OWL Cyber Defense

WHITE PAPER

Secure Printing

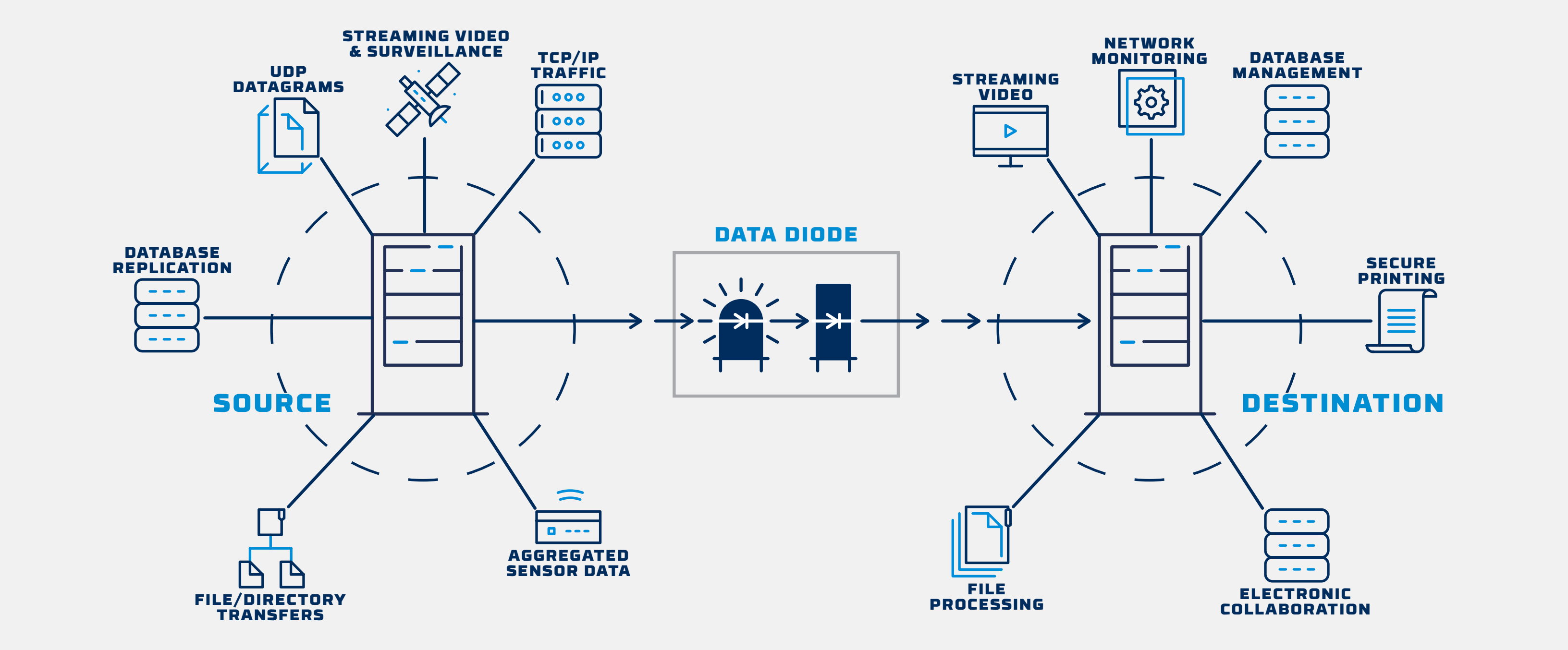
Using TCP Packet Transfer System

Abstract

This document describes the use of Owl TCP Packet Transfer System (TPTS) for secure printing across isolated network security domains.

