SauceLabs

WHITE PAPER

Sauce Connect 5.0 Security Overview

LEARN MORE AT SAUCELABS.COM

UPDATED NOVEMBER 2023

SauceConnect

Sauce Connect is a built-in HTTP proxy server, providing a secure gateway for access to local environments behind a corporate firewall while running tests on Sauce Labs. This extra layer of security ensures that no internal data is exposed to the public internet, and allows Sauce users to securely test their web and mobile applications.

The Sauce Connect Security Overview provides insight into Sauce Connect 5.0 architecture, security requirements and protocols. The goal is to equip network and security engineering teams with the necessary knowledge to effectively optimize Sauce Connect within their development environments.

Introduction

Sauce Connect Proxy establishes a secure connection between Sauce Labs infrastructure (virtual machine, emulator, simulator, or real device), and the application or website you want to test. This connection remains secure, even if the target application or website resides on your local machine or behind a corporate firewall.

The latest iteration of Sauce Connect, version 5.0, introduces a host of enhancements, with a particular focus on security and performance. It now leverages the industry-standard and high-performance HTTP/2 protocol, resulting in substantial speed improvements, with speeds up to five times faster. This upgrade also optimizes traffic management, reducing memory consumption by up to 50 times, thus eliminating the need for high-memory VM instances to host Sauce Connect clients.

Additionally, Sauce Connect 5.0 simplifies integration and onboarding, ensuring that the testing process is both seamless and secure. The enhancements extend to upstream proxy configuration with the addition of SOCKS5 support, improved PAC integration, and more flexible authentication.

Moreover, it eliminates the complexities associated with integration and onboarding, ensuring seamless and secure testing. Upstream proxy configuration is improved by adding SOCKS5 support, improved PAC integration and more flexible authentication.

Sauce Connect is not required for running tests on Sauce Labs, except when testing websites or applications that are not publicly accessible. Given the complexities of network architectures, it is highly recommended to engage a network administrator or engineer from the outset of the implementation process to ensure seamless integration.
Beyond providing Sauce Labs access to your application or website, Sauce Connect opens up opportunities to enhance your network architecture in the following ways:

- Monitoring upstream traffic effectively
- Stabilizing network connections, including the ability to resend failed requests
- Offering a superior alternative to traditional allowlisting mechanisms for secure testing

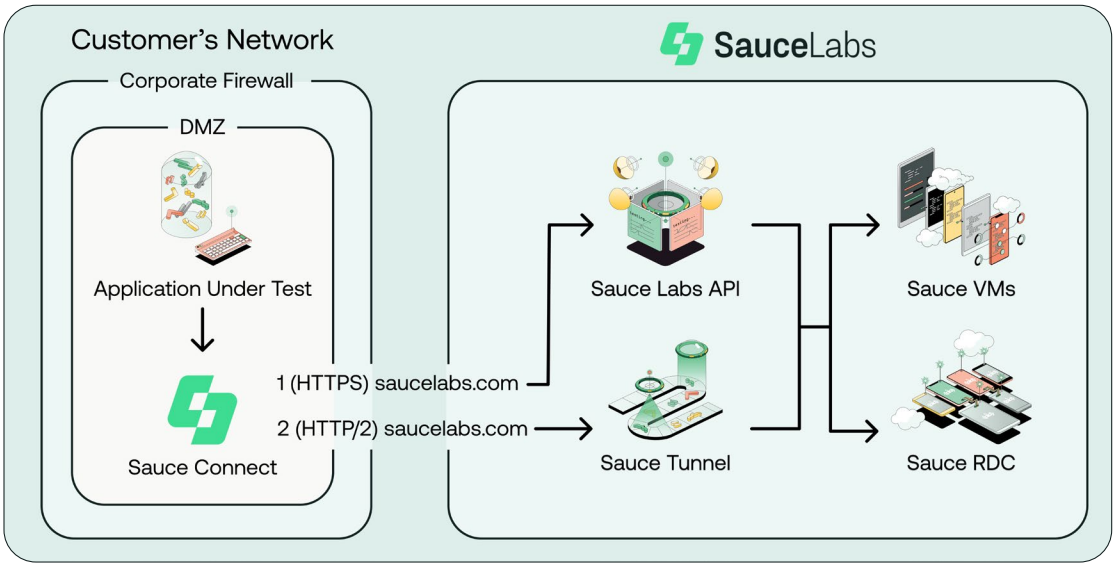


Figure 1: Sauce Connect Proxy, High Level Architecture

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:

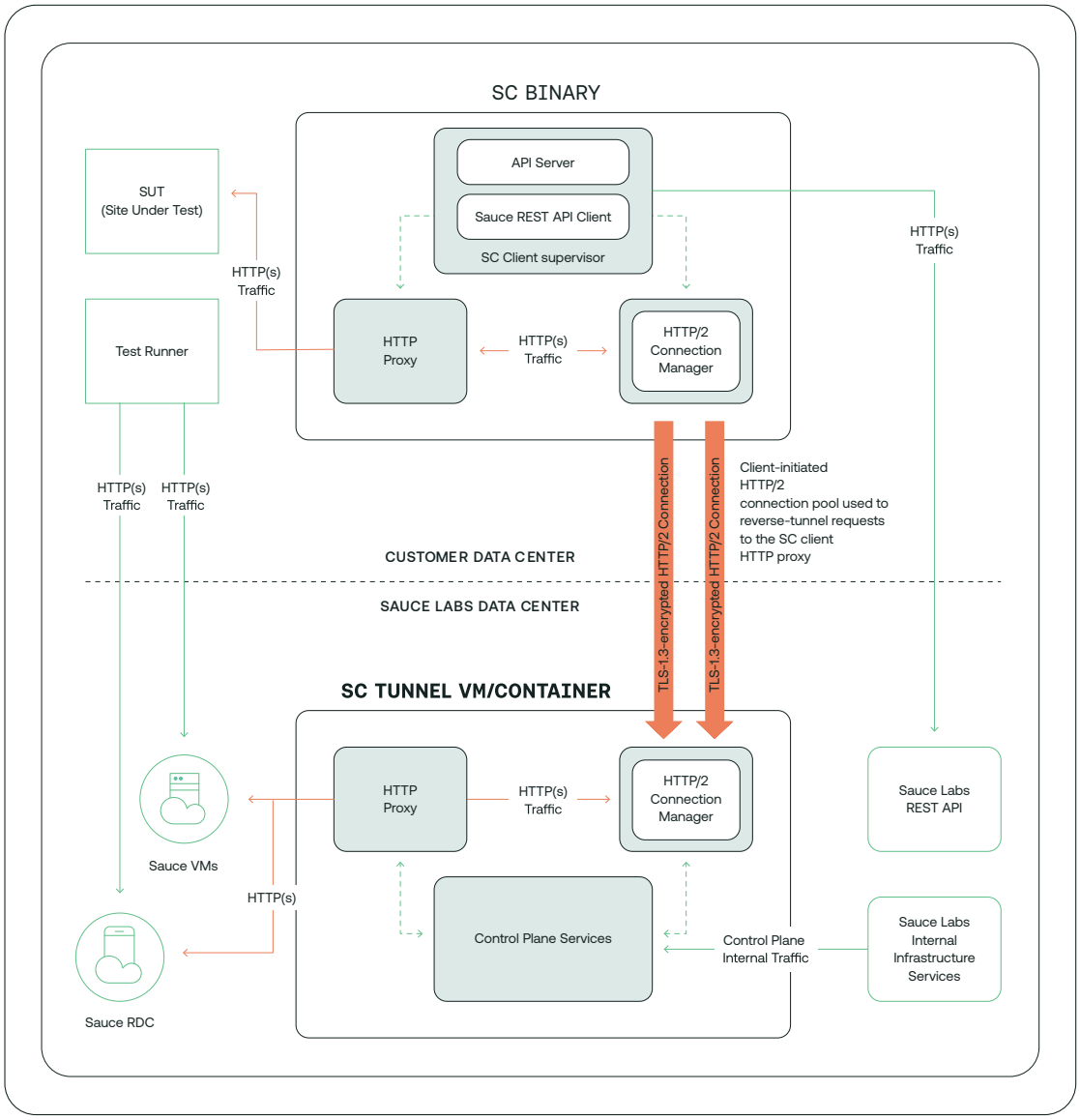


Figure 2: Sauce Connect components interacting with user's environment

Direction	Protocol(s)
Outbound from customer network	HTTPS (TCP/443)
Outbound from customer network	HTTP/2 (TCP/443)

Components Overview

Sauce Connect Client

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

- SC Client supervisor: 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.
- API Server: this is an HTTP server providing an API to query the SC Client supervisor and exposing the client-side metrics
- HTTP/2 Connection Manager: the client-side implementation of the HTTP/2 connection used for tunneling requests.
- HTTP Proxy: this contains a non-caching HTTP proxy (also available as a standalone proxy) that proxies HTTP requests coming from tests that run on virtual machines (VMs) or devices on the Sauce Labs infrastructure to the website or app 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.

