Proofpoint Network Content Sentry

As enterprises have become increasingly concerned about enforcing outbound email policies, defending against leaks of confidential information and ensuring compliance with regulations, they are also realizing the risks presented by other outbound messaging streams including HTTP and FTP traffic. A recent survey by Proofpoint and Forrester Consulting[1] found that more than half of companies polled were concerned or very concerned about web-based email as a source of private information leaks. A similar number say that it is important to reduce the risks associated with outbound HTTP traffic. The Proofpoint Network Content Sentry extends Proofpoint's data loss prevention and content security features to additional outbound message streams including web-based email, blog and message board postings and other HTTP- or FTP-based activity.

overview

The Proofpoint Network Content Sentry™ is a hardware appliance that inspects all outbound network traffic in real time, monitoring for confidential information, private customer or employee data (including private healthcare, financial or identity information) and other sensitive content that may leak outside the enterprise. When such breaches are detected, the Proofpoint Network Content Sentry—working in concert with Proofpoint Protection Server™ software or the Proofpoint Messaging Security Gateway™ appliance—actively alerts managers (such as compliance officers) so appropriate actions can be taken.

Enhanced protection for intellectual property and improved compliance

By adding the Proofpoint Network Content Sentry to your Proofpoint software or appliance deployment, you can apply the same content security, regulatory compliance and acceptable use policies defined for SMTP-based email to HTTP and FTP protocol-based communications.

○ **Intellectual property and confidential information protection:** In conjunction with the Proofpoint Digital Asset Security™ module, the Proofpoint Network Content Sentry monitors outbound network traffic for any type of confidential asset. Leveraging Proofpoint MLX™ message classification techniques, Proofpoint Digital Asset Security analyzes and classifies confidential documents and then continuously monitors for that information, or parts of that information, in outgoing network traffic. Proofpoint Digital Asset Security can be used to protect hundreds of document types including email messages, text files, word processing files, source code, CAD drawings, spreadsheets and presentation formats.

○ **Privacy protection and regulatory compliance:** In conjunction with the Proofpoint Regulatory Compliance™ module, the Proofpoint Network Content Sentry monitors outbound network traffic for a wide array of non-public information including PHI (protected health information including drug names, disease names, patient identifiers and treatment codes as defined by HIPAA), personal identifiers (including US Social Security Numbers and UK National Insurance Numbers) and personal financial information (such as credit card numbers and ABA routing numbers). This module also accurately detects Japan's Jyuminhyou (residence registration), driver's license IDs and international credit card numbers. Proofpoint's "smart identifiers" ensure accurate detection of private information with low false positives.

[1]Outbound Email Security and Data Loss Prevention in Today's Enterprise, 2008.

Enterprise Content Security

Beyond the inbound messaging threats of spam, viruses, and phishing attacks, corporations, universities, and government organizations are looking for messaging security solutions that help them enforce outbound email policies, defend against leakages of confidential information, and help them comply with email-related regulations. Proofpoint provides a complete suite of easy-to-configure modules that solve these problems.

Along with the Proofpoint Network Content Sentry, Proofpoint's Content Compliance™, Digital Asset Security™, and Regulatory Compliance™ modules represent a complete content security solution for today's enterprise.

Content security modules

○ Proofpoint Content Compliance allows enterprises to define and enforce acceptable-use policies for message content and attachments.

○ Proofpoint Digital Asset Security keeps valuable assets and confidential information from leaking outside your organization. Proofpoint MLX technology creates a statistical representation of documents and then compares all messages against these statistical representations, looking for matches.

○ Proofpoint Regulatory Compliance protects your organization from liabilities associated with privacy regulations such as HIPAA and GLBA by accurately detecting private financial, healthcare and identity data in outgoing messages.

Proofpoint Network Content Sentry

features

Robust HTTP and FTP protocol monitoring

The Proofpoint Network Content Sentry intelligently captures and reconstructs all outbound HTTP and FTP protocol traffic at high data rates. All HTTP posting activity—such as web-based email posting (including webmail services such as MSN Hotmail, Yahoo! Mail, AOL Mail and Google GMail), blog postings, message board submissions, use of web-based file storage systems (such as GMail FS) and other general posting activity—is intercepted and scanned for information leaks and policy violations.

The system monitors both active and passive mode FTP transmissions of binary or text files sent to remote servers. As with HTTP posting, a wide variety of policies can be enforced around FTP activity, including monitoring for specific files, file size limits and detecting FTP transmissions to inappropriate destinations.

Flexible policy definition and incident management

The same interface used to define outbound SMTP-email policies is used for setting Proofpoint Network Content Sentry policies. Each policy can trigger based on specific document type and a customizable document similarity score. HTTP- or FTP-based messages that trigger a policy can be quarantined for further review.

