



Perimeter-level Layer 7 security for Comprehensive Web Security

BACKGROUND

Right since its very birth, WWW challenged enterprises with productivity losses. Internet based services for disseminating user generated content like social networks, file sharing, etc. offer new avenues for loss of confidential data and information.

Profitability of targeted advertising incentivizes Social Networking and e-Commerce giants to innovate privacy breaching technologies.

Multitude of web developers, inadvertently adopt free software components that disguise malware, making visitors vulnerable to financial and identity attacks.

Rising popularity of Internet based banking services motivates cyber-criminals to increase Phishing efforts.

SaaS based revenue models of sophisticated Ransomware and Botnet services on the dark-web, demand very basic skillsets to launch lucrative cyber-crime start-ups.

The race to excite users with innovative applications beget the “deliver first and fix later” culture, consistently betrays users to new zero-day vulnerabilities.

Heralding the information age, the WWW is the primary driver of enterprise knowledge quotient, and key to enhancing business efficiency.

WWW evolved quite explosively over the last few decades due to rapid adoption of innovative technologies. General users now enjoy easy to use web-based services, delivered by a very complex inter-connect of diverse technologies. Transparency of these technologies, particularly those implemented on the Layer 7 / HTTP, makes them also very difficult to comprehend for even an average IT technician, much less anticipate the underlying risks. Thus, Internet enablement though necessary, exposes business establishments to substantial risks.





Office Efficiencies (INDIA) Private Limited
Simplifying Technology!

MITIGATION

Security solutions for mitigating web-based threats are historically as old as the WWW itself. Effective solutions must deliver real-time threat mitigation and require adequate computing power and interaction with remote security validation services.

Use of *End Point Security* (EPS) solutions such as anti-malware pre-dates the *Internet Age*. Evolution of EPS solutions over last couple of decades improved defence against web-based threats. The host operating system, and the application initiating the web traffic limit the effectiveness of EPS. EPS shares a large slice of the computing power and network bandwidth provisioned for the end-point user's routine business functions, thus reducing the individual's efficiency. Difficulty quotient of implementing granular policies to facilitate the business needs of individual users or functional groups, rises exponentially as the number of subject endpoints increases. The latency in effecting the security strategies, prevents timely corrections and validation of the effectiveness.

Perimeter Security solutions like *Network Layer Firewalls* (NLF) and *Proxy Servers*, enable mitigation of threats before they impact an endpoint. NLF scrutinizes traffic Layer 3 and 4 traffic, to prevent connection of enterprise cyber-assets and endpoints to or from undesirable external entities. Proxy Servers are *Application Layer Firewalls* (ALF) that scrutinize Layer 7 traffic and mitigate exploits in the application protocol. An HTTP Proxy server prevents endpoints from establishing a direct network connection with external web services and inspects web-based traffic to eliminate undesirable exchange information.

Legacy strategy of mitigating web-based threats focussed on blocking access to certain websites, generically termed as URL Filtering. Early generations of perimeter solutions could thus deliver both - NLF and ALF requirements.

Evolution of the WWW introduced new capabilities such as user-generated content, multi-media experiences, and seamless inter-connect of Layer 7 services from multiple services. Threat mitigation thus requires real-time Deep Inspection of payload and new dimensions presented by continuously evolving HTTP protocols. Rapid adoption of SSL increases the data volume scrutinized by ALF, manifold. The challenge overwhelms the limited computing power of traditional firewalls both volumetrically and subjectively.

Enterprises with high security awareness employ solutions distinctively specialized for NLF and ALF technologies. As both technologies present different challenges, engaging technicians specializing with relevant skill sets ensures optimal use of both.



+91 22 3550 3063 +91 22 3521 0202

www.safesquid.com information@safesquid.net

A-304, Neelkanth Business Park, Vidyavihar West,
Mumbai 400086, Maharashtra, INDIA



Office Efficiencies (INDIA) Private Limited
Simplifying Technology!

THE SAFESQUID® APPROACH

Traditional ALF 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.

SafeSquid is a HTTP Proxy Server, specifically designed for Application Layer Security. The purpose-oriented architecture promises scalable performance while ensuring comprehensive mitigation of Layer 7 threats.

Pioneering solutions to mitigate web-based threats, yet unaddressed by alternatives, highlights SafeSquid's evolution since its maiden release in 2004. Collaboration with security specialists, administrators, and vendors world-wide sets the innovation goals.

Mitigation of Key Layer 7 Security Threats

Malware Defense

Stop malware threats at the perimeter, before they reach targeted endpoint.
Disable traction with Ransomware and Botnet command-and-control centers.

Data Leakage Prevention

Prevent undesirable egress of confidential data and sensitive information.
Intelligence to distinguish legitimate traffic from unwarranted activities.

Phishing Prevention

Prevent inadvertent traction with malicious websites.
Sandbox unsanctioned websites to prevent inadvertent user interaction.

XSS Protection

Prevent hijacking of authenticated web sessions.
Safeguard cloud-based assets and facilitate safe adoption of cloud technologies.

Cyber-Slacking

Role Based Granular Web Access to curb misuse of privileges.
Regulate use of Internet Applications.



+91 22 3550 3063 +91 22 3521 0202

www.safesquid.com information@safesquid.net

A-304, Neelkanth Business Park, Vidyavihar West,
Mumbai 400086, Maharashtra, INDIA



Office Efficiencies (INDIA) Private Limited

Simplifying Technology!

Context-Aware Perimeter Security

Web Framework Discovery and Proactive Threat Mitigation

Legacy URL Filtering based web security technologies lack the intelligence required to mitigate the rising sophistication in breaches

Limitations of traditional perimeter security forces security administrators to adopt Blacklisting web sites as the primary web security strategy.

The Blacklisting strategy essentially trusts any web service unless explicitly deemed harmful.

Zero-Hour attacks accomplish their missions before their publication in danger lists.

SafeSquid reserves a narrow defined secure path for accessing critical business application resources.

Maintains sterility of secure path, by preventing its use for non-critical objectives.

Provides an alternate path for non-critical web applications and traffic.

Prevents access to critical business application resources unless via defined secure path.

360° Application Layer Security

Realtime Protocol and Payload Threat Mitigation

Cross-Site Request Detection

Application Session Security

API-Based Web 2.0 Controls

Re-Programmable Application Identification

Real-Time Cloud-Based Threat Intelligence Feed

Categorized database of over 20 Million web-sites



+91 22 3550 3063 +91 22 3521 0202

www.safesquid.com information@safesquid.net

A-304, Neelkanth Business Park, Vidyavihar West,
Mumbai 400086, Maharashtra, INDIA



Office Efficiencies (INDIA) Private Limited
Simplifying Technology!

Contextual Intelligence Neural Network

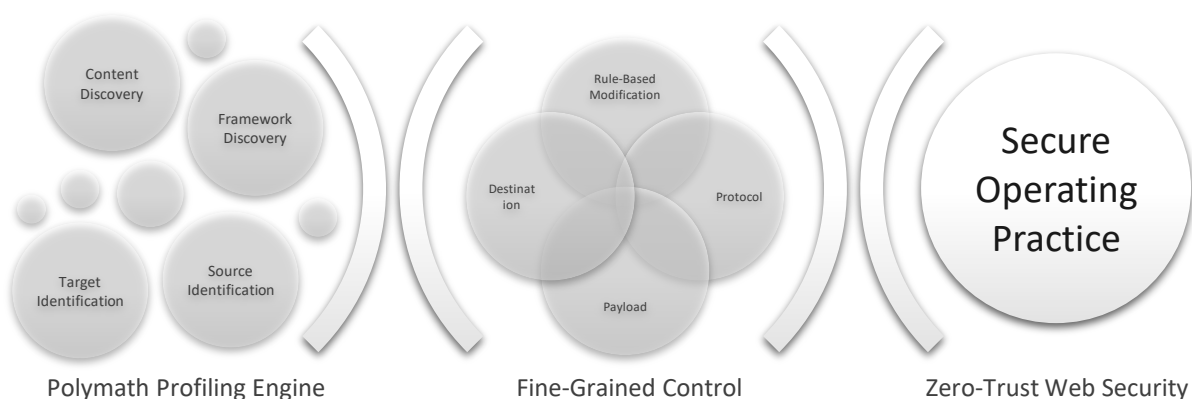
Zero-Trust Web Security Correlation Engine

Security engine unravels the protocol & payload data and does rule based reassembly before retransmission.

Profiling engine neurons collaboratively classify each element of protocol and payload data structure for contextual intelligence.

Dedicated Security Processors recalibrate the protocol and payload data in consonance with the secure operating practice.

The underlying contextual intelligence neural network provides granular sensitization to the features of every security processor.



