2010 The SANS Institute As part of the Information Security Reading Room Author retains full rights.

2. Business aspect: Choosing an instant messaging system

In this section the matter of business decision is discussed. The section will cover benefits and risks of IM in general terms ,take a closer look at comparison of IM clients and address a bit about audit controls.

2.1. Why – the benefits and value-add

Instant messaging differs from many other ways of communication because of its real-time nature of user interaction. (Amman, Mohammad; van Oorschot, P.C, 2005) Similar real-time user interaction can be achieved also via telephone. However, IM provides an easy way to see if a user is available for chat without actually communicating with the user. IM also makes possible to share documents within a conversation. As people are using more and more IM services at home, they expect workplaces to have similar communication methods available.

Instant messaging provides a faster channel to communicate when both users are available to do so. It also provides a cheaper way to communicate causing need for conference rooms and telephone calls to reduce. When looking at the big picture, the main reason to implement instant messaging system is to provide cheap and more efficient communications. (Pergamon, 2007)

Some organizations need to follow some form of compliancy of handling confidential data. Controlling and logging the data of internal messaging must be enforced. These kinds of requirements are placed in Sarbanes-Oxley Act and Health Insurance Portability and Accountability Act (HIPAA).

Enterprise instant messaging clients also allow better encryption for data-in-transit, monitoring patching levels and file transfer.

© 2010 The SANS Institute As part of the Information Security Reading Room Author retains full rights.

2.2. Risks

To help to understand whether implementing an instant messaging system is a valuable choice we go through the most important risks that come with these systems. The most important threat is information disclosure, which can be intentional or accidental. (SANS Institute, 2009)

Internal information disclosure happens when someone inside the corporation reveals valuable information to outsiders. This is possible if external instant messaging is allowed. Mitigating this risk is to raise awareness and make clear legal statements how information disclosure will be handled. Technically the ability to log conversations and file transfers is the most important.

External information disclosure can happen when someone outside the corporate network manages to fetch valuable information. A common way for this to happen is through exploiting vulnerabilities that are present in instant messaging software, sniffing instant messaging packets and fooling users to accept malicious software via file transfer.

2.3. Corporate instant messaging systems

In this section we introduce some of the most popular instant messaging systems. We take a look at fully internal, fully external and mixed systems. Sometimes external users are allowed to join conversations with some features disabled, for example file transfer outside corporate network could be forbidden.. We take a look at interoperability, support and licensing. Key features are presented in Table 1.

Instant messaging systems are typically defined by two categories: internal and external.

Internal systems are self-hosted by the corporate itself where as external systems are hosted by a service provider. The important difference is the control and location of the data. Internal systems allow total control of the data. In external systems the provider will also be able to access data. It can't be said which one is more secure, but negotiations about liability usually end to corporations hosting instant messaging systems themselves.

© 2010 The SANS Institute As part of the Information Security Reading Room Author retains full rights.

There are some features we don't cover in this research that we still think are important to consider:

- User management

How easy it is to add internal or external users? Integration with the current directory service, AD or LDAP?

- User education

How easy it is to use, and how much education end-users and administrators need?

- System & compliance requirements

How well the workstations can handle the software? Does the corporate network meet the bandwidth requirements? Does the software stay compliant after implementing IM?

- Localization

What languages are supported? Is it possible to make own translations? Is there user manual in different languages?

Most of the following systems are internal systems with internal servers and in-house management. However there are many service providers that offer these instant messaging products as hosted ASP / cloud service.

2.3.1. Microsoft Office Communications Server

Microsoft Office Communications Server (OCS) is a market leader in enterprise instant messaging. It provides a scalable internal instant messaging system for environments that are already using Microsoft products. OCS has native integration to Active directory and Microsoft management tools, which usually is a key feature when

© 2010 The SANS Institute As part of the Information Security Reading Room Author retains full rights.

choosing product. Pricing is dependant of other Microsoft products licensed and the size of the enterprise.

Microsoft does not advertise OCS as an independent product as it is considered to be more of a communication add-on for Microsoft infrastructure.

