|  |  |
| --- | --- |
| Layer 7 Perimeter Security for Customer X  Software and Technical Assistance Overview | Abstract  Global Surge in web‑based Layer 7 threats, like Zero‑Hour Phishing, XSS, Ransomware, and Data Theft, underscores the failure of legacy measures, and “all-in-one” technologies. Purpose-built for Zero-Trust Web Security, SafeSquid Secure Web Gateway's architecture ensures maximum flexibility, secure connectivity, seamless integration, regulatory compliance, and a future-ready enterprise security posture.  SafeSquid Labs  Your trusted OEM for web security solutions |
| SafeSquid Labs is a strategic business unit of Office Efficiencies (India) PVT. LTD., 127, Damji Shamji Industrial Estate, L.B.S. Marg, Vikhroli (West), Mumbai - 400083 | |  |  | | --- | --- | | F:\russel\MAKE-IN-INDIA.jpg | | | GST | 27AAACO7414P1Z1 | | CIN | U72100MH2004PTC148591 | | PAN | AAACO7414P | |

# Confidentiality Statement

This document contains proprietary and confidential information related to SafeSquid Labs and its solution and intended solely for the designated recipient(s). The information herein is strictly confidential, privileged, and protected under data privacy regulations and intellectual property rights.

Confidential Information Includes:

* Proprietary details of SafeSquid’s platform and solution, technical specifications, and security controls.
* Design, deployment strategies, implementation and project management methodologies.
* Customer-specific configurations, policies, and security frameworks.
* SafeSquid Labs’ infrastructure, corporate security policies, and operational procedures.
* Technical insights, research, and innovation related to SWG.

Obligations & Restrictions:

* This document must not be shared, reproduced, or disclosed—in full or in part—to any unauthorised individual or third party without prior written consent from an authorised SafeSquid representative.
* Access is strictly limited to authorized recipients with a legitimate purpose.
* Any use of the information outside the intended scope requires explicit written consent from an authorised SafeSquid representative.
* The recipient must ensure compliance with applicable data privacy laws, including but not limited to DPDPA, GDPR, CCPA, and industry security standards.
* Any unauthorised use, alteration, or distribution of the content within this document is strictly prohibited and may result in legal consequences.

Ownership & Data Privacy Compliance:

All information contained in this document remains the intellectual property of SafeSquid Labs. Any processing, storage, or sharing of customer-related data as part of the solution deployment must adhere to strict data privacy protocols, encryption standards, and regulatory requirements to ensure data security and compliance.

By accessing this document, the recipient acknowledges and agrees to the confidentiality obligations and commits to maintaining the security and integrity of the information contained herein.

Table of Contents

[Confidentiality Statement 2](#_Toc212250152)

[1 Executive Summary 4](#_Toc212250153)

[2 Introduction 5](#_Toc212250154)

[3 Business Case 6](#_Toc212250155)

[4 SafeSquid Secure Web Gateway 10](#_Toc212250156)

[5 Scope of Work 11](#_Toc212250157)

[6 Proposed Solution 13](#_Toc212250158)

[7 Solutioning 22](#_Toc212250159)

[8 Deployment Plan 24](#_Toc212250160)

[9 Training & Capacity Building 27](#_Toc212250161)

[10 Service Model 28](#_Toc212250162)

[11 Disclosure and Acceptance 30](#_Toc212250163)

# Executive Summary

Rapid digitalization increases exposure of enterprise digital assets and productivity to cyber threats.   
A variety of studies, highlight the ongoing evolution of Zero‑hour exploits such as Phishing, XSS, Ransomware and Data theft.

Comprehensive mitigation of security threats using reliable technology empowers the enterprise to adopt innovative solutions that boost productivity and enhance its competitive edge.

Primarily designed for curbing cyber‑slacking, and conserving bandwidth, the legacy technologies offer very basic security cover. The global surge in the web‑based security incidences clearly underscore the failure of the various “all-in-one” technologies. Technological limitations of such solutions force the security administrators to trade-off between security needs and productivity demands.

The sheer quantum of factors, and pace of evolution associated with the web technologies, highlight the need of a dedicated approach towards mitigation of web‑based threats. SafeSquid is a purpose‑built Application Layer Firewall to shield enterprise workers and data from both external threat actors and mischievous insiders.

The SafeSquid Secure Web Gateway (SWG) is purpose-built to defend against Application Layer risks. Granular, Zero-Trust web access policies ensure maximum flexibility for ideal security realisation. On-The-Wire Deep Content Inspection sanitises all inbound and outbound web traffic to prevent data leakage and neutralise threats. Deep Visibility ensures proactive incident response and in-depth forensic analysis.

The SMP-aware, cluster-ready architecture delivers elastic scalability, high availability, and disaster recovery, while remaining agentless for simplified operations. Whether deployed on-premises, in the cloud, or hybrid, SafeSquid SWG ensures secure connectivity, policy consistency, and resilient performance across distributed and remote workforces.

SafeSquid SWG enables enterprises to neutralise web‑based Layer 7 threats without compromising productivity, compliance, or user experience—delivering a future-ready security posture aligned with Zero-Trust principles.

# Business Case

The current environment exhibits several weaknesses in securing web-bound traffic, exposing users, applications, and data to risk.

## Existing Infrastructure

Customer X’s IT environment is distributed across five locations: Manesar, Gurugram, Mumbai, Bangalore, and Noida. The Noida Airtel Data Centre (DC) functions as the primary server facility, while the regional offices (Manesar, Gurugram, Mumbai, and Bangalore) operate as small branch sites.

### Data Centre (Noida, Airtel DC)

* Hosts 2 Active Directory (AD) servers, Citrix Workstation Servers, and a firewall.
* Serves as the central hub for authentication, application hosting, and data services.
* Interconnected with other branch locations via IPSec tunnels.

### Branch Offices (Manesar, Gurugram, Mumbai, Bangalore)

* Each branch provides local internet and intranet access to employees.
* The Manesar office hosts the corporate firewall, which routes outbound web traffic from the branch offices.

