Protecting the Enterprise from Rogue Protocols

The dangers of instant messaging, peer-to-peer file sharing and other opportunistic protocols

Rogue Protocols are nonstandard application protocols that can expose confidential information, invite viruses into the network and provide conduits for malicious external attacks

Instant messaging and peer-to-peer file sharing applications have invaded the enterprise, piercing the firewall and exposing corporations to serious security, legal and compliance risks. Leveraging nonstandard protocols, also known as *Rogue Protocols*, these popular applications covertly travel through the network perimeter, rarely detected or controlled with current network security devices.

Because they use Rogue Protocols, instant messaging and peer-to-peer file sharing applications subject the enterprise to a wide range of threats. If not properly controlled, Rogue Protocols can expose confidential information, invite viruses into the network, provide a conduit for malicious external attacks, and create corporate liability due to inappropriate content and waste expensive network resources. This paper examines the risks of Rogue Protocols and addresses steps enterprises can take to control them.

The Evolution of Rogue Protocols

The traditional process of developing protocols took years of involved negotiations between standards groups

In the world of networking, traditional protocols are developed through extensive negotiations between groups. For example, the adoption of TCP, IP and HTTP protocols involved educational institutions, government organizations and standards groups working together to create a reliable communication model. The traditional process of developing protocols takes years, requires the consensus of many people and is based on negotiated policies.

With the introduction of the web, newer protocols have emerged from nonstandard methods. Because the Internet enables the mass distribution of applications, downloaded networking programs that are widely used

can contain nonstandard protocols that present a threat to the enterprise. Now employees can simply download and begin running applications that use Rogue Protocols, unaware of the security consequences to themselves or their employer.

Rogue Protocols generally include any of the following characteristics:

- Encoded in proprietary format; not based on industry standards
- Pierce the firewall without detection as the result of masquerading, port scanning and tunneling
- Expose corporate networks and assets to a variety of security risks

Rogue protocols are designed to efficiently accomplish their communication objectives regardless of corporate security standards

Consider Napster, a peer-to-peer file sharing application that used a nonstandard protocol for sharing files between two systems regardless of firewalls. Because Napster had millions of users, its Rogue Protocol became a common file sharing protocol without ever going through the rigorous, time-consuming standards process. The same can be said for AOL's Instant Messenger and the KaZaA file sharing network. Unlike traditional protocols, Rogue Protocols were developed to efficiently accomplish their objectives while bypassing existing control standards within the enterprise.

Because applications based on Rogue Protocols go undetected by corporate firewalls, enterprises face many unidentified network security vulnerabilities. As more applications begin to utilize Rogue Protocols, corporations will need a dynamic solution to monitor and control these nonstandard protocols.

The Risks of Rogue Protocols

The dangers presented by Rogue Protocols are real and have been widely reported by major security institutions and publications including CERT and the SANS Institute. There are two primary classes of Rogue Protocol risk: security and compliance management.

Rogue Protocol Security Risks

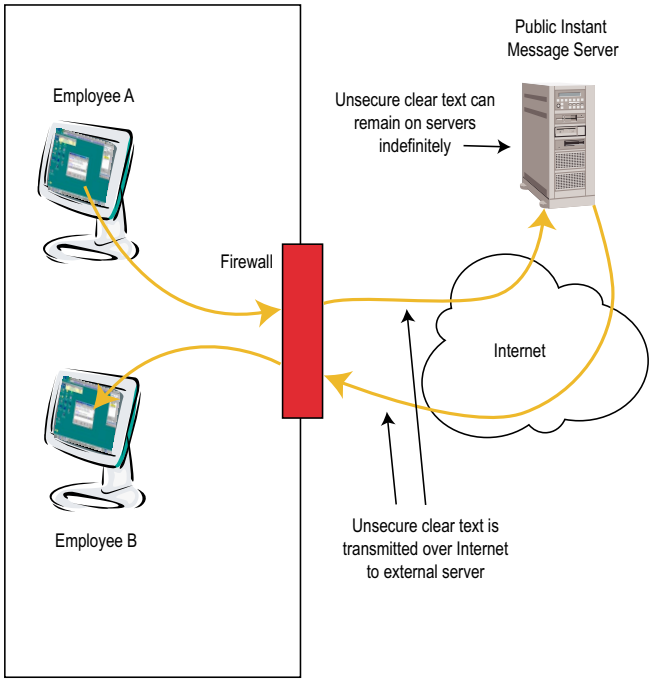
The security risks associated with Rogue Protocols include exposing outsiders to confidential content, infecting systems with viruses and opening the corporation to external attacks.