OCS comes in two sizes: Standard Edition server supports internal IM and conferencing with a user base of less than 5,000 and Enterprise Edition user base more than 5,000.

The choice of Standard or Enterprise edition is also dependant on high availability requirements, network topology (multiple geological locations) and if external users are allowed. For example small companies can use the standard edition with an edge server to allow external users to participate in web conferences.

Enterprise edition provides tools for larger and more complex deployment, for example deployment with support for external user access and voice in multiple locations.(Microsoft, 2008)

2.3.2. IBM Lotus Sametime

IBM Lotus Sametime is an internal IM that comes with standard version called Entry featuring Microsoft office integration and typical instant messaging features. Licensing is based on number of users and products introduced below. IBM Lotus Sametime Entry is a product for enterprise to get started with Sametime instant messaging system. It includes basic IM features and Microsoft Office integration.

IBM Lotus Sametime Standard adds Web conferencing.

IBM Lotus Sametime Connect client comes for Sametime Standard and Sametime Entry. Connect for Standard provides more customization, richer location based presence, video and telephoning features are also available. Sametime Connect has additional plug-ins to add more features.

© 2010 The SANS Institute As part of the Information Security Reading Room Author retains full rights.

IBM Lotus Sametime Advanced provides persistent chat rooms, screen sharing and connectivity to social media.

IBM Lotus Sametime Gateway allows integration to other instant messaging networks, for example public IM networks.

IBM Lotus Sametime Enterprise Meeting Server provides load balancing and failover capabilities.

IBM Sametime Unified Telephony adds telephone calling features and integration to corporate telephone network.

(IBM, 2010)

2.3.3. Jabber XCP

Jabber and XMPP are usually mixed up because early name of XMPP used to be Jabber. However Jabber Inc, a company owned by Cisco, provides instant messaging services for corporations. The system is called Jabber Extensible Communications Platform, Jabber XCP.

Jabber Extensible Communications Platform software platform is designed for commercial use allowing scalability up to a million users concurrently in a distributed configuration. Jabber XCP allows interoperability with Microsoft OCS, Google Talk, AOL and IBM Lotus Sametime and integrates with directory services, databases, web portals and mobile devices. Cisco provides integration with WebEx Connect IM, Unified Presence, and Unified Personal Communicator.

Jabber Inc provides custom support, development and integration services. Licensing for the product is individual seat-based.

Jabber XCP is reported to meet compliance requirements for the Securities Exchange Commission (SEC) and Health Insurance Portability and Accountability (HIPAA).

It is also possible to integrate Jabber XCP to corporate telephone systems with 3rd party products.

© 2010 The SANS Institute As part of the Information Security Reading Room Author retains full rights.

(Cisco LLC, 2010)

2.3.4. Skype for business

Skype for business is the only one of these systems that does not provide a fully internal system. It comes with three different products including Skype for business client, Skype manager and Skype Connect. In this paper we take a look at the current version 4.2.

Skype for business client enables typical Skype features. Skype manager is used for managing corporate clients, enabling and disabling features, monitoring usage and allocating credit for outbound telephone calls. Skype Connect integrates Skype to corporate phone numbers.

Licensing is based on concurrent channels for external phone calls and support is bought separately from Skype.

(Skype limited, 2010)

© 2010 SANS Institute, Author retains full rights.

© 2010 The SANS Institute As part of the Information Security Reading Room Author retains full rights.

	OCS	IBM	Jabber	Skype
Internal	X	X	X	
External				X
External users supported	X	X	X	X
User base size	up to 5,000 with Standard edition. Unlimited with Enterprise edition.	Unlimited	Over 1,000,000	Unlimited
Videoconferencing	X	X	With Cisco WebEx Meeting Center	X
Telephone	X	X	With Cisco WebEx Connect IM	X
Directory service integration	AD / LDAP	AD / LDAP	AD / LDAP	Only with 3rd party products
Licensing	Standard / Enterprise Edition. Price varies of other MS products licensed and number of users.	Based on separate products for different set of features.	Individual seat based licensing.	Based on concurrent outbound phone lines.

