Dialogic®
Making Innovation Thrive™

White Paper

Safe and Secure Faxing with Dialogic® Brooktrout® Fax Boards

Safe and Secure Faxing with Dialogic® Brooktrout® Fax Boards

White Paper

Executive Summary

IT administrators look for solutions that balance the need for network security with those of reducing costs and incorporating new technology. This white paper explains how fundamentally different Dialogic® Brooktrout® TR1034 Fax Boards are from data/fax modems when it comes to impacting security for the fax data. It also discusses three types of threats that can be introduced into a network when not using a secure fax technology like that provided by the Brooktrout TR1034.

Safe and Secure Faxing with Dialogic® Brooktrout® Fax Boards

White Paper

Table of Contents

Safe and Secure Faxing with Dialogic® Brooktrout® Fax Boards

White Paper

Introduction

In today's fast moving Internet economy, protecting a network from malicious hacker attack, virus, worm, or fraud is more than a concern; it is a necessity.

Connecting a fax server to a network can save a company time and money in terms of reduced labor costs and improved productivity. However, for IT administrators, concerns revolve around security issues, such as network break-ins through their fax server, and security breaches that could surface as their companies migrate voice and data networks to IP.

This white paper discusses three types of threats that can affect corporate networks and how adding a fax server using Dialogic® Brooktrout® TR1034 Fax Board instead of a data/fax modem does not impact the security of the entire network.

Dialogic® Brooktrout® Fax Boards "Fax Only" Security

Unlike other alternative fax boards that are dual-purpose fax and data modems, Brooktrout TR1034s transmit information only via the T.30 and T.38 "fax only" protocols. By using only these specific protocols, the Brooktrout TR1034 fax boards, when interfacing to the outside network, do not impact the security risk to the entire network.

T.30 is a fax handshake protocol that describes the overall procedure for establishing and managing communication between two fax devices. Because T.30 does not allow for the processing of data or the transmission of data, and only allows for the transfer of fax images (known as T.4 and T.6 images), there is no way to pass data through the fax server, either for removing data from the network or uploading malicious code.

T.38 is an IP-based protocol that closely inter-works with T.30 to enable the same fax procedures over IP in real-time. T.38 only passes images, not files that could potentially contain viruses, worms, or Trojans. T.38 also only handles image data that is not executable.

A "fax-only" Brooktrout TR1034 interprets the content of the data that was sent to it, either over the PSTN or over the IP network, prior to passing it on to the network. This interpretation means that malicious code cannot pass through the Brooktrout TR1034. If the data is not a valid T.30 message, it gets dropped. If anything other than image information is embedded in the image data, the error handling that is implemented during image decoding discards it.

Other types of fax boards are just simple data modems that support both the V.90 and V.92 protocols, which are 56 kbps data transfer standards and have data exchange capability. Data modems are merely transport devices that do not interpret the data packets they are carrying, which means that when a data modem is connected to the network it is just like having an IP connection to the computer network. A data modem, because it allows the transfer of data, and not just fax images like the Brooktrout TR1034, makes a network susceptible to security breaches by potential hackers, viruses, worms, or Trojan horses.

If a company decides to switch its fax traffic from PSTN to IP, a fax server running a Brooktrout TR1034 will not introduce additional vulnerability to the network.

Still Secure Despite the Type of Threat

This section discusses the types of security threats facing company networks and reveals how fundamentally different Brooktrout TR1034 and its data/fax modem alternatives are when it comes to impacting security for the fax data.

IT administrators are concerned with three types of security threats to their networks:

- An attack on the network itself
- Privacy infringement
- Information content theft

Network Attack

A network attack, such as denial of service, consists of a virus or malicious attack by a hacker. This type of attack is in most cases stopped by the network's security products, such as firewall and virus protection software. However, if a malicious packet did get through the firewall, then "fax only" T.30 protocol used by a Brooktrout TR1034 will immediately recognize that it is a non T.4/T.6 or T.30/T.38 packet and drop it.

The following are the four main levels where a packet can be identified as an improper packet:

- It is not a valid T.38 packet
- It is not a proper T.30 message
- It is not a proper T.4/T.6 image
- It is not a proper T.30 message or T.4/T.6 image for the point in the call that it appears

In the event that the network does not have an appropriate firewall, or malicious code was spawned within the company WAN by an employee, then the malicious packets will be discarded if they attempt to go through the Brooktrout TR1034. The Brooktrout TR1034 will examine each packet, recognize the malicious code as an invalid T.4/T.6 or T.30/T.38 fax packet, and drop it. If it is not a valid T.30 or T.38 packet, there is no communication path to the network via a Brooktrout TR1034.

