CYBERSECURITY CENTRE of EXCELLENCE
A joint initiative of DSCI & Government of Telangana

DSCI
PROMOTING DATA PROTECTION
A nasscom Initiative

SafeSquid® LABS

WHITEPAPER

EXTENDING ZERO TRUST SECURITY STRATEGIES FOR MITIGATING LAYER 7 VULNERABILITIES

Table of Contents

Executive Summary

Enterprise digital transformation has fundamentally altered the threat landscape, exposing critical inadequacies in traditional security models. Modern Web 2.0 applications have evolved beyond simple client-server interactions into complex distributed systems leveraging interconnected JavaScript frameworks, dynamic API calls, and embedded third-party services. However, this architectural evolution has spawned sophisticated attack vectors, that exploit Layer 7 vulnerabilities, creating multifaceted attack surfaces. Traditional security solutions fail to detect or prevent Zero-Day threats like phishing, malware, session hijacking, data theft, and cyberslacking. This fundamental mismatch between modern web architecture and legacy security controls exposes organizations to significant risks that demand new defensive approaches.

The limitations of existing security approaches demand a paradigm shift. Network Layer Firewalls, while effective at Layer 3/4 traffic control, remain blind to application-layer threats. End Point Security (EPS) attempts to address these gaps through device-level protection but introduces significant computational overhead and exponentially growing policy management complexity. These constraints necessitate Secure Web Gateways (SWGs) as dedicated Layer 7 security control planes, enabling deep content inspection of encrypted web traffic and real-time policy enforcement without compromising performance or manageability.

The dissolution of traditional network boundaries through hybrid architectures—encompassing cloud services, IoT devices, and remote endpoints—demands integration of Zero Trust Architecture (ZTA) principles within SWGs. Modern SWGs implement this enhanced architecture through a structured framework of Policy Engine, Administrator, and Enforcement components, working in concert with SSL/TLS termination points for deep content inspection. This system interfaces with enterprise security infrastructure including Identity Management, SIEM, DLP, and threat intelligence systems. For dynamic security posture assessment, Trust Algorithms evaluate multiple risk dimensions—environmental context, device metrics, user behaviour patterns, resource sensitivity, and transaction characteristics—to continuously recalibrate access permissions, based on a contextual trust score.

To effectively implement Zero Trust principles, Secure Web Gateways require a fundamental shift from legacy multi-process proxy architectures to multi-threaded designs. While traditional implementations rely on process-based separation and Inter-Process Communication, Zero Trust's demand for contextual awareness and granular control necessitates direct memory access between threads and shared variable architecture for real-time context sharing. The multi-threaded architecture enables efficient resource utilization and scalability while maintaining the contextual awareness required for granular Zero Trust security policies.

Furthermore, The integration of AI-powered behavioural analytics enhances threat detection through machine learning models that establish contextual baselines and identify anomalies, particularly crucial for detecting Advanced Persistent Threats, social engineering attempts, and insider threats.
This whitepaper examines how modern SWGs address these fundamental security challenges through architectural innovation, enabling secure business operations in an increasingly complex digital landscape.

The Evolution of Enterprise Web Security

Digital transformation has created an inescapable dependency on Internet connectivity in modern enterprises. The **World Wide Web (WWW)** drives operational efficiency and competitive advantage through enhanced collaboration and knowledge sharing, yet simultaneously expands the attack surface for web-based threats.

Traditional security approaches fail to keep pace with the evolving threat landscape, and enterprise architectures. **End Point Security (EPS)** solutions operating at the device level face fundamental architectural limitations. Host operating system capabilities and application-specific implementations constrain EPS effectiveness, while imposing significant computational overhead that degrades endpoint performance. Enterprise scaling multiplies the complexity of managing distributed EPS deployments exponentially, creating policy enforcement delays that compromise threat response times.

Network Layer Firewalls (NLFs) established perimeter defence strategies by providing critical Layer 3 and 4 traffic inspection to prevent unauthorized network access. The Web 2.0 paradigm shift has rendered this protection insufficient. Modern web applications leverage complex Layer 7 technologies to enable dynamic content generation, real-time interactivity, and rich multimedia experiences. The proliferation of interconnected JavaScript frameworks, dynamic API calls, and embedded third-party services creates new attack vectors that bypass traditional NLF controls, exposing organizations to sophisticated threats including Application-layer phishing attacks, Polymorphic malware delivery, Covert data exfiltration, Session hijacking, Resource misuse through cyber slacking.