Micro-define your Zero-Trust
Web Security strategy

Enforce Secure Operating
Practices at the perimeter-level

Immunize your enterprise against
Zero-Day threats



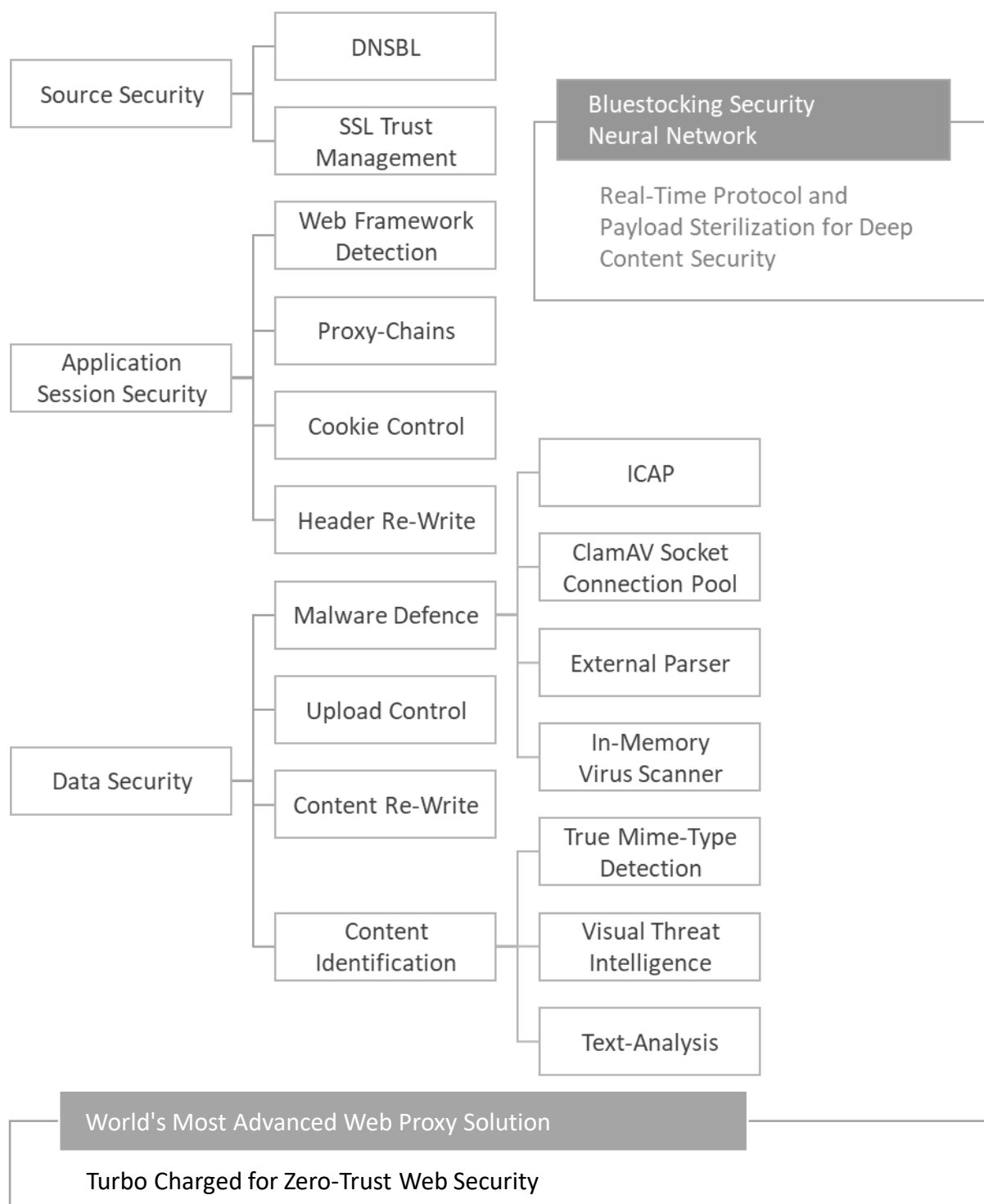
+91 22 3550 3063 +91 22 3521 0202

www.safesquid.com information@safesquid.net

A-304, Neelkanth Business Park, Vidyavihar West,
Mumbai 400086, Maharashtra, INDIA



Office Efficiencies (INDIA) Private Limited
Simplifying Technology!





Office Efficiencies (INDIA) Private Limited
Simplifying Technology!

The state-of-the-art design enables SafeSquid® to load content security technologies into shared memory directly accessible by the proxy service.

Integrated update manager seamlessly updates the signatures for content discovery, application identification, malware detection, etc. directly in proxy service application memory, eliminating any down-time or session loss.

Structured Data Pools enable SafeSquid to share intelligence in real-time across all active connections.

The robust MT architecture provides SafeSquid the intrinsic SMP-awareness, and powers it to natively scale-up on demand.

Cloud-backed backup and restore and of policies, for seamless data recovery.

Cloud-backed secured synchronization of SSL Certificates, Custom Categorization, etc. across cluster nodes.

SafeSquid® is a compact MT (multi-threaded) network application that provides a high-performance HTTP(S) Proxy Service.

Unique architecture for high performance parallel processing, instead of legacy inter-process communication used by traditional solutions

Shared Memory

Network Service	Contextual Intelligence	Policy Management	Signature Updates	Machine Learning
-----------------	-------------------------	-------------------	-------------------	------------------



+91 22 3550 3063 +91 22 3521 0202

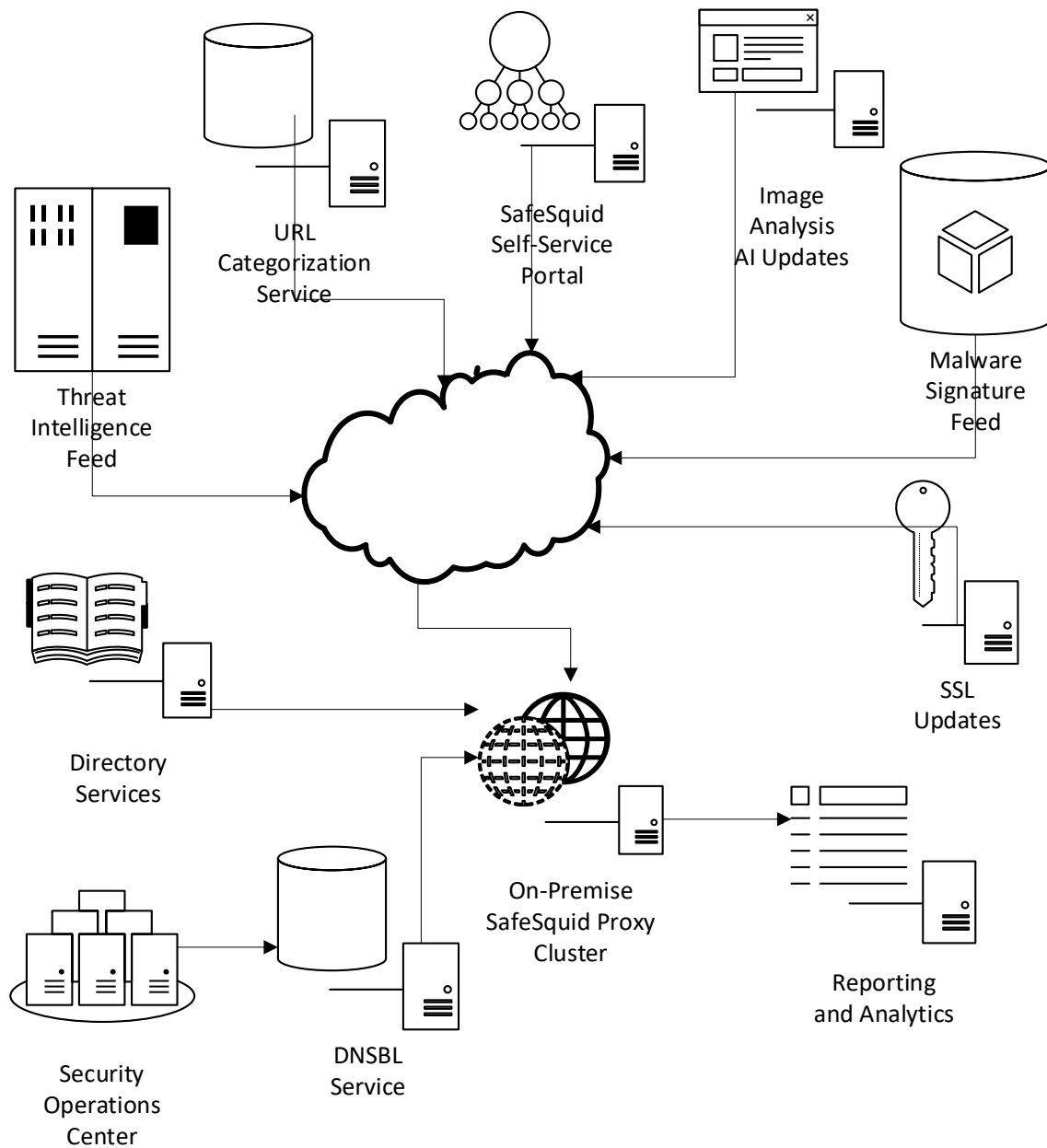
www.safesquid.com information@safesquid.net

A-304, Neelkanth Business Park, Vidyavihar West,
Mumbai 400086, Maharashtra, INDIA



Office Efficiencies (INDIA) Private Limited
Simplifying Technology!

