SAUCELABS

WHITE PAPER

# Sauce IPSec Proxy Overview

Sauce IPSec Proxy is a solution that allows virtual machines (VMs) running customer tests in the Sauce Labs network to access HTTP(s) application servers in the customer's private network. The solution provides an alternative to Sauce Connect Proxy™ to accommodate enterprise customers' requirements.

This white paper provides an overview of Sauce IPSec Proxy architecture to assist customers' network and security engineering teams to better understand how to integrate Sauce IPSec Proxy solution into their own development environment.

# TABLE OF CONTENTS

# INTRODUCTION

IPSec Proxy is a trusted connection solution providing a secure connection between a Sauce Labs VM, emulator, simulator, or real device running your browser or native app tests, and an application or website you want to test that is behind a corporate firewall. The high-level architecture of the solution is shown in Figure 1. A trusted connection is not required to run tests with Sauce Labs, except for websites or applications that are not publicly accessible.

IPSec is generally used when two remote sites need to establish secure communications over an untrusted network. It is also a good solution when latency is a concern. Because IPsec operates at the network layer of the TCP/IP model, it does not inherently suffer the same throughput issues that would affect an encryption protocol running over TCP (e.g., TLS).

# SAUCE IPSEC PROXY ARCHITECTURE

## OVERVIEW

Sauce IPSec Proxy allows test VMs and real mobile devices in the Sauce Labs network to access application servers in customer's private network. However, Sauce IPSec Proxy doesn't allow application servers to access Sauce test VMs. The solution consists of several components. See below for more details.

## HIGH LEVEL ARCHITECTURE

The diagram in Figure 1 shows Sauce Labs proxy over IPSec high level architecture.