Secure Web Gateways (SWGs) have emerged as a dedicated security control plane to address these advanced **Layer 7 threats**. Modern SWG Deep Content Inspection capabilities analyse protocol behaviours and payload contents simultaneously, allowing real-time detection and remediation of suspicious web transaction. The combination of granular policy enforcement with comprehensive web transaction visibility enables both preventive and detective security controls.

Role of SWG in Zero Trust Architecture

Dynamic threat environment

The obsolescence of the "Castle and Moat" security model has fundamentally altered enterprise security architecture. Modern enterprises operate across hybrid environments encompassing cloud services, Internet of Things (IoT) devices, and distributed access points. Bring Your Own Device (BYOD) policies introduce non-enterprise devices accessing sensitive resources from untrusted networks, eliminating clear network boundaries. This dissolution of definitive perimeters mandates continuous verification of every connection and transaction, regardless of origin or destination, positioning Secure Web Gateways (SWGs) as critical components within Zero Trust Architecture.

Zero Trust

The verification mechanisms in modern security systems mirror human trust dynamics in evaluating subject (user/device) access to resources (system/data/application).

Imagine meeting someone for the first time—you don't immediately trust them with secrets. Instead, you offer minimal access, carefully observing their behaviour and verifying their identity over time. As they prove themselves reliable, you gradually increase the level of trust. Even so, trust is never absolute or unconditional. If they act suspiciously or violate your expectations, you reduce their access accordingly. Trust in human relationships is fluid, and sceptics are always safe.

Zero Trust Architecture (ZTA) codifies these principles. ZTA enforces default-deny policies, disregarding network position or historical behaviour. Access grants adhere to minimal permissions, with dynamic adjustments based on real-time verification, behavioural analysis, and continuous monitoring. The security framework reassesses trust at each interaction, incorporating new contextual data. Unexpected behaviour or emerging threats trigger immediate access restrictions, establishing trust as an evolving, context-dependent metric.

Core Principles of Zero Trust Applied to SWG

Least Privilege Access

The concept of least privilege, a cornerstone of Zero Trust, is implemented within SWG by minimizing access permissions to the strict minimum necessary. Granular web access control policies must consider multiple contextual factors—such as user identity, location, device security posture, behavioural patterns, and risk scores—ensuring precise access controls. This principle limits the attack surface, reducing the risk of exposure if a breach occurs.

Never trust, Always verify

Trust is never assumed, not even within the perimeter. No connection is established until explicitly authorized, ensuring that malicious actors—internal or external—are not granted unchecked access to sensitive data or resources. The SWG continuously verifies every access request, inspecting and validating traffic at the web application layer.

Adaptive Trust Assessment

In line with Zero Trust's dynamic nature, SWGs monitor web traffic for anomalies, conducting real-time risk assessments based on user behaviour, device posture, and web traffic patterns. SWGs monitor for anomalies such as unauthorized access attempts, suspicious data transfers, or deviations from established behaviour baselines. If abnormalities are detected, access policies are adjusted dynamically, with the gateway either restricting or revoking access.

Micro-Segmentation

Just as ZTA advocates for network segmentation to limit lateral movement during a breach, SWGs segment web traffic, isolating interactions between subjects and resources. By enforcing this application-layer segmentation, SWGs ensure that even if a web session is compromised, the risk is contained, preventing unauthorized access from spreading to other systems or applications. This minimizes the "blast radius" of an attack.

Assume Breach

A Zero Trust framework operates under the assumption that breaches are inevitable. Therefore, SWGs are designed to function as if the network is already compromised, continuously sanitizing data transfers and actively blocking exfiltration attempts. Even when an attacker gains access to the network, the SWG serves as a vital defence layer, reducing the likelihood of successful data theft.

In summary, Secure Web Gateways embody the core principles of Zero Trust to continuously verify, segment, analyse, and sanitise web traffic at the application layer.