Sauce Connect Proxy Client Traffic

- Sauce Connect Proxy client sends requests to the Sauce Labs REST API
  - Start/stop requests as well as various status queries to the Sauce Labs public REST API
- Sauce Connect Proxy client establishes several (two by default) long-lived secure HTTP/2 connections to Sauce Connect Server
  - These connections form a secure “tunnel” between the client and the server
  - These connections are alive as long as Sauce Connect Proxy client process is alive
- Sauce Connect Proxy built-in HTTP proxy processes requests initiated by a browser or a mobile app in the Sauce Labs data center

Sauce Connect Proxy Server

The server is a container running in Sauce Labs data centers and it includes the following components:

- Tunnel Controller: this is the logic that is responsible for configuring the server, making sure all components are functional, and reporting back to other internal services.
- SC Server: the server side implementation of HTTP/2 Connection Manager.
- HTTP Proxy: a non-caching HTTP proxy that is responsible for sending requests from tests running in Sauce Labs VMs or devices to the SC Server.

Sauce Labs REST API

- The Sauce Labs REST API allows the Sauce Connect Proxy Client (or any authenticated client) to start and stop tunnels and/or get information about existing tunnels. For more information, refer to the Sauce Connect Proxy API documentation.

Tunnels Web UI

If you're executing tests through Sauce Connect Proxy, you'll be able to see all information about the tunnels you're running through the web UI (log in to Sauce Labs and go to the Tunnels page).

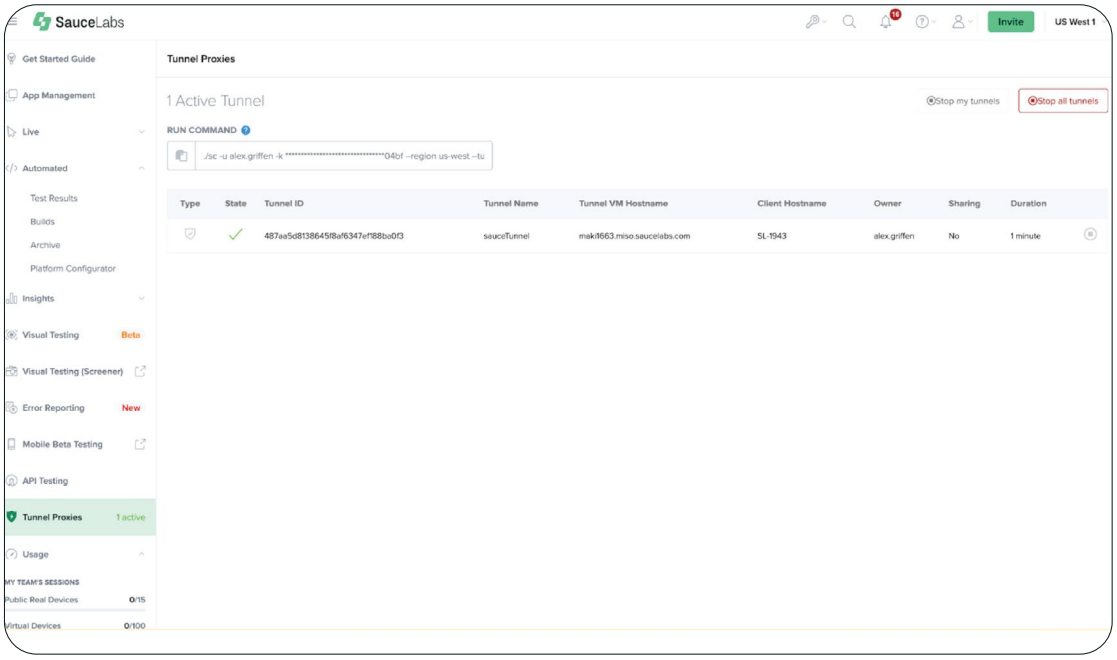


Figure 3: Sauce Connect tunnel information found in the Sauce Labs UI

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.

