SauceLabs

WHITE PAPER

Sauce Connect Proxy™ Security Overview

LEARN MORE AT SAUCELABS.COM

UPDATED DECEMBER 2022

Introduction

Sauce Connect Proxy™ is a built-in HTTP proxy server that allows users to access Sauce Labs infrastructure from their local environment or behind a corporate firewall. This extra layer of security ensures that no sensitive data is exposed, and allows Sauce users to securely test their web and mobile applications.

This white paper provides an overview of Sauce Labs architecture, security requirements and protocols to assist customer network and security engineering teams to better understand how to optimize Sauce Connect Proxy™ within their own development environment.

Table of Contents

4 Introduction

5 Sauce Connect Architecture

5 Overview

6 Components Overview

6 Sauce Connect Client

6 Sauce Connect Server

6 Sauce Labs REST API

6 Tunnels Web UI

7 Security Overview

7 Sauce Labs hosted VMs and real devices

7 Sauce Labs Tunnel VMs security features

7 Sauce Labs Tunnel communication security features

7 Customer Firewall Requirements

8 Sauce Connect Tunneling Protocol - KGP

SauceLabs

Introduction

Sauce Connect Proxy™ is a proxy server that opens a secure connection between a Sauce Labs virtual machine, emulator, simulator or real device running your browser or native app tests, and an application or website you want to test that is on your local machine or behind a corporate firewall. Figure 1 illustrates the high-level architecture of the solution (please note that this diagram is for high level illustrative purposes only). Sauce Connect is not required to run tests with Sauce Labs, except for websites or applications that are not publicly accessible, where it is required. Because network architectures can be complex, it is imperative that a network administrator or engineer be involved in the implementation process as soon as possible. In addition to providing a means for Sauce Labs to access your application or website, Sauce Connect has some other uses in your testing network architecture:

- As a means of monitoring upstream traffic through a proxy like BrowserMob;
- As a way to stabilize network connections (for instance, detecting/re-sending dropped packets).
- As a superior alternative to allowlisting ("whitelisting").

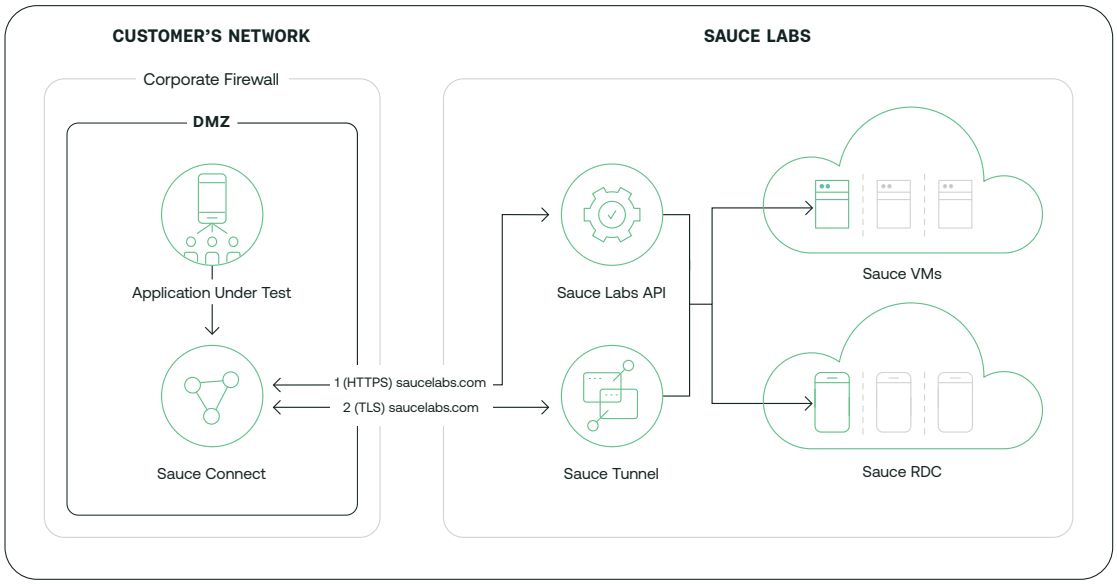

Figure 1: Sauce Connect Proxy, High Level Architecture

Sauce Connect Architecture

Overview

From the Sauce Labs side, the Sauce Connect system includes the following components:

