

RTI Secure WAN Transport

BENEFITS

- Allows RTI Data Distribution Service applications to use public Wide Area Networks for secure data-sharing
- Reduces development time and costs by eliminating the need for private network infrastructure
- Minimizes configuration challenges and security risks by utilizing proven, standards-based components

FEATURES

- Seamless participant discovery and data exchange over public Wide Area Networks (WAN)
- Secure: participant, session & channel authentication, data encryption over WAN or LAN
- Works within existing infrastructure: communicates through firewalls and NATs without the use of Virtual Private Networks (VPNs)
- Based on standards and proven techniques, such as OpenSSL for encryption and STUN protocol for NAT traversal

RTI Secure WAN Transport allows RTI Data Distribution Service applications to share data securely over either private or Wide Area Networks (WAN), such as the Internet. RTI Secure WAN Transport combines proven techniques for firewall and Network Address Translator (NAT) traversal with standard network security protocols to facilitate seamless, secure participant discovery and data exchange.

Standard Protocols & Proven Techniques

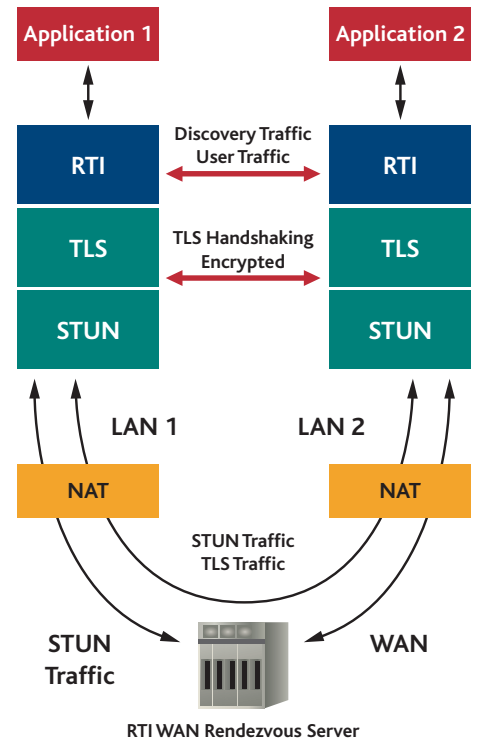
RTI uses standard protocols and proven techniques to address NAT traversal, participant authentication and data encryption. Specifically, NAT traversal is addressed by implementing UDP hole punching using the STUN protocol, and security is provided to channels by leveraging DTLS (Datagram TLS), an extension of SSL/TLS:

NAT Traversal Using STUN Protocol

RTI uses the STUN protocol to address firewall and NAT traversal. STUN (Simple Traversal of UDP through NATs) is a network protocol that allows a client behind a NAT (or multiple NATs) to find out its public address, the type of NAT it is behind and the internet-side port associated by the NAT with a particular local port. This information is used to set up UDP communication between two hosts that are both behind NAT routers.

The STUN protocol implements NAT traversal through ‘UDP hole punching’. In essence, each host behind the NAT contacts a third, well-known server (usually a STUN server) in the public address space. Once the NAT devices have established UDP state information they can then switch to direct communication, expecting that the NAT devices will keep the states despite the fact that packets are coming from a different host.

This technique is widely used in peer-to-peer software and VoIP telephony to bypass firewalls and NAT devices. The STUN protocol works with any kind of cone NAT, which account for the majority of NATs



RTI enables seamless data exchange over public or private networks

deployed. The protocol also traverses multiple levels of NATs, and it does not require any NAT reconfiguration.

Authentication and Security via DTLS

RTI provides data security and participant authentication using DTLS, an extension of SSL/TLS security protocol. SSL/TLS is a widely deployed connection-oriented standard protocol to provide authentication and security. It sits at the transport layer and is usually wrapped around application protocols such as HTTP (referred to as HTTPS). SSL/TLS is one of the most successful security protocols in existence, used daily by millions of users.

RTI uses an extension of TLS called DTLS (Datagram TLS) protocol, designed to support a datagram low-level transport,



which is appropriate for a peer-based application protocol like DDS. As there is not a strict connection to socket mapping, it is possible to service several connections from the same receive socket/port, as long as the proper connection can be identified. For its DTLS implementation, RTI uses OpenSSL v0.9.8e crypto libraries and supports industry-standard authentication via X.509 certificates.

RTI Advantages

Low or no latency overhead: The STUN protocol used for LAN and WAN data exchange adds no visible overhead in latency

compared to using the default UDP LAN-based adapter. The data security components (using 256-bit AES algorithm) add a latency of about 65 microseconds for small data elements.

Standards-based and easy to configure: RTI is standards-based (RFC 3489) and requires no NAT configuration. It uses standard tools that come with OpenSSL to create certificate authority (CA) and supports an XML-based configuration file to specify QoS and certificate administration parameters. RTI also provides validation for FIPS 140-2, as all software products that use OpenSSL are validated by default.

Specifications

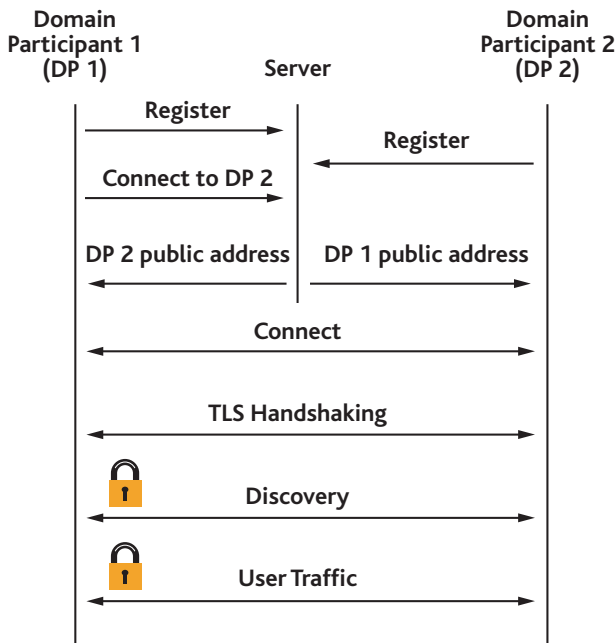
Supported Operating Systems

- Red Hat Linux
- Red Hat Enterprise Linux
- Solaris
- Windows 2000/XP Pro

Supported Architectures

- UltraSPARC
- X86

Note: RTI continually adds support for new operating systems and architectures. Also, not all combinations of operating systems and architectures are available. Please contact RTI for additional availability and supported combinations.



RTI provides data security and participant authentication using standard protocols

About RTI

Real-Time Innovations (RTI) works in partnership with its customers to develop and integrate the world's most demanding real-time applications. RTI takes the risk out of distributed application development and system integration by providing deep expertise in real-time communications coupled with the highest performance messaging middleware. The company's software and services have been leveraged in a broad range of industries including defense, intelligence, simulation, industrial control, transportation, finance, medical and communications. Founded in 1991, RTI is privately held and headquartered in Sunnyvale, California. For more information, please visit www.rti.com.