Proofpoint's Compliance Incident Manager™ interface makes it easy for business users—such as compliance, security, risk management, HR and other line-of-business managers—to administer their own email and network content security policies, review violations, approve exceptions and monitor incidents through an easy-to-use interface and email-based notification system. The Compliance Incident Manager actively notifies managers of policy violations and associated severity levels, so they can easily and effectively track and review non-compliant messages and release, reroute, approve or otherwise manage incidents using Proofpoint's graphical user interface.
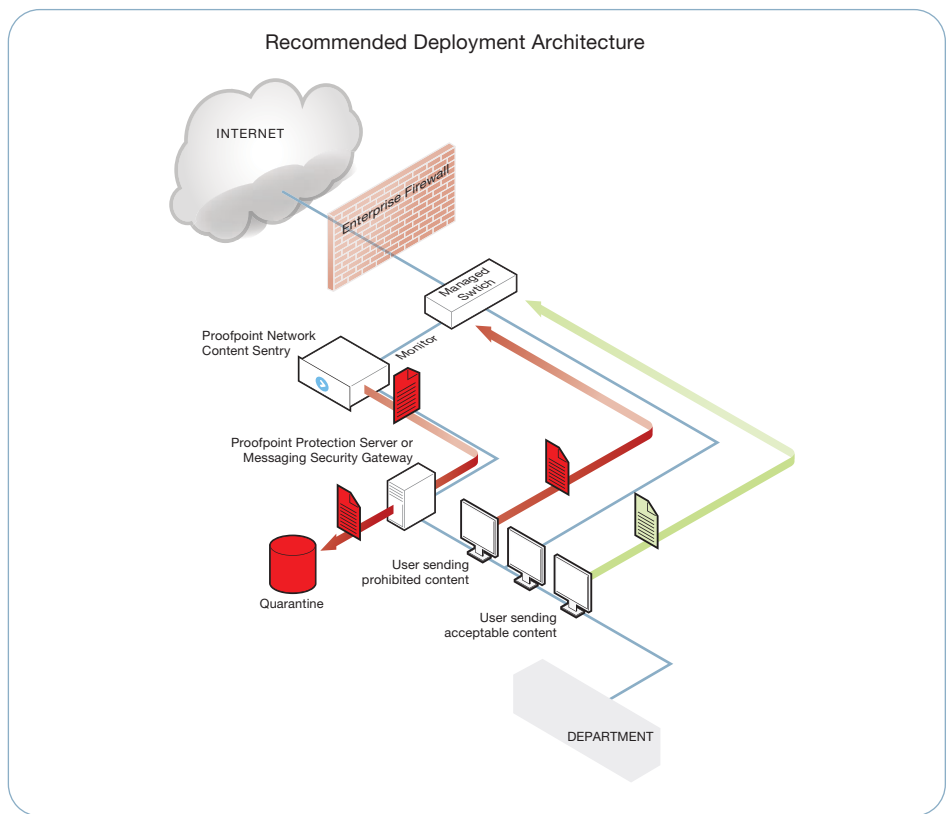
Supported protocols

Proofpoint Network Content Sentry captures and analyzes all outbound HTTP and FTP traffic. Detection capabilities include:

HTTP webmail posts including:

- MSN Hotmail
- Yahoo! Mail
- AOL Mail
- Google GMail (webmail as well as Gmail FS File System transfer)
- Lycos webmail
- Network Solutions webmail
- Comcast webmail
- Custom webmail applications

Generic HTTP posts including:

- Web blog postings
- Message board postings
- General HTTP posts, attachments and web form submissions

FTP traffic:

- Transmitted text or binary files
- Supports active and passive mode FTP

Deployment options

Any Proofpoint appliance can be configured as a Proofpoint Network Content Sentry, installed at the egress point of your enterprise network.

- The appliance should be connected as close to the firewall as possible on the inside. If connected in front of the firewall, client IP information cannot be captured.

- There are two deployment options for capturing HTTP and FTP traffic:
    1. Attach to the span port of a managed switch or router.
    2. Connect via a network tap into the live egress network stream.

- There are two network ports on the appliance. One is a management port for connection to the LAN. The second port is the capture port ("Monitor" in the diagram at left), which is promiscuous and does not require an IP address.

Recommended Deployment Architecture

INTERNET

Enterprise Firewall

Managed Switch

Monitor

Proofpoint Network Content Sentry

Proofpoint Protection Server or Messaging Security Gateway

Quarantine

User sending prohibited content

User sending acceptable content

DEPARTMENT