On-premise Architecture Overview

Surfly

November 2023

On-premise Server
CentOS 8 Stream/ RHEL 7-9 | 4 core 2.5 GHz CPU | 8GB RAM | HA Pair supported

Responsibility of Network Admin
Additional Firewall Configuration | Update Execution * | Database Restore

* server updates will require access to Surfly via the internet

Firewall
Firewalld | IPv4 / IPv6 | Port 80/443

Connections
TLS 1.3 | AES-256 | Surfly request / response headers

Database
PostgreSQL | Recommend 60GB Margin | Backups taken with version update

Network Requirements
Allow Surfly Server access to web/origin server | 100Mbps network connection

Surfly Application
~100 concurrent sessions benchmark | Email server / database included

Features Not Supported (Cloud Required)
Videochat | Recordings

More Information
https://docs.surfly.com/installation

No Resource Whitelisting Required

Any request to a web resource from within a Surfly session comes from the Surfly static server IP.

You just need allow the server IP access to the internet

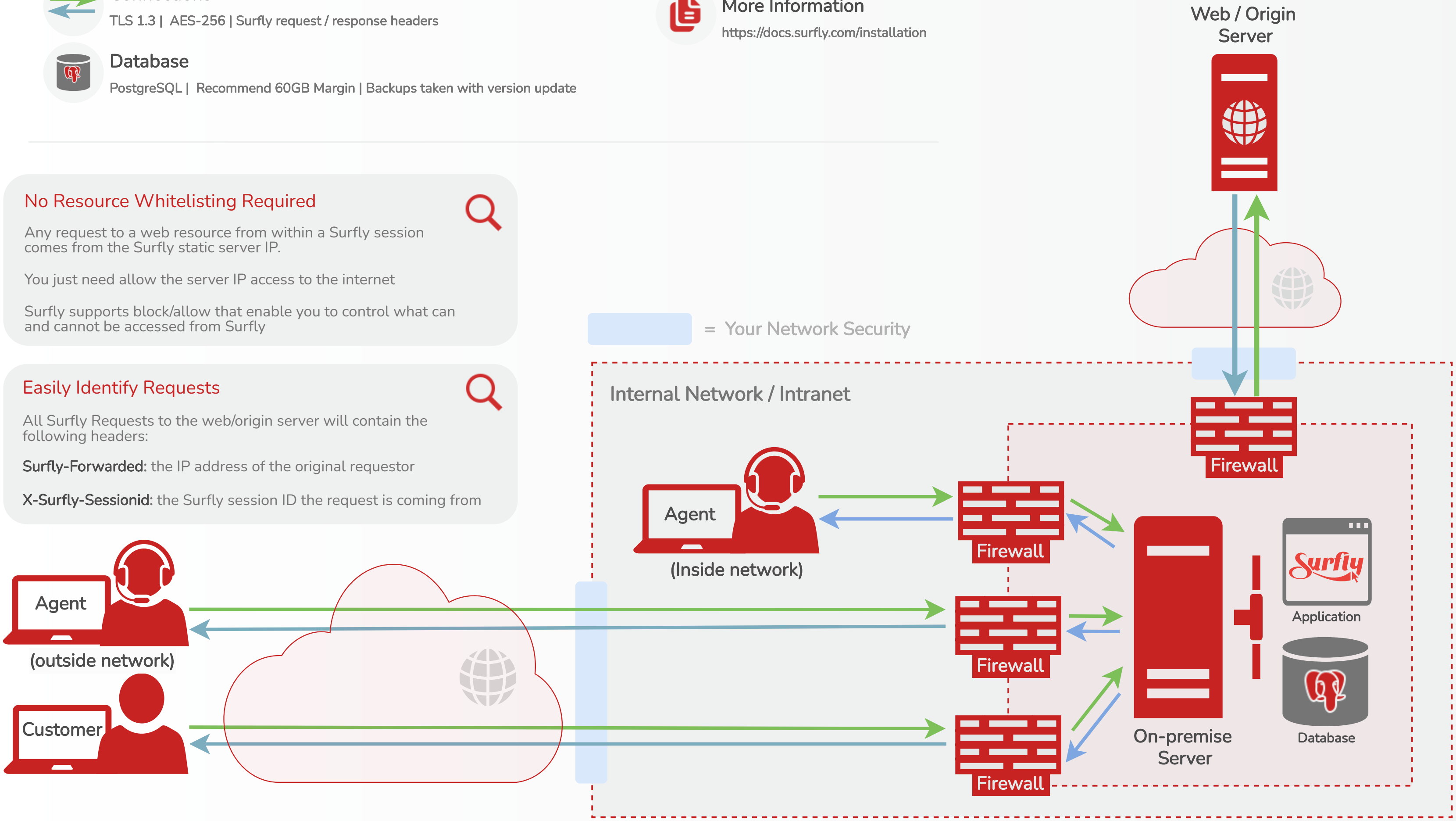
Surfly supports block/allow that enable you to control what can and cannot be accessed from Surfly

Easily Identify Requests

All Surfly Requests to the web/origin server will contain the following headers:

Surfly-Forwarded: the IP address of the original requestor

X-Surfly-Sessionid: the Surfly session ID the request is coming from


Web / Origin Server
🟦 = Your Network Security
Internal Network / Intranet
Firewall
Agent
(Inside network)
Firewall
Firewall
Firewall
Surfly
Application
Database
On-premise Server
Agent
(outside network)
Customer