HIGH-LEVEL SOLUTION ARCHITECTURE





Office Efficiencies (INDIA) Private Limited

Simplifying Technology!

Cluster Management

Effortlessly Scale Out

- Enterprise-Dedicated Product Activation Key
- Cluster-Wide Seamless Policy Replication
- Encrypted Passphrase Protection for Trusted Root CA
- Seamless Dispersal of Custom Categorization
- Cluster-Aware SSL Session Tickets
- Cluster-Aware Interception SSL Certificates
- Workflow Integrated Policy Backup
- Secure Policy Restore
- WCCP Aware

Extensive Logging

Easy Trouble-Shooting, Comprehensive Analytics

- Browser-Level Policy Validation
- Policy Application Logging
- Comprehensive Transaction Visualization
- Human Readable Text-based logging
- Time-Stamped Configuration Archiving
- Application Service Performance Counters
- Multi-Cast UDP Broadcast for Log Aggregation
- SIEM-Ready Logs
- Cross-Domain Web Traffic Logging
- UI Access Logs
- Privileged Access Logs
- Egressing Data Capture
- Configurable Reporting

Open Architecture

Bespoke Security Fabric

- 100% Software Based Solution
- Customize Access Security as per Enterprise Secure Operating Practice
- Self-Heal Technology
- Configurable NTP
- Secure DNS
- Extend Platform Capabilities



Extensible Security Fabric



High Application Availability



Intuitive Application Management

HIGH-LEVEL SOLUTION HIGHLIGHTS



+91 22 3550 3063 +91 22 3521 0202

www.safesquid.com information@safesquid.net

A-304, Neelkanth Business Park, Vidyavihar West,
Mumbai 400086, Maharashtra, INDIA



Office Efficiencies (INDIA) Private Limited
Simplifying Technology!

100% Software Based Solution	Hypervisor agnostic virtualization
	Transform bare metal x86_64 platform into Hardware Appliance
	Cloud hostable
Application Layer Firewall	Full compliance with RFC 2616 and inheritors
	User / End-Point Agnostic
	Transparently redirect primitive web applications
	VPN based web security client for off-premise users
Enforce Secure Operating Practices	Translate your requirements from a document into action.
	Logical security objectives
	Customizable ready-to-use policy templates.
	Re-Programmable Security Engine
Hybrid Management	Automatic replication of your policies across cluster nodes.
	Standard Linux Platform
	REST based cluster node micro-management
	Cloud Based Portal for cluster macro-management
	Automatic Policy Backup and Restore



Office Efficiencies (INDIA) Private Limited
Simplifying Technology!

HIGH-LEVEL PLATFORM HIGHLIGHTS

Use SafeSquid Appliance Builder to quickly setup your Secure Web Gateway	<ul style="list-style-type: none">•ISO installer for optimized Operating System setup•Cloud-Init for PaaS / Virtualization setup
Ubuntu 18.04 compatible X86_64 Server Platform	<ul style="list-style-type: none">•Dedicated Hardware•Virtual Machine•Cloud PaaS Instance
Minimal Hardware Requirement	<ul style="list-style-type: none">•8+CPU Cores•8GB+RAM•4+ NIC•50GB+Disk Storage

SafeSquid Appliance Builder (SAB) the ISO installer packaging for distribution enables you to easily transform a standard Intel Server platform into a web proxy hardware appliance, matching your needs. SAB also enables easy creation of virtual proxy appliances on any virtualization infrastructure. A cloud-init script is also available, should you prefer to use any of the public cloud PaaS or your own private cloud infrastructure.



+91 22 3550 3063 +91 22 3521 0202

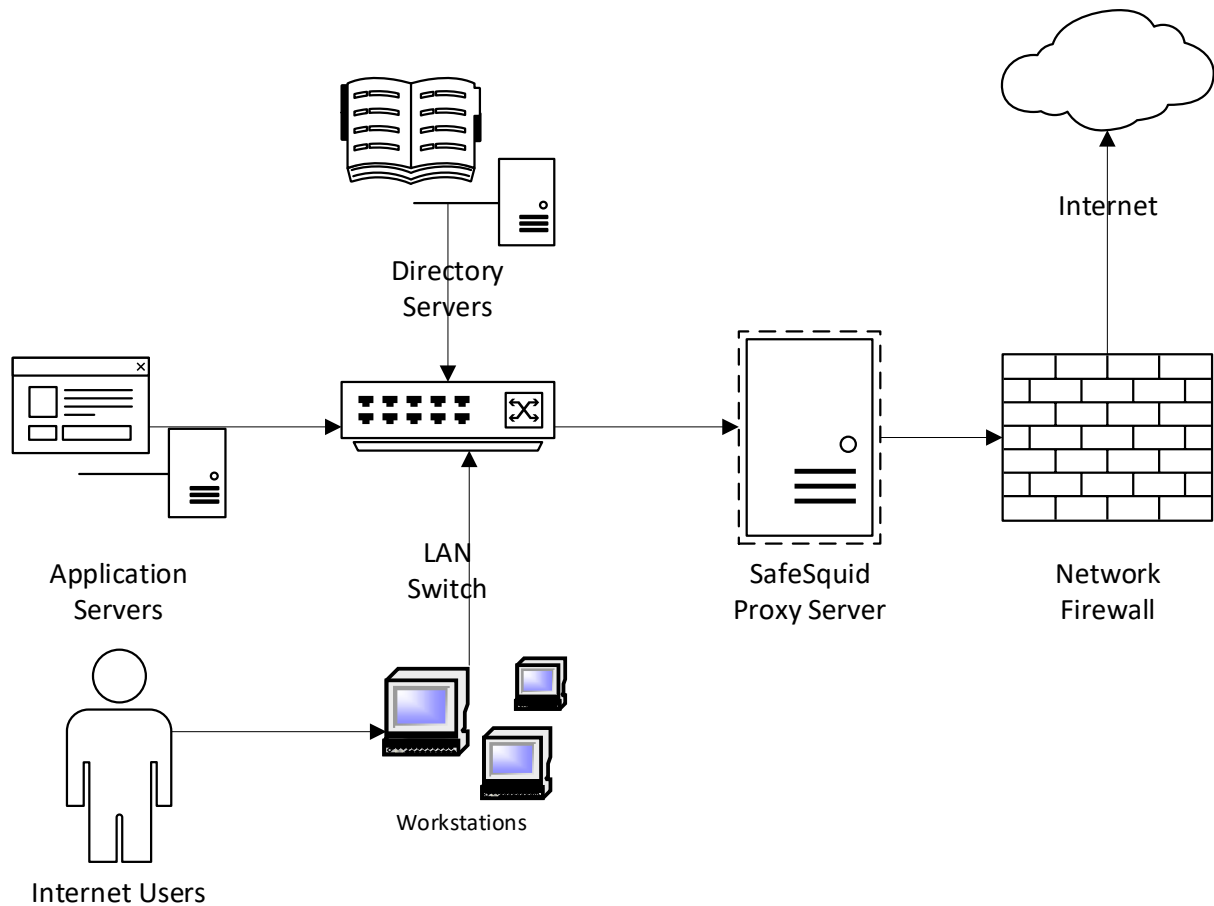
www.safesquid.com information@safesquid.net

A-304, Neelkanth Business Park, Vidyavihar West,
Mumbai 400086, Maharashtra, INDIA



Office Efficiencies (INDIA) Private Limited
Simplifying Technology!

STANDARD NETWORK ARCHITECTURE





Office Efficiencies (INDIA) Private Limited
Simplifying Technology!

Unique Feature implementation

Each feature designed to enable maximum granularity and compliance of security needs

✓ Application Control	✓ Categorized Web-Site DB	✓ DLP
✓ Cluster-Ready	✓ Content Caching	✓ ICAP Ready
✓ Content Pre- Fetching	✓ Cookie Control	✓ SMP-Aware
✓ Time Profiles	✓ Customizable URL DB	✓ Content Control
✓ DNSBL Filter	✓ External Parsers	✓ Text Analyzer
✓ HTTPS Inspection	✓ On-the-Wire Anti-Malware	✓ DNS Caching
✓ LDAP-Aware	✓ Custom Templates	✓ Header Control
✓ Open Format Logs	✓ Orchestration Metrics	✓ PAM-Aware
✓ Kerberos Aware	✓ Pornographic Image Detection	✓ IPv6-Ready
✓ Response Profiling	✓ Basic / SSO Authentication	✓ REST WebUI
✓ User Limits	✓ Real-Time Content Modification	✓ WCCP V1/V2
✓ PCRE-Aware	✓ Content Security Policy Level 3 Compliant	✓ User Consented Web Access
✓ Appliance ISO	✓ YouTube Video Category Control	✓ SNI Aware
✓ VPN Integration	🕒 Customization Library	🕒 Visual Threat Intelligence



TECHNICAL SPECIFICATIONS

1 ACCESS CONTROLS

Profiled Internet Access for granular enforcement of Internet Usage Policies.