Unlike a Brooktrout TR1034, a dual-purpose fax and data modem that supports V.90 or V.92 would allow these packets through when in a non-fax mode.

Privacy Infringement

A privacy infringement involves a fax being intercepted in transit and read by someone other than the designated recipient or fax machine. In a real-time Fax over Internet Protocol (FoIP) setting, a Brooktrout TR1034 that is IP-enabled does not pose an additional risk to privacy because the IP portion of the fax traffic is contained within a properly configured and secure enterprise Wide Area Network (WAN). Within this enterprise WAN, FoIP transmission can take place in the following two scenarios:

- Fax originating on the PSTN to a T.38 endpoint
- T.38-to-T.38 endpoints connected to IP WAN

The first scenario is a fax origination on the PSTN, being sent over the PSTN to a T.38 endpoint, as shown in the Figure 1 example.

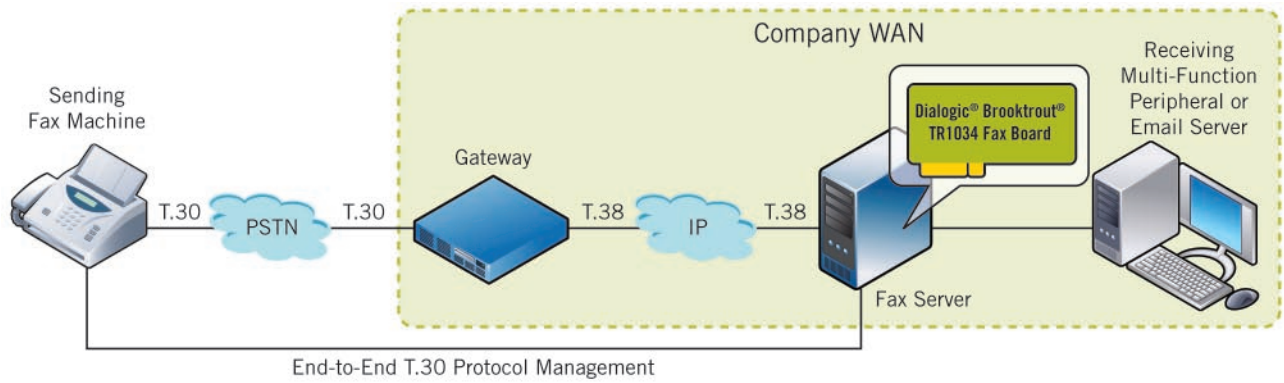

Figure 1. Fax Originating on the PSTN Sent to a T.38 Endpoint

In this scenario, the PSTN portion of the fax transmission is secure, just like today's standard PSTN-based fax transmissions, because hacking into a PSTN line requires physical access to the line or switching equipment. In addition, the T.30 protocol only permits passage of T.4/T.6 image streams between Group 3 fax image transmission devices, so there are no opportunities to add rogue content. Also, in many countries there exist Federal Laws that prevent wiretapping, thus providing another safeguard for the PSTN portion of the fax transmission. On the IP portion of the fax transmission, when the fax passes through the T.38 gateway, it travels across the enterprise WAN, or private IP network, which under normal business practices is also safe and secure from external threats because it is internal to the company.

The second scenario is a T.38 endpoint sending a fax to another T.38 endpoint that is connected to an IP WAN, as depicted in the Figure 2 example.