Exposure of Confidential Content

Peer-to-peer file sharing and instant messaging applications expose confidential content to outsiders

Rogue Protocol-based applications, such as peer-to-peer file sharing and instant messaging, allow outsiders to view unauthorized information or files. Confidential information can be willfully disclosed by employees or captured unknown to users. For example, with peer-to-peer file sharing, an employee could unintentionally share access to confidential information on the corporate network or on his or her system.

With instant messaging, the traffic from two communicating employees sitting across from each other actually travels outside the organization, through a public messaging server and back to the other employee (see illustration below). Eavesdroppers can intercept instant messages en route to the recipient, conversations may be logged indefinitely on a public messaging server and confidential conversations can easily be recorded by unauthorized third parties.



Using an instant messaging application, the messages of two employees communicating within a company are actually transferred in clear text over the Internet for anyone to see

Infections from Files

Damaging viruses, worms and Trojan horses can pass through firewall and virus protection systems with instant messaging and peer-to-peer file sharing protocols

With both instant messaging and peer-to-peer file sharing applications, content can pass through firewall and virus protection systems, introducing damaging viruses, worms and Trojan horses into the network. These infections can result in serious damage to important network assets and may even provide access to or control of employees' computers.

External Attacks

File sharing and instant messaging applications are notoriously buggy and can easily lead to malicious external attacks. Buffer overflow problems are common, allowing a hacker to execute code on a user's system or perform a denial of service attack. With instant messaging applications, a hacker could identify the buddies of the victim and attack them. Some web browsers have integrated instant messaging, resulting in the potential for attack without even activating the instant messenger part of the browser. Peer-to-peer file sharing and instant messaging applications that share files often allow third parties to view the user's IP addresses, increasing the risk of an attack.

Corporate Management and Government Compliance

Applications that use Rogue Protocols often go unrecognized by IT departments, making it difficult to enforce corporate and governmental policies. In the financial industry, regulators mandate that financial services companies log all electronic communication with customers, including instant messages. Because instant messaging traffic is not logged by existing network security systems, corporations can not fully comply with regulations.

It is impossible to fully enforce corporate policy if Rogue Protocol communications evade existing security systems

Enforcing corporate policy is challenging if the activities in question are undetected. Corporations may not want employees using the network to transfer music or other files to outside entities. Simply blocking ports will not solve the usage problem because instant messaging and peer-to-peer file sharing applications scan for open ports and may also tunnel through port 80 (the port used for web traffic).

Extending employee Internet management to Rogue Protocol-based applications is not possible if the protocols are difficult to detect and control. There may

be a need to scan messages and files for potentially damaging content such as pornography or encrypted transmissions.

Finally, there's the issue of employee productivity. Some organizations want to control the use of instant messaging to ensure their staffs are not spending excessive time with personal communications. File sharing applications bog down the corporate network at the expense of normal business traffic, impacting the response time for employees and customers, leading to lower productivity.

Because more than 30 percent of corporations are using instant messaging applications and the number is projected to reach 70 percent by 2003, there are clear and present dangers that must be addressed (Osterman Research, March 2002 and Gartner, October 2001, respectively).