### Hybrid Workforce

* Employees can remotely connect through a corporate VPN for access to internal applications.
* VPN users’ web traffic exits directly to the internet, bypassing the corporate firewall.

### Contractual Workers

* Access provided via Citrix Workstations.
* Internet access is enabled within the Citrix environment, with limited visibility and control at the gateway.

### Internal Application Web Access

* Internal web applications are permitted unrestricted internet access.
* This creates potential exposure since application-to-internet communication is not monitored or filtered.

### User Authentication

* All users are authenticated against the `Corp.hcil` domain.
* Some privileged users also belong to the`User.hcil` domain.

## Security Gaps

Traditional firewalls, UTMs, and URL filters were built for a time when enterprise networks were centralised, traffic patterns were predictable, and the security perimeter was well-defined. Applications were hosted in corporate datacentres, users worked primarily on-site, and internet usage was limited to a narrow set of business tools.

Today’s cloud-first, hybrid work environment has completely disrupted those assumptions. Enterprise traffic now flows directly to cloud applications, collaboration platforms, and SaaS ecosystems—often bypassing datacentre security controls altogether. Users access corporate data from unmanaged devices, remote locations, and public networks. More than 90% of this traffic is encrypted, and attackers increasingly disguise their activity within legitimate services.

Legacy perimeter solutions are unable to adapt to these conditions. Their static rule sets, limited inspection capacity, and reliance on signature-based defences create blind spots that adversaries exploit. As organisations adopt cloud, mobility, and regulatory compliance frameworks, the inability of legacy tools to deliver real-time visibility, granular control, and scalable protection exposes enterprises to critical blind spots.

### Modern Web-Based Threats Bypass Signature-Based Defences

Zero-Hour phishing, ransomware delivery, command-and-control callbacks, and malicious scripts are increasingly disguised within legitimate domains and dynamic web content. Static signature or reputation checks cannot adapt to polymorphic code or context-aware attacks, leaving enterprises exposed.

### SSL/TLS Blind Spots Leave Encrypted Attack Channels

With over 90% of traffic encrypted, adversaries routinely hide payloads inside HTTPS. Legacy devices lack scalable SSL/TLS decryption and inspection, creating exploitable gaps without visibility.

### Shadow IT Introduces Uncontrolled Cloud Risks

Employees adopt unsanctioned SaaS and cloud tools beyond IT oversight. Legacy web filters cannot differentiate sanctioned from unsanctioned applications, resulting in unmanaged data flows and compliance violations.

### Legacy Perimeters Fail to Protect Remote Users

Remote and hybrid users often connect over public ISPs, bypassing traditional firewalls and UTMs tied to datacentre perimeters. VPN-based approaches add latency and complexity, making it difficult to ensure consistent, high-performance policy enforcement for distributed workforces.

### Lack of Contextual Controls Hinders Zero Trust Adoption

Legacy filters block at the domain level but cannot enforce policies based on user identity, device posture, application type, or content classification—making Zero Trust enforcement unachievable.

### Performance Trade-Offs Weaken Security Enforcement

Layering multiple engines on legacy devices introduces latency and downtime. This forces security teams to relax controls, weakening protection to preserve user experience.

### Rising Web Traffic Volume Overwhelms Legacy Infrastructure

The surge in cloud applications, video streaming, collaboration platforms, and encrypted sessions has multiplied both traffic volume and inspection complexity. Legacy appliances lack elastic scalability, quickly hitting performance ceilings that result in latency, dropped sessions, or reduced inspection depth—directly weakening security effectiveness.

## Key Drivers for a Secure Web Gateway

As organizations increasingly adopt cloud applications, enable hybrid work environments, and provide internet access to a distributed workforce, the traditional network perimeter has become obsolete. Users are accessing corporate data and web services from various devices, locations, and networks—exposing the organisation to advanced threats, data leakage, and policy violations.

A Secure Web Gateway (SWG) is essential to address these modern security challenges. It acts as a critical enforcement point between users and the internet, inspecting all web-bound traffic in real time to block malicious content, enforce acceptable use policies, and prevent sensitive data from leaving the organisation. Unlike legacy web filters, a modern SWG provides deep SSL/TLS inspection, granular user- and application-level controls, and integrated threat intelligence to detect zero-day attacks and sophisticated phishing campaigns.

Moreover, regulatory mandates such as GDPR, HIPAA, and PCI-DSS require organisations to monitor and secure internet communications, making an SWG a key component of a compliant and resilient security architecture. In essence, a Secure Web Gateway empowers organisations to safely embrace the cloud, support remote work, and maintain full control and visibility over internet usage without compromising performance or user experience.

### Advanced Threat Protection Beyond Signatures

An SWG leverages real-time behavioural analysis, sandboxing, and threat intelligence feeds to detect and block zero-hour phishing, ransomware payloads, malicious cross-site scripts, and command-and-control callbacks. This eliminates reliance on static signatures, protecting against polymorphic and context-aware attacks that legacy tools cannot identify.

### Decryption and Inspection of Encrypted Traffic

Modern SWGs perform scalable SSL/TLS decryption, inspection, and re-encryption of HTTPS traffic. This capability closes the visibility gap exploited by attackers while using policy-based exceptions to maintain compliance, preserve privacy, and prevent breakage of sensitive business applications.

### Governance over Shadow IT and SaaS Usage

By providing application-level visibility, an SWG distinguishes between sanctioned and unsanctioned SaaS platforms. It enables IT teams to block or restrict risky services, apply granular controls to approved applications, and enforce data handling policies—reducing exposure to data exfiltration and compliance violations.

### Consistent Security for Remote and Hybrid Workforces

SWGs extend enterprise-grade web protection to users wherever they connect—office, home, or mobile—without forcing traffic back through a central VPN. This ensures consistent enforcement of corporate policies while maintaining high availability, low latency, and positive user experience across distributed environments.