Logical Components

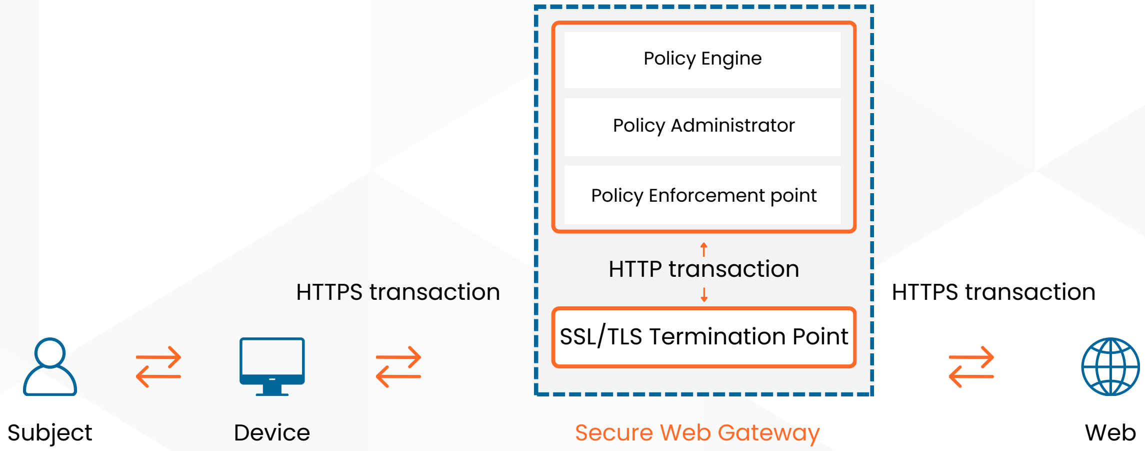

Figure 1: Logical Components of a Zero Trust Secure Web Gateway

Extending the NIST-defined Zero Trust Architecture components, the following logical elements are critical in an SWG for enforcing Zero Trust policies:

Policy Engine (PE)

The Policy Engine evaluates access requests using the enterprise's web access policies combined with external threat intelligence. The PE assesses various factors, such as user identity, device health, and web risk factors like URL reputation, content analysis, and site behaviour, to make real-time decisions on the scope of access given to a subject.

Policy Administrator (PA)

The Policy Administrator executes the decisions made by the PE, applying them directly at the web gateway. By dynamically configuring enforcement points, SWG ensures real-time adaptation of policies based on current risk levels.

Policy Enforcement Point (PEP)

The Policy Enforcement Point is responsible for enforcing the access decisions made by the PE. Operating in-line with web traffic, the PEP ensures that security policies—such as blocking unauthorized content or preventing access to malicious sites—are consistently applied.

SSL/TLS Termination Point (STP)

To enable deep inspection of encrypted traffic, the SSL/TLS Termination Point decrypts HTTPS sessions. The decrypted traffic is analysed by the PEP, which inspects protocol headers and payload content for threats or policy violations. Once inspection is complete, the traffic is re-encrypted before it reaches its destination, maintaining end-to-end security.

Several external systems integrate with an SWG to enhance security, enforce policies, and provide comprehensive visibility into web traffic.

Identity and Access Management (IAM) systems

Integration with IAM systems ensures that the SWG can authenticate users based on multi-factor authentication (MFA) or risk-based identity verification. The SWG uses identity data, such as user roles and group memberships, to apply role-based access controls aligned with the principle of least privilege.

Industry Compliance System

SWGs must ensure compliance with industry-specific regulatory standards (e.g., GDPR, HIPAA). By enforcing access restrictions to non-compliant services or protecting sensitive data in transit, SWGs help organizations meet regulatory requirements while minimizing the risk of sanctions.

Continuous diagnostics and mitigation (CDM) system

A CDM system provides real-time assessments of the security posture of devices attempting to access web resources. The SWG can adjust security controls based on the device's health status, enforcing stricter policies if the device shows signs of compromise or vulnerability.

Security Information and Event Management (SIEM)

By forwarding web traffic logs to a broader SIEM system, the SWG contributes to enterprise-wide threat detection and response efforts. The SIEM correlates web access logs with other security data (e.g., firewall events, endpoint security alerts) to identify sophisticated threats. This allows the SWG to adapt its access controls in real-time based on SIEM-generated insights.

Enterprise Public Key Infrastructure (PKI)

PKI systems play a crucial role in validating the digital identities of users, devices, and applications through the use of certificates. The SWG checks the validity of digital certificates in real-time to ensure secure, authenticated communications.

Web Categorisation Engines

URL Categorisation Engines categorize websites based on content, reputation, and risk profiles. SWGs leverage this information to block access to harmful sites or restrict access to categories deemed inappropriate for specific user groups.

