WHITE PAPER

BLOCKING INSTANT MESSAGING AND PEER-TO-PEER FILE SHARING APPLICATIONS WITH CISCO IOS SOFTWARE RELEASE 12.3(14)T

Most organizations view instant messaging and peer-to-peer file sharing (P2P) applications as frivolous consumers of expensive resources—employee time and network bandwidth. Furthermore, some P2P networks can act as a conduit for malicious software such as worms, offering an easy path around firewalls into an organization to compromise desktop computing resources.

Cisco IOS® Software Release 12.3(14)T introduced application inspection engines and granular inspection, two critical new features that allow Cisco IOS Firewall to control instant messaging and P2P applications on networks. This document offers some sample configurations to use these features to monitor and block instant messaging and P2P file sharing traffic.

BACKGROUND

P2P and instant messaging traffic generally offer two modes of operation—a native mode, where the application runs on a uniquely defined set of Transmission Control Protocol (TCP) or User Datagram Protocol (UDP) ports, and "HTTP cloaked" mode, in which the application masquerades as HTTP (TCP Port 80) traffic in order to gain passage through firewalls and other network policy controls. Some of the more advanced P2P and instant messaging applications implement sufficient RFC 2616 dialogue to appear as a legitimate conversation between a Web browser and a Web server.

Prior to Release 12.3(14)T, Cisco IOS Software was bound by two major restrictions in the control of P2P and instant messaging applications—a limited list of applications that were supported in Cisco IOS Firewall Stateful Inspection (formerly known as Context-Based Access Control (CBAC)), and some lack of application inspection capability.

Cisco IOS Firewall Stateful Inspection is the fundamental basis of the Cisco IOS Firewall feature set. If a specific application was not built into Cisco IOS Firewall (see the list of original supported protocols in Appendix 1), the **inspect tcp** or **inspect udp** commands were used to watch for any outbound connection activity through a firewall, and anticipated return traffic was subsequently allowed through firewall blocking policies with access control list (ACL) bypass capability. Unfortunately, these commands allow all traffic that is not specifically filtered out to make a connection with the appropriate server through a firewall, and return traffic is allowed back in. This mode of operation offers little granularity in allowing or disallowing specific protocols.

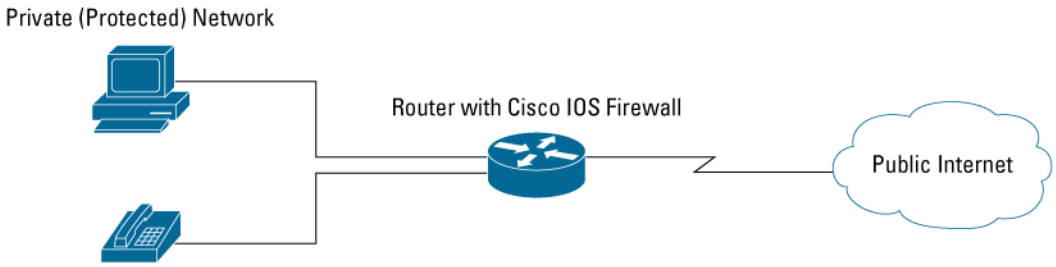
From an application inspection standpoint, HTTP inspection was one of the more thorough protocol inspections that Cisco IOS Firewall offered. However, even if an extremely restrictive Cisco IOS Firewall policy allowing only "HTTP out" was applied, users might still be able to use P2P and instant messaging applications that offered HTTP cloaking.

Cisco IOS Software Release 12.3(14)T introduced application inspection and granular inspection capabilities to address both of these shortcomings.

EXAMPLE NETWORK

We can examine a simple network to build an example of an effective inspection policy that will prohibit P2P and instant messaging traffic, and that will offer control over cloaked applications that try to exploit TCP Port 80 to gain access though the firewall (Figure 1). This network consists of one or more client PCs in a private network, connected to the public Internet through a Cisco IOS router running Cisco IOS Software Release 12.3(14)T.