Table 1. Comparison of IM features.

2.4. Audit controls

Whether an internal or an external system has been chosen, audit controls should also be deployed. Audit controls are used to measure the performance of a control within our systems or processes. When any system is set up, we have to know it is up, running

© 2010 The SANS Institute As part of the Information Security Reading Room Author retains full rights.

and configured like we planned. By implementing audit controls we make sure that the system is in good shape and in use. (SANS Institute, 2009; Ramos, 2008)

The paper will demonstrate how to implement audit controls with Snort. Snort is a popular packet sniffer, intrusion detection system and de facto standard for intrusion prevention system. It is widely used worldwide and open source community reacts quickly when new attack vectors show up. Snort uses specific rules to trigger alerts when signature of an attack or prohibited action is detected. (The Snort project, 2010)

2.5. Summary

The most important reason to implement an instant messaging system is to boost internal communication efficiency. There are many products in the market and we discussed some of their features that might help when making a business decision to implement a system. We discussed different types of instant messaging systems and what kind of risks these systems come with.

Instant messaging systems can be divided into two categories: internal and external systems. Whether internal or external system has been chosen, audit controls should also be deployed. Valid audit controls help us to measure the performance of the system.

3. Technical aspect: Implementing audit controls

© 2010 The SANS Institute As part of the Information Security Reading Room Author retains full rights.

In this section we discuss and demonstrate how to implement audit controls to verify that no other instant messaging systems are in use than what is chosen by management. We go through blocking default ports, creating alerts for IM activity and controlling the perimeter.

To implement audit controls we first need to determine what are the goal of the controls. For audit controls the difference of internal or external systems is very important. When an internal system is chosen we have to make sure no outbound or inbound traffic is allowed at network perimeter. When an external system is used, we have to make sure that only the chosen system is in use and no other instant messaging activity is present.

We start by disabling default ports of all other instant messaging systems at the perimeter. Then we create Snort rules to alert if instant messaging activity is present. Finally we set the perimeter to block outbound and inbound instant messaging traffic. In the case of legitmate IM, inbound and outbound traffic must be allowed.

All the three most popular IM clients MSN, AOL and Yahoo allow using flexible port numbers and HTTP cloaking. HTTP cloaking means that instant messaging software uses port 80 to communicate with the server or other peers. To address this issue, Cisco introduced application inspection. The HTTP Application Inspection Engine offers the port-misuse option to scan traffic for specific known applications that disguise their undesired traffic as legitimate HTTP traffic. (Cisco LLC, 2005)

3.1. IM clients, ports and protocols

Many IMs have default ports used for communication. However they can also be configured to use different ports. If instant messaging is generally not allowed, it is good to start to block these default ports to reduce IM usage by default settings. In the table below are shown typical default ports for common instant messaging protocols.

© 2010 The SANS Institute As part of the Information Security Reading Room Author retains full rights.

Instant messaging system	Default port numbers
ICQ	4000
AIM	5190-5193
XMPP / Jabber	5222 – 5223
MSNP (Microsoft IM)	1863
YMSG (Yahoo)	5050
Skype	80, 443 and other random ports

Table 2. Default IM ports.

If the network perimeter is configured to disable these ports, there should be only HTTP (port 80) and HTTPS (443) left open for instant messaging use.

We will demonstrate how to implement application inspection for port 80 but first lets take a look at implementing IM activity monitoring and alerting with Snort IDS.

3.2. Detecting IM with Snort

In this section we demonstrate how to detect typical personal IM clients such as AOL, YAHOO, MSN and Skype. We use Snort rules to generate alerts when this type of IM activity shows up.

3.2.1. AOL IM

AOL IM communicates with a specific server, login.oscar.aol.com. However, oscar uses quite a bit of IP space when traversing corporate networks. So the snort.conf default variable ttAIM_SERVERS/tt catches the AIM protocol in use when connecting to the known servers.

```
# This will detect when the client is logging into AOL
Alert tcp $HOME_NET any - $AIM_SERVERS any (msg:"Chat AIM
login"; flow:to_server,established; content:"*01|"; depth:2;
classtype: policy-violation; sid:1632; rev:1;)
```

The following rule logs all traffic between AIM clients. If you have AIM users, you'll soon be flooded with alarms, but it may at least yield some interesting results.