Threat intelligence updates

Real-time threat intelligence from internal and external sources allows the SWG to stay updated on emerging threats. SWGs ingest this intelligence to proactively block malicious traffic based on known bad actors (e.g., IP addresses, domains) and current threat trends.

Web Application Identification and Control

Determine the nature of the request and/or response from the protocol headers, to prevent unsanctioned web sites or applications. Such determination enables SWGs to deny undesirable features of a web-site such as login, privacy violations, inadvertent form submissions, unnecessary background traffic, execution of cross-site JavaScript, etc.

Malware Scanners

Malware scanners analyse HTTP(S) payloads and attachments for viruses, trojans, ransomware, or any other malicious software attempting to enter the network. Beyond signature-based detection, modern malware scanners integrated with an SWG leverage behaviour-based analysis to detect zero-day threats or advanced persistent malware. With inline malware scanning, the SWG can block malicious files or scripts in real-time before they reach the endpoint or user device. If malware is detected, the SWG can either quarantine the file or prevent the connection entirely.

DLP Systems

The integration of SWGs with DLP systems allows for real-time policy enforcement and alerts based on user actions and data transfers. As users interact with web applications, the DLP system continuously monitors for any attempts to access or share sensitive information, applying pre-defined rules dynamically. If a policy violation is detected—such as a user attempting to upload sensitive data to an unapproved site—the DLP system can trigger immediate alerts, block the action, or redirect the user to a secure channel for proper data handling.

Sandbox Environments

In addition to analysing suspicious files, modern sandbox environments integrated with SWGs can trigger automated remediation actions based on analysis results. If malicious behaviour is detected in the sandbox, the SWG can immediately quarantine the associated session, revoke access, or trigger alerts for security teams, ensuring swift containment of potential threats without manual intervention.

Trust Assessment Framework

A Secure Web Gateway (SWG) typically employs a Trust Algorithm (TA) to dynamically assess the trustworthiness of both the users and the web resources they are interacting with, and operate in real-time. At the core, the actual access decision hinges on the Policy Engine (PE), by leveraging a Trust Algorithm (TA), to evaluate the security posture of the request. The policy engine acts as the brain of the system, and the trust algorithm as its primary thought process.