Introduction

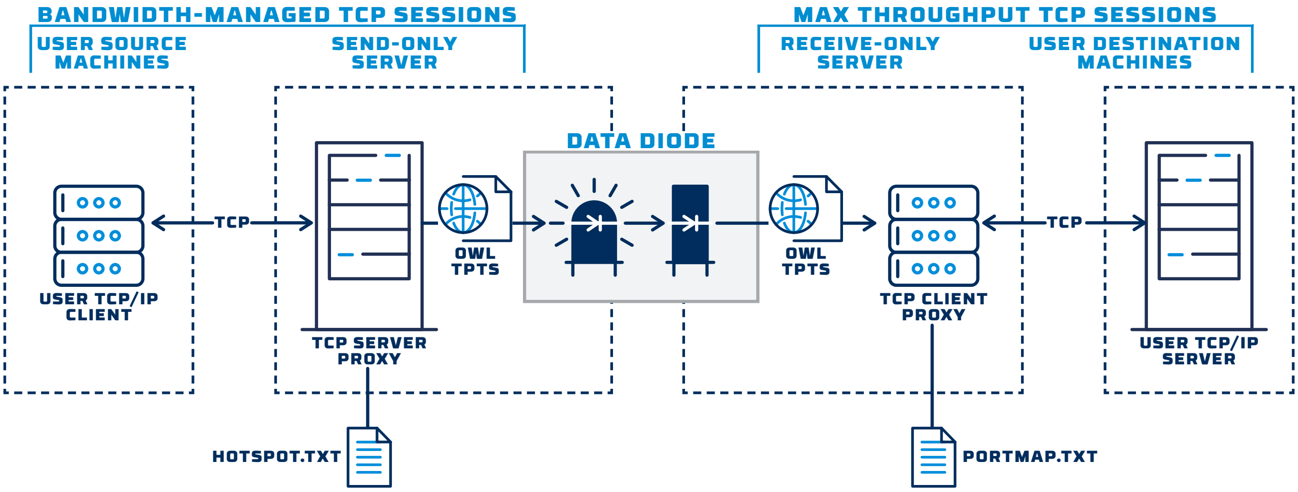
Owl products are one-way data transfer systems that provide network security in both the physical and logical sense. They are used to isolate high security networks from external threats, while allowing them to import or export data at high speed in a controlled way. Significant hardening of existing networks is achieved by separating inter-network communications into one-way data transfers. One-way data transfers naturally compliment the inherently different security checks required for transferring data to (read-up) or from (read-down) any isolated high-security domain. Among other advantages, one-way data transfers deny the possibility of network probing for vulnerability; a prelude for most cyber attacks. Intelligent utilization of one-way data transfer also simplifies creation of data archives whose contents cannot be deleted, corrupted, or repudiated. Unlike commercially available firewalls, Owl data diode technology hardware is designed to pass information in one direction only at high throughput rates. It is physically impossible to send messages of any kind in the reverse direction. This "trust nothing" design ensures that data residing on the isolated LAN is fully protected. Owl physical one-way links provide a true "protocol break" and cannot be hacked with software.



All Owl hardware is EAL certified, according to Common Criteria standards jointly developed by the National Institute of Standards (NIST), the National Security Agency (NSA), and a number of similar international organizations. Using non-specialized "commodity" components from the telecommunications industry, our latest generation Owl hardware attained the widely respected EAL4 certification by subjecting its engineering designs to rigorous independent security analysis. Owl continues to actively develop and improve its products in performance, function, and certifications. Owl products are recognized by all major US accreditation organizations as providing the controlled interface components for many existing Cross Domain Solutions. Owl products are used by the government intelligence community and DOD for isolating their high security networks. Using Owl one-way TCP Packet Transfer System (TPTS), it is easy to route print jobs to or from high security networks without using specialized software.

TCP Proxy Communication

Construction of a TCP Socket requires bilateral communications, and cannot be implemented directly across the one-way link. However, Owl TCP Packet Transfer System creates TCP proxy interfaces in the Sending and Receive machines as shown.



TCP Applications Running in Send and Receive Machines

The TCP Server Proxy is "tuned" to receive packets at predetermined throughput limits that are matched to the capabilities of the Receiving Client (red) on the other side of the one way link. If TCP packets arrive while the socket is busy reading, they are pushed back to the sender. This provides upstream notification of data throughput limits during periods of maximum use.

Closing the socket on the BLUE side will close the socket on the RED side. Any data transfer error identified by the Owl RED machine will close the socket connection on the RED side. In this way, only correct data is transferred to the destination machine. Any data sent from the destination machine to the RED machine is blocked and discarded since our hardware moves the payload in a unidirectional manner.

Data Transmission at the Transport Layer

The actual data transfer is performed through a proprietary protocol that does not involve the TCP/IP stack, and does not pass IP information across the link. IP routes are defined at the time of system configuration in the form of channel mapping tables, which will be described in greater detail below.