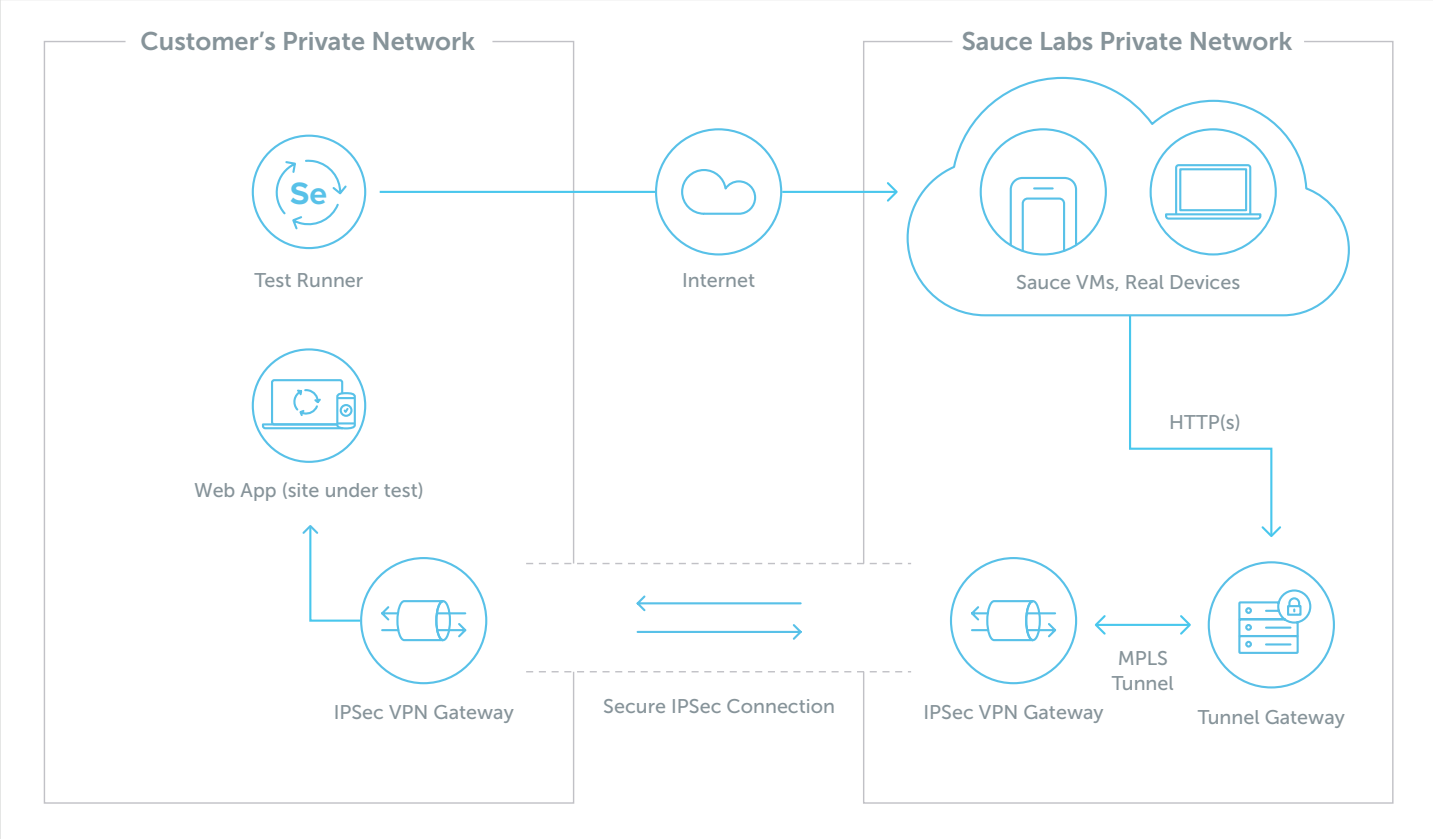


*Figure 1: Sauce IPSec Proxy System-Level Architecture*

## COMPONENTS

### Customer and Sauce Labs Private Networks

The Sauce Labs private network contains Sauce Labs internal services, test VMs, real mobile devices, and other services and infrastructure.

### IPSec Gateways and VPN Connection

IPSec is a collection of standardized protocols designed for authenticating and encrypting data communications between two points. It operates at Layer 3 of the OSI Model or the Network Layer of the TCP/IP Model, and while various data flow models can be applied, Sauce IPSec Proxy solution utilizes network-to-network (a.k.a. site-to-site) data flow model often used as a mechanism to bridge two disparate networks.

IPSec provides a number of security-related services and authentication occurs mutually between two entities. Encryption keys are created and shared after mutually authenticating the identity of the two parties.

The Sauce Labs offers two tunnel implementations: policy-based and route-based. The table below summarizes the differences between policy- and route-based IPSec VPNs.

| POLICY-BASED | ROUTE-BASED |
|---|---|
| Older implementation based on Proxy IDs, sometimes called "interesting subnets," "encryption domains," or "traffic selectors." | Newer implementation that uses BGP for exchanging the equivalent of a Policy-Based Proxy ID |
| Multiple Phase 2 tunnels, one for each (local, remote) Proxy ID pair | One Phase 2 tunnel, regardless of number of subnets on either side |
| Failover may be manual depending on topology, even when multiple Phase 1 tunnels are used | Dynamic and automatic failover when multiple Phase 1 tunnels are used |
| Requires coordination between customer and Sauce Labs when adding or removing additional Proxy IDs | Only customer needs to update their BGP policy |

### Supported Phase 1 and Phase 2 Parameters

For IPSec tunnels in Phase 1 and Phase 2, Sauce Labs is able to support the following configuration parameters:

| PHASE | PARAMETER | RECOMMENDED VALUES |
|---|---|---|
| Phase 1 (IKE) | Authentication Method | Pre-Shared Key |
| Phase 1 (IKE) | Authentication Algorithm | SHA256, SHA384 |
| Phase 1 (IKE) | Encryption Algorithm | DES CBC, 3DES CBC, AES128/256 (CBC or GCM), AES192 CBC |
| Phase 1 (IKE) | Lifetime Seconds | 180 to 86400 |
| Phase 1 (IKE) | Diffie-Hellman Group | 1, 2, 5, 14, 19, 20, 24 |
| Phase 1 (IKE) | NAT Traversal | Enabled or Disabled |
| Phase 1 (IKE) | IKE Mode | Main or Aggressive |
| Phase 1 (IKE) | IKE Version | v1, v2 |
| Phase 2 (IPSec) | Authentication Algorithm | SHA2 (SHA256) |
| Phase 2 (IPSec) | Encryption Algorithm | DES CBC, 3DES CBC, AES128/256 (CBC or GCM), AES192 CBC |
| Phase 2 (IPSec) | Lifetime Seconds | 180 to 86400 |
| Phase 2 (IPSec) | Perfect Forward Secrecy (PFS) | None or Diffie-Hellman Groups: 1, 2, 5, 14, 19, 20, 24 |
| Phase 2 (IPSec) | Proxy IDs (Encryption Domain, Interesting Subnet, Traffic Selector) | Any |