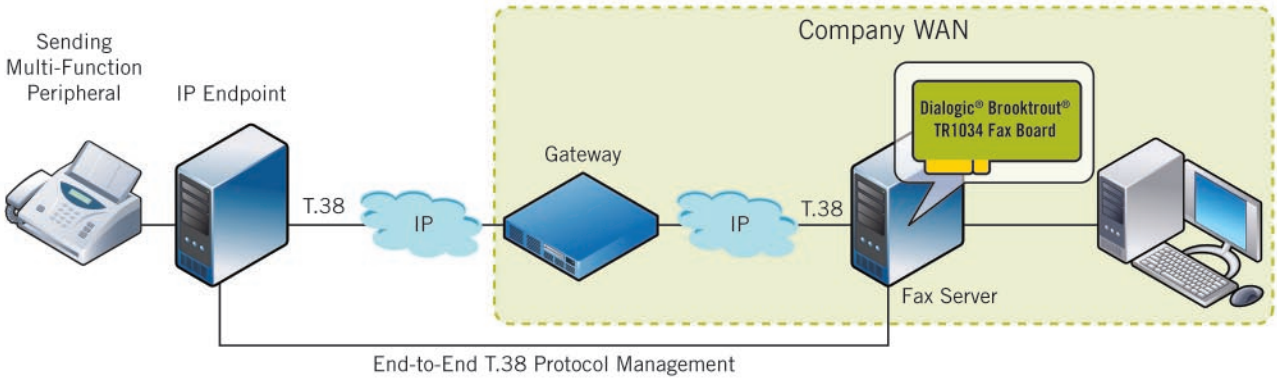

Figure 2. T.38-to-T.38 Endpoints Connected to IP WAN

In this scenario, the fax that is transmitted from a multi-function peripheral is converted to T.38, and then travels over IP to a gateway located on the company WAN. As in Scenario 1, when the fax is on the company's internal WAN and thus is normally safe and secure. A security breach could conceivably occur due to an employee internal to the company attempting to meddle with the IP traffic inside the WAN, but that is an IP network issue that needs to be addressed for all IP applications; fax presents no additional security issues of this sort. An example of a solution to cover passage within an enterprise is the use of a VPN to connect the T.38 gateway and T.38 endpoint, or T.38 endpoint to T.38 endpoint, in order to limit the risk to only include those persons authorized to use the corporate VPN resources.

Content Attack

The third threat scenario is a content attack, which means that the fax content is intercepted and altered. Again, as with a privacy infringement threat, this is very difficult to do in PSTN mode due to wire tapping laws and the difficulty intercepting a fax transmission over the PSTN. In IP mode, the fax would travel over IP only over the enterprise WAN, which would be protected behind a properly configured firewall, and again, as with the privacy infringement threat, a Brooktrout TR1034 that is IP-enabled does not pose an additional risk to privacy because it is contained within the WAN. Even within the company, a hacker would need complex software tools in order to decode the fax image, T.30 protocol, and ASN.1 (Abstract Syntax Notation), which underpins T.38. It would pose a very formidable challenge to decode, change, and re-encode T.38 packet content in real-time without causing the session to end due to timeouts. Again, as with any IP network, these are network security issues that would be addressed by standard network security products. The public portion of the fax transmission would travel over the PSTN via T.30 and would be at no greater risk than if it were transmitted in standard PSTN format.

Safe and Secure Faxing with Dialogic® Brooktrout® Fax Boards

White Paper

Summary

The Dialogic® Brooktrout® TR1034 Fax Boards provide safe, secure, and reliable fax transmission capability.

For PSTN connections, the Brooktrout TR1034s use the T.30 "fax-only" protocol, which does not have any data exchange capability, unlike fax boards that support the V.90 or V.92 protocol.

For IP connections, the Brooktrout TR1034 support the T.30 and T.38 fax protocols only, which, as previously discussed, are two "fax-only" protocols that do not allow the transmission of data. In addition, choosing to install a real-time FoIP solution into an organization's network does not pose an additional risk, as the IP-enabled fax server would sit within a WAN and behind a properly configured firewall. Dialogic® Brooktrout® onboard "fax-only" processing will recognize the non-T.30/T.38 packets attempting to enter the network through the fax server and drop them. If a packet is not a valid T.30 or T.38 packet, then it has no communication path to the network through a Brooktrout TR1034 fax board.

Consequently, choosing to install an FoIP solution using a Brooktrout TR1034 does not pose an added threat to network security because trying to gain access to the organization's network through a Dialogic Brooktrout-based fax server would be like trying to hack into a standalone fax machine.

For More Information

Dialogic® Brooktrout® TR1034 Fax Board —
http://www.dialogic.com/products/tdm_boards/fax_boards/TR1034.htm

Dialogic®
Making Innovation Thrive™

www.dialogic.com

Dialogic Corporation
9800 Cavendish Blvd., 5th floor
Montreal, Quebec
CANADA H4M 2V9

08/08 11044-01