© 2010 The SANS Institute As part of the Information Security Reading Room Author retains full rights.

```
Alert tcp $HOME_NET any - $AIM_SERVERS any (msg:"Chat AIM
Message"; Flow:from_client,established; content:"*|02|";
depth:2; content:"|00 04 00 06|"; depth:4; offset:6;
classtype: policy-violation; sid:1633; rev:6;)
```

You can also detect and block port TCP 5190, as this is the default port AIM uses to communicate.

(Orebaugh, Biles & Babbin, 2005; Archibald & al, 2006)

3.2.2. Yahoo! IM (YIM)

This rule looks for the protocol even when trying to avoid the default port TCP 5050.

```
alert tcp $HOME_NET any - $EXTERNAL_NET any (msg:"Chat Yahoo
IM login"; flow:from_client,established; content:"|70 61 74
83 d2 f3 b2 06 46 f6 d6 61 9e 3d 2e|"; classtype:policy-
violation; sid:10570; rev:1;)
```

While this example tracked the application protocol, the following rule is looking for an actual conversation in the flow. This rule will filter out packets that have a TCP payload of less than 52 bytes to help reduce false positives.

```
alert tcp $HOME_NET any - any any (msg:"Chat Yahoo IM
Message"; flow:to_server,established; content:"YMSG";
dsize:52; content: "TYPING"; sid:10571; rev:1;)
```

(Orebaugh, Biles & Babbin, 2005; Archibald & al, 2006)

3.2.3. MSN IM

Microsoft MSN client uses same protocol as Hotmail and MSN Mail accounts. Distinguishing IM traffic from normal MSN mail traffic is a problem. One way is to look for MSN traffic over the default port TCP 1863 and then determine if the traffic is a result of a chat or mail connections.

```
alert tcp $HOME_NET any $EXTERNAL_NET 1863 (msg:"Chat MSN IM
message"; flow:established; content:"MSG"; depth:4; content:
"Content-Type|3A|"; distance:0; nocase;
```


© 2010 The SANS Institute As part of the Information Security Reading Room Author retains full rights.

```
content:"text/plain"; distance:1; classtype:policy-
violation; sid:540; rev:11;)
```

The following rule looks for a file transferred over the MSN IM protocol.

```
alert tcp $HOME_NET an $EXTERNAL_NET 1863 (msg:"Chat MSN IM
file transfer accept";flow:established; content:"MSG";
depth:4; content:"Content-Type|3A|"; nocase;
content:"text/x-msmsgsinvite"; distance:0;
content:"Invitation-Command|3A|"; content:"ACCEPT";
distance:1; classtype: policy-violation; sid:1988; rev:3;)
```

(Orebaugh, Biles & Babbin, 2005; Archibald & al, 2006)

3.2.4. Skype

Detecting Skype is very difficult because of the nature of Skype's traffic. Skype uses encrypted TCP and UDP traffic with random ports. For example network traffic analysis shows random encrypted packets going to different ports.

One way to prevent this traffic is to configure firewall only allow encrypted traffic from port 443. That leaves Skype only one port to go. Port 443 is usually left open because need for secure web surfing.

With the following Snort rules it is possible to create alerts when Skype traffic is present. We show three easy rules to detect Skype login from client end and Skype update request.