### Context-Aware, Identity-Driven Policy Enforcement

Unlike domain-level blocking, modern SWGs integrate with IAM systems to apply policies based on user identity, device posture, application type, and data sensitivity. This contextual enforcement enables practical Zero Trust implementation, ensuring that access decisions reflect business risk in real time.

### High-Performance Security Without Latency Penalties

SWGs are engineered for high-throughput inspection, using optimized engines to minimize latency even under heavy loads. This allows enterprises to maintain strong security enforcement without degrading collaboration tools, SaaS performance, or end-user productivity.

### Elastic Scalability for Growing Web Traffic

Cloud workloads, collaboration platforms, and video conferencing are generating unprecedented traffic volumes. SWGs are designed with elastic scalability, allowing inspection capacity to grow with demand. This prevents performance bottlenecks, ensures uninterrupted enforcement, and supports evolving enterprise traffic patterns.

# SafeSquid Secure Web Gateway

Traditional SWG solutions seek to re-purpose legacy web caching proxy technologies. Inherent limitations thus not only restrict security capabilities but also impact performance when multiple security options are enabled.

Introduced in 2004, SafeSquid® our flagship offering, is an HTTP Proxy Server, specially designed for web security. A dedicated team of security experts and technology specialists ensure its constant evolution and enable you to meet new challenges.

SafeSquid SWG is the latest generation in this product family. Combined with a proven HTTP Proxy technology, innovative set of security features, and a state-of-the-art implementation architecture, it gives you fullest capabilities for gateway-level access and content security.

SafeSquid Secure Web Gateway is Layer-7 firewall designed to safeguard Zero-Trust enterprises against modern, Zero-Hour web-based threats, such as phishing, malware infiltration, cross-site scripting, data exfiltration, and productivity loss from cyber-slacking. SafeSquid combines robust policy enforcement, real-time threat detection, deep content inspection, and user activity monitoring into a unified, highly customizable platform. It serves as a trusted access control point between end-users and the internet, ensuring that only safe, compliant, and policy-allowed web traffic passes through the organization’s network.

Built on a modular proxy architecture, SafeSquid SWG offers unmatched flexibility in configuration and deployment—suitable for enterprises, ISPs, educational institutions, and government organizations. It supports both on-premises and hybrid deployments, with a strong emphasis on privacy, regulatory compliance, and integration with existing security infrastructure.

# Scope of Work

## Overview

The scope of work involves the end-to-end implementation of the SafeSquid Secure Web Gateway (SWG) to ensure secure, policy-driven, and compliant web access across the organisation. This includes planning, deployment, integration, configuration, testing, training, and support services necessary to operationalise the solution effectively.

The SWG will be deployed in alignment with the organisation’s security architecture, providing advanced content filtering, threat protection, SSL decryption, and user identity-based access control. The engagement will also cover integration with existing infrastructure such as Active Directory, SIEM, DLP systems, and other security tools to ensure a seamless and centralised approach to web security management.

## Business Objectives

The primary business objective of implementing the SafeSquid Secure Web Gateway (SWG) is to establish a secure, controlled, and compliant internet access environment that protects the organisation’s digital assets, workforce, and reputation from evolving web-based threats. As enterprises increasingly adopt cloud services, support remote workforces, and digitise their operations, it becomes critical to ensure that all web-bound traffic is inspected, filtered, and governed through intelligent, identity-aware policies.

This initiative aims to:

* Protect Internet Users, Data and Internal Web Applications  
  Prevent malware, ransomware, phishing attacks, and other web-based threats from compromising endpoints and exfiltrating sensitive data.
* Ensure Visibility and Control  
  Provide centralized visibility into user behaviour, internet usage, and policy violations across all departments and locations.
* Maintain Regulatory Compliance  
  Support compliance with standards such as CERT-In, ISO 27001, GDPR, HIPAA, and other industry-specific guidelines by enabling granular policy enforcement and logging.
* Enforce Acceptable Use Policies (AUP)  
  Control access to inappropriate or non-business websites to ensure productivity, reduce bandwidth abuse, and uphold organizational standards.
* Integrate with Existing Security Ecosystem  
  Seamlessly connect with existing identity, DLP, SIEM, and access control systems to form a unified cybersecurity posture.
* Support Hybrid and Remote Work Models  
  Extend consistent security policies to users regardless of their location or network, enabling safe and productive remote work.

By achieving these objectives, the organisation can enhance its overall cybersecurity maturity, reduce operational risks, and ensure secure digital transformation while keeping user experience and system performance intact.

# Proposed Solution

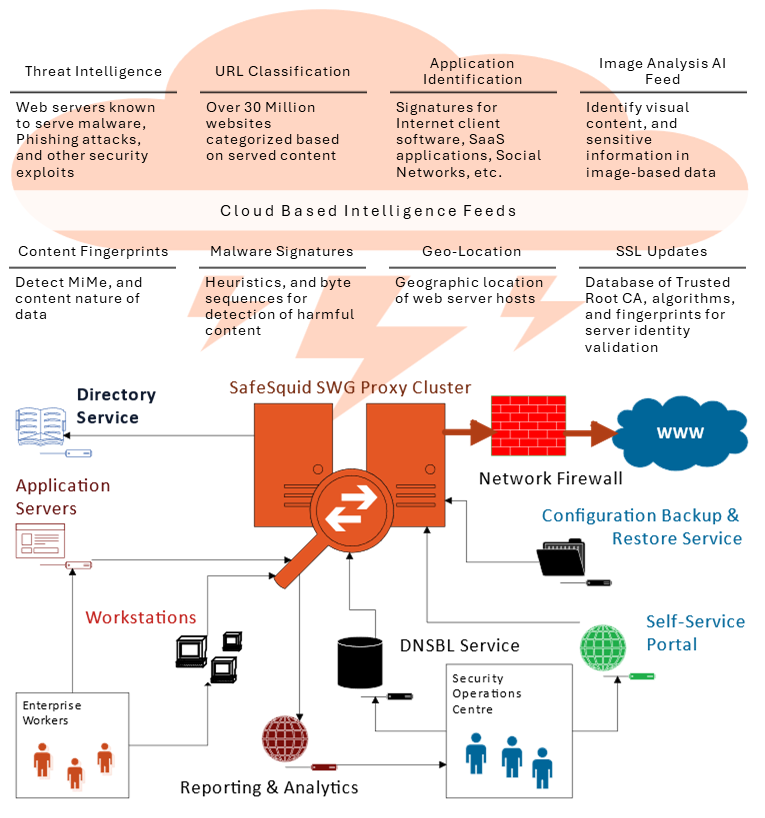
The proposed solution is a comprehensive deployment of the SafeSquid Secure Web Gateway, designed to serve as a centralised, policy-enforced gateway for secure, compliant, and intelligent internet access. The solution architecture ensures secure web communication for all users—whether on-premises or remote—while offering flexibility, scalability, and deep visibility into web traffic.