Figure 1. Example Network

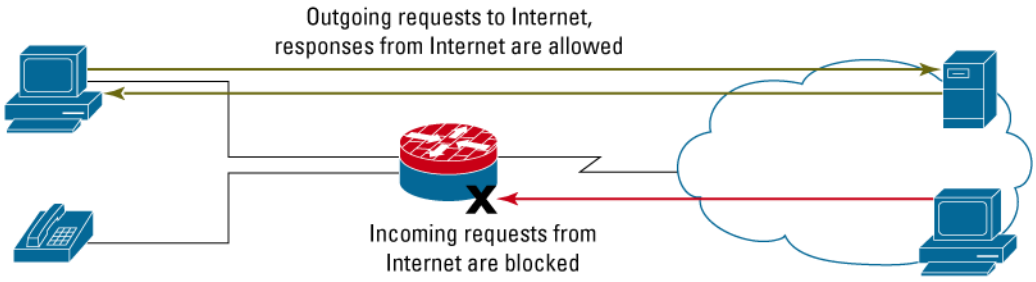


This sample network needs standard services, such as Web access (HTTP and Secure HTTP [HTTPS]), Internet e-mail (Simple Mail Transport Protocol [SMTP], POP3, and Internet Message Access Protocol [IMAP]), packet voice (H.323), Domain Name System (DNS) lookup, File Transfer Protocol (FTP), Network Time Protocol (NTP), and Internet Control Message Protocol (ICMP). Furthermore, the network users employ VNC, an open-source remote console application that runs by default on TCP 5900, and they need HTTP access on atypical ports (TCP Port 81 and 8080) for connectivity to vendor or customer e-commerce Webpages.

BACKGROUND

Cisco IOS Firewall uses Cisco IOS Firewall Stateful Inspection to restrict a public network's access to protected networks, while maintaining the private network's ability to access resources located in the public network (Figure 2).

Figure 2. Cisco IOS Firewall Stateful Inspection



Cisco IOS Firewall Stateful Inspection protects networks with two basic components. ACLs restrict inbound connections, and stateful inspection examines activity traversing the Cisco IOS Firewall from the protected network to the public network and anticipates the return traffic. Stateful inspection is a mechanism that observes the initiation, maintenance, and closure of network data connections.

Cisco IOS Firewall Stateful Inspection with granular inspection supports several of the specific application protocols listed in Appendix 1. Some of these protocols are common, simple protocols such as HTTP and Telnet, which only use one connection between client and server (or peers) to request and return application data. More complex supported protocols, such as FTP and H.323, employ a control channel to establish communications and a secondary data channel to transmit application data.

Some common protocols are not specifically predefined in IP inspection. Prior to Cisco IOS Software Release 12.3(14)T, **ip inspect tcp** and **ip inspect udp** were used as universal options for any services not covered by specific inspection services to inspect outgoing traffic and allow return traffic through a Cisco IOS Firewall's inbound permission ACL. Unfortunately, the **inspect tcp** option's capability to allow any return traffic is problematic in circumstances where specific protocols must be disallowed, particularly when a complex application such as instant messaging or P2P employs unpredictable port numbers and other mechanisms that make the traffic difficult to detect and block as it leaves the network. Undesired complex applications can be blocked by denying all return traffic except the traffic allowed by specific inspection services.

CONTROLLING P2P AND INSTANT MESSAGING APPLICATIONS

Cisco IOS Software Release 12.3(14)T introduced granular protocol inspection, which offers the capability to use Port-Application Mapping (PAM) protocol definitions with Cisco IOS Firewall inspection. PAM offers users the capability to define specific, named protocols. This significantly changes the older paradigm of employing specific inspection statements for advanced protocols that required comprehensive inspection to allow return access back through a firewall (commonly called "fixup" on Cisco PIX® products), then using **inspect tcp** to cover simpler protocols that don't require close scrutiny to allow additional data connections. Granular inspection uses PAM with Cisco IOS Firewall Stateful Inspection to associate user-defined application labels to traffic on specific ports, in order to define the list of desired traffic to be inspected so the return traffic "pinholes" are allowed in the inbound ACL; this protects the private network from unwanted access from the public network. Since the complete list of desired traffic can be specified, there is no need for **inspect tcp** to offer blanket coverage for previously unrecognized application traffic.