Skype from client to server login attempt

```
alert tcp $HOME_NET 1024: -> $EXTERNAL_NET 1024: (msg:"Skype
client login -- from client"; flags:AP,SUFR12;
flow:to_server,established; dsize:5; content:"|16 03 01|";
depth:3; flowbits:set,skype.login; sid:1000009; rev:2;)
```

P2P Skype client login startup

© 2010 The SANS Institute As part of the Information Security Reading Room Author retains full rights.

```
alert tcp $HOME_NET any -> $EXTERNAL_NET any (msg:"P2P Skype
client login startup"; flow:to_server,established; dsize:5;
content:"|16 03 01 00|"; depth:4; flowbits:set,skype.login;
metadata:policy security-ips drop; classtype:policy-
violation; sid:5998; rev:4;)
```

P2P Skype client setup get newest version attempt

```
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS
(msg:"P2P Skype client setup get newest version attempt";
flow:to_server,established; uricontent:"/ui/";
uricontent:"/getnewestversion"; content:"Host|3A|
ui.skype.com"; classtype:policy-violation; sid:5694; rev:4;)
```

(Snort, 2010; Archibald & al, 2006)

3.2.5. Gmail chat and encrypted chats

Google introduced instant messaging style chat with Gmail and Google Apps e-mail web clients. The chat itself is using HTTPS to communicate with Google's servers and makes it hard to detect by the perimeter. One way to monitor and block encrypted IM traffic is to watch for DNS requests and HTTP handshakes.

The following Snort rule allows detectection of Google's chat when DNS request happens.

```
alert udp $HOME_NET any -> $EXTERNAL_NET 53 (msg:"CHAT deny
Gmail chat DNS request"; byte_test:1,!&,128,2;
content:"|0B|chatenabled|04|mail|06|google|03|com"; nocase;
classtype:policy-violation; sid:16443; rev:1;)
```

(Snort, 2010)

© 2010 The SANS Institute As part of the Information Security Reading Room Author retains full rights.

3.2.6. Website based IM

There are website based services such as meebo.com, ebuddy.com and koolim.com that allow individual to use instant messaging services via web browser. These services use valid HTTP and can't be blocked with application inspection or port-misuse. It is possible to create Snort rules to alert when traffic to these sites is present, but more convenient way is to disable these services by blacklisting at the perimeter. Blacklists are efficient, however they need to be updated and maintained on daily basis because new sites show up every month.

3.3. Blocking IM traffic with CISCO

Now we have a situation where all obvious IM protocol ports are closed and the only way to deliver IM traffic is using ports 80 and 443. First we introduce example configuration to block IM traffic from perimeter by Cisco ASA/PIX. Configuration is followed by another configuration to detect, block and allow IM activity with Cisco IOS.

All of the devices used in this example are started with default configuration. If your network is live, make sure that you understand the potential impact of any command.

3.3.1. Blocking all IM activity with CISCO PIX/ASA 7.2 and Later

```
CiscoASA#show running-config
: Saved
: ASA Version 8.0(2)
!
hostname pixfirewall
enable password 8Ry2YjIyt7RRXU24 encrypted names

!--- Output Suppressed
```


© 2010 The SANS Institute As part of the Information Security Reading Room Author retains full rights.

```
class-map inspection_default
     match default-inspection-traffic
class-map imblock
     match any

!--- The class map "imblock" matches
!--- all kinds of traffic.

class-map P2P
     match port tcp eq www

!--- The class map "P2P" matches
!--- http traffic.

!
policy-map type inspect dns preset_dns_map
     parameters
          message-length maximum 512

policy-map type inspect im impolicy
     parameters
     match protocol msn-im yahoo-im
          drop-connection

!--- The policy map "impolicy" drops the IM
!--- traffic such as msn-im and yahoo-im.

policy-map type inspect http P2P_HTTP
     parameters
     match request uri regex _default_gator
          drop-connection log
     match request uri regex _default_x-kazaa-network
          drop-connection log

!--- The policy map "P2P_HTTP" drops the P2P !--- traffic
that matches the some built-in reg exp's.

policy-map IM_P2P
     class imblock
          inspect im impolicy
     class P2P
          inspect http P2P_HTTP

!--- The policy map "IM_P2P" drops the
!--- IM traffic matched by the class map "imblock" as well
as P2P traffic matched by class map "P2P".

policy-map global_policy
     class inspection_default
          inspect dns preset_dns_map
          inspect ftp inspect h323 h225
          inspect h323 ras
          inspect netbios
          inspect rsh
```


© 2010 The SANS Institute As part of the Information Security Reading Room Author retains full rights.

```
          inspect rtsp
          inspect skinny
          inspect esmtp
          inspect sqlnet
          inspect sunrpc
          inspect tftp
          inspect sip
          inspect xdmcp
!
service-policy global_policy global
service-policy IM_P2P interface inside

!--- Apply the policy map "IM_P2P"
!--- to the inside interface.

prompt hostname context
Cryptochecksum:d41d8cd98f00b204e9800998ecf8427e
: end
CiscoASA#
```

Use these commands to confirm the configuration works properly.