## High-Level Architecture

Legacy security devices often fragment enforcement across multiple appliances, creating policy gaps, inspection blind spots, and administrative overhead. SafeSquid Secure Web Gateway (SWG) consolidates critical web security controls into a modular, Application Layer focused architecture, ensuring granular policy enforcement, seamless integration, and scalable performance.

At a high level, the SafeSquid SWG solution consists of the following core components:

1. SafeSquid Proxy Server  
   Central enforcement point for all HTTP/HTTPS traffic, performing full proxying, in-line inspection, and enforcement of security policies.
2. Policy Management Console  
   Web-based administrative interface for defining, simulating, and enforcing access control, URL filtering, SSL inspection, and DLP policies with full version tracking.
3. Authentication Layer  
   Integration with enterprise identity providers (ZTNA, Active Directory, LDAP, SAML, RADIUS) to enforce identity- and group-aware access policies aligned with Zero-Trust principles.
4. SSL Inspection Module  
   Provides secure decryption, inspection, and re-encryption of encrypted web sessions, with selective bypass for privacy-sensitive applications.
5. Contextual Intelligence Neural Network  
   Applies behavioural analytics and machine learning to detect zero-hour phishing, anomalous uploads, polymorphic malware, and insider misuse beyond static signatures.
6. Antivirus & Content Filtering Engine  
   Scans all data exchange in real time using integrated AV engines, and filters malicious, inappropriate, non-business, or policy-violating web content.
7. Reporting & Analytics Module  
   Captures forensic-grade logs of user activity and threat events, generating real-time and scheduled reports.



## Solution Components

The SafeSquid Secure Web Gateway (SWG) is composed of modular, policy-driven components that work together to provide deep web security, granular content filtering, encrypted traffic inspection, and regulatory compliance. Each component addresses a specific challenge in ensuring secure, intelligent, and controlled access to internet resources.

### Web Proxy & Policy Engine

The Web Proxy & Policy Engine acts as the core of the SWG, intercepting all HTTP/HTTPS traffic, inspecting content, and applying rule-based policies by user, group, IP, schedule, or content type.

### SSL/TLS Inspection Module

The SSL/TLS Inspection Module decrypts, inspects, and re-encrypts HTTPS traffic to expose hidden threats. It supports custom root CA integration for enterprise environments and allows selective SSL bypass for privacy-sensitive websites such as banking or healthcare.

### Identity & Authentication Integration

Static IP or network-based controls cannot enforce Zero Trust. The Identity and Authentication Integration module enables user- and group-level policy enforcement through AD, LDAP, SAML, RADIUS, or local authentication. It generates audit trails that link actions directly to identities.

### Web Categorisation Engine

The Web Categorisation Engine classifies web destinations into granular categories (business, productivity, social, gaming, adult, streaming, etc.). Policies can be applied at the user, group, or role level, ensuring that business traffic is prioritised while unsafe or non-essential categories are blocked. Continuous updates to the categorisation database keep pace with new and emerging websites, including multilingual and regional content.

### Contextual Intelligence Neural Network

Signature- and rule-based systems miss polymorphic or context-aware attacks. The Contextual Intelligence Neural Network applies machine learning models to analyse web traffic patterns, user behaviour, and content attributes in real time. It can detect zero-hour phishing, anomalous uploads, evasive scripts, and insider misuse that bypass static defences. By continuously learning from traffic, it adapts to evolving threats while reducing false positives.

### Content Filtering Engine

The Content Filtering Engine enforces controls based on MIME type, file type, URL category, keywords, regex patterns, and dynamic page content (including Indian languages). It can block or rewrite disallowed elements such as scripts, pop-ups, or Flash.

### On-The-Wire Malware Scanner

Malware-infected files and phishing attempts bypass traditional filters. The Antivirus & Threat Detection Layer scans web content in-memory using integrated AV engines. It supports ICAP integration with external sandboxes, blocking trojans, spyware, ransomware, and zero-hour phishing campaigns.

### Bandwidth Control

Unrestricted streaming, torrents, and recreational applications consume bandwidth needed for critical services. The Bandwidth Control module monitors and regulates bandwidth usage per user, group, application or content type. It enforces QoS (Quality of Service) policies and prioritises business-critical applications while throttling or blocking high-bandwidth non-business traffic such as YouTube, Netflix, or torrents.

### Reporting & Analytics Module

Limited visibility hinders compliance and incident response. The Reporting & Analytics Module captures detailed logs of every user transaction, producing real-time and scheduled reports on web usage, threat events, policy violations, and bandwidth consumption. It integrates with third-party SIEMs (Splunk, QRadar, etc.) via syslog and REST APIs to support forensic investigations and centralised monitoring.

### Management Console

The Management Console provides a web-based GUI for centralised configuration and policy management. It supports role-based access control (RBAC) for administrators, and includes dashboards, alerts, logs, and diagnostic tools to simplify daily operations and reduce response times.

### Custom Scripting Engine

Static rule sets cannot adapt to dynamic user behaviour or evolving risks. The Custom Scripting Engine enables administrators to create logic-based, context-aware policies using an embedded scripting environment. It supports triggers based on content, user behaviour, or network context, and can enforce adaptive filtering, redirection, or transformation of traffic.