- Sauce Connect client
- Sauce Connect server
- Sauce Connect REST API server
- Tunnels Web UI

Here is an overview of how these components interact with a user's environment:

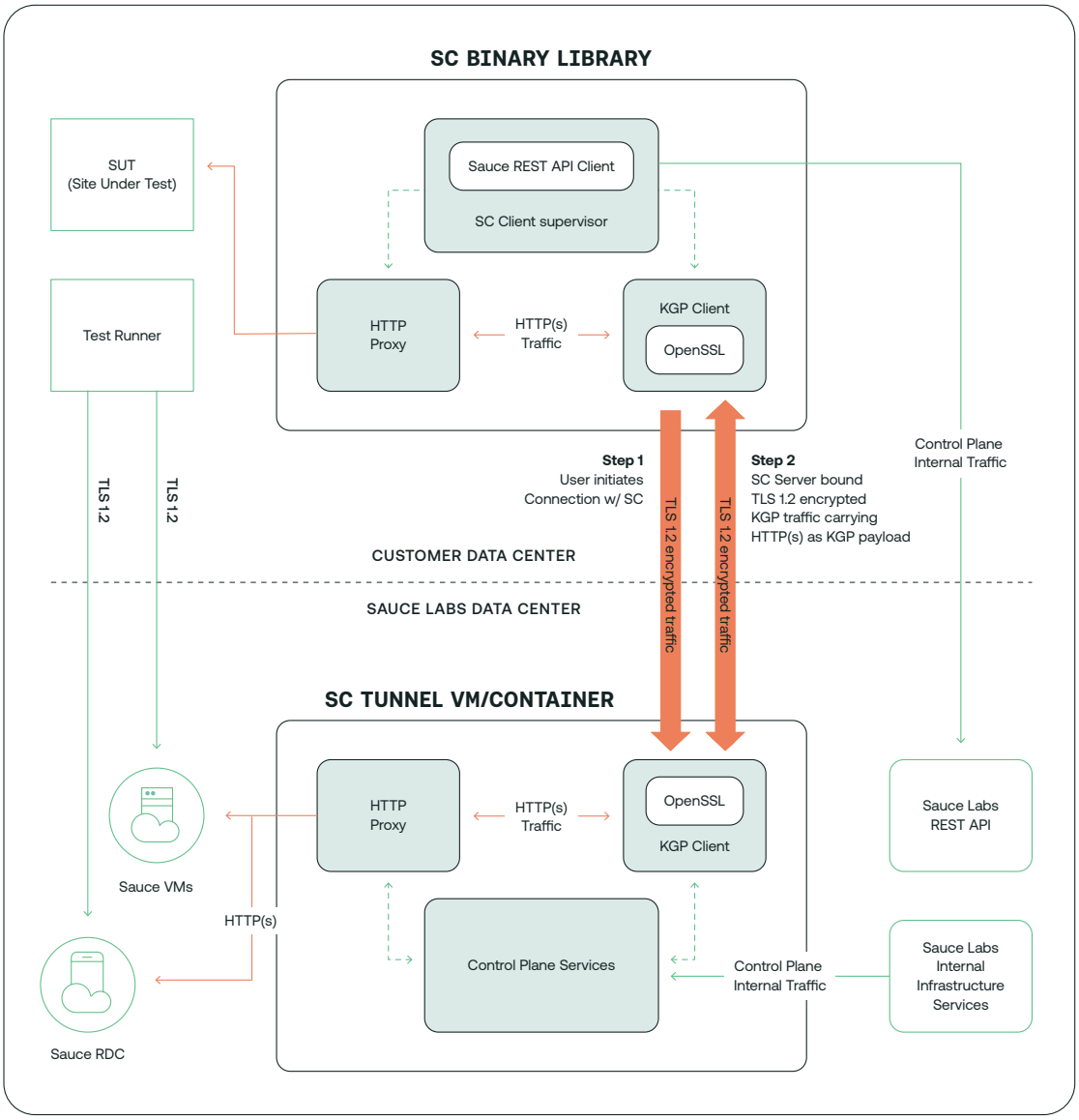

Figure 2: Sauce Connect components interacting with user's environment

Direction	Protocol(s)
Outbound from customer network	HTTPS (TCP/443)
Outbound from customer network	KGP (TCP/443)

Components Overview

Sauce Connect Client

The Sauce Connect client (also known as SC) is distributed as a single binary that contains several distinct components. These include:

- SC Client controller - this is the "brain" of the SC client. It issues requests to the Sauce Labs REST API, starts all the other included components and ensures that everything is working as expected.
- KGP Client - the client side implementation of KGP, Sauce Labs proprietary protocol.
- HTTP Proxy - this contains a non-caching HTTP proxy that sends HTTP requests coming from tests that run on virtual machines (VMs) or devices on the Sauce Labs infrastructure to the website or application that is hosted inside the user's firewall (either on an intranet, or a local machine).

All of this is available for download on the Sauce Labs technical documentation website.

Sauce Connect Server

The Sauce Connect Server is a VM (or container) running in Sauce Labs data centers and it includes the following components:

- Tunnel VM Controller - this is the logic that is responsible for configuring the VM, making sure all components are functional, and reporting back to other internal services.
- KGP Server - the server side implementation of KGP, Sauce Labs proprietary protocol. To learn more about this, please reference the Protocol section of this white paper (page 8).
- HTTP Proxy - off the shelf HTTP proxy that is responsible for sending requests from tests running in Sauce Labs VMs or devices to the KGP Server. Note that SSL traffic is "bumped" by default. This can be disabled.

Sauce Labs REST API

The Sauce Labs REST API allows the Sauce Connect client (or any authenticated client) to start and stop tunnels and/or get information about existing tunnels.

To learn more about the Sauce Labs REST API please reference our technical documentation website.

Tunnels Web UI

Users that are executing tests through Sauce Connect can see all information about the tunnels they are running through the web UI. This can be accessed by logging into your Sauce Labs account.

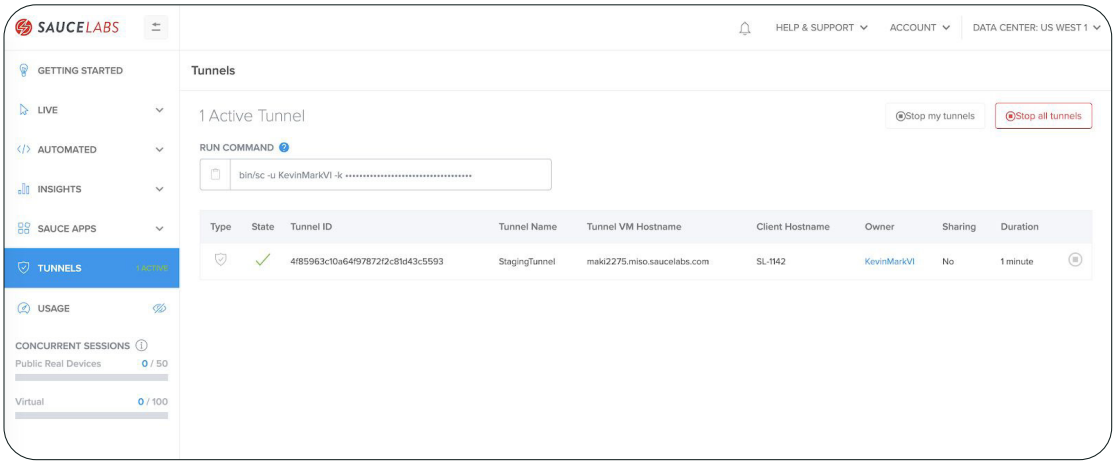

Figure 3: Sauce Connect tunnel information found in the Sauce Labs UI

Security Overview

This section contains more detailed information on the features and procedures that govern Sauce Connect in order to provide the best, most secure experience.