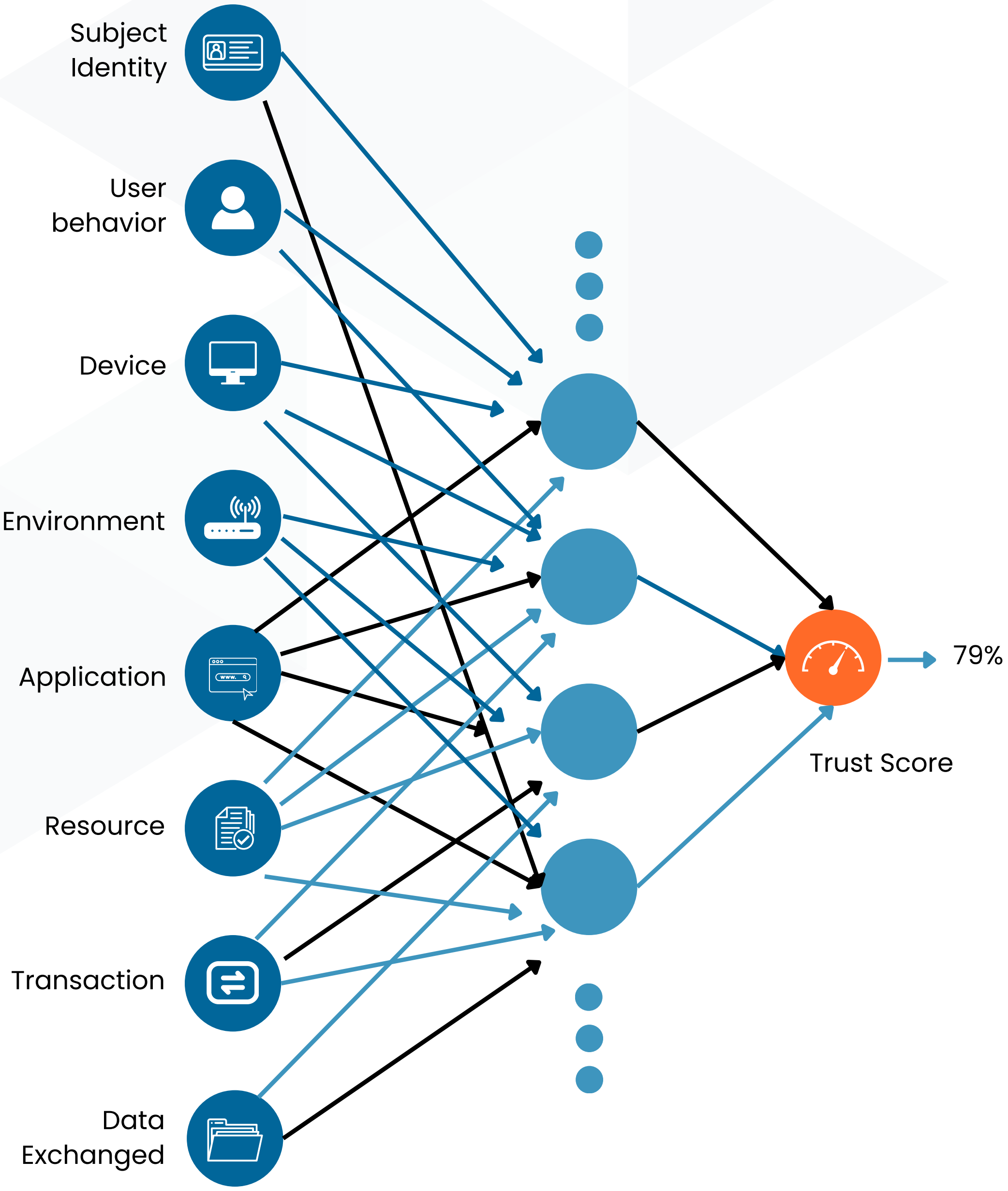

Figure 2: Trust Algorithm in a SWG

Variables and Metrics

In a Zero Trust framework, this algorithm is foundational to enforcing policies and ensuring secure access, incorporating an extensive set of variables and metrics that work together to create a comprehensive security posture assessment. The following elements represent an enhanced approach to trust evaluation:

A. Environmental Context Metrics

The system continuously monitors and evaluates the environmental context in which access requests occur, incorporating temporal, spatial, and network-related factors. This includes analysing access patterns relative to established working hours, detecting geographical anomalies through velocity checks, and assessing network characteristics such as connection types and routing paths. By considering factors like impossible travel scenarios, ISP reputation, and network security posture, the system can identify suspicious access attempts that might indicate compromise or unauthorized access attempts.

B. Enhanced Device Metrics

Device security evaluation goes beyond basic compliance checks to encompass a comprehensive assessment of hardware security features, software integrity, and system health indicators. The system examines hardware security elements like TPM status and encryption capabilities, while also monitoring software-related factors such as application inventory risks and process reputation. System health metrics including resource utilization patterns, boot sequence integrity, and crash frequency provide additional context for trust decisions, ensuring that access is only granted to devices maintaining appropriate security standards.

C. Advanced User Behaviour Analytics

User behaviour analysis employs sophisticated monitoring of interaction patterns and authentication characteristics to build a detailed profile of normal user activity. The system tracks authentication patterns including MFA strength and password complexity, while also analysing user interaction metrics such as mouse movements, keyboard dynamics, and command execution patterns. Data access patterns are scrutinized for volume, type, and frequency of requests, creating a comprehensive behavioural baseline against which future activities can be compared for anomaly detection.

D. Resource Risk Metrics

Resource evaluation encompasses detailed analysis of content sensitivity, service health, compliance status, and SSL certificate validation to determine appropriate access levels. The system performs content analysis to assess data classification levels and sensitivity scores, while monitoring service health indicators such as API security posture and performance baselines. SSL certificate validation includes checking certificate chain integrity, revocation status, cipher strength, key length, and certificate authority trustworthiness. The system also monitors for certificate pinning violations, man-in-the-middle attempts, and SSL/TLS protocol version compliance. Certificate expiration monitoring and real-time certificate transparency log verification provide additional security layers. Compliance status verification ensures alignment with regulatory requirements and industry standards, creating a multi-faceted approach to resource risk assessment that informs access decisions.

E. Transaction Risk Scoring

Transaction analysis involves detailed examination of both request and response characteristics, along with contextual evaluation of business process alignment. The system monitors request patterns for header anomalies and payload deviations, while analysing response characteristics including status code patterns and content-type verification. Transaction context evaluation considers business process alignment and workflow sequence validation, creating a comprehensive view of transaction legitimacy and risk level.