Verifying commands are shown following the correct configuration data that should be seen when using above configuration.

The Output Interpreter Tool (OIT) supports certain **show** commands. Use the OIT to view an analysis of **show** command output.

To display the HTTP maps that have been configured:
show running−config http−map

```
CiscoASA#show running-config http-map http-policy
!
http-map http-policy
content-length min 100 max 2000 action reset log
content-type-verification match-req-rsp reset log
max-header-length request bytes 100 action log reset
max-uri-length 100 action reset log
!
```

To display all the policy−map configurations as well as the default policy−map configuration:
show running−config policy−map

```
CiscoASA#show running-config policy-map
!
policy-map type inspect dns preset_dns_map
     parameters
          message-length maximum 512
```


© 2010 The SANS Institute As part of the Information Security Reading Room Author retains full rights.

```
policy-map type inspect im impolicy
     parameters
     match protocol msn-im yahoo-im
          drop-connection
policy-map imdrop
     class imblock
          inspect im impolicy
policy-map global_policy
     class inspection_default
          inspect dns preset_dns_map
          inspect ftp inspect h323 h225
          inspect h323 ras
          inspect netbios
          inspect rsh inspect rtsp
          inspect skinny
          inspect esmtp
          inspect sqlnet
          inspect sunrpc
          inspect tftp
          inspect sip
          inspect xdmcp
```

You can also use the options in this command as shown here:

```
show running-config [all] policy-map [policy_map_name | type
inspect [protocol]]
```

```
CiscoASA#show running-config policy-map type inspect im
!
policy-map type inspect im impolicy
     parameters
     match protocol msn-im yahoo-im
          drop-connection
!
```

To display the information about the class map configuration:
show running−config class−map

```
CiscoASA#show running-config class-map

! class-map inspection_default
     match default-inspection-traffic
class-map imblock
     match any
```

To display all currently running service policy configurations:
show running−config service−policy

```
CiscoASA#show running-config service-policy
```


© 2010 The SANS Institute As part of the Information Security Reading Room Author retains full rights.

```
service-policy global_policy global
service-policy imdrop interface outside
```

To display the access−list configuration that is running on the security appliance:
show running−config access−list

```
CiscoASA#show running-config access-list
access-list 101 extended deny ip host 10.1.1.5 any
access-list 101 extended deny ip host 10.1.1.10 any
access-list 101 extended permit ip any any
```

(Cisco LLC, 2008)

3.3.2. CISCO IOS Configuration for blocking and allowing IM

Cisco IOS provides HTTP Inspection engine to enforce an instant messaging policy efficiently. Following configuration shows how to create instant messaging policy called my-im-policy. The configuration enables Yahoo instant messaging, but blocks AOL and MSN. First we go through the most important commands that can be used to detect and block IM traffic from port 80.

The port-misuse command blocks all three public IM applications using the HTTP protocol. It is always recommended that you block IM activity through HTTP and allow IM traffic to pass, if at all, through its native port.

The server permit commands help to identify all the servers for Yahoo. A connection to any one of the specified servers will be recognized by the firewall as a Yahoo IM session—even if the Yahoo client uses port-hopping techniques. Port-hopping techniques can be accomplished by using server port-numbers such as 25 instead of the standard 5050.

If a server permit command is not issued within the application IM yahoo command, the Cisco IOS firewall will classify only the traffic going to server port 5050 as Yahoo traffic. Because the port classification scheme breaks if any of the Yahoo clients are configured to use a port other than 5050, it is more reliable to have server permit command entries instead of relying on the port classification method.

© 2010 The SANS Institute As part of the Information Security Reading Room Author retains full rights.