Granular inspection is an effective solution for blocking applications using port-hopping techniques that defy ACLs attempting to block the traffic, because the only traffic that is allowed to return through the firewall is running on the specific desired ports that the user allows with existing, predefined inspection capabilities, as well as user-specific, PAM-defined granular inspection policies. **inspect tcp** did not offer this application-specific mechanism to permit traffic—it simply anticipates all traffic running over TCP.

APPLICATION INSPECTION

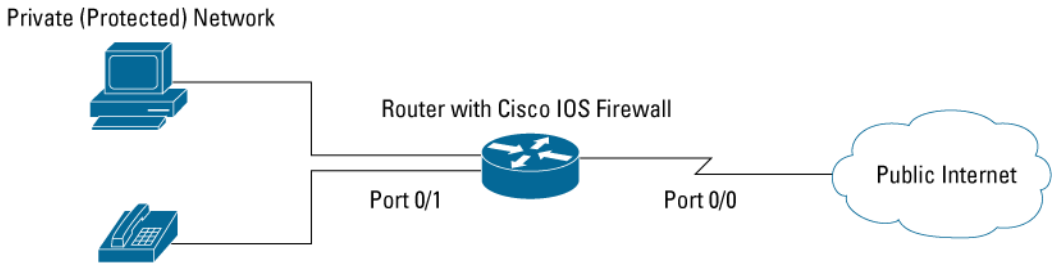
Granular inspection leaves some openings that advanced P2P and instant messaging applications may exploit. Most networks allow HTTP traffic through their firewalls, as it is the standard transport of many business applications, including ordinary Web traffic. Many instant messaging and P2P applications have developed mechanisms to disguise their traffic within TCP Port 80 (HTTP) traffic, thus offering their application an additional mechanism to work around restrictive firewalls. To address this issue, Cisco IOS Software Release 12.3(14)T 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. Presently, HTTP inspection can recognize Yahoo! Messenger traffic, Gnutella and KaZaA file sharing activity, and some applications that can tunnel other traffic through TCP Port 80 to avoid an otherwise restrictive firewall.

By combining granular inspection with the HTTP Application Inspection Engine, network engineers can allow desired protocols' traffic to return to their networks through access lists that protect the private network from unwanted public-net traffic. Application inspection can control specific unwanted application traffic that has been concealed inside legitimate HTTP traffic.

CONFIGURING CISCO IOS FIREWALL

Consider a simple network consisting of a Cisco IOS router with two Fast Ethernet ports. Port 0/0 is connected to the public Internet through a broadband connection, and Port 0/1 is connected to an Ethernet switch in the private network (Figure 3).

Figure 3. Example Network



The first configuration step restricts hosts on the public Internet from reaching the protected network with an ACL blocking all traffic from the public Internet, and applying the list to an interface:

```
access-list 101 deny ip any any
interface Fastethernet 0/0
  ip access-group 101 in
```

In the next step, specific inspection statements are configured based on the acceptable traffic that the router will allow out through the firewall, and on the expected return traffic:

```
ip inspect name my-ios-fw http
ip inspect name my-ios-fw https
ip inspect name my-ios-fw esmtp
ip inspect name my-ios-fw pop3
ip inspect name my-ios-fw imap3
ip inspect name my-ios-fw dns
ip inspect name my-ios-fw ftp
ip inspect name my-ios-fw ntp
ip inspect name my-ios-fw icmp
```

Cisco IOS Software supports the most popular Internet protocols, as well as several protocols that require additional effort to accommodate secondary data connections (listed in Appendix 1). This example requires support for VNC, which is not supported by default IP inspection capability; VNC runs on TCP 5900 by default. Granular protocol inspection provides the capability to configure inspection for specific protocols that are not natively supported by IP inspection. Configure inspection for VNC by defining the PAM entry for the protocol. Note: User-defined protocol labels must begin with "user-":

```
ip port-map user-vnc port tcp 5900
```