The Solution:
Akonix L7 Perimeter Security Gateway

Akonix L7 is the first perimeter security application dedicated to reducing the risks of Rogue Protocols

For enterprises seeking to detect and control Rogue Protocols, Akonix offers Akonix L7, a powerful security gateway that guards the network at its perimeter. Akonix L7 extends the capabilities of the firewall, keeping confidential communications inside the boundaries of the network while preventing outsiders from leveraging the security weaknesses of Rogue Protocols.

Akonix L7 is the first perimeter security application that eliminates the risks of Rogue Protocols by subjecting them to standard network security policies.

Unauthorized connections are blocked while authorized communications occur within corporate-defined Akonix L7-imposed policy constraints. Additionally, Akonix L7 logs and reports all Rogue Protocol activity to bring corporations in compliance with internal policy and industry regulations.

Engineered for change, Akonix L7 is designed to adapt to new Rogue Protocol threats via easy to install protocol updates. The current version of Akonix L7 supports all major public instant messaging protocols and the next release will add popular file sharing protocols.

Benefits of Akonix L7

Akonix L7 provides a wide range of security, policy, compliance and management benefits to enterprises.

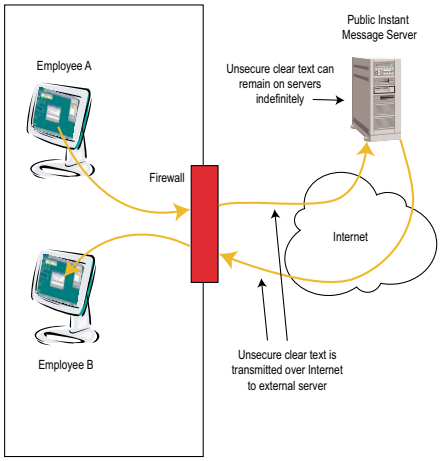
Security Benefits

- Keeps interactions between employees secure within the network perimeter or over a wide area network via virtual private networking (VPN)
- Prevents unauthorized content from being shared via peer-to-peer file sharing and unauthorized discussions from occurring with instant messaging
- Stops Rogue Protocols from letting viruses, worms and Trojan horses slip through the firewall
- Blocks outdated Rogue Protocol-based desktop applications that are susceptible to hackers
- Manages protocol traffic to prevent unauthorized use of Rogue Protocols
- Seals potential security holes common with Rogue Protocols

Instant Messaging Example

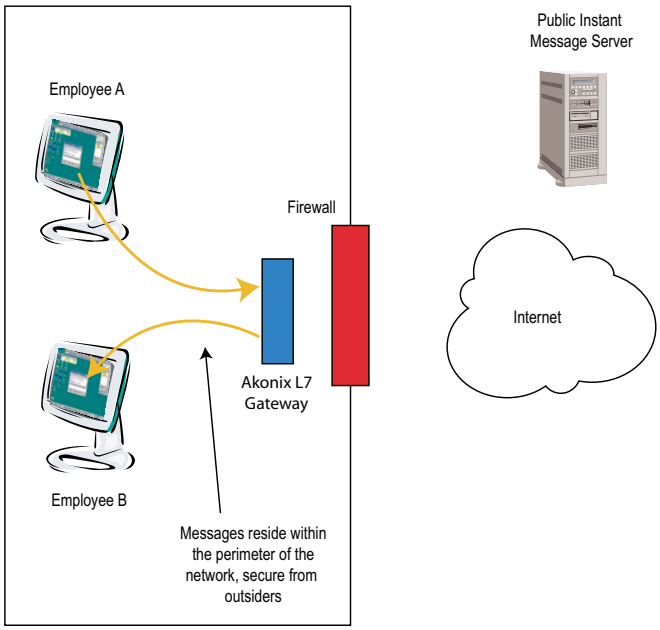
Without Akonix L7, instant messaging traffic is exposed to outsiders and remains on public messaging servers indefinitely

Without the Akonix L7 solution, instant messages between employees located within and external to the network are delivered in plain text over the Internet to public servers (see illustration to right).