Trust Score Calculation

The final trust score calculation synthesizes all these elements through a weighted algorithm that considers the relative importance of each factor based on organizational context and risk tolerance. The algorithm employs **dynamic weight adjustment** based on current threat landscapes and compliance requirements, while maintaining predefined trust level categories that trigger specific response actions. This comprehensive approach ensures that access decisions are based on a holistic evaluation of all relevant security factors, maintaining zero trust principles while enabling necessary business operations.

A score-based TA calculates a trust score based on various factors that represent the subject's trustworthiness in relation to a resource they want to access, including the policy database with observable information about subjects, subject attributes and roles, historical subject behaviour patterns, threat intelligence sources, and other metadata sources. Enterprises can also customize the weight assigned to each data source based on their priorities, reflecting the relative importance of different risk factors. A contextual TA is particularly effective in detecting a potentially malicious request, like insider attacks or compromised accounts by analysing deviations in behaviour, even if the access requests appear typical on the surface.

By dynamically adjusting trust levels based on a score that reflects real-time data, contextual, score-based TAs enhance both security and user experience, enabling more granular, adaptive access control. This approach balances security, usability, and cost-effectiveness, offering a more responsive and robust defence against evolving threats compared to static, rule-based systems.

Multi-Threading for Granular Control

Modern Secure Web Gateways must balance granular security controls with business productivity. While marketing teams require social media access and technical teams need educational platforms, unrestricted access poses operational risks. SWGs address these challenges by implementing feature-specific controls over Web 2.0 applications.

The SWG architecture centers on a proxy server core, traditionally built on **Squid Caching Web Proxy** with integrated modules for URL filtering and malware scanning. Legacy implementations use a **multi-process architecture** where the parent process orchestrates overall proxy operations, and spawn child processes to handle specific functions (DNS lookups, authentication, URL filtering, SSL validation). As each process needs its own stack, file descriptors, and resources, Inter-Process Communication is employed to share the configuration, cached data, and system resources. However, this architecture's limitations in sharing structured data impede contextual intelligence needed for granular access control.