Next, apply the new protocol to the stateful inspection set:

```
ip inspect name my-ios-fw user-vnc
```

Now that the IP inspection set is complete, apply the inspection policy to the outbound traffic. Since this example protects traffic sourced on the private side of the router, **ip inspect in** is applied to the private interface. The router will inspect traffic passing from the private network to the public Internet, and the appropriate ACL bypass entries will be entered on the public side of the router to allow desired return traffic from the public Internet to pass back to the private network.

```
interface fastethernet 0/1
  ip inspect my-ios-fw in
```

The Cisco IOS Firewall Stateful Inspection configuration that you have defined blocks unwanted connections from the public Internet and allows return traffic for desired applications. Some P2P and instant messaging applications may be able to carry their traffic over TCP Port 80, so we'll use the HTTP Application Inspection Engine to inspect further into TCP Port 80 packets, and look for indications of the unwanted P2P and instant messaging traffic.

First, define the application inspection policy name, then configure HTTP inspection. Next, set up the policy. This policy will only inspect TCP Port 80 traffic for misuse by non-HTTP traffic; you may wish to define other application inspection features. Check the configuration reference list at the end of this document for details on using other features in HTTP application inspection:

```
appfw policy-name abuse-control
  application http
    port-misuse default action reset alarm
```

Apply the application inspection policy to the existing inspection set:

```
ip inspect name my-ios-fw appfw abuse-control
```

This completes the configuration for Cisco IOS Firewall with granular inspection and application inspection.

VERIFYING CISCO IOS FIREWALL CAPABILITY

You can check the Cisco IOS Firewall configuration and activity with several **show** commands:

```
show ip inspect config
```

Displays protocol timeouts and limits for Cisco IOS Firewall session activity.

```
show ip inspect interfaces
```

Displays interfaces with Cisco IOS Firewall rules applied.

```
show ip inspect name
```

Displays configuration of specific Cisco IOS Firewall rules.

```
show ip inspect sessions
```

Displays active sessions, including source and destination host addresses and port numbers.

```
show ip inspect statistics
```

Displays statistics for current active sessions, total sessions reset, session creation rate, number of sessions since Cisco IOS Firewall was configured or the router was rebooted, and other Cisco IOS Firewall statistics.

```
show ip inspect all
```

Displays all Cisco IOS Firewall information in the previous five commands.

REFERENCES

Configuring Cisco IOS Firewall Stateful Inspection:
http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/products_configuration_guide_chapter09186a00800ca7c5.html

Configuring HTTP application inspection:
http://www.cisco.com/en/US/products/sw/iosswrel/ps5207/products_feature_guide09186a0080420260.html

Configuring granular protocol inspection:
http://www.cisco.com/en/US/products/sw/iosswrel/ps5207/products_feature_guide09186a008040afd7.html

Configuring PAM: http://www.cisco.com/en/US/products/sw/iosswrel/ps1831/products_configuration_guide_chapter09186a00800d981c.html

APPENDIX 1: CISCO IOS FIREWALL STATEFUL INSPECTION PROTOCOL SUPPORT

802-11-iapp	IEEE 802.11 WLANs WG IAPP
ace-svr	ACE Server/Propagation
aol	America Online
appfw	Application firewall
appleqtc	Apple QuickTime
bgp	Border Gateway Protocol (BGP)
bliff	Bliff mail notification
bootpc	Bootstrap Protocol Client
bootps	Bootstrap Protocol Server
cddbp	CD Database Protocol
cifs	Common Internet file system (CIFS)
cisco-fna	Cisco FNATIVE
cisco-net-mgmt	cisco-net-mgmt
cisco-svcs	Cisco license/perf/GDP/X.25/ident svcs
cisco-sys	Cisco SYSMAINT
cisco-tdp	Cisco Tag Distribution Protocol (TDP)
cisco-tna	Cisco TNATIVE
citrix	Citrix IMA/ADMIN/RTMP
citriximaclient	Citrix IMA client
clp	Cisco Line Protocol
creativepartnr	Creative Partner
creativeserver	Creative Server
cuseeme	CUSeeMe Protocol
daytime	Daytime (RFC 867)
dbase	dBASE UNIX
dbcontrol_agent	Oracle dbControl Agent po
ddns-v3	Dynamic DNS Version 3
dhcp-failover	Dynamic Host Control Protocol (DHCP) failover
discard	Discard port
dns	Domain Name System (DNS)