1.1 USER IDENTITY MANAGEMENT

Dynamic User and Group Identity Management System with configurable identification options

1.1.1 Network Identifier-Based Access Control

Device-specific network signatures for authentication.

1.1.1.1 Static IP address mapping

Allows manual association of static IP addresses with user profiles.

1.1.1.2 Isolated configuration portal

Dedicated network service for policy configuration

1.1.1.3 Application-Specific Network Segregation

Dedicated network channels for mission-critical applications

1.1.2 Credential Verification System

Access control based on validated user credentials.

1.1.2.1 Comprehensive Credential Integration

Compatible with diverse credential storage mechanisms

1.1.2.1.1 Local Credential Database

Secure XML-based storage system for usernames and passwords

1.1.2.1.2 Pluggable Authentication Modules (PAM) Aware

Configurable support for Linux-PAM authentication modules

1.1.2.1.3 Directory Services Integration

Customizable options for connecting with enterprise-grade directory services like Microsoft® Windows Active Directory and OpenLDAP.



Office Efficiencies (INDIA) Private Limited
Simplifying Technology!

1.1.2.1.3.1 *Directory Service Aggregation*

Uniform user management across varied network environments

1.1.2.1.3.1.1 *Multi-Directory Service Integration*

Enables concurrent connection with multiple LDAP-based directory services

1.1.2.1.3.1.2 *Intelligent Directory Resolution*

Automated user-directory identification based on entered credentials

1.1.2.1.3.2 *Dynamic Group Membership Sync*

Real-time extraction and synchronization of group information from connected directory services

1.1.2.1.3.3 *Directory Info Caching*

Efficient caching mechanism for quick retrieval of user group membership data

1.1.2.1.3.4 *LDAP Connection Resiliency*

Automated failover capabilities for uninterrupted connectivity with LDAP services

1.1.2.2 *Versatile Authentication Systems*

1.1.2.2.1 *Interactive Login Prompt*

HTTP RFC-compliant Basic Authentication for secure user verification

1.1.2.2.1.1 *Transient Session Handling*

Secure, disk-less in-memory management of user sessions

1.1.2.2.1.2 *Credential Lifecycle Management*

Automated process for invalidating and purging outdated user credentials.

1.1.2.2.2 *Single Sign On (SSO) Implementation*

Kerberos-based authentication for seamless domain network access

1.1.3 *Multi Factor Authentication*

Combining IP-based and credential-based authentication for heightened security

1.1.4 *Secured Policy Management Interface*

Restricted access to configuration portal, reserved for administrators

1.1.5 *Elevated Access Rights Management*

Configurable privileged user access for restricted web resources





Office Efficiencies (INDIA) Private Limited
Simplifying Technology!

1.2 APPLICATION SIGNATURE-BASED IDENTIFICATION

Utilizes a comprehensive database of application signatures for precise identification of Internet applications.

1.2.1 Dynamic Application Signature Sync

Cloud-integrated, real-time updates to the application signature database, encompassing over thousand applications for timely and accurate identification.

1.2.2 Customizable Application Signature Framework

Enables security administrators to define and integrate bespoke application identification logic, enhancing adaptability to unique enterprise needs.

1.3 DYNAMIC WEBSITE CLASSIFICATION

Utilizes advanced algorithms to categorize websites in real-time, based on content type, functionality, target audience, and thematic focus.

1.3.1 Continuous Web Categorization Updates

Cloud-integrated, real-time updates to the web categorization database, supporting accurate classification of more than a million websites to over 100 categories

1.3.2 Custom Web Categorisation

Empowers security administrators with the ability to manually classify websites into predefined or newly created custom categories via configuration portal or via APIs

1.3.3 Flexible Website Recategorization Capabilities

Enables security administrators to modify or replace the default categorization of websites, ensuring alignment with specific security policies or content standards

1.3.4 Metadata keyword filtering

Utilizes PCRE (Perl Compatible Regular Expressions) logic for pinpoint detection of inappropriate content in payloads and protocol headers

1.3.5 Heuristic Web Analysis

Employs heuristic techniques to categorize websites based on URL analysis, content scrutiny, and web traffic behavioural patterns.

1.3.6 Domain Name Variance Detection

Sophisticated system for identifying domains that share identical names but are registered under different top-level domains (TLDs), crucial for mitigating spoofing and phishing risks.





Office Efficiencies (INDIA) Private Limited
Simplifying Technology!

1.3.7 Advanced Cross-Site Traffic Analysis

Advanced algorithms to differentiate between direct user-initiated web navigation and automated background cross-site interactions.

1.4 DEEP PAYLOAD CONTENT ANALYSIS

Performs an in-depth examination of response payload content, assessing various aspects for security and compliance

1.4.1 Universal Content Scanning Capability

Equipped to analyse a wide array of data formats, including compressed (zipped), encrypted, corrupted files, and multipart media types, ensuring thorough security coverage

1.4.2 Advanced Content Type Analytical Processing

Specialized analysis of content types to detect and manage various data formats accurately

1.4.2.1 Accurate MIME Type Identification

Utilizes advanced techniques to identify true MIME types for more than hundred file types and three thousand data identifier combinations, effectively thwarting file extension spoofing and preventing unauthorized data transfer

1.4.2.2 Dynamic Content Signature Update System

Maintains an up-to-date content signature database through real-time feeds, ensuring current and accurate tracking of MIME types for enhanced security.

1.5 ADVANCED PROFILING ENGINE

A sophisticated system designed to create detailed profiles based on various web traffic parameters for enhanced security policy application.

1.5.1 Request Fingerprinting with PCRE

Utilizes Perl Compatible Regular Expressions (PCRE) for intricate request profiling, facilitating the application of precise security policies based on unique request characteristics.

1.5.2 Time-Based Policy Implementation

Offers customizable scheduling options for the application of security policies, allowing temporal control over web traffic management

1.5.3 Response Profiling with PCRE

Enables web response profiling using Perl Compatible Regular Expressions on HTTP response headers.





1.6 ADVANCED TRAFFIC FLOW MANAGEMENT

Facilitates diverse actions for traffic manipulation, catering to specific security and operational needs.

1.6.1 Fundamental Traffic Access Control

Employs binary decision-making to either permit or block network traffic based on predefined rules and criteria.

1.6.2 Selective Cookie Exchange Management

Implements restrictions on cookie transmission between end-users and web entities, enhancing privacy and security.

1.6.3 Header Obfuscation

Enables manipulation of HTTP headers in both requests and responses

1.6.4 Payload Content Rewrite

Provides customizable options to modify the payload content, including the removal or modification of elements like ActiveX, JavaScript from web pages for enhanced security.

1.6.5 Selective Web Application Feature Access

Implements a nuanced access control to specific functionalities of web applications, allowing granular management without fully blocking website access

1.6.6 URL Redirection Management

Capable of handling and controlling URL redirections, encompassing both HTTP 302 response-based and transparent redirection mechanisms

1.6.7 Cache Control

User configurable settings over caching rules, and customisable bypass for specific URLs

1.7 ADVANCED PERIMETER SECURITY POLICIES

Establishes detailed web usage policies at the network perimeter for robust cybersecurity.

1.7.1 Web Filtering

Implements stringent controls to regulate user access to internet content.

1.7.1.1 Targeted IP Address Blocking

Employs IP blacklisting to restrict access to specific IP addresses deemed harmful or irrelevant.

1.7.1.2 Categorized URL Access Control

Filters and blocks URLs belonging to specific categories.





Office Efficiencies (INDIA) Private Limited
Simplifying Technology!

1.7.1.3 *Selective Keyword Filtering*

Screens and blocks web pages containing designated keywords or phrases, preventing exposure to inappropriate or harmful content.

1.7.1.4 *Dynamic Content-Based Filtering*

Analyses and blocks web pages based on their actual content, offering a layered defence against unsuitable online material

1.7.1.5 *Filtering Exemption*

Enables configuration of bypass rules for certain IP addresses or URLs

1.7.2 *Content Filtering*

Advanced Content Filtering Mechanisms: implements sophisticated content filtering strategies to control and monitor data transfers based on various criteria

1.7.2.1 *Data Type-Specific Filtering*

Enforces rules that allow upload and download of only designated data types.

1.7.2.2 *Targeted Website Filtering*

Restricts data upload and download activities to and from only authorized websites.