### Recommended Phase 1 and Phase 2 Configuration

While Sauce Labs supports a wide variety of options for IPSec tunnels, we recommend the following as a minimum for enhanced security and to prevent known vulnerabilities in older protocols:

| PHASE | PARAMETER | RECOMMENDED VALUES |
|---|---|---|
| Phase 1 (IKE) | Authentication Method | Pre-Shared Key |
| Phase 1 (IKE) | Authentication Algorithm | SHA256 |
| Phase 1 (IKE) | Encryption Algorithm | AES256 (CBC or GCM) |
| Phase 1 (IKE) | Lifetime Seconds | 180 to 86400 |
| Phase 1 (IKE) | Diffie-Hellman Group | Diffie-Hellman Groups 14, 19, 20 |
| Phase 1 (IKE) | NAT Traversal | Enabled or Disabled |
| Phase 1 (IKE) | IKE Mode | N/A (IKEv2 does not use a configurable mode), Main if IKEv1 must be used |
| Phase 1 (IKE) | IKE Version | v2 |
| Phase 2 (IPSEC) | Authentication Algorithm | SHA2 (SHA256) |
| Phase 2 (IPSEC) | Encryption Algorithm | AES256 (CBC or GCM) |
| Phase 2 (IPSEC) | Lifetime Seconds | 180 to 86400 |
| Phase 2 (IPSEC) | Perfect Forward Secrecy (PFS) | Enabled, Diffie-Hellman Groups 14, 19, 20 |
| Phase 2 (IPSEC) | Proxy IDs (Encryption Domain, Interesting Subnet, Traffic Selector) | Any |

Although Diffie-Hellman Group 24 is a higher number than others, it is recommended to be avoided due to a known vulnerability in Group 22, which shares implementation details with Group 24.

### Sauce Labs Infrastructure Services

The Sauce Labs infrastructure includes load balancers, REST API, monitoring, and other internal services that allow continuous operation of the Sauce IPSec Proxy offering.

### Sauce Labs Hosted VMs and Mobile Devices

The Sauce Labs platform hosts VMs and mobile devices running customer tests.

### Tunnel Gateways

Tunnel gateways are created as part of a customer Sauce IPSec Proxy setup and can be seen in Web UI as "tunnels." Tunnel gateways host an HTTP proxy that proxies test traffic to the customer network. The tunnel gateway runs a firewall and only allows authorized test VMs to connect through the firewall.

### SSL Bumping

Self-signed and invalid SSL certificates, commonly used in test environments, are not trusted by stock browsers, such as those installed on the Sauce Labs infrastructure. The **SSL Bumping** feature automatically re-signs these certificates. This can be enabled for selected domains.

### DNS Resolution

If a customer's test requires URLs that can't be resolved via a public DNS server, Tunnel Gateway can be configured to forward name resolution requests to the customer private name servers for predefined user domains.

All other requests are resolved through public DNS servers.

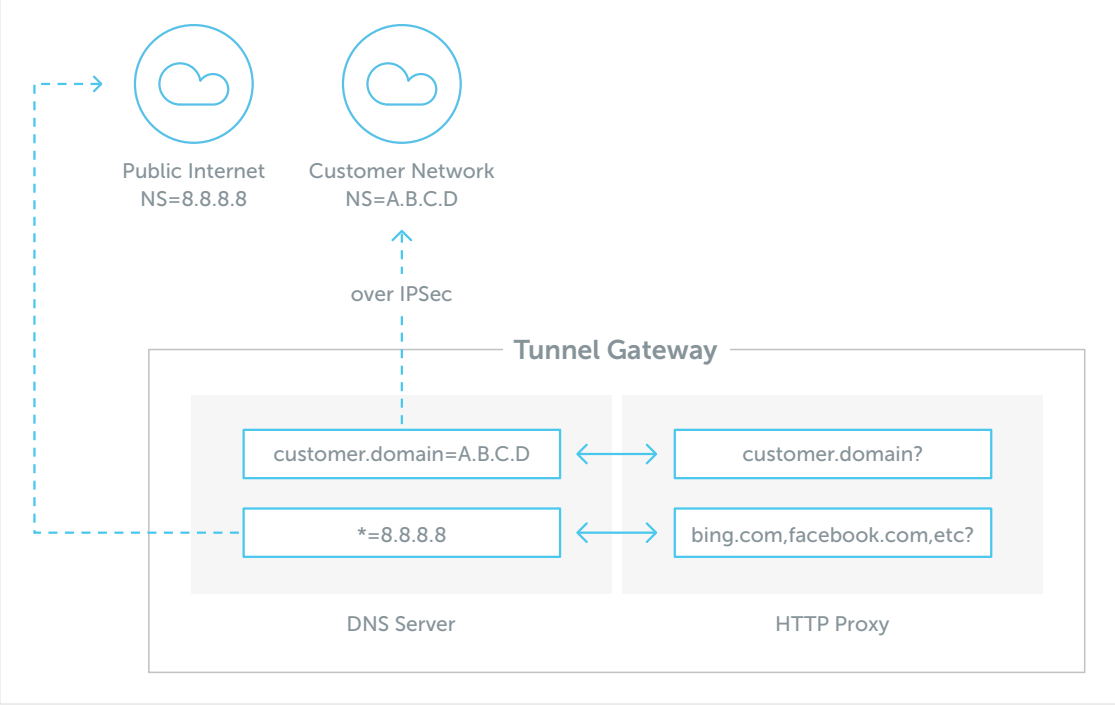


*Figure 2: Sauce IPSec Proxy DNS*

### Routing

Test VMs using the IPSec tunnel will route all their HTTP(s) test traffic to the tunnel gateway. The tunnel gateway routes all the traffic to the IPSec tunnel.