The server deny commands under other IM applications deny connection to respective servers. This action operates at the network layer connection level—not at the application session level. When traffic is denied, the TCP connection to the server is denied, no data traffic is allowed and all packets are dropped in the firewall. (Cisco, 2005)

```
appfw policy-name my-im-policy
 application http
  port-misuse im reset
!
 application im yahoo
  server permit name scs.msg.yahoo.com
  server permit name scsa.msg.yahoo.com
  server permit name scsb.msg.yahoo.com
  server permit name scsc.msg.yahoo.com
  service text-chat action allow
  service default action reset
!
 application im aol
  server deny name login.oscar.aol.com
!
 application im msn
  server deny name messenger.hotmail.com
!
ip inspect name test appfw my-im-policy

interface FastEthernet0/0
 description Inside interface
 ip inspect test in
```

(Cisco LLC, 2005)

3.4. Summary

We started by disabling known default ports for typical instant messaging clients. By doing this we left only ports 80 and 443 open.

© 2010 The SANS Institute As part of the Information Security Reading Room Author retains full rights.

We demonstrated how to create Snort rules to alert when instant messaging activity is present. After that sample configuration to block all instant messaging traffic from the perimeter.

Some applications allow http cloaking. However non-valid http traffic can be detected with application inspection and port-misuse, which we demonstrated in the end of the section.

4. Conclusion

The most important reason for a business to implement an instant messaging system is to improve internal communication efficiency. When implementing an instant messaging system, audit controls should also be implemented. With internal systems it is quite straight forward. Organizations can disable all outbound IM traffic. With external systems all other IM traffic should be disabled but the chosen one enabled.

To stop people from using public IM, closing default ports is a good start. Then there is the possibility for some clients to use HTTP cloaking or port reconfiguration. By implementing application inspection and / or port-misuse we can disable IM traffic using port 80. For IM clients using encryption there is blacklisting. Blacklisting known servers allows us to block these IMs when they try DNS requests.

5. References

Mikko Niemelä, mikko@silverskin.fi

© 2010 The SANS Institute As part of the Information Security Reading Room Author retains full rights.

Amman, Mohammad; van Oorschot, P.C. (2005). Secure Public Instant Messaging: A Survey

Archibald, Neil, Ramirez, Gilbert, Rathaus, Noam, Caswell, Brian, Russell, Ryan, Moss, Jeff, Giuseppini, Gabriele, Burnett, Mark, Long, Johnny, Mullen, Timothy, Russell, Ryan, Gregg, Michael, Watkins, Stephen, Long, Johnny, Skoudis, Ed, Bayles, Aaron, Hurley, Chris, Long, Johnny, Brindley, Ed, Klaus, Christopher, Deraison, Renaud, Meer, Haroon, Beale, Jay, Walt, Charl, Foster, James, Foster, Stephen, Bradley, Tony, & Carvey, Harlan. (2006). *Essential computer security*. Syngress Media Inc.

Bankes, Tim, Hatter, David, Fernández, Marcelo, & Cole, Eric. (2002). *Hackers beware*.

Orebaugh, Angela, Biles, Simon, & Babbin, Jacob. (2005). *Snort cookbook*. O'Reilly.

Ramos, Michael. (2008). *How to Comply with sarbanes-oxley section 404*. Wiley.

Pergamon. (2007). *Management Extra Effective Communications*. Pergamon Flexible Learning.

Company, R.R., & Miller, Robin. (2003). *The Online rules of successful companies*. FT Press.