1.7.2.3 *Role-Based Data Transfer Control*

Implements user privilege-based restrictions on data upload and download activities

1.7.3 *Internet Access Control for Applications*

Regulates which applications can access the internet, limiting the potential for exposure to cyber threats.

1.7.4 *Protocol Filtering*

Filters and controls data transmission based on the communication protocols in use.

1.7.5 *Role-based Web Access*

Configures website accessibility based on user roles and identities.

1.7.6 *Temporal Internet Access Control*

Implements time regulation for internet access





Office Efficiencies (INDIA) Private Limited
Simplifying Technology!

1.7.6.1 *Time-Based Website Access Limitation*

Configures access to specific websites based on the time of day

1.7.6.2 *Scheduled Application Usage Enforcement*

Implements time-based restrictions for the use of various internet applications

1.7.7 *Duration-Based Internet Access Control*

Permit only a predefined amount of time for surfing a site

1.7.8 *Granular Web Application Feature Control*

Limits access to specific functionalities within web-based applications, enabling precise and secure management of online activities

1.7.9 *Managed Data Transfer Capacity*

Sets boundaries on the size and volume of data transfers

1.7.9.1 *File Transfer Size Regulation*

Imposes maximum size limits on file uploads and downloads, including overall volume quota management

1.7.9.2 *Non-Critical Traffic Bandwidth Management*

Allocates Quality of Service (QoS) and concurrency limits for trivial or non-essential web traffic

1.7.10 *Multifactorial Web Access Control*

Offers customizable control over internet access depending on the user identity, website requests, client application, and data transfer nature and size

1.7.11 *Advanced Web 2.0 Application Governance*

Implements sophisticated controls over the use of modern web applications.

1.7.11.1 *Mandatory SafeSearch Enforcement*

Compulsorily activates SafeSearch filters on all major search engines.

1.7.11.2 *Secure Web Login Authorisation*

Manages authentication protocols for website sign-ins

1.7.11.2.1 *Role-Specific Website Login Restrictions*

Permit role-based login to only specified websites.



+91 22 3550 3063 +91 22 3521 0202

www.safesquid.com information@safesquid.net

A-304, Neelkanth Business Park, Vidyavihar West,
Mumbai 400086, Maharashtra, INDIA



Office Efficiencies (INDIA) Private Limited
Simplifying Technology!

1.7.11.2.2 Personal Account Login Restriction

Restricts logins through personal email accounts while permitting corporate email account access.

1.7.11.3 Social Media Access Management

Comprehensive controls over social networking site usage

1.7.11.3.1 Read-Only Access to Social Media

Permits viewing of social media content without interactive capabilities

1.7.11.3.2 Selective Social Media Accessibility

Grants access to certain social media platforms while restricting others.

1.7.11.3.3 Restrictive User Engagement Policy

Implements limitations to user Interaction such as logging in, posting, and uploading on social media platforms.

1.7.11.3.4 Time-Restricted Social Media Access

Enables the use of social networking sites during designated periods, like lunch hours

1.7.11.4 Instant Messaging (IM) Traffic Regulation

Manages the use of IM services

1.7.11.4.1 Chat and File Exchange Oversight

Controls the use of Web 2.0 applications for chatting and file transfers

1.7.11.4.2 Embedded URL Reputation

Scrutinizes URLs shared in chat sessions for category and reputation

1.7.11.5 YouTube Content Category Filtering

Applies specialized filtering mechanisms to YouTube content, categorizing and managing videos for safe and relevant viewing

1.7.12 Proactive Proxy Anonymizer Blockade

Enforces a strict ban on accessing web categories and applications associated with proxy anonymizers

1.7.13 Sandboxing Suspicious Sites

Utilize an isolated environment to safely examine and assess the behaviour of potentially harmful websites.





2 THREAT MITIGATION

2.1 REAL-TIME CONTENT SECURITY

Actively prevents the transfer of malware and unsuitable content in both uploads and downloads.

2.1.1 Full-Spectrum Malware Traffic Analysis

Continuously scans and evaluates both inbound and outbound web traffic to detect and mitigate malware threats, including viruses, rootkits, Trojans, worms, system monitors, Key loggers

2.1.1.1 Integrated SqScan Malware Detection

Features a built-in scanner specifically designed to identify and neutralize various forms of malicious software

2.1.1.1.1 Diskless In-Memory Malware Scanning

Processes data in memory, eliminating the need for temporary disk storage during malware analysis

2.1.1.1.2 Heuristic Payload Analysis

Employs advanced heuristic techniques to evaluate and sanitize payloads

2.1.1.1.3 All-Encompassing File Inspection

Capable of examining malware hidden within various file types, including those that are compressed or encrypted

2.1.1.2 Meta-Scan Integration

Offers configurable options for incorporating external, third-party malware detection systems for enhanced security.

2.1.1.2.1 Generic ICAP Threat Detection Interface

Facilitates connectivity with ICAP-based threat detection services for broader security coverage

2.1.1.2.1.1 Multi-Engine ICAP Integration

Supports simultaneous connection with various ICAP services

2.1.1.2.1.2 Intelligent Threat Quarantine Mechanism

Automatically isolates content flagged by ICAP services, segregating benign from malignant data

2.1.1.2.2 ClamAV Malware Scanning Integration

Seamlessly integrates with the ClamAV engine for comprehensive virus and malware detection.



Office Efficiencies (INDIA) Private Limited
Simplifying Technology!

2.1.1.2.2.1 Customizable Virus Signature Configuration

Allows security administrators to deploy bespoke virus signatures, tailoring malware defence strategies

2.1.1.2.3 Adaptable External Parser Integration

Offers configurable options for integration with a variety of third-party security applications.

2.1.1.3 Dynamic Virus Signature Updating

Continuously refreshes virus signature database in real-time, bolstering defences against Zero-Day threats

2.1.1.4 Customizable Malware Detection Bypass

Allows specific configuration of bypass rules for malware detection, tailored to certain websites and HTTP protocol parameters.

2.1.2 Advanced Detection of Potentially Unwanted Programs

Identifies and mitigates PUPs that may perform unwanted or harmful operations.

2.1.3 Real-Time Content Filtering

Actively scrutinizes multimedia content to prevent the exposure to unsuitable materials such as pornography or violence from various sources.

2.1.3.1 Comprehensive Multimodal Content Inspection

Thoroughly examines both textual and visual content for a well-rounded content security approach

2.1.3.2 Text Analysis

2.1.3.2.1 Extensive Multilingual Analysis Capability

Equipped to analyse web content in a wide range of languages, catering to diverse linguistic needs

2.1.3.2.2 PCRE-Based Keyword Analysis

Utilizes Perl Compatible Regular Expressions for sophisticated keyword detection in content filtering

2.1.3.3 Flexible Detection Logic Customization

Allows users to adapt and modify the content detection logic to suit specific security requirements

2.1.3.4 Configurable Detection Sensitivity

Offers user-adjustable settings to fine-tune the sensitivity of the content detection system.





Office Efficiencies (INDIA) Private Limited

Simplifying Technology!

2.1.3.5 False Positive Mitigation Strategies

Provides configurable options to tweak policy logic, reducing the occurrence of incorrect flagging.

2.1.3.6 Dynamic Image Filter AI Updating

Ensures real-time refreshes of image filtering AI systems for up-to-date and effective visual content analysis

2.2 ROBUST SOURCE SECURITY MEASURES

Actively prevents user access to potentially harmful or dangerous website sources.

2.2.1 DNS Blacklist (DNSBL) Integration

Allows users to incorporate any third-party DNSBL service, supplementing the built-in categorized website database

2.2.2 Enhanced SSL Certificate Security

Blocks access to HTTPS sites with illegitimate SSL certificates, ensuring secure and trusted connections

2.2.2.1 Selective HTTPS Inspection Bypass

Configurable policy relaxations of HTTPS inspection based on user identity, application, and website classification

2.2.2.2 Realtime SSL Certificate Validation

Continuously verifies the authenticity of SSL certificates from remote web servers.

2.2.2.3 Trusted Root CA Customization

Enables users to modify the list of Trusted Root Certificate Authorities, tailoring trust anchors according to organizational needs.

2.2.2.4 Intranet SSL Validation Stringency Adjustment

Allows for the customization of SSL certificate validation stringency levels for trusted internal websites

2.2.2.5 Secure Sub-CA Utilization

Facilitates the use of passphrase-protected sub-Certificate Authorities created by the Trusted Enterprise Certificate Authority





Office Efficiencies (INDIA) Private Limited

Simplifying Technology!

2.2.2.6 Automatic Certificate Chain Repair

Proactively retrieves missing issuer certificates through Authority Information Access (AIA) Fetching, fixing broken certificate chains

2.2.2.7 Continuous SSL Security Updates

Provides real-time refreshes to the list of Trusted Root Certificate Authorities, maintaining up-to-date SSL security

2.2.2.8 External SSL Traffic Management Synergy

Offers the option to delegate SSL/encrypted traffic management to specialized third-party solutions for optimized handling

2.2.3 Advanced URL Redirection Management

Sophisticated system for directing users to alternative web pages or sites, based on predefined rules and conditions.