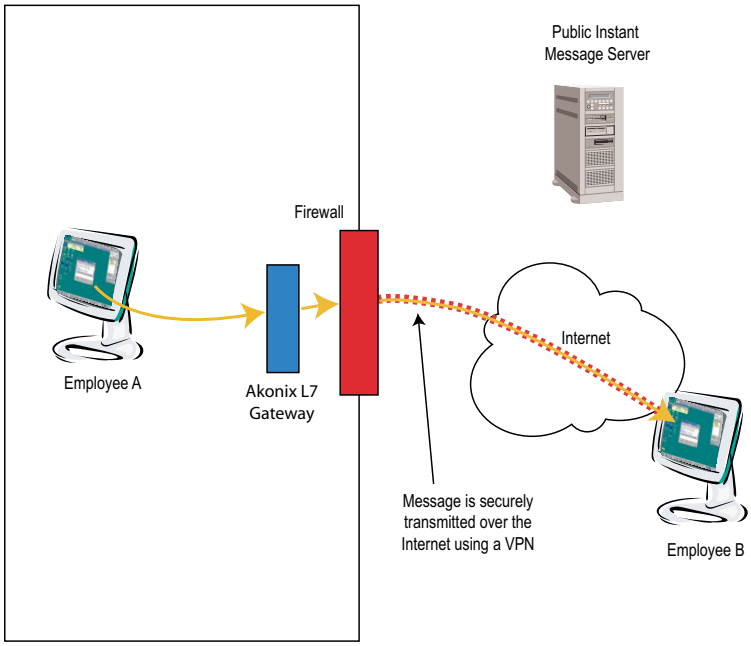


The result is that confidential communications are open to interception by outsiders. Akonix L7 secures instant messaging traffic while taking both the Internet and public servers out of the communication path. Akonix L7 also associates screen names with corporate identities to provide a layer of protection against impersonation.

Akonix L7 allows the instant messaging communication between two internal employees to remain within the network (see illustration below). The Akonix L7 Gateway, independent of the firewall and external messaging servers, transparently handles communication.



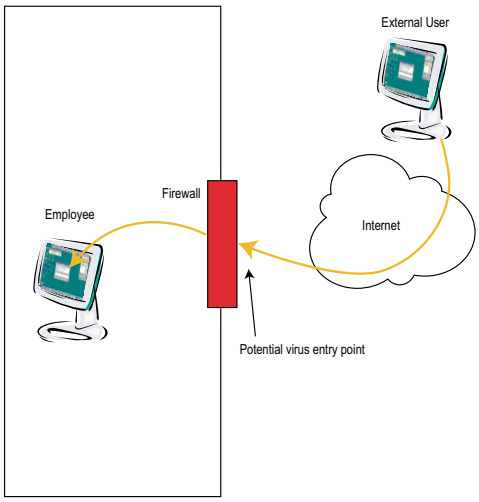
Alternatively, Akonix L7 allows secure communications between authorized users located outside the network via a secure VPN. In this case, the Akonix L7 Gateway transmits messages to the firewall and over a VPN to the receiving party (see illustration below).