dnsix	DNSIX Securit Attribute Token Map
echo	Echo port
entrust-svc-handler	Entrust KM/Administration Service Handler
entrust-svcs	Entrust sps/aaas/aams
esmtp	Extended SMTP
exec	Remote process execution
fcip-port	FCIP
finger	Finger
fragment	IP fragment inspection
ftp	File Transfer Protocol (FTP)
ftps	FTP over Transport Layer Security/Secure Sockets Layer (TLS/SSL)
gdoi	Group Domain of Interpretation (GDOI) Protocol
giop	Oracle GIOP/SSL
gopher	Gopher
gtpv0	General Packet Radio Service (GPRS) Tunneling Protocol Version 0
gtpv1	GPRS Tunneling Protocol Version 1
h323	H.323 Protocol (Microsoft NetMeeting, Intel Video Phone)
h323callsigalt	H.323 Call Signal Alternate
h323gatestat	H.323 Gatestat
hp-alarm-mgr	HP Performance data alarm manager
hp-collector	HP Performance data collector
hp-managed-node	HP Performance data managed node
hsrp	Hot Standby Router Protocol (HSRP)
http	HTTP
https	Secure HTTP
ica	ica (Citrix)
icabrowser	icabrowser (Citrix)
icmp	Internet Control Message Protocol (ICMP)
ident	Authentication Service
igmpv3lite	Internet Group Management Protocol (IGMP) over UDP for SSM
imap	IMAP
imap3	Interactive Mail Access Protocol 3
imaps	IMAP over TLS/SSL
ipass	IPASS
ipsec-msft	Microsoft IP Security (IPSec) NAT-T
ipx	IPX
irc	Internet Relay Chat Protocol
irc-serv	IRC-SERV
ircs	IRC over TLS/SSL
ircu	IRCU
isakmp	ISAKMP
iscsi	iSCSI

iscsi-target	iSCSI port
kazaa	KAZAA
kerberos	Kerberos
kermit	kermit
l2tp	Layer 2 Tunneling Protocol (L2TP)/Layer 2 Forwarding (L2F)
ldap	Lightweight Directory Access Protocol (LDAP)
ldap-admin	LDAP admin server port
ldaps	LDAP over TLS/SSL
login	Remote login
lotusmtap	Lotus Mail Tracking Agent Protocol
lotusnote	Lotus Notes
microsoft-ds	Microsoft-DS
ms-cluster-net	Microsoft Cluster Net
ms-dotnetster	Microsoft .NETster Port
ms-sna	Microsoft SNA Server/Base
ms-sql	Microsoft SQL
ms-sql-m	Microsoft SQL Monitor
msexch-routing	Microsoft Exchange Routing
mysql	MySQL
n2h2server	N2H2 Filter Service Port
ncp-tcp	NCP (Novell)
net8-cman	Oracle Net8 Cman/Admin
netbios-dgm	NETBIOS Datagram Service
netbios-ns	NETBIOS Name Service
netbios-ssn	NETBIOS Session Service
netshow	Microsoft NetShow Protocol
netstat	Variant of systat
nfs	Network File System (NFS)
nntp	Network News Transport Protocol (NNTP)
ntp	Network Time Protocol (NTP)
oem-agent	OEM Agent (Oracle)
oracle	Oracle
oracle-em-vp	Oracle EM/VP
oraclenames	Oracle Names
orasrv	Oracle SQL*Net v1/v2
parameter	Specify inspection parameters
pcanywheredata	pcANYWHEREdata
pcanywherestat	pcANYWHEREstat
pop3	POP3
pop3s	POP3 over TLS/SSL
pptp	Point-to-Point Tunneling Protocol (PPTP)
pwdgen	Password Generator Protocol