2.2.3.1 Selective Website Version Directing

Configurable option to automatically redirect users to preferred or region-specific versions of websites

2.2.3.2 Customizable Redirection Mechanisms

Facility to configure redirection methods, encompassing both HTTP 302 responses and seamless, transparent redirections.

2.3 ENHANCED USER PRIVACY PROTECTION

Configurable settings designed to safeguard user privacy

2.3.1 Proxy Chain Implementation

User-configurable option to route all internet traffic through specified remote proxy services for added anonymity and security.

2.3.2 Dynamic Cookie Exchange Management

Configurable restrictions on cookie transmission between users and websites, adjustable based on time and the client application used.

2.3.3 HTTP Header Customization

Allows users to reprogram and alter HTTP headers for outbound requests and responses.





2.4 DATA EGRESS MANAGEMENT

Offers user-configurable controls to regulate the transmission of data uploaded to external websites, ensuring data security and compliance.

2.4.1 Advanced Data Leakage Prevention

User-configurable options to restrict the nature of the content that may be uploaded to any website, for each user, using specific Internet Browsers.

Regex based keyword detection in uploaded content to prevent egress of sensitive information

The configuration should allow scoping to be done on a per-user, and on user-group basis.

2.4.2 Elevated Privacy

User-configurable option to limit the tracking data (like HTTP-Referrer, Cookies, User-Agent) received by remote websites, bolstering user privacy.

2.4.3 Inappropriate Content Upload Prevention

Detects and blocks the upload of objectionable content, such as pornographic material, to maintain a safe and professional online environment.

2.5 BROWSER SECURITY

Share intelligence with web browsers for securely accessing web applications.

2.5.1 Native Browser Isolation

CSP Injection to securely sandbox web applications

2.5.2 Remote Browser Isolation Integration

Integration with Remote Browser Isolation Solutions and Content Reconstruction solutions.

3 THROUGHPUT ACCELERATION

Enhances data processing and transmission efficiency through various optimization techniques

3.1 COMPREHENSIVE HTTPS TRAFFIC ANALYSIS

In-depth inspection of HTTPS traffic for security and compliance purposes

3.1.1 On the Wire TLS/SSL Encryption / Decryption

Performs all encryption and decryption processes within the application's memory space, negating the need for external services.

3.2 DIVERSE CACHING STRATEGIES

Utilizes various caching methods to enhance overall web performance and speed





Office Efficiencies (INDIA) Private Limited
Simplifying Technology!

3.2.1 TCP Connection Reuse

Leverages existing network connections with remote services to minimize TCP connection latency.

3.2.2 Smart In-Memory DNS Cache Manager

Manages DNS resolutions within memory to expedite DNS lookup processes.

3.2.3 Server-Side SSL Session Optimization

Intelligently caches SSL sessions to reduce latency and implements workarounds for servers lacking SSL session caching support

3.2.4 Client-side SSL session caching

Enables caching of SSL sessions when requested by client applications to enhance secure communication efficiency.

3.2.5 Adaptive Web Object caching

Offers configurable caching of web content from remote servers, utilizing both disk and in-memory storage solutions

3.2.6 Proactive Content Pre-fetching

Analyses and pre-emptively downloads additional components from web pages for quicker browser rendering

3.3 VERSATILE DATA COMPRESSION SUPPORT

Accommodates multiple compression algorithms and facilitates inspection of compressed files

3.3.1 Intelligent Decompression Delivery

Dynamically decompresses data for client applications that do not support compressed data exchange

3.3.2 Selective Streaming Buffering Bypass

User-configurable option to circumvent buffering for direct streaming responses from web servers

3.3.3 Payload-Specific Encoding

Configurable encoding settings based on payload MIME types to optimize data transmission efficiency

3.4 QoS MANAGEMENT

Implements Quality of Service throttling configurable per application or website to manage network saturation





Office Efficiencies (INDIA) Private Limited
Simplifying Technology!

3.5 OPTIMIZED TCP CONNECTION POOLING

Enhances TCP performance through intelligent data packet sizing and multiplexing of connections to remote servers for multiple clients

3.6 SMP-AWARE

Optimized for symmetric and shared-memory multiprocessing, allowing scalable performance improvements with additional hardware resources.

3.7 MULTI-QUEUE NIC UTILIZATION

Leverages Multi-Queue NIC capabilities for enhanced Receive Side Scaling and Packet Steering efficiency

3.8 INTERNALIZED DNS RESOLUTION SYSTEM

Utilizes Root DNS servers and internal network DNS services, offering significantly faster resolution compared to standard ISP-provided DNS.

4 SOLUTION MANAGEMENT & SCALING

Scalable, and open-architecture engineered for adaptability, it supports non-proprietary hardware for traffic expansion and integrates with various network load-balancing solutions

4.1 FULLY SOFTWARE-BASED SOLUTION

Compatible with standard hardware, manageable by technicians with general Linux skills, without specialized proprietary certifications

4.2 PLATFORM-AGNOSTIC DEPLOYMENT

Open-architecture software appliance installable on any standard Linux OS, suitable for diverse deployment scenarios

4.2.1 Virtual Appliance Compatibility

Operable as a virtual guest on varied virtualization platforms

4.2.2 Hardware Appliance Flexibility

Installable on standard Intel architecture server-class hardware without requiring proprietary systems.

4.2.3 Cloud-Ready Configuration

Easy provision in private cloud settings, aligning with evolving IT infrastructures.





Office Efficiencies (INDIA) Private Limited
Simplifying Technology!

4.3 HARDENED OPERATING SYSTEM

Utilizes a Security-Enhanced version of Ubuntu OS, ensuring only essential and vetted applications are installed.

4.4 WEB CONFIGURATION PORTAL

REST WebUI to manage Internet usage policies and modify SafeSquid configuration

4.5 STATE FULL POLICY INSPECTION TECHNOLOGY

Analyses the state of active connections to make informed decisions on network packet management.

4.6 COMPLIANCE WITH INDUSTRY STANDARDS AND INTEROPERABILITY

Ensures adherence to established protocols and supports diverse communication methods.

4.6.1 Compliant with RFC 2616 and its descendants

Adheres to established norms for proxy-aware hosts and applications as outlined in RFC 2616 and subsequent updates.

4.6.2 Compliant with TLS

Facilitates secure communication by supporting TLS versions 1.0 through 1.3

4.6.3 WebSocket Protocol Support

Enables interactive communication sessions between web browsers and servers for real-time data exchange.

4.6.4 HTTP/HTTPS Support

Supports inspection and regulation of HTTP and non-HTTP traffic within SSL/TLS connections, including transparent and proxy-unaware connections

Configurable adjustment of Encryption algorithms and Cipher Suites

4.6.5 FTP Support

Facilitates Active/Passive FTP over HTTP/HTTPS

4.6.6 CONNECT Method Proxy Functionality

Provides tunnelling for applications using the CONNECT method to a proxy service

4.6.7 Configurable Multi-Listen Capabilities

Enables setting up HTTP Proxy services on various sockets for use of specific application.

4.6.8 IPv6 Compatibility

Supports IPv6 clients and intelligently manages transitions between IPv6 and IPv4 networks



+91 22 3550 3063 +91 22 3521 0202

www.safesquid.com information@safesquid.net

A-304, Neelkanth Business Park, Vidyavihar West,
Mumbai 400086, Maharashtra, INDIA



Office Efficiencies (INDIA) Private Limited

Simplifying Technology!

4.6.9 SNMP Protocol Support

Compatible with SNMP versions V1, V2, and V3

4.6.9.1 SNMP trap alert Exchange

Utilizes SNMP trap alerts to communicate network events and anomalies for proactive management

4.6.9.2 Enterprise-Grade MIBS Management

Offers fully manageable and comprehensive Management Information Bases (MIBs)

4.6.10 Universal Browser Compatibility

Ensures seamless access to websites across all major browsers like MS IE, Mozilla Firefox, Chrome, Safari, etc

4.7 ENHANCED REMOTE CONNECTION CAPABILITIES

Offers diverse options for secure and efficient remote access.

4.7.1 VPN Service Integration

Facilitates secure and authenticated user identification through VPN integration

4.7.2 Optimized Remote Access Security

Enhances user mobility and security in remote access scenarios, integrating with various network controls

4.7.3 Strategic Traffic Ingress Management

Implements stringent controls on traffic ingress via Software Defined Networks, VPNs, or firewalls

4.8 VERSATILE PROXY OPERATIONAL CONFIGURATION OPTIONS

Offers a range of settings for proxy operations, catering to diverse network requirements

4.8.1 Forward Proxy

Enables establishment of a proxy configuration where client applications are explicitly set to use a specified proxy server

4.8.2 Reverse Proxy

Can be used as a reverse proxy to route traffic to destined web services.