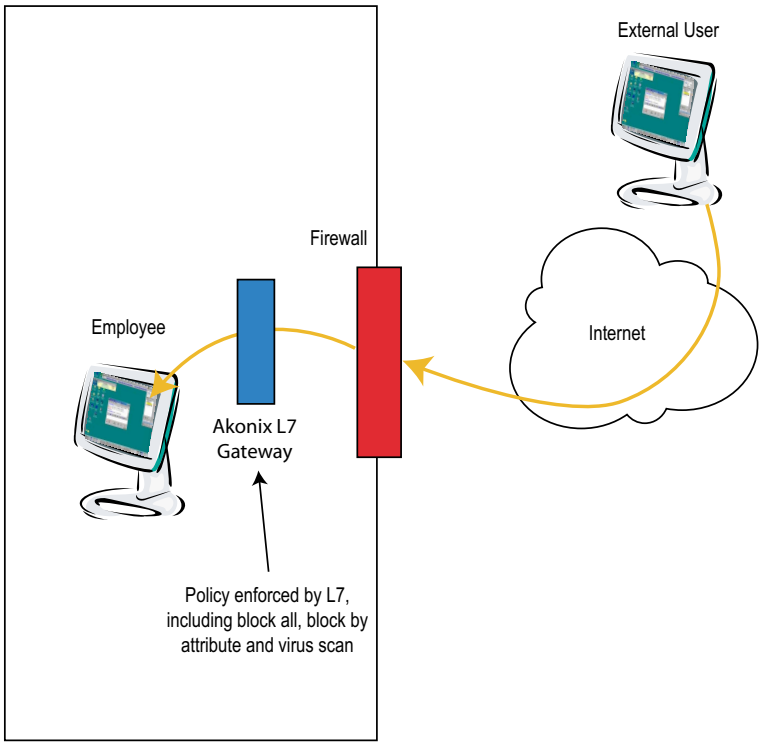
With Akonix L7, external instant messaging communication remains secure via a VPN, free from Internet threats

Peer-to-Peer File Sharing Example

Without the Akonix L7 solution, peer-to-peer file sharing applications allow employees to download files while circumventing policy enforcement and centralized virus scanning mechanisms (see illustration to right).



Akonix L7 can control or block peer-to-peer file sharing use based on attributes such as sender, recipient, message content and file attachment type, size and name (see illustration below). Message content and file names can be further controlled based on keywords and pattern matching. Akonix L7 can also interface with centralized virus scanners to assure that all files transmitted are virus-free.



Corporate Policy and Industry Compliance Benefits

- Logs and records messages and file exchanges for industry compliance and investigations
- Automates policy enforcement and tracks usage at the group or employee level
- Impedes inappropriate messages and files that may contain unsuitable content such as pornography and pirated content, reducing the risk of lawsuits because of improper content transmission
- Blocks the use of specific terms from instant messages that are forbidden by corporate policy (i.e., words like *guarantee* or *confidential* and offensive language)
- Provides an audit trail showing who is transferring what content to what location at what time and to whom
- Provides analysis at the employee level for forensics purposes

Management Benefits

- Controls employee use of Rogue Protocol-based applications at granular levels including user, group, time of day and keyword content
- Provides a layer of protection from impersonation by associating screen names with corporate users via interfaces with enterprise corporate directories such as Active Directory, NTLM and LDAP
- Allows management across multiple gateways from a centralized location
- Provides application version control to assure employees are using authorized and up to date software
- Supports all major instant messaging applications: AOL Instant Messenger, ICQ, Yahoo! Messenger, MSN Messenger and IRC
- Includes a rich API and scripting language for site-specific customization
- Generates a variety of high-level reports such as what applications are being used, how many messages are being transmitted each day, who the top users/abusers are and how many attachments are being transmitted
- Helps recover lost bandwidth and storage due to restricting peer-to-peer file sharing
- Limits lost productivity from non-business use of instant messaging and peer-to-peer file sharing
- Increases network responsiveness by selectively blocking file transfers that can bog down the network

Summary

Akonix L7 is the solution for corporations seeking protection against applications that use Rogue Protocols, such as instant messaging and peer-to-peer file sharing. Designed to prevent Rogue Protocols from piercing the firewall and exposing corporations to serious security, legal and compliance risks, Akonix L7 is the first perimeter security application that eliminates the risks of Rogue Protocols by subjecting them to standard network security policies.

Akonix Systems, Inc., is a network security software company dedicated to protecting corporate networks against the dangers of Rogue Protocols. Founded in the summer of 2000, Akonix is headquartered in San Diego, California. To learn more about Akonix or Akonix L7, or to download a free trial version of Akonix L7, visit www.akonix.com.