### Protocols

Sauce IPSec Proxy supports HTTP, HTTPS (including WebSockets). Secure WebSockets are only supported for the connections without SSL bumping enabled.

## SECURITY

This section describes the features and procedures that govern Sauce IPSec Proxy in order to provide the best, most secure experience.

For more detailed information on the technology, processes and security operations that govern the Sauce Labs Continuous Testing Platform, read our white paper, An Overview of Sauce Labs Security Processes.

### TUNNEL GATEWAY SECURITY FEATURES

When considering the security of Sauce Labs tunnel gateways, 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 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 allow-list necessary internal services to communicate with the control plane services running on tunnel gateways (such as monitoring services or firewall controller). Each customer's tunnel gateway VM is customized at the time of provisioning per customer's specification and configured to direct all traffic via IPSec.

The tunnel gateway's firewall allows only authorized test VMs to connect. Authorized test VMs include:

- Test VMs that run VPN tunnel owner jobs
- Test VMs that run jobs started by the accounts with which the tunnel is shared

## SAUCE IPSEC PROXY SECURITY

The firewall allows these ports and protocols through the IPSec VPN connection:

| DIRECTION | PROTOCOL |
|---|---|
| Inbound from customer network | BGP (TCP/179) |
| Both directions | ICMP |
| Outbound from Sauce | HTTP (TCP/80, TCP/8080), HTTPS (TCP/443, TCP/8443) |
| Outbound from Sauce | DNS (UDP/53, TCP/53, TCP/853) |

*NOTE: Customers can request additional ports and protocols.*

## SAUCE LABS HOSTED VMS AND REAL DEVICES

The Sauce Labs infrastructure is configured so that each VM and real device is fully isolated and prohibited from communicating with any other VMs or devices in our infrastructure. The only exception for this would be tunnel gateway VMs.

While VMs and real devices are allowed to connect to the internet, Sauce Labs also offers a "Lockdown" feature that locks traffic down to that particular user's tunnels only. Finally, we only permit allow-list necessary internal services to communicate with VMs and/or real devices.

# SAUCE IPSEC PROXY VS. SAUCE CONNECT PROXY

Sauce Connect Proxy and Sauce IPSec Proxy accomplish the same thing: establishing a secure connection between applications hosted on a private network and the Sauce Labs cloud.

Sauce IPSec Proxy tunnels use industry standards to establish a secure connection and transfer data, while Sauce Connect Proxy utilizes a reverse proxy server that opens a secure tunnel connection and proprietary protocol. The main differences are:

| SAUCE CONNECT PROXY | SAUCE IPSEC PROXY |
|---|---|
| Customer can manage tunnels lifespan:<br>• Ephemeral/per-build tunnels<br>• Long-lived tunnels | Customer cannot manage the lifespan:<br>• Sauce IPSec Proxy tunnels are static |
| Sauce Connect client starts a single tunnel. Redundant, a.k.a. High Availability tunnel pools can be established by running multiple clients using special command line options; HA pools also provide improved performance. | Sauce IPSec Proxy tunnels are always started in High Availability mode. Every customer VPN connection includes two Tunnel Gateways. |
| Customer needs to run Sauce Connect client (binary) within their network to establish the tunnels; tunnels use proprietary protocol over TLS 1.2 | Sauce IPSec Proxy tunnels use industry standard IPSec to establish the connection between customer private network and Sauce Labs datacenter |
| Sauce Connect is a part of Sauce Labs offering for all accounts (no additional fees) | Sauce IPSec Proxy is a feature that requires an additional fee |
| Sauce Connect is usually demonstrated and set up as part of the PoC. Minimal setup time is required. | Sauce IPSec Proxy requires tight collaboration and coordination between the customer and the Sauce Labs teams which increases the setup time |

# ADDITIONAL RESOURCES

- Overview of Sauce Labs Security Processes
- Sauce Connect Proxy™ Security Overview
- Sauce Labs Documentation

SAUCELABS

## ABOUT SAUCE LABS

Sauce Labs is the leading provider of continuous testing solutions that deliver digital confidence. The Sauce Labs Continuous Testing Cloud delivers a 360-degree view of a customer's application experience, ensuring that web and mobile applications look, function, and perform exactly as they should on every browser, OS, 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/signup/trial

**FREE TRIAL**

**SAUCE LABS INC. - HQ** 116 New Montgomery Street, 3rd Fl San Francisco, CA 94105 USA