### Configuration Backup & Restore Service

Configuration errors or hardware failures can disrupt enforcement. The Configuration Backup & Restore Service provides automated and on-demand snapshots of system policies, rules, and operational settings. In the event of a failure, configurations can be restored quickly across cluster nodes or replacement appliances, ensuring minimal downtime and business continuity. Versioning and scheduled backups further reduce risk from accidental misconfigurations.

### Cloud-Based Threat Intelligence Feeds

Traditional security databases quickly become outdated, leaving gaps against zero-hour attacks. The Cloud-Based Threat Intelligence Feeds component continuously ingests live threat data from global intelligence networks, including indicators of compromise (IoCs), malicious domains, IP addresses, phishing sites, and malware signatures. By dynamically updating security policies, it ensures real-time blocking of new and evolving threats before they reach end-users. Integration with the SWG’s enforcement layers (proxy, filtering, AV, and DLP) ensures a unified and adaptive defence posture.

### Image Scanner

Text-based filters cannot detect harmful or non-compliant imagery. The **Image Scanner** inspects multimedia traffic, applying **AI-based visual recognition** to identify pornography, violent imagery, hate symbols, or policy-violating visuals. This ensures compliance with HR policies, regulatory frameworks, and safe workplace standards while reducing legal and reputational risk.

## Authentication and Access Control Process

A core pillar of the SafeSquid Secure Web Gateway (SWG) solution is its robust Authentication and Access Control framework. It ensures that only authorized users can access web resources based on predefined security policies, user roles, and organizational compliance requirements. The process enforces identity-aware access, enabling precise control over user activity, web traffic, and policy application.

### User Authentication Process

SafeSquid supports multiple enterprise-grade authentication mechanisms to verify user identity and assign appropriate access levels.

**Supported Authentication Methods**

* Active Directory (AD) – Integration via NTLM, Kerberos, or LDAP
* LDAP/LDAPS – Lightweight Directory Access Protocol-based directory services
* Local User Database – For smaller deployments or guest access
* Captive Portal – Web-based login page for unauthenticated users
* Browser-Based NTLM / Kerberos (SSO) – Seamless authentication for domain-joined devices

**User Authentication Workflow**

1. User initiates a web request
2. SafeSquid intercepts and checks for an authenticated session
3. If not authenticated, the user is prompted via:
   1. Captive Portal
   2. Browser SSO (NTLM/Kerberos)
4. Credentials are validated against the configured directory or identity provider.
5. Upon successful authentication, SafeSquid assigns the user a session with identity context (user ID, group, IP, device).
6. The session is cached for performance, and all subsequent traffic is associated with this identity.

### Access Control Mechanism

Once authenticated, SafeSquid enforces access control policies based on:

* User Identity (e.g., [john.doe@company.com](mailto:john.doe@company.com))
* Group Membership (e.g., HR, Finance, IT)
* Source IP Address or Subnet
* Device Type or Location
* Time-of-Day or Day-of-Week
* Authentication Method Used
* Web Category, Application, or URL

**Policy Enforcement Examples**

* Allow YouTube access for the Marketing team but block video uploads.
* Block social media access during working hours for all except the PR team.
* Allow file downloads but block file uploads for external consultants.
* Permit internet access only during business hours for contract staff.

### Policy Administration

* Policies are managed via a centralised, web-based Policy Management Console.
* Role-based access control (RBAC) is implemented for administrators to control policy changes.
* Policies can be defined in a hierarchical or exception-based format.
* Real-time testing and preview of policies are available before activation.
* All authentication attempts (successful/failed) are logged.
* Access decisions and policy enforcement actions are recorded per user.
* Logs can be forwarded to SIEM tools (e.g., Splunk, QRadar) via syslog or REST API.
* Audit trails support compliance with GDPR, HIPAA, CERT-In, and ISO 27001.

**Key Benefits of the Workflow**

Implementing a robust Authentication and Access Control workflow in the SafeSquid Secure Web Gateway (SWG) delivers significant operational, security, and compliance advantages. By ensuring every web request is validated and governed by identity-aware policies, the organisation achieves both control and transparency without compromising user experience.

1. Identity-Based Policy Enforcement  
   Generic access policies fail to reflect organisational structure. The workflow enforces per-user and per-group web access controls, mapping permissions to HR, Finance, IT, and other departments. This ensures least-privilege access and alignment with enterprise roles.
2. Enhanced Security Posture  
   Unmonitored access enables data leaks and misuse. By enforcing real-time user and device-aware policies, the workflow prevents unauthorised internet access, blocks insider threats, and restricts shadow IT usage.
3. Comprehensive Visibility and Auditability  
   Security investigations suffer when user actions aren’t traceable. The workflow provides session-level visibility of every user’s internet activity, supporting forensic analysis, CERT-In compliance, GDPR audits, and ISO 27001 reporting requirements.
4. BYOD and Guest Access  
   External devices often introduce unmanaged risks. The workflow allows restricted, captive-portal based access for BYOD and guest users, applying differentiated controls while safeguarding the core network.
5. Seamless User Experience  
   Repeated login prompts frustrate users and slow adoption. The workflow integrates with SSO providers (Active Directory, SAML), enabling transparent authentication for domain-joined users and minimising disruption.
6. Centralised and Simplified Policy Management  
   Distributed rule sets create complexity and errors. The workflow provides a centralised web console with role-based administration, real-time policy testing, rule simulation, and rollback to ensure safe and efficient policy updates.
7. Productivity Optimisation  
   Unregulated browsing reduces workplace efficiency. The workflow enforces Acceptable Use Policies (AUP), blocking non-business or time-wasting websites during work hours, while prioritising bandwidth for business-critical applications.
8. Enterprise Ecosystem Integration  
   Standalone controls create silos in security monitoring. The workflow integrates with SIEM, IAM, and DLP platforms, exposing logs via REST APIs and syslog, enabling orchestration and unified visibility across the enterprise security stack.