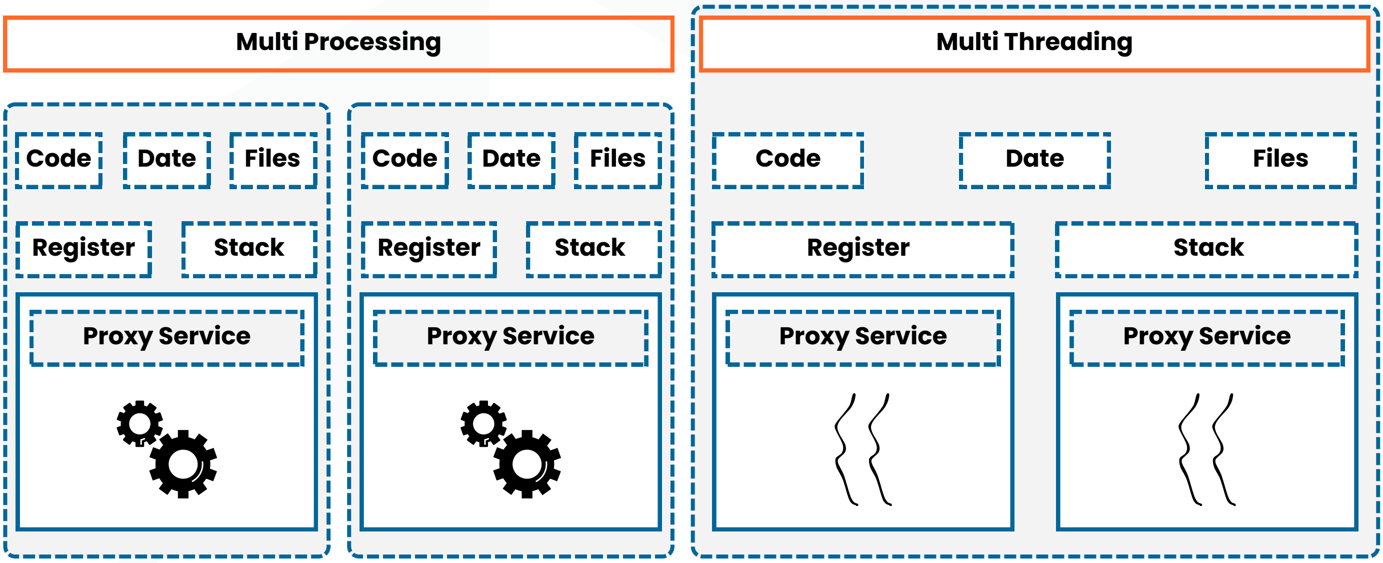

Figure 3: Multi-Processing vs Multi-Threading

These constraints necessitate a **multi-threaded proxy service** explicitly designed for **Zero-Trust Web Security**. Direct memory access between threads enables efficient communication. Shared variable architecture enables **real-time context sharing**. Thread-based processing improves resource utilization and scalability. This revised architecture delivers the performance and contextual awareness required for implementing granular Zero-Trust security policies.

AI- Powered Behavioural Analytics

Behavioural analytics is a key component of intelligent web security, providing deeper insights into user actions and potential threats. Behavioural analytics enhances the cybersecurity posture by monitoring and analysing user and system behaviour to detect deviations from normal patterns. SWGs can leverage machine learning (ML) algorithms to make context-aware decisions, and detect anomalies in real-time.

Behavioural Profiling

SWGs can employ behavioural profiling by establishing baselines of normal user and device web activities over time. These profiles evolve as AI models process more data, allowing more accurate detection of anomalous behaviour. For example, user login times, geographic access patterns, and resource interaction frequency can be continuously tracked, enabling precise identification of deviations that may signal threats.

Contextual Analysis

Contextual data plays a key role in behavioural analysis. SWGs combine behavioural analytics with contextual information such as user role, location, device health, and even time of day to make more informed security decisions. For example, a user attempting to access sensitive resources from an unfamiliar device or location can be flagged for additional verification.

Broader Role of AI and ML

AI and machine learning significantly enhance the capabilities of Secure Web Gateways (SWGs) by enabling more advanced threat detection and response mechanisms. These technologies allow SWGs to dynamically adapt to emerging threats and evolving user behaviours, ensuring real-time protection against both known and unknown risks.

AI - driven Anomaly Detection

Machine learning models embedded within SWGs can detect anomalies by learning from large volumes of past behaviour. These models evolve, improving over time as they are exposed to more patterns, allowing them to flag suspicious behaviour more accurately. If a user who typically accesses the web from a specific region suddenly starts accessing from a different location, the system can trigger an alert or require additional verification.

Enhanced Detection of Sophisticated Threats

AI and ML algorithms empower SWGs to detect more complex, hard-to-identify threats such as zero-day exploits, insider threats, and account takeovers. Instead of relying on static rules, SWGs dynamically adjust security policies based on real-time behavioural insights. This level of adaptability is crucial for identifying subtle signs of compromised accounts that might bypass conventional security controls.

Real- Time Risk Assessment

ML algorithms continuously assess the risk level of web traffic based on a variety of contextual signals such as the user's past behaviour, the reputation of the websites they're visiting, the time of day, and more. This helps the SWG make dynamic decisions on whether to allow, block, or challenge access.

Practical Applications

Behavioural analytics provides tangible security benefits by enabling SWGs to detect and respond to complex threats more effectively. From identifying insider threats to preventing phishing attacks, these analytics help safeguard organizations by continuously monitoring and analysing user behaviour in real-time.

Detecting Advanced Persistent Threats (APTs) Through Insider Activity

Behavioural analytics plays a pivotal role in detecting **insider threats**, which often evade traditional security controls. SWGs analyse user behaviour for subtle signs of compromise—such as accessing resources outside of normal working hours, downloading unusual volumes of sensitive data, or attempting to disable security mechanisms. When these patterns are detected, the SWG triggers alerts or enforces stricter controls in real-time.

Preventing Social Engineering Through Phishing Detection

AI-powered behavioural analytics can identify **phishing** attempts and fraudulent activities by detecting irregularities in web traffic or abnormal communication patterns. This is especially critical for detecting **zero-day** attacks that do not match known signature-based threat patterns. When a user clicks on a suspicious link or interacts with a site showing abnormal communication patterns, the system can flag the event as high-risk. Real-time analysis of user actions, combined with external threat intelligence feeds, allows SWGs to block access to malicious websites before any damage is done.