Sauce Labs hosted VMs and real devices

The Sauce Labs infrastructure is configured so that VMs and/or real devices are fully isolated from each other. This means that VMs and/or devices are not able to communicate to any other VMs or devices in our infrastructure. The only exception for this would be tunnel VMs, which are described in the next section. While VMs and devices are allowed to connect to the internet, Sauce Labs also offers a "Lockdown" feature that locks traffic down to that particular user's tunnel only. We only permit allowlist ("whitelist") internal services to communicate to VMs and/or real devices.

Sauce Labs Tunnel VMs security features

When considering the security of Sauce Labs tunnel VMs, it is important to note that while they communicate with the VM or real device running a test, they are fully isolated from each other through traffic filtering. This means that a VM and/or real device being accessed through a tunnel will send HTTPS traffic owned by the customer only, and is not able to communicate with other VMs or real devices in the Sauce Labs cloud. Additionally, Sauce only permits allowlist necessary internal services to communicate with tunnel VMs. Users can customize tunnel VMs from their side, and configure them to direct all traffic through the tunnel, to the internet, or any combination of the two using wildcards. Only user-initiated and authenticated sessions are allowed to utilize that user's tunnel.

Sauce Labs Tunnel communication security features

The Sauce Labs team ensures the security of our tunnels through a number of different methods:

- Certificate status is continually validated by leveraging OCSP
- TLS connections below 1.2 are not permitted
- Sauce tunnels adhere to a minimum standard for allowable cipher suites (at least ECDHE)

Customer Firewall Requirements

In order to successfully run in a customer's environment, the Sauce Connect client requires access to port 443 of the following Sauce Labs domains. This includes control plane requests (HTTPS traffic), as well as the data plane (KGP traffic). It's also important to note that only a user can initiate a tunnel connection from their network to the Sauce Labs cloud, and not the other way around.

Direction	Protocol(s)
Outbound from customer network	HTTPS (TCP/443)
Outbound from customer network	KGP (TCP/443)

To learn more about Sauce Labs public data center endpoints, please reference our technical documentation website.

Sauce Connect Tunneling Protocol - KGP

KGP is an application layer protocol that carries all HTTP(s) traffic as its payload. It is developed and maintained by Sauce Labs, and is used to multiplex established connections for multiple HTTP requests/responses.

KGP packets contain the following components:

- Data packets carrying HTTP(s) traffic
- Control packets, which include:
  - Connection requests
  - Keepalive timers

KGP is preferred over conventional protocols for a number of reasons:

- It's lightweight
- It reconnects when a connection accidentally disconnects
- It ensures that all the data is sent and received, even over an unstable or intermittent connection
- It provides information about the connection state

All KGP packets are encrypted with the industry standard TLS 1.2 protocol. It's also important to note that KGP is not responsible for encryption. Instead, all encryption is processed according to the industry standards defined by the OpenSSL library.

About Sauce Labs

Sauce Labs is the leading provider of continuous test and error reporting solutions that gives companies confidence to develop, deliver and update high quality software at speed. The Sauce Labs Continuous Testing Cloud identifies quality signals in development and production, accelerating the ability to release and update web and mobile applications that look, function and perform exactly as they should on every browser, operating system and device, every single time. Sauce Labs is a privately held company funded by TPG, Salesforce Ventures, IVP, Adams Street Partners, and Riverwood Capital.

For more information, please visit
→ saucelabs.com

saucelabs.com/sign-up

FREE TRIAL

SAUCE LABS INC. - HQ 450 Sansome Street, 9th Floor, San Francisco, Ca Usa 94111

SauceLabs