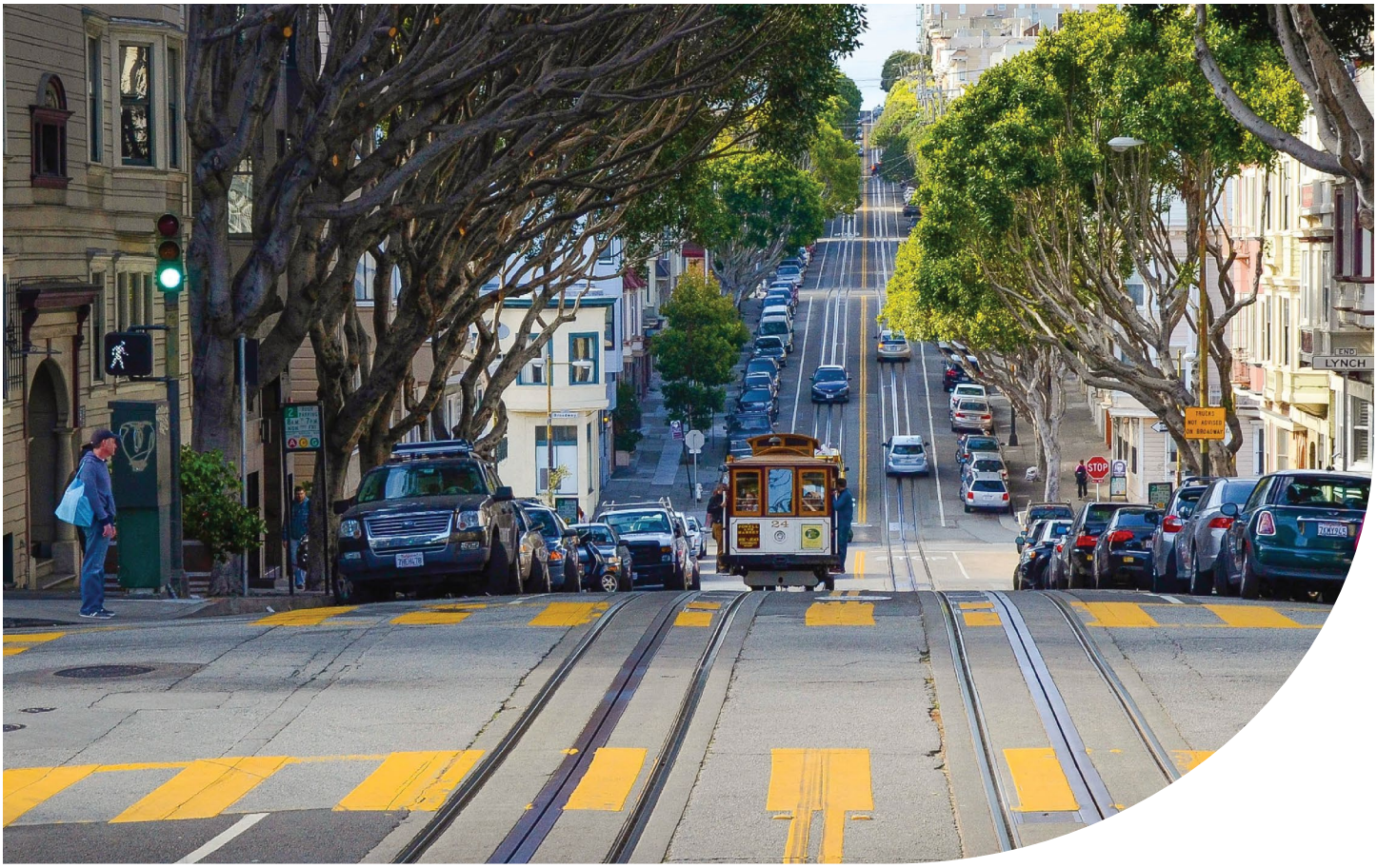
Sauce Labs Tunnel communication security features

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

- 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 (HTTP/2 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.



About Sauce Labs

With over 15 years of experience and 6 billion tests executed, Sauce Labs is the industry leader in ensuring software quality. Seamlessly integrate continuous testing into the software development lifecycle, by harnessing Sauce Labs Platform for Test. We provide robust infrastructure that includes extensive Device Lake™, Browser & OS Lake™, as well as powerful Test Runtime Tooling. Plus access to first-party applications and integrations, AI-driven insights, along with industry-leading expertise, support, and security certifications. As test automation pioneers, we partner with over 100,000 global customers including Walmart, Verizon, and Bank of America to deliver quality software. 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