SANS Institute. (2009) *507.1 Audit Principles, Risk assessment, and effective reporting.*

IBM. IBM Lotus Sametime 8 Information Center. Retrieved August 1, 2010, from: http://publib.boulder.ibm.com/infocenter/sametime/v8r0/index.jsp

Skype limited. (2010) Skype Connect™ Requirements Guide, version 3.0

Microsoft. (2008). Office Communications Server 2007 Planning Guide

Cisco LLC. Jabber XCP Frequently Asked Questions. Retrieved August 1, 2010, from: http://www.cisco.com/en/US/prod/voicesw/ps6789/ps10969/jabber_faq.html

Cisco. Jabber Extensible Communications Platform (XCP). Retrieved August 1, 2010, from: http://www.cisco.com/en/US/products/ps10969/index.html

Snort rules. Retrieved August 1, 2010, from: http://www.snort.org/snort-rules/

The Snort project. SNORT® Users Manual 2.8.6

Cisco LLC. (2005). Blocking instant messaging and peer-to-peer file sharing applications with Cisco IOS software release 12.3(14)T

Cisco LLC. (2008). PIX/ASA 7.x and Later: Block the Peer-to-Peer (P2P) and Instant Messaging (IM) Traffic Using MPF Configuration Example

Mikko Niemelä, mikko@silverskin.fi

© 2010 SANS Institute, Author retains full rights.

© 2010 SANS Institute, Author retains full rights.

Mikko Niemelä, mikko@silverskin.fi

© 2010 The SANS Institute As part of the Information Security Reading Room Author retains full rights.

Last Updated: September 2nd, 2015

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

SANS Crystal City 2015	Crystal City, VAUS	Sep 08, 2015 - Sep 13, 2015	Live Event
SANS Network Security 2015	Las Vegas, NVUS	Sep 12, 2015 - Sep 21, 2015	Live Event
SANS Seoul 2015	Seoul, KR	Sep 14, 2015 - Sep 19, 2015	Live Event
Data Breach Investigation Summit & Training	Dallas, TXUS	Sep 21, 2015 - Sep 26, 2015	Live Event
SANS Baltimore 2015	Baltimore, MDUS	Sep 21, 2015 - Sep 26, 2015	Live Event
SANS Perth 2015	Perth, AU	Sep 21, 2015 - Sep 26, 2015	Live Event
SANS Tallinn 2015	Tallinn, EE	Sep 21, 2015 - Sep 26, 2015	Live Event
SANS ICS Amsterdam 2015	Amsterdam, NL	Sep 22, 2015 - Sep 28, 2015	Live Event
SANS Bangalore 2015	Bangalore, IN	Sep 28, 2015 - Oct 17, 2015	Live Event
SANS DFIR Prague 2015	Prague, CZ	Oct 05, 2015 - Oct 17, 2015	Live Event
SANS Seattle 2015	Seattle, WAUS	Oct 05, 2015 - Oct 10, 2015	Live Event
SANS Tysons Corner 2015	Tysons Corner, VAUS	Oct 12, 2015 - Oct 17, 2015	Live Event
SOS: SANS October Singapore 2015	Singapore, SG	Oct 12, 2015 - Oct 24, 2015	Live Event
SANS Gulf Region 2015	Dubai, AE	Oct 17, 2015 - Oct 29, 2015	Live Event
SANS Cyber Defense San Diego 2015	San Diego, CAUS	Oct 19, 2015 - Oct 24, 2015	Live Event
SANS Tokyo Autumn 2015	Tokyo, JP	Oct 19, 2015 - Oct 31, 2015	Live Event
SANS South Florida 2015	Fort Lauderdale, FLUS	Nov 09, 2015 - Nov 14, 2015	Live Event
SANS Sydney 2015	Sydney, AU	Nov 09, 2015 - Nov 21, 2015	Live Event
SANS London 2015	London, GB	Nov 14, 2015 - Nov 23, 2015	Live Event
Pen Test Hackfest Summit & Training	Alexandria, VAUS	Nov 16, 2015 - Nov 23, 2015	Live Event
SANS Hyderabad 2015	Hyderabad, IN	Nov 24, 2015 - Dec 04, 2015	Live Event
SANS Cape Town 2015	Cape Town, ZA	Nov 30, 2015 - Dec 05, 2015	Live Event
SANS San Francisco 2015	San Francisco, CAUS	Nov 30, 2015 - Dec 05, 2015	Live Event
SANS Milan 2015	OnlineIT	Sep 07, 2015 - Sep 12, 2015	Live Event
SANS OnDemand	Books & MP3s OnlyUS	Anytime	Self Paced