CPI

The OpenFox Company®

OpenFox® Proxy Server

OPENFOX® PROXY SERVER

Computer Projects of Illinois, Inc. (CPI), with its headquarters in Bolingbrook, Illinois, is a privately held corporation and an acknowledged leader in information-sharing software systems for the law enforcement and criminal justice community.

CPI is the only information sharing solutions provider that focuses solely on the unique needs of professionals in the law enforcement, and criminal justice fields. Simply, CPI products act as conduits that allow information to flow easily between various systems such as NCIC and NLETS.

Because of CPI's focus, over half of all law enforcement users within the U.S. (including federal, state and local agencies) rely on our comprehensive and proven OpenFox® suite of information sharing products.

In Brief

The OpenFox® TCP Proxy Server allows users to access secured information from unsecured locations such as the internet, without exposing the server application. It is an extremely cost effective, easy-to-maintain tool that allows law enforcement and criminal justice users lacking traditional private network connectivity the ability to access secure law enforcement information without exposing the system to internet threats.

Overview

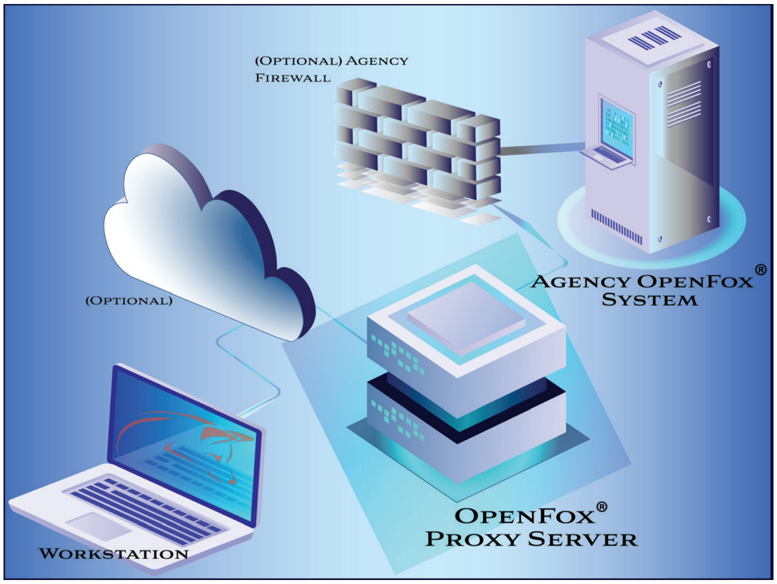
Application Example – State officials propose a Messenger workstation in the lobby of all Sheriff offices in order for their personnel to register sex offenders via the Internet.

Other users who are not true law enforcement personnel, such as prosecuting attorneys or homeland security employees, generally do not have broad access to the system. Using the Proxy Server, they can access the information they are cleared to receive. Casual law enforcement users can run queries for investigative purposes without disturbing a busy dispatcher.

Technical Information

In general, the function of a proxy is to perform connections and access requests on behalf of a requesting client without the client directly accessing the services being requested.

The TCP Proxy Server is a stand-alone application running on the public-facing gateway server. The proxy front-ends the unsecured locations and provides a pathway to connect these locations to the Desktop launch page and the FoxTalk protocol port without allowing a direct Internet connection to the application server. Because the TCP Proxy Server is developed in JAVA, it can execute on a Unix, Linux or Windows platform.