4.8.3 Proxy-Chain

Offers user-configurable options to route all traffic through chosen remote proxy services

4.8.4 TCP Proxy

Provides various configurable options for managing TCP traffic through the proxy





Office Efficiencies (INDIA) Private Limited

Simplifying Technology!

4.8.4.1 Destination IP:PORT Configuration

Configurable options to define specific destination IP and PORT

4.8.4.2 TCP Traffic Control

Configures restrictions based on the client's IP, and the intended destination IP:PORT

4.8.4.3 T-Mode Proxy Configuration

Offers support for Direct Response Routing with T Mode Proxy

4.8.5 Adaptive Transparent Proxy Configuration

Facilitates traffic management from applications lacking explicit proxy support, including handling of HTTPS traffic

4.8.5.1 Transparent Traffic Redirection

Supports seamless redirection of traffic originating from proxy-unaware applications

4.8.5.2 SSL SNI Awareness in Transparent Proxying

SSL-SNI aware for transparently proxying HTTPS traffic.

4.9 ESTABLISHED PERFORMANCE BENCHMARKS

4.9.1 Concurrent User and Concurrent Connection Capacity

CPU (cores)	RAM (GB)	HDD	Max Concurrent Connections	Approx. Users
4	8	500GB	100	25
4	16	1TB	500	150
8	16	2TB	1000	350
8	32	4TB	1500	600
16	32	4TB	2000	1000
16	64	8TB	2500	1500

4.9.2 High Throughput Capabilities

Supports more than 200 Mbps with all functionality enabled



+91 22 3550 3063 +91 22 3521 0202

www.safesquid.com information@safesquid.net

A-304, Neelkanth Business Park, Vidyavihar West,
Mumbai 400086, Maharashtra, INDIA



Office Efficiencies (INDIA) Private Limited
Simplifying Technology!

4.10 CLUSTER READY

Enhances performance and reliability by linking multiple Proxy nodes in a load-balanced or failover cluster.

4.10.1 Flexible Cluster Operational Modes

Supports deployment in either active-active or active-standby modes, catering to different operational requirements

4.10.2 Proxy Auto-Configuration

Leverages PAC files to enable automatic traffic distribution across different proxy servers

4.10.3 Seamless policy synchronisation

Ensures consistent policy replication across all cluster nodes, both locally and in remote locations, without additional hardware or software.

4.10.4 Category Synchronization

Maintains consistent custom web-site categorizations across all nodes in a load-balanced cluster and remote sites.

4.10.5 Web Cache Communication Protocol Integration

Utilizes WCCP V1/V2 for intelligent traffic management and load balancing with compatible routers and switches

4.10.6 Zero Downtime Assurance

Implements replication technology to apply policies uniformly across the cluster while preserving session integrity.

4.10.7 Centralized Certificate Management System

Centralizes the handling and distribution of digital certificates across the cluster for streamlined security management

4.10.7.1 Cluster CA technology

Automates the replication of Trusted Root Certificates across cluster nodes

4.10.7.2 Consistent SSL Intermediate Root CA Certificate generation

Ensures uniformity of SSL/TLS certificates across proxy cluster nodes

4.10.8 Efficient Cluster Authentication Mechanism

Enables single-instance authentication across the proxy cluster, streamlining user verification processes.





Office Efficiencies (INDIA) Private Limited
Simplifying Technology!

4.11 FALSE POSITIVE REPORTING

Allows end-users to report websites they believe are wrongly categorized or blocked

4.11.1 Administrative Oversight of False Positives

Provides a mechanism for administrators to review and potentially authorize access to reported false positive websites.

4.11.2 False Positive Auditing

Maintains detailed logs of all user requests regarding false positives for thorough review and analysis

4.12 SELF-HEAL TECHNOLOGY

Proactively resolves potential problems with essential dependency files, ensuring continuous operation.

4.12.1 Dynamic Certificate File Restoration

Automatically regenerates any missing, expired, or corrupted certificate files

4.12.2 Configuration File Auto-Recovery

Substitutes missing or inaccessible configuration files with default settings to prevent service disruption

4.12.3 Virus Signature File Auto-Update

Ensures the latest virus signatures are downloaded and updated in case of outdated or missing files.

4.12.4 Category Database Regeneration

In case of corruption or loss, automatically downloads the latest version of the category database.

4.13 INTEGRATED DISASTER RECOVERY MECHANISM

Automatically recovers configuration settings upon activation of a replacement solution, minimizing manual intervention

4.14 COMPREHENSIVE INTERNAL MONITORING SYSTEM

Continuously monitors and manages various aspects of the service for optimal performance.

4.14.1 Auto-Service Restart Functionality

Ensures the service is automatically rebooted in the event of unexpected shutdowns or system failures

4.14.2 Continuous Process Optimization

Routinely evaluates and improves operational processes





Office Efficiencies (INDIA) Private Limited
Simplifying Technology!

4.14.3 Automated Disk Space Management

Actively cleans up unnecessary or temporary files, optimizing storage utilization.

4.15 DETAILED POLICY VERSION TRACKING

Records and controls different policy versions, noting timestamps, change authors, and specific alterations

4.16 ZERO COST REDUNDANCY

Provides various failover and performance improvement options without additional charges.

4.16.1 Complimentary Failover Node Provisioning

Offers failover capabilities across multiple cluster nodes without additional costs.

4.16.2 Unified Activation Key System

Simplifies administration by providing a single Product Activation Key for use across multiple cluster nodes.

4.16.3 Flexible Pay-As-You-Go Model

Adapts to changing web traffic or user numbers, with additional costs only for extra subscriptions

4.16.4 Geographically Agnostic Deployment

Offers the flexibility to operate and deploy the solution across various global locations

4.17 CUSTOMIZABLE TO ORGANIZATION NEEDS

Provides extensive options for customization to meet specific organizational demands and user experiences.

4.17.1 User Interface Personalization

Allows alterations to the dashboard, reporting interfaces, and analytics to suit user preferences and requirements

4.17.2 Extensive Customization Option

Utilizes a comprehensive library of customization features to enhance functionality and user experience

4.17.3 Branding- Aligned Blocking Templates

Enables administrators to customize blocking templates to conform to organizational branding and communication styles

4.17.4 Custom scripts

Supports the creation of custom bash scripts for specialized tasks and automation.



+91 22 3550 3063 +91 22 3521 0202

www.safesquid.com information@safesquid.net

A-304, Neelkanth Business Park, Vidyavihar West,
Mumbai 400086, Maharashtra, INDIA



4.18 ROBUST SECURITY FRAMEWORK

Incorporates advanced security measures to protect data and communications within the solution.

4.18.1 Enhanced Password Encryption

Safeguards passwords for Directory Services integration using a minimum of 2048-bit asymmetric encryption

4.18.2 Protected SSL Certificate Handling

Maintains the security of all SSL private key certificates required for HTTPS inspection, ensuring they are unusable outside the solution

5 SYSTEM AUDIT, USAGE ANALYTICS AND FORENSICS

Offers in-depth logging, reporting, and forensic capabilities for enhanced network security and usage analysis.

5.1 LOGGING

Custom-designed logging options for diverse requirements including usage analytics, debugging, and performance assessment.

5.1.1 Multiple Interfaces

Purpose designed logging options for usage analytics, debugging, and performance validation.

5.1.1.1 Open Format Logs

Human readable logs, structured for programmatic analysis using elementary tools such as *Awk*, *Grep*, *Less*, etc.

Exportable for analysis using standard spread-sheet / ASCII text-readers.

5.1.1.2 Direct Database Injection

Direct recording of Internet usage into an SQL-based database.

Supports direct access to the database for querying and analytics.

5.1.1.3 Graphical Visualisation

Streams logs to configuration interface for quick impact analysis of configuration changes.

Compatible with various open-source analysis and report generation applications.



Office Efficiencies (INDIA) Private Limited
Simplifying Technology!

5.1.1.4 *Real-Time Streaming to Remote Collectors*

Facilitates real-time transport of logs to remote aggregators and analytics facilities such as SIEM, asset and network monitoring systems.

Customizable for integration with bespoke facilities.

5.1.1.5 *Storage Management*

Automatic time-stamped rotation.

Option to compress for foot-print reduction.

Options to scavenge of old data for preserving system stability.

5.1.2 *Process Logs*

Adjustable detailing of information for process audit, system performance, and traffic forensic analysis.

5.1.2.1 *Module Operations*

Validation of each modular function such Identity Management, Security Policy enforcement, etc.

5.1.2.2 *Security Updates*

Validation of updates to Category Database, Virus Signature Database, SSL Certificates, Application Signatures, Content Identification Signatures, etc.