## Solution Key Capabilities

SafeSquid Secure Web Gateway delivers a comprehensive set of features designed to provide secure, policy-controlled, and compliant web access across enterprise environments. The following core capabilities define the solution’s value proposition for organisations seeking advanced threat protection, granular access control, and regulatory compliance.

### Granular Web 2.0 Application Controls

SafeSquid SWG’s Policy Engine makes access decisions based on a combination depending on the user identity, web category, client application, transaction headers, data transfer nature and size. SafeSquid SWG can limit access to specific functionalities within web applications.

### Real-Time Content Filtering

SafeSquid SWG actively prevents the transfer of malware and unsuitable content in both uploads and downloads. It continuously scans inbound and outbound web traffic using antivirus and heuristic techniques to detect, block, or sanitise hidden threats. Both textual and visual content are examined to stop inappropriate material, even in spoofed files.

### Deep Visibility

Enterprises struggle to detect anomalies without detailed monitoring. SafeSquid SWG provides forensic-grade reporting, customisable anomaly detection logic, and real-time alerts to SOC teams, ensuring that suspicious behaviour and policy violations are identified before they escalate.

### Extensibility and Customisability

Siloed tools weaken security and increase admin overhead. SafeSquid’s enterprise-ready architecture integrates with IAM, ICAP, DLP, SIEM, DNSBL, and SOC threat intelligence platforms. It also supports custom enterprise root CA certificates, blending seamlessly into existing infrastructure and extending security coverage.

### Deployment Flexibility

SafeSquid SWG can be deployed on-premises, in the cloud, or in hybrid mode, operational within minutes to align with diverse enterprise network requirements.

## Key Differentiators

SafeSquid is the World's Most Advanced Web Proxy Solution, explicitly designed for Zero-Trust Web Security. The current generation of SafeSquid SWG offers more real-time content security capabilities than any traditional perimeter security solution

### Zero-Trust Web Access

Traditional access models grant broad permissions once a user is authenticated, creating opportunities for lateral movement, shadow IT usage, and accidental or malicious misuse. Zero-Trust principles demand that every web request is continuously evaluated against context-aware policies.

The granularity of control across these parameters is what makes Zero-Trust enforcement practical. Instead of binary “allow/deny” decisions, SafeSquid enforces fine-grained, identity-aware, and context-driven rules that continuously validate each web transaction. This ensures business-critical access is preserved while risk surfaces are minimised—achieving Zero-Trust at the web layer without degrading productivity.

### On-The-Wire Deep Content Inspection

Conventional security tools introduce latency by writing traffic to disk before scanning, creating performance bottlenecks and opportunities for evasion. SafeSquid SWG performs all HTTPS inspection, content filtering, and threat analysis entirely in memory, enabling real-time enforcement without delays while ensuring that malicious payloads are intercepted before reaching users.

### Integrated DNS Security

Relying on external DNS resolvers introduces latency, privacy risks, and exposure to DNS-based attacks such as spoofing or tunnelling. SafeSquid SWG includes an internal DNS resolution system that accelerates lookups, prevents data leakage, and blocks malicious or suspicious domains in real time, ensuring secure and efficient name resolution.

### Native Browser Isolation

Malicious scripts within legitimate sites exploit browser vulnerabilities. SafeSquid enforces Content Security Policies (CSP) to natively sandbox web applications inside the browser, isolating risky content and preventing direct compromise of endpoints.

### Homograph Detection

Attackers register lookalike domains using homoglyph characters to trick users into visiting spoofed sites. SafeSquid detects these homograph attacks in real time, blocking deceptive domains before they can be used for phishing or credential theft.

### Geo-location Blocking

Malware operators often host infrastructure in high-risk geographies. SafeSquid enforces geo-location-based blocking, preventing outbound or inbound traffic to servers in restricted regions and reducing exposure to global threat actors.

### True MIME type detection

File extension spoofing enables malicious executables to masquerade as safe documents. SafeSquid validates the true MIME type of more than a hundred file types and thousands of data identifiers, preventing disguised malware and stopping unauthorised data transfers.

### Agentless Enforcement

Endpoint agents create overhead and complicate updates. SafeSquid requires no agent installation, leveraging built-in OS and browser settings. All endpoint configurations can be centrally managed via Active Directory, simplifying administration and reducing operational costs.

### SMP Aware Architecture

Traditional gateways fail to utilise modern multi-core systems efficiently, causing performance bottlenecks under heavy load. SafeSquid’s SMP-aware architecture is optimised for symmetric and shared-memory multiprocessing, scaling linearly as hardware resources increase and delivering consistent high throughput.

### Elastic Scalability

Legacy appliances degrade under traffic growth. SafeSquid’s SMP-aware architecture scales up throughput to absorb bursts, while its cluster-ready technology allows proxy nodes to be added seamlessly for scale-out, load balancing, and failover.

### Self-Heal Technology

SafeSquid’s Self-Heal Technology proactively monitors critical dependencies, automatically regenerating missing, expired, or corrupted configurations and signatures to ensure uninterrupted protection

### Integrated Cloud Disaster & Recovery

Environmental failures or hardware loss often wipe out critical configurations. SafeSquid ensures resilience with integrated cloud-based backup and restoration, allowing painless recovery of policies and signatures even after a total disaster.

# Solutioning

## System Requirements

Sizing a Secure Web Gateway deployment requires translating business usage patterns into technical workloads. The following values are based on reasonable assumptions; actual sizing should be validated against live traffic analysis for greater accuracy.

|  |  |  |
| --- | --- | --- |
|  | Estimated Value | Definition |
| Total Internet Users | 100 Users | All unique internet users |
| Maximum User Concurrency | 50% | Share of users active simultaneously during peak load windows |
| Maximum Concurrent Users | 50 Users | Peak number of simultaneously active users |
| Maximum Concurrent Connections | 2500 Connections per second | Aggregate peak connection rate across all active users |
| Log Data Retention Period | 1 Year | Duration for storing proxy logs for compliance and forensics |

## Hardware Provisioning

SafeSquid SWG is SMP-aware and scales efficiently across CPU cores. Provisioning must account for SSL/TLS inspection (CPU-intensive), logging (I/O intensive), and traffic bursts (network throughput).