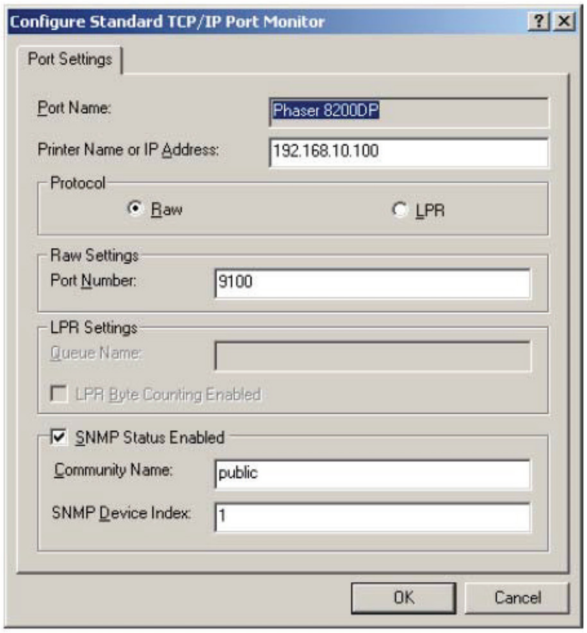
When IP packets are received by the Send (Blue) computer, IP information normally carried in the packets is replaced with pre-assigned channel numbers. After passing across the one way link, the channel numbers are mapped to their predetermined IP destinations in the Receive (Red) computer. The mapping tables residing in Send and Receive machines are different. Neither table alone can be used to construct the other, and neither table alone provides IP routing information that might compromise security of the overall system. TCP/IP proxy software provides standard network connectivity on either side of the one-way link, but no message traffic is possible from Receiver to Sender. Data integrity is verified in several ways during transfer across the one-way link. The integrity of every ATM cell is verified in hardware using CRC tests, and ATM cell sequence numbers are tracked, in accordance with the AAL5 communication protocol. Advanced hash algorithms are used to verify the integrity of data at the IP packet level. Packet sequence numbers are also tracked. The Send machine calculates a hash number for the contents of each packet, the Receive machine recalculates the hash number, and the results are compared. In the rare occurrence of unequal hash numbers, the packet is dropped and an error is logged. Packet sequence numbers are tracked. The integrity of larger data structures assembled from IP packets is verified in similar fashion. Owl systems have proven exceptionally reliable. When Send and Receive machines are matched in performance and properly configured, packet losses are extremely rare.

Secure Printing

Secure printing across Owl one way link does not require special purpose software. Once Owl system is configured, print jobs are simply sent to an established IP address and port number on the Send machine. Owl system routes the print job to the appropriate destination device as shown in Figure 5. Available routes are established at time of system configuration.

The TPTS can be configured as a printer proxy server for delivering print jobs from the BLUE side to a network printer on the RED side. This will work for using the printer protocol, RAW, instead of LPR, which usually means sending print jobs to port 9100 of the network printer. Each print job will be treated as a new TCP session; the TCP session ends at the end of the print job. For Windows users, the normal network printer set up would appear as shown below.

This window is accessed via the printer settings: Properties › Ports › Configure Port.



Configure Standard TCP/IP Port Monitor

Port Settings

Port Name: Phaser 8200DP

Printer Name or IP Address: 192.168.10.100

Protocol: ● Raw ○ LPR

Raw Settings
Port Number: 9100

LPR Settings
Queue Name:
□ LPR Byte Counting Enabled

☑ SNMP Status Enabled
Community Name: public
SNMP Device Index: 1

Network Printer Settings

For secure printing, the printer IP address and port number point to the Send (blue) machine. IP addresses and port numbers are set at time of Owl system configuration.

Note that printer problems cannot be detected by the Send machine, due to the inherent nature of the one-way link. TPTS does not manage printer problems, such as “out of paper,” or “printer offline.” At time of system configuration, it is suggested that buffer and timeout parameters be tuned to the anticipated file sizes for the largest printing jobs.

OWL Cyber Defense

Owl Cyber Defense Solutions, LLC leads the world in data diode and cross domain network cybersecurity. With a constant focus on customers in the military, government, critical infrastructure, and commercial communities, Owl develops market-first, one-way data transfer products to meet a variety of operational needs, from entry level to enterprise.

For more information on Owl, or to schedule a demo, visit www.owlcyberdefense.com

@OwlCyberDefense

203-894-9342 | Info@owlcyberdefense.com