5.1.2.3 *Integration Checks*

Integration Checks, with LDAP, ICAP, YouTube

5.1.2.4 *Synchronisation with Proxy Cluster*

Validation of policy synchronization.

5.1.2.5 *Backtracking Information*

Debugging of application malfunction, and unhandled exceptions.

5.1.2.6 *Connection Logs*

Identification of systemic failures and network performance.

Time-stamped records of DNS queries, responses, and triggering clients.





Office Efficiencies (INDIA) Private Limited
Simplifying Technology!

5.1.2.7 *Internet Usage Analytics*

Structured records of each web transaction with comprehensive detailing of client, server, applied policies.

Request and response headers in client-proxy and proxy-destination.

Comprehensive details of threat detection and mitigation policy efficacy.

5.1.2.8 *Security Administration Records*

Structured records of access to policy management interface.

Automatic backup of existing policies precedes permanent changes.

Record changes made in policy configuration in a tab separated format.

5.1.2.9 *Orchestration Metrics*

Structured records of system and application performance metrics.

Comprehensive time-stamped detailing of resource utilization and throughput.

Compatible with standard enterprise asset monitoring tools.

Human readable for selective analysis of historic data.

Compatible with open-source tools for graphical charting.

Direct visualization within management interface.

5.1.2.10 *Bypass logs*

Structured records of security policy override events.

Human-readable format enables security administrators to fine-tune security policies.

5.1.2.11 *Deep Content Security Logs*

Structured records of events necessitating protocol headers / payload modification in lieu of traffic obstruction.

5.1.2.12 *Content Security Policy Violation Logs*

CSP-3 compliant reporting of content security policy breach avoidance.



+91 22 3550 3063 +91 22 3521 0202

www.safesquid.com information@safesquid.net

A-304, Neelkanth Business Park, Vidyavihar West,
Mumbai 400086, Maharashtra, INDIA



Office Efficiencies (INDIA) Private Limited
Simplifying Technology!

5.2 COMPREHENSIVE REPORTING SUITE

Delivers a range of customizable reporting tools for in-depth analysis, aiding strategic decision-making and operational oversight.

5.2.1 Customizable Reporting Configurations

Offers a variety of configurations for tailoring reports to specific analytical and operational needs

5.2.1.1 *Interactive Real-time dashboard*

Enables live monitoring and reporting directly within the configuration interface for immediate data access and analysis

5.2.1.2 *Versatile Report Export Options*

Supports exporting reports in various formats including Excel/CSV and PDF, facilitating data sharing and further analysis

5.2.1.3 *Automated Report Distribution*

Features the capability to schedule and automatically send reports to designated recipients, enhancing communication and awareness.

5.2.2 Threat Prevention Reports

Generates detailed reports on a variety of security threats, providing insights into prevention strategies and incident responses.

5.2.2.1 *Real-Time DLP Activity Monitoring*

Displays current data on blocked requests, crucial for preventing data breaches and ensuring information security

5.2.2.2 *Malware Incident Reporting*

Detailed reports on occurrences of malicious file uploads or downloads, highlighting areas of concern and action

5.2.2.3 *Malicious Site Connection Analysis*

Offers statistical data on user connections to command and control (C2D) domains and blacklisted websites.





Office Efficiencies (INDIA) Private Limited
Simplifying Technology!

5.2.2.4 Cross-Site Scripting Violation Metrics

Provides detailed metrics on incidents such as CSRF and XSS, enhancing understanding of cross-site security breaches.

5.2.2.5 Image Analysis Metrics

Records and analyses interactions with images, including those scanned, blocked, or bypassed, for enhanced content security insights

5.2.2.6 In-Depth DLP Log Reports

Detailed records of upload activities including user identity, data type, size, destination, and application used, offering a thorough view of data movement.

5.2.2.7 User Policy Violation Reporting

Captures and reports metrics on users who violate established policies, aiding in identifying and addressing rogue behaviours.

5.2.2.8 ClamAV Antivirus Activity Monitoring

Displays live data from the ClamAV antivirus system, providing insights into ongoing threat scanning and detection.

5.2.2.9 ICAP Service Usage Analysis

Reports data from ICAP services, including details on scanned requests and blocked responses, crucial for understanding external service integration.

5.2.3 Comprehensive System Reporting

Detailed reports offering real-time insights into various system metrics for enhanced operational understanding and management.

5.2.3.1 In-Depth System Performance Monitoring

Real-time visualization of critical system metrics such as User Time, System Time, Memory Usage, and Page faults, crucial for assessing system health

5.2.3.2 System Component Status Overview

Provides instant checks on the operational status of key system databases and components, like the Categorization Engine, Antivirus Engine, and LDAP Integration





Office Efficiencies (INDIA) Private Limited
Simplifying Technology!

5.2.3.3 LDAP Integration Monitoring

Displays real-time information on LDAP entries fetched, including timestamps and entry counts, for efficient directory service tracking.

5.2.3.4 Website Categorization Metrics

Shows details on the categories of websites accessed and highlights instances of unknown categorizations, aiding in content management.

5.2.3.5 Signature Tracking

Real-time tracking of application and content signature updates and usage, ensuring up-to-date threat detection

5.2.3.6 User Interaction Analysis

Reports on interactions with the proxy, detailing named users and corresponding IP addresses, for user behaviour analysis.

5.2.3.7 Host Interaction Reporting

Provides comprehensive data on host interactions, including details on visited websites and IPs, and frequency of visits

5.2.3.8 Connection Failure Analysis

Real-time monitoring and reporting of connection issues, including DNS and authentication failures, for network reliability assessment.

5.2.3.9 Detailed Live Traffic Reporting

Offers insights into both inbound and outbound network traffic, including successful connections, data transmission statistics, and types of HTTP requests.

5.2.3.10 Cache Utilization Metrics

Displays the efficiency of cache usage with detailed reports on cache hits and misses, indicating data retrieval efficiency.

5.2.3.11 Cookie Management Statistics

Reports on cookie control policies, displaying which websites have been permitted or restricted for cookie exchange.



+91 22 3550 3063 +91 22 3521 0202

www.safesquid.com information@safesquid.net

A-304, Neelkanth Business Park, Vidyavihar West,
Mumbai 400086, Maharashtra, INDIA



Office Efficiencies (INDIA) Private Limited
Simplifying Technology!

5.2.4 Detailed Performance Analysis

A comprehensive suite of tools to track and analyse various performance metrics for optimal system functionality.

5.2.4.1 System Utilization and Resource Monitoring

Focuses on tracking and analysing key system resources like CPU, memory, and process activities, providing insights into the overall health and efficiency of the system

5.2.4.1.1 CPU Utilization Assessment

Analyses trends in CPU consumption, including system and user time, to identify usage patterns and potential performance bottlenecks

5.2.4.1.2 Virtual Memory and Process Lifecycle Monitoring

Tracks SafeSquid's virtual memory usage and evaluates the age of processes to detect proxy service restarts and assess memory allocation efficiency.

5.2.4.1.3 Active Process and Thread Surveillance

Continuously monitors current running and waiting processes, alongside thread utilization, for real-time resource management and optimization.

5.2.4.2 Network and Connection Analytics

Encompasses detailed analysis of network connections, traffic flow, and error tracking to ensure optimal network performance and reliability

5.2.4.2.1 Detailed Network Connection and Bandwidth Analysis

Monitors active and idle TCP connections, inbound and outbound bandwidth utilization, evaluates outbound connection pool efficiency, and conducts server performance analysis based on client transaction patterns and demands.

5.2.4.2.2 Network Error and Failure Diagnostics

Tracks and analyses DNS and connection failures, along with threading errors, to identify issues impacting network reliability and performance.

5.2.4.3 Performance and Efficiency Metrics

Provides metrics and analyses related to system load, caching efficiency, and concurrent connections, highlighting overall system performance





Office Efficiencies (INDIA) Private Limited
Simplifying Technology!

5.2.4.3.1 Load Average and System Efficiency Metrics

Compares system load averages to estimate overall utilization and monitors cache hit/miss ratios alongside concurrent connections to gauge server efficiency.

5.2.4.3.2 DNS Query Efficiency Assessment

Analyses the ratio of total to reused DNS queries to evaluate the effectiveness of DNS caching mechanisms.

5.2.4.4 Security and Compliance Monitoring

Focuses on monitoring user and content interactions, along with compliance to security policies and updates, ensuring robust security management

5.2.4.4.1 User and Host Interaction Logs

Provides detailed reports on user interactions with the proxy and logs data on host communications, including website visit frequencies.

5.2.4.4.2 Signature Update and Policy Compliance Tracking

Monitors real-time updates in application and content signatures for threat detection, and maintains logs on cookie control policy applications across websites.



+91 22 3550 3063 +91 22 3521 0202

www.safesquid.com information@safesquid.net

A-304, Neelkanth Business Park, Vidyavihar West,
Mumbai 400086, Maharashtra, INDIA