IBM®TSA
Technical Support Appliance

IBM® Technical Support Appliance Connectivity Security White Paper

Version 2.4.0.0

February 2019

Table of Contents

Introduction

The IBM® Technical Support Appliance (TSA) solution includes the IBM appliance that discovers and shares datacenter hardware and software product information with IBM Support, and the correlated proactive service reports that IBM shares with the Client. This document describes the connectivity, security and service information transmitted by the Technical Support Appliance (hereafter also *known* as TSA) when communicating with the IBM Service Delivery Center (SDC).

For security and connectivity information relating to end points that TSA communicates with inside a customer's network, reference the TSA Setup Guide or the TSA Configuration Assistant Guide.

Useful documentation

A complete set of the TSA documentation is included with TSA itself.

Terms and definitions

Users should have a basic understanding of Internet Protocol (IP) networks and protocols. The following is a list of terms and acronyms used in this document.

Term	**Definition**
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
IP	Internet Protocol
NIST	National Institute of Standards and Technology
RFC	Requests for Comments
RSA	A public-key cryptosystem
SDC	Service Delivery Center
SNAT	Source Network Address Translation
SHA	Secure Hash Algorithm
SSL	Secure Sockets Layer
TCP	Transmission Control Protocol
TLS	Transport Layer Security

TSA	Technical Support Appliance
VPN	Virtual Private Network

The appliance

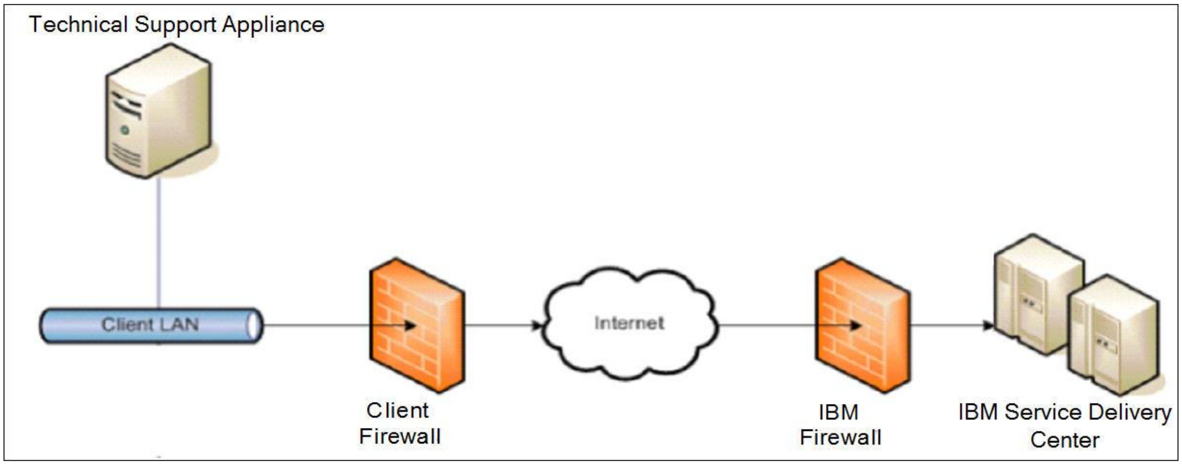
TSA includes IBM Service and Support software to share information with IBM Support. For both the hardware and virtual appliance, you are given limited access to the operating system in the appliance to run the configuration script.

Technical Support Appliance connectivity

TSA only supports outbound initiated internet connectivity to IBM. VPN, modem, and inbound connectivity are not supported.

Outbound connectivity without proxy server

The following diagram shows TSA connecting to IBM without a proxy server. This is the default setup.



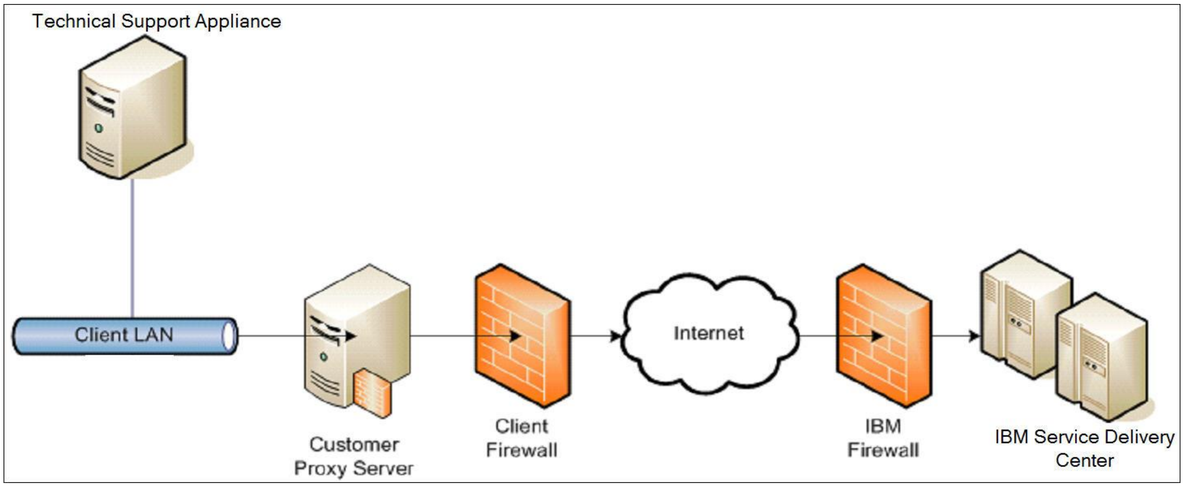
In this setup, TSA connects through your internet connection by the default route.