Deploy resources on separate physical hosts or hypervisors for resilience. SafeSquid Deployment on virtual infrastructure is recommended for simplified scaling and faster disaster recovery.

**Design Considerations**

* CPU: Intel x86 with AES-NI for accelerated SSL inspection
* Storage: NVMe SSD preferred for high-speed log writes.
* Networking:   
  NIC bonding recommended (LACP Mode 4; fallback Active-Backup Mode 1).   
  Dedicated interfaces for LAN and WAN improve traffic isolation and troubleshooting.  
  Multi-queue NICs on Virtualised instances will substantially amplify performance
* Scalability: Clustering enables horizontal scale-out and centralised log aggregation.

**Baselines**

* RAM: 10 MB / Concurrent Connection
* CPU: 1 Core / 50 Concurrent Connection (Can handle more depending on network performance)
* Dedicated NICs on base Hardware: 1 + 1 (LAN+WAN) / 1000 Concurrent Connections
* NIC bonding on Base Hardware will amplify performance
* 1+2+2 (Data Backup + LAN + WAN) vNICs for SafeSquid Virtual Appliance
* Dedicated range of 5 IP Addresses (WAN) per 500 Users per SafeSquid VM
* SafeSquid VM at 1 TB and Schedule Backup of Logs every day to centralised storage

### Pilot Provisioning

Suitable for proof-of-concept or small environments.

Architecture: Single SafeSquid instance deployed on physical or virtual hardware

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Resource | CPU | RAM | Storage | Interfaces |
| SafeSquid SWG | 8 cores @ 2.5 GHz | 16 GB | 1.5 TB | 2 vNICs, IPs |

### Minimal Production Provision

Recommended for production deployments where uptime is critical. Two SafeSquid servers in active-passive failover mode ensure high availability during upgrades and system management.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Resource | CPU | RAM | Storage | Interfaces |
| SafeSquid SWG / A | 8 cores @ 2.5 GHz | 16 GB | 1.5 TB | 2 vNICs, 4 IPs |
| SafeSquid SWG / B | 8 cores @ 2.5 GHz | 16 GB | 1.5 TB | 2 vNICs, 4 IPs |

### Recommended Production Provisioning

SafeSquid Proxy Cluster ensures Load-balanced throughput as well as high-availability service.  
A Load Balancer is needed for this.

To deploy a SafeSquid SWG Cluster, two SafeSquid servers are configured in active-active, with one load balancer distributing the load.  
Also, need to aggregate logs in one reporting and analytics server.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Resource | CPU | RAM | Storage | Interfaces |
| SafeSquid SWG / A | 8 cores @ 2.5 GHz | 16 GB | 200 GB | 2 vNICs, 4 IPs |
| SafeSquid SWG / B | 8 cores @ 2.5 GHz | 16 GB | 200 GB | 2 vNICs, 4 IPs |
| Load Balancer | 8 cores @ 2.5 GHz | 8 GB | 200 GB | 4 Dedicated NICs |
| Reporting & Analytics | 8 cores @ 2.5 GHz | 8 GB | 2 TB | 1 vNIC |

## Solution Topology

A diagram of a computer security

AI-generated content may be incorrect.

# Deployment Plan



The deployment of the SafeSquid Secure Web Gateway is structured into five strategic phases, ensuring a smooth, risk-mitigated rollout while minimising disruption to business operations. Each phase includes clearly defined objectives, activities, and deliverables to align with customer expectations and security goals.

## Planning & Assessment

Understand the current infrastructure, define the scope, and prepare a tailored deployment roadmap.

### Key Activities

* Conduct stakeholder meetings to gather business, security, and compliance requirements.
* Identify network topology, user groups, and existing security controls (e.g., proxy servers, firewalls, directory services).
* Define integration points: AD/LDAP, SIEM, DLP, AV, etc.
* Assess SSL inspection needs and traffic volumes.
* Prepare deployment architecture (single node, HA, cloud, hybrid).
* Define user acceptance test (UAT) criteria.

### Deliverables

* Network readiness checklist.
* Deployment design document (logical + physical).
* Project schedule with milestones.

## Infrastructure Preparation

Provision and prepare systems and network for SafeSquid installation.

### Key Activities

* Allocate servers or virtual instances (VMware, KVM, AWS, etc.).
* Configure DNS, firewall, and NAT rules to redirect web traffic to SWG.
* Setup internal/external storage for logs and reports.
* Provision secure communication channels (VPN, VLANs, tunnels).
* Validate network connectivity and performance prerequisites.

### Deliverables

* Hardened OS image (Linux) with SafeSquid prerequisites.
* IP plan and system baseline snapshot.
* Finalized hardware/VM allocation checklist.

## SafeSquid Installation & Configuration

Deploy SafeSquid SWG and configure core modules.

### Key Activities

* Install SafeSquid SWG using ISO/OVA/cloud image.
* Configure proxy mode (explicit, transparent, or PAC).
* Integrate with AD/LDAP/RADIUS/SAML for user authentication.
* Enable SSL decryption with root certificate rollout.
* Configure default security policies, DLP rules, AV/ICAP integration.
* Setup logging to local and SIEM systems.

### Deliverables

* Configured SafeSquid instance(s) with policy templates.
* Authentication test reports
* SSL cert deployment report

## User Acceptance Testing (UAT)

Validate the deployed solution in a controlled environment with real users

### Key Activities

* Conduct pilot tests for various departments (IT, HR, Finance, etc.).
* Simulate business scenarios (file uploads, web browsing, blocked URLs, malware test files).
* Validate alerting, logging, and reporting functionality.
* Capture end-user feedback and fine-tune access policies.

### Deliverables

* UAT report and sign-off from IT/security team
* List of recommended policy adjustments
* Issue resolution tracker

## Go-Live & Post-Deployment Support

Transition to full production and handover operations.