qmtp-tcp	Quick Mail Transfer Protocol
r-winsock	remote-winsock
radius	RADIUS and accounting
rcmd	R commands (r-exec, r-login, r-sh)
rdb-dbs-disp	Oracle RDB
realaudio	Real Audio Protocol
realmedia	RealNetwork's Realmedia Protocol
realsecure	ISS Real Secure Console Service Port
router	Local Routing Process
rpc	Remote Procedure Call (RPC) Protocol
rsvd-tcp	RSVD
rsvp-encap	RSVP ENCAPSULATION-1/2
rsvp_tunnel	RSVP Tunnel
rtc-pm-port	Oracle RTC-PM port
rtelnet	Remote Telnet service
rtsp	Real-Time Streaming Protocol (RTSP)
send-tcp	SEND
shell	Remote command
sip	Session Initiation Protocol (SIP)
sip-tls	SIP-TLS
skinny	Skinny Client Control Protocol (SCCP)
sms	SMS RCINFO/XFER/CHAT
smtp	Simple Mail Transfer Protocol (SMTP)
snmp	Simple Network Management Protocol (SNMP)
snmptrap	SNMP Trap
socks	Socks
sql-net	SQL-NET
sqlnet	SQL Net Protocol
sqlserv	SQL Services
sqlsrv	SQL Service
ssh	SSH Remote Login Protocol
sshell	SSLshell
ssp	State Sync Protocol
streamworks	StreamWorks Protocol
stun	cisco STUN
sunrpc	SUN Remote Procedure Call
syslog	Syslog service
syslog-conn	Reliable Syslog service
tacacs	Login Host Protocol (TACACS)
tacacs-ds	TACACS-Database Service
tarantella	Tarantella
tcp	Transmission Control Protocol (TCP)

telnet	Telnet
telnets	Telnet over TLS/SSL
tftp	Trivial File Transfer Protocol (TFTP)
time	Time
timed	Time server
tr-rsrb	Cisco RSRB
ttc	Oracle TTC/SSL
udp	User Datagram Protocol (UDP)
uucp	UUCPD/UUCP-RLOGIN
vdolive	VDOLive Protocol
vqp	VQP
webster	Network dictionary
who	Whois service
wins	Microsoft WINS
x11	X Window System
xdmcp	XDM Control Protocol

Corporate Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

European Headquarters
Cisco Systems International BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands
www-europe.cisco.com
Tel: 31 0 20 357 1000
Fax: 31 0 20 357 1100

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-7660
Fax: 408 527-0883

Asia Pacific Headquarters
Cisco Systems, Inc.
168 Robinson Road
#28-01 Capital Tower
Singapore 068912
www.cisco.com
Tel: +65 6317 7777
Fax: +65 6317 7799

Cisco Systems has more than 200 offices in the following countries and regions. Addresses, phone numbers, and fax numbers are listed on **the Cisco Website at www.cisco.com/go/offices.**

Argentina • Australia • Austria • Belgium • Brazil • Bulgaria • Canada • Chile • China PRC • Colombia • Costa Rica • Croatia • Cyprus Czech Republic • Denmark • Dubai, UAE • Finland • France • Germany • Greece • Hong Kong SAR • Hungary • India • Indonesia • Ireland • Israel Italy • Japan • Korea • Luxembourg • Malaysia • Mexico • The Netherlands • New Zealand • Norway • Peru • Philippines • Poland • Portugal Puerto Rico • Romania • Russia • Saudi Arabia • Scotland • Singapore • Slovakia • Slovenia • South Africa • Spain • Sweden • Switzerland • Taiwan Thailand • Turkey • Ukraine • United Kingdom • United States • Venezuela • Vietnam • Zimbabwe

205298.K_ETMG_KL_7.05

Printed in the USA