For TSA to communicate successfully, your external firewall must allow outbound packets to flow freely on port 443. All transactions use the HTTPS protocol.

The use of Source Network Address Translation (SNAT) and masquerading rules to hide the TSA's source IP address are both acceptable. Ensure your firewall allows connections to the IBM IP addresses and ports in the table in Appendix A.

Outbound connectivity with your proxy server

The following diagram shows TSA connecting to IBM using a proxy server supplied by you. This is not the default setup and you will need to configure the TSA to use your proxy.



To forward packets, the proxy server must support the basic proxy header functions (as described in RFC #2616) and the CONNECT method. Optionally, basic proxy authentication (RFC #2617) may be configured so that TSA authenticates before attempting to forward packets through your proxy server.

To configure TSA to use a proxy server, see "Setting up IBM connectivity" in the TSA Setup Guide.

SSL inspection is not supported, if utilizing it on the proxy, disable it for these flows.

For Blue Coat proxies, disable "protocol detection" to IBM servers. Add these configuration rules:

- url.domain=esupport.ibm.com detect_protocol (none)
- url.address=129.42.54.189 detect_protocol (none)
- url.address=129.42.56.189 detect_protocol (none)
- url.address=129.42.60.189 detect_protocol (none)

Security protocols and encryption

Communication between the Technical Support Appliance and IBM

TSA uses the HTTPS protocol for all transactions including transmission of inventory data between your site and the IBM Service Delivery Center, downloading software updates, and configuration information. HTTPS is achieved by encapsulating the HTTP application protocol within the Transport Layer Security (TLS) version 1.2 cryptographic protocol.

Communication between your browser and the Technical Support Appliance

The TSA web user interface uses the HTTPS protocol for securing administrative requests between your browser and the appliance.

Service information sent to IBM

This section outlines what service information is transmitted to IBM and the reasons for sending this information when TSA connects to the IBM Service Delivery Center.

Reasons TSA connects to IBM

1. Scheduled and/or manual transmission of service, inventory and system configuration information for use in Client TSA Reports
2. Manual and periodic automated connectivity tests to IBM
3. Manual and automatic checks for TSA software update availability
4. User initiated TSA software downloads and updates
5. Registration of contact and location information

Data transmitted to IBM

This table shows the data transmitted to IBM, the TSA component that collects the information, and a description of the contents.

Type of Data	Component	Description
Hardware service Information	Discovery Manager	TSA collects hardware information such as manufacturer, machine type, model, serial number, and selected hardware elements such as memory, CPUs, and attached storage.
Software service Information	Discovery Manager	TSA collects software information such as manufacturer, product id, and selected software elements such as version, fix level, and requisites.
Basic appliance configuration information	Discovery Manager	Scope set information, appliance version and unique appliance ID are transmitted in order to associate discovered endpoints with your specific TSA. TSA and endpoint credential information are never transmitted.
Customer contact information	The TSA User Interface	Customer contact information that is provided in the TSA user interface is transmitted and securely stored at IBM. This information is used to associate inventory data with a specific client and used only by designated IBM service personnel for

		contacting clients about service and support of their products. ✚ It is optional to provide customer personal contact information.

Data handling at IBM

Transmitted data is stored in IBM's secure Client database and is firewall restricted. Access to this data is restricted within IBM in accordance with IBM Security policies.

TSA reports are accessible only by designated IBM Support personnel, such as your account team, and by other IBM Support personnel to assist you if needed.

All data is associated with a unique identifier and can be purged if required.

Appendix A

Configuration requirements for connections to IBM Support

TSA connects to IBM Support through a direct connection or through a user-supplied proxy that must be configured to allow communication with IBM.

All TSA transactions to IBM Support route through a server cluster that consists of several physical machines that are load balanced through a single host name. This server environment is fully NIST SP800-131A compliant, supporting TLS 1.2 protocol, SHA-256 or stronger hashing functions, and at least 2048-bit strength RSA keys.

For TSA to communicate successfully, the external firewall must allow outbound connections on port 443. Ensure your firewall allows connections to the IP addresses and ports in the table below.

Host Name	IP Address(es)	Port(s)	Protocol
esupport.ibm.com	129.42.54.189	443	HTTPS (to IBM)
	129.42.56.189		
	129.42.60.189		

In some failover scenarios, HTTP (port 80) may be attempted when downloading software updates as part of Update processing.

IBM Corporation
Marketing Communications
Systems and Technology Group
Route 100
Somers, New York 10589
Produced in the United States of
America
February 2019.
All Rights Reserved

This document was developed for products and/or services offered in the United States. IBM may not offer the products, features, or services discussed in this document in other countries.

The information may be subject to change without notice. Consult your local IBM business contact for information on the products, features and services available in your area.

All statements regarding IBM future directions and intent are subject to change or withdrawal without notice and represent goals and objectives only.

IBM, the IBM logo, POWER, System I, System p, i5/OS are trademarks or registered trademarks of International Business Machines Corporation in the United States or other countries or both. A full list of U.S. trademarks owned by IBM may be found at http://www.ibm.com/legal/copytrade.shtml.

Blue Coat is a registered trademark of Blue Coat Systems.

Other company, product, and service names may be trademarks or service marks of others.

IBM hardware products are manufactured from new parts, or new and used parts. Regardless, our warranty terms apply.

This equipment is subject to FCC rules. It will comply with the appropriate FCC rules before final delivery to the buyer.

Information concerning non-IBM products was obtained from the suppliers of these products.

Questions on the capabilities of the non-IBM products should be addressed with the suppliers.

The IBM home page on the Internet can be found at http://www.ibm.com.