### Key Activities

* Activate SafeSquid across all defined users and branches.
* Monitor system performance, user complaints, and policy enforcement
* Train internal IT and helpdesk teams on SafeSquid management
* Handover documentation and administrative access

### Deliverables

* Go-Live confirmation with rollback plan (if required).
* Admin & troubleshooting guide.
* Final deployment and configuration documentation.

### Ongoing Support & Maintenance

* Patch management: Monthly updates or security hotfixes.
* Policy review workshops: Quarterly fine-tuning based on usage data.
* Health checks: Bi-annual performance and compliance audits.
* Support model: Email, ticketing, and phone-based technical assistance.

# Training & Capacity Building

SafeSquid will conduct comprehensive training sessions for all designated stakeholders and teams as part of the deployment scope. The Training and Capacity Building Plan is structured to ensure that IT teams and security personnel acquire the necessary skills to effectively operate, manage, and troubleshoot the SafeSquid SWG solution. The primary objective is to facilitate seamless adoption, efficient system administration, and long-term sustainability through a well-structured training approach.

Training will be delivered by the Service Provider or System Integrator, in collaboration with the Original Equipment Manufacturer (OEM) or its Certified Training Partner. The sessions will cover all key aspects of the solution, including core features, system architecture, configuration settings, security policies, and troubleshooting methodologies.

## Train-the-Trainer (TTT) Approach

The Train-the-Trainer (TTT) model will be employed for administrator training, ensuring that IT administrators and security teams gain in-depth knowledge and hands-on expertise in managing the SafeSquid SWG solution. These trained administrators will subsequently be responsible for training end-users within the organisation, enabling efficient knowledge transfer, operational continuity, and effective system utilisation.

## Key Training

|  |  |  |  |
| --- | --- | --- | --- |
| Phase | Training Focus | Target Audience | Mode of Delivery |
| Phase 1: Implementation & Operational Training | System setup, configuration, integrations, and initial troubleshooting. Role-based access control, policy enforcement, incident response, monitoring & reporting. | IT Administrators, Security Teams, IT Teams, Network Engineers | Instructor-led training (Onsite/Remote as per the tender scope) |
| Phase 2: End-User Training | Secure access usage, MFA setup, self-service troubleshooting. | Employees, Remote Users | Video Tutorials, User Guides |
| Phase 3: Post-Deployment Capacity Building | Advanced troubleshooting, log analysis, performance optimization. | Senior IT Staff | Product Documentation and Knowledge Base |

# Service Model

## Product Documentation

SafeSquid provides comprehensive product documentation and knowledge resources to support IT administrators, security teams, and end-users in effectively deploying, managing, and troubleshooting the SafeSquid SWG solution. These resources are accessible through dedicated online portals, ensuring continuous learning and support.

### Knowledge Base

For additional support and technical assistance, users can access the SafeSquid Knowledge Base at <https://docs.safesquid.com/>

The Knowledge Base Portal offers:

* Technical Support Articles – Solutions for frequently encountered issues.
* Best Practices & Use Cases – Recommended security configurations and deployment strategies.
* Ticketing System – Submit queries and get assistance from the support team.

### Project-Specific Documentation

After successful project completion, the following customised documents will be provided:

* Admin Training Document – Comprehensive guide for IT administrators.
* Test Plan & UAT Documents – Validation checklists for ensuring system functionality.
* Configuration Document – Detailed system settings and integration details.

## Technical Support

To ensure uninterrupted operations, timely issue resolution, and continuous optimisation of the SafeSquid Secure Web Gateway (SWG), a robust technical support framework is provided as part of the solution. The support model is designed to assist during deployment, post-implementation, and operational phases.

|  |  |  |
| --- | --- | --- |
| Support Tier | Impact Severity | Expected Resolution Time |
| L1 (Basic Helpdesk) | Less than 5% of users affected or Less than 5% of web applications affected | 4 hours |
| L2 (Technical Assistance) | 5 to 10% of users affected or  5 to 10% of web applications affected | 2 hours |
| L3 (Product Experts) | More than 10% of users affected or More than 10% of web applications affected | 1 hour |

### Support Channels

* Email: Dedicated support email for issue reporting and escalation.
* Ticketing System: Web-based portal for tracking and managing support tickets.
* Phone Support: Direct phone line for critical issues and real-time troubleshooting.

### Escalation Matrix

If the incident is deemed to be of high severity or poses a significant risk to the organisation, it will be escalated through the predefined escalation matrix. For any escalation, use the below escalation matrix.

|  |  |  |
| --- | --- | --- |
| Escalation Level | Email | Description |
| Level 1 | support.l1@safesquid.net | Initial escalation for unresolved or minor issues. |
| Level 2 | support.l2@safesquid.net | Secondary escalation for issues needing faster resolution. |
| Level 3 | support.l3@safesquid.net | Final escalation for critical issues requiring immediate attention. |

## Service Level Agreement

In accordance with the contract, SafeSquid Labs will establish a Service Level Agreement (SLA) that outlines clear response and resolution timelines for all types of tickets, including general support, security incidents, compliance issues and any other issues. This SLA is designed to ensure that all concerns are managed promptly and effectively. Should any issue exceed the specified resolution timeframe, our escalation matrix will be activated to ensure a swift and decisive resolution.

# Disclosure and Acceptance

This solution document is provided solely for informational purposes and is intended to assist in understanding the capabilities and features of our offering. By utilizing this document and our services, you acknowledge and accept our Privacy Policy, Responsible Disclosure Policy, Service End User Agreement, Mobile App Terms of Use, and any other policies all of which are incorporated by reference. The information contained herein is subject to change without notice and does not constitute a binding commitment, guarantee, or warranty of any kind regarding the performance, features, or functionality of the solution. SafeSquid reserves the right to modify, update, or discontinue any aspect of the solution at its discretion. Users are advised to exercise their own judgment and conduct independent evaluations before relying on the information presented in this document.