# SafeSquid Installation Handbook

## Pre-Installation Checklist

Complete all sections before proceeding with installation. Mark N/A where items are not applicable.

# 1. Portal & Keys

|  |  |
| --- | --- |
| **Item** | **Status / Value** |
| Registered Email on https://key.safesquid.com | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| C-Code | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| Downloaded Activation Key (client desktop) | ☐ Yes ☐ No |
| Trusted Root SSL Certificate Authority | ☐ Self-Signed ☐ Enterprise CA |
| SSL Certificate Downloaded | ☐ Yes ☐ No |

# 2. Platform

|  |  |
| --- | --- |
| **Item** | **Status / Value** |
| Platform Type | ☐ Bare Metal ☐ Type-1 Hypervisor |
| Processor Make & Model | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ (Intel) |
| Architecture | ☐ x86 |
| CPU Allocated | \_\_\_\_\_\_\_ Core (Min: 8 CPU) |
| RAM Allocated | \_\_\_\_\_\_\_ GB (Min: 8 GB) |
| Storage Allocated | \_\_\_\_\_\_\_ GB (Min: 100 GB) |
| Hypervisor Name & Version | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |

# 3. SafeSquid Appliance Builder (SAB)

|  |  |
| --- | --- |
| **Item** | **Status / Value** |
| SAB ISO Downloaded from https://download.safesquid.com/sab.iso | ☐ Yes ☐ No |
| SAB ISO Available on your Type-1 Hypervisor Platform | ☐ Yes ☐ No |

# 4. Network Configuration

|  |  |
| --- | --- |
| **Item** | **Status / Value** |
| a) DHCP | Yes  No |
| b) Static IP address | Yes  No |
| Proxy server IP/CIDR netmask  (Eg: 10.200.5.100/24) **(Required)** |  |
| Gateway IP **(Required)** |  |
| Name server address **(Required)** |  |
| Proxy Hostname **(Required)** |  |
| Proxy Domain name **(Required)** |  |

# 5. Authentication

|  |  |
| --- | --- |
| **Item** | **Status / Value** |
| AD/LDAP Server IP | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| AD/LDAP Server FQDN | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| Domain Admin Username | \_\_\_\_\_\_@\_\_\_\_\_\_\_\_\_\_\_ |
| Domain Admin Password Recorded | ☐ Yes ☐ No |
| Record LDAP basedn (For example, for a domain test1.testdomain1.com, enter dc=testdomain1, dc=com) | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| Record LDAP Domain name (For example if you set: LDAP Domain: somedomain.com then all users who present their credentials as username@somedomain.com will be identified and validated from this LDAP server.) | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |

# 6. Firewall Whitelist

## DNS Access (Port 53 and below IP address to be allowed)

|  |  |
| --- | --- |
| **Item** | **Status / Value** |
| Outbound DNS to Root Servers Permitted | ☐ Yes ☐ No |
| **A.ROOT-SERVERS.NET →** 198.41.0.4 | ☐ Whitelisted |
| **B.ROOT-SERVERS.NET →** 170.247.170.2 | ☐ Whitelisted |
| **C.ROOT-SERVERS.NET →** 192.33.4.12 | ☐ Whitelisted |
| **D.ROOT-SERVERS.NET →** 199.7.91.13 | ☐ Whitelisted |
| **E.ROOT-SERVERS.NET →** 192.203.230.10 | ☐ Whitelisted |
| **F.ROOT-SERVERS.NET →** 192.5.5.241 | ☐ Whitelisted |
| **G.ROOT-SERVERS.NET →** 192.112.36.4 | ☐ Whitelisted |
| **H.ROOT-SERVERS.NET →** 198.97.190.53 | ☐ Whitelisted |
| **I.ROOT-SERVERS.NET →** 192.36.148.17 | ☐ Whitelisted |
| **J.ROOT-SERVERS.NET →** 192.58.128.30 | ☐ Whitelisted |
| **K.ROOT-SERVERS.NET →** 193.0.14.129 | ☐ Whitelisted |
| **L.ROOT-SERVERS.NET →** 199.7.83.42 | ☐ Whitelisted |
| **M.ROOT-SERVERS.NET →** 202.12.27.33 | ☐ Whitelisted |
| Custom DNS Server IPs (if required) | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |

## SafeSquid Update Servers

|  |  |
| --- | --- |
| **Item** | **Status / Value** |
| 161.35.135.35:443 | ☐ Whitelisted |
| 192.241.241.158:80 | ☐ Whitelisted |
| 157.245.103.186:443 | ☐ Whitelisted |