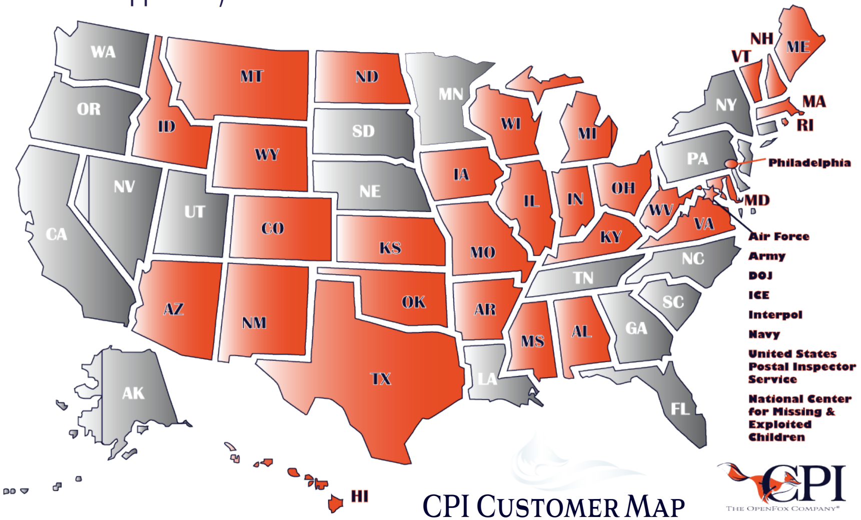


The TCP Proxy Server will listen on both the Tomcat Web server port and the FoxTalk protocol port for connection requests from the Internet. When these requests arrive, the program grants the connection and inspects the security file to determine if the requestor is valid. If the originator is valid, the proxy will request a connection to the resource requested; either the Tomcat port or the FoxTalk port on the application server. The application server will see all inbound connections from the unsecured locations as arriving from the proxy server IP address and will identify the device from the license data exchanged after connection.

Once the communications session is established, the proxy program will function as a transparent tunnel, channeling data between the client connection and the application server. The connection from the client to the server traverses two TCP sessions, one from the client to the proxy program and a matched session from the proxy program to the application. The proxy program will not alter the traffic in any way. It will only forward the data between the paired TCP sessions. The server applications provide security for the traffic itself.

Security for the Tomcat Web server is accomplished by installing a Web server security certificate and placing the Tomcat server in https mode so that all Web traffic to and from Tomcat is protected by SSL/TLS encryption.

Security to the FoxTalk port on the OpenFox® System is provided by one-way authentication through a 2048-bit RSA (FIPS approved asymmetrical encryption algorithm) certificate, random and protected session key negotiation, 128-bitAES in CBC mode (AES is the Advanced Encryption Standard, which is a FIPS approved symmetrical block cipher encryption algorithm. CBC is Cipher Block Chaining which is a FIPS approved method of operation for symmetrical block ciphers) and SHA-1 (SHA-1 is the Secure Hash algorithm which is FIPS approved).



CPI Customer Map

Current Clients:

Air Force Office of Special Investigations
Alabama Law Enforcement Agency
Arkansas Crime Information Center
Arizona Department of Public Safety
Colorado Department of Public Safety
Hawaii Attorney General
Idaho State Police
Illinois State Police
Indiana State Police
US Immigration and Customs Enforcement
Iowa Department of Public Safety
Kansas Bureau of Investigation
Kentucky State Police
Maine State Police
Massachusetts CJIS
Maryland Department of Public Safety
Michigan State Police
Mississippi Justice Information Center
Missouri State Highway Patrol
Montana Department of Justice
National Center for Missing & Exploited Children
Naval Criminal Investigative Services
New Hampshire State Police
New Mexico Department of Public Safety
North Dakota Dept. of Emergency Services
Ohio Attorney General
Ohio State Police
Oklahoma Bureau of Investigation
Oklahoma Department of Public Safety
Philadelphia Police Department
Rhode Island State Police
Rhode Island Attorney General
Texas Department of Public Safety
US Army
US Department of Justice
US National Central Bureau
US Postal Inspection Service
Vermont Department of Public Safety
Virginia State Police
West Virginia State Police
Wisconsin Bureau of Criminal Investigation
Wyoming Division of Criminal Investigation

Computer Projects of Illinois, Inc.

400 Quadrangle Drive, Suite F
Bolingbrook, IL 60440
Tel: (888) 353-4095
Help Desk: 866-471-6305

www.openfox.com