## URL Categorization Servers

|  |  |
| --- | --- |
| **Item** | **Status / Value** |
| 157.245.103.186:443 | ☐ Whitelisted |
| 80.225.239.96:8080 | ☐ Whitelisted |
| 80.225.239.96:8080 | ☐ Whitelisted |
| 80.225.239.96:8080 | ☐ Whitelisted |
| 141.148.219.83:8080 | ☐ Whitelisted |
| 141.148.219.83:8080 | ☐ Whitelisted |

## Antivirus Updates

|  |  |
| --- | --- |
| **Item** | **Status / Value** |
| 64.185.189.238:80 | ☐ Whitelisted |

## 6. Troubleshooting

|  |
| --- |
| **Note:** |
| To monitor live installation just hit “Alt+ F2” and to esc the console hit “ALT+F1” and if any error occurs than you can monitor it and also check the installation logs using the command “tail -F syslog”. |

## 7. Post Installation Client Check

## Following steps should be done in the client’s desktop

|  |  |
| --- | --- |
| **Item** | **Status / Value** |
| Check connectivity using ping (ping proxy IP address) | Yes  No |
| Ensure SafeSquid service is running and use telnet to check port connectivity | Yes  No |
| Activation key (check if the downloaded key is present in your client desktop) | Yes  No |
| Firefox Installation | Yes  No |
| Configure your System/Browser to use Proxy | Yes  No |
| Access SafeSquid User Interface using this link [http://safesquid.cfg/](http://safesquid.cfg/%20%20) | Yes  No |
| Import Activation key to your SafeSquid User Interface which you have downloaded from the self-service portal. | Yes  No |
| Check License Details in Support section of your SafeSquid Interface | Yes  No |
| SSH Client Installed (e.g., PuTTY) | ☐ Yes ☐ No |
| SSH Keys added in your proxy server | ☐ Yes ☐ No |

**Installation Process**

# Phase 1: System Boot & Initial Setup 2-18

**Step 1.1: Boot from SAB ISO**

• For Bare Metal: Boot from USB with SAB ISO

• For Type-1 Hypervised: Mount SAB ISO and boot virtual machine

• Automated installation of Debian Linux begins

• SafeSquid SWG and dependencies install automatically

# Phase 2: Network Configuration

**Step 2.1: Configure Network Settings**

• Enter Proxy Hostname/FQDN (from Section 4)

• Configure LAN IP Address

• Configure WAN IP Address

• Set Subnet Mask and Default Gateway

• Configure Primary and Secondary DNS Servers

• Verify network connectivity

# Phase 3: SafeSquid Activation 32-34

**Step 3.1: Activate SafeSquid License**

• Access SafeSquid admin interface

• Enter Product Activation Key (from Section 1)

• Complete activation process

# Phase 4: SSL Certificate Setup 35-47

**Step 4.1: Configure SSL Certificate**

• Upload SSL certificate (from Section 1)

• Configure SSL interception settings per enterprise policy

**SafeSquid Integration/Configuration Validation Form**

# Authentication & Domain Integration

|  |  |
| --- | --- |
| **Item** | **Status / Value** |
| AD/LDAP Integration Configured | ☐ Done |
| Domain Joined Successfully | ☐ Done |
| User Authentication Tested | ☐ Done |

# Policy & Security Configuration

|  |  |
| --- | --- |
| **Item** | **Status / Value** |
| Web Filtering Policies Configured | ☐ Done |
| URL Categorization Enabled | ☐ Done |
| Antivirus Scanning Configured | ☐ Done |
| SSL Interception Verified | ☐ Done |
| Policy Enforcement Tested | ☐ Done |

# System Operations

|  |  |
| --- | --- |
| **Item** | **Status / Value** |
| Updates Verified & Scheduled | ☐ Done |
| Logging Configured | ☐ Done |
| Monitoring/Alerting Configured | ☐ Done |
| Backup Configuration Completed | ☐ Done |

# Testing & Validation

|  |  |
| --- | --- |
| **Item** | **Status / Value** |
| Proxy Connectivity Tested from Client Devices | ☐ Done |
| Internet Access Verified Through Proxy | ☐ Done |
| Policy Filtering Validated | ☐ Done |
| Reporting Dashboard Accessible | ☐ Done |

# Installation Sign-Off

|  |  |
| --- | --- |
| **Item** | **Status / Value** |
| Installation Date | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| Installed By | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| Signature | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| Verified By | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| Signature | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |

*SafeSquid Support: https://key.safesquid.com*