Safeguarding Against Cross - Site Attack Vectors

Behavioural analytics provides sophisticated detection capabilities for **cross-site scripting (XSS)**, and **cross-site request forgery (CSRF)** attacks by monitoring patterns in web interactions. The SWG analyses HTTP headers, request parameters, and payload content for suspicious patterns that might indicate injection attempts. By establishing baselines of normal application interaction patterns—such as typical form submission sequences, API call patterns, and request parameter structures—the system can identify anomalous behaviour in real-time. When a user's session suddenly exhibits unusual **cross-origin requests**, unexpected parameter modifications, or suspicious script injections, the SWG can immediately block the connection and isolate the affected session. This dynamic analysis is particularly effective in detecting sophisticated attacks that attempt to exploit trust relationships between the user and legitimate web applications.

Monitoring Workplace Productivity and Resource Usage

Behavioural analytics enables organizations to identify and manage productivity risks associated with inappropriate web usage during work hours. The SWG employs multiple analytical layers to detect **cyber-slacking patterns**—such as excessive time spent on social media, streaming services, or gaming sites during core business hours. The system builds baseline profiles of acceptable web usage based on role-specific requirements and organizational policies. Advanced analytics track metrics like time distribution across different website categories, frequency of non-work-related site visits, and patterns of attempting to circumvent access controls. When usage patterns deviate significantly from established baselines—for instance, a sudden increase in streaming media consumption or attempts to access blocked sites through proxy servers—the SWG can automatically implement graduated response measures, from displaying warning messages to temporarily restricting access to non-essential services.

Conclusion

As cyber threats evolve in complexity and volume, traditional security models are no longer sufficient to protect enterprise systems and sensitive data. The adoption of Zero Trust Architecture (ZTA), reinforced by Secure Web Gateways (SWGs), offers a robust solution by addressing security at the application layer and ensuring that trust is continuously validated. By enforcing granular policies, SWGs provide the visibility and control needed to secure web traffic in real time, irrespective of whether users or devices operate inside or outside the network perimeter.

The incorporation of advanced behavioural analytics further strengthens this security framework. Through AI and machine learning, SWGs can dynamically monitor user behaviour and identify anomalies that may signal potential threats. This proactive approach ensures rapid detection and response to emerging attacks, from phishing attempts to insider threats, thereby significantly reducing the risk of breaches. Moreover, by adapting access controls in real-time based on a combination of contextual data and behaviour patterns, SWGs enhance the security experience while minimizing disruptions to legitimate users.

In a world where cyber threats are increasingly sophisticated and attack surfaces continue to expand, combining ZTA with SWGs that leverage AI-driven behavioural analytics is the key to a resilient and future-ready cybersecurity strategy. By continuously evolving to meet emerging threats, enterprises can ensure secure web access, protect critical data, and maintain business continuity in an ever-changing digital landscape.

SafeSquid SWG

SafeSquid SWG is an **HTTP Proxy server**, explicitly designed for setting up enterprise Layer 7 perimeter security. It is the 4th generation of SafeSquid series of proxy servers. Conceived initially as an add-on for Squid Web-Caching proxy for high performance web filtering, but the later generations serve as independent solutions for perimeter-level implementation of **Zero-Trust web security** strategies.

Primary objective of SafeSquid remains mitigation of **Layer 7 risks** when enterprise knowledge workers, or digital assets interact with the web. Realtime content analysis and threat mitigation while preserving user's web-experience is central to SafeSquid's feature implementations. A unique multithreaded architecture underlying a **neural network** of software processors, provides the vital **SMP-awareness** for high performance content inspection.

- Cloud based updates of **Web Application Signatures** for maintaining policy fidelity with hundreds of SaaS offerings, high-performance implementation of TLS interception, pre-emptive enforcement of **CSP-3** in protocol headers, are highlights of the current SafeSquid generation.
- SafeSquid based Secure Web Gateways enable reliable enforcement of granular policy across diverse and large number of users or information systems that need web access across geographically distributed network locations of an enterprise.

Distributed as a **download-and-deploy** network application service, for generic Linux, enables regular Linux technicians to setup and implement as per enterprise requirements.

- **Cloud-init scripts** enable easy deployment on PaaS infrastructure to service networks where on-premise solution may not be feasible. Integration via private networking technologies for seamless solution adoption.
- Optimized operating system ISO to deploy SWG as a **virtual appliance**.
- Shareable Product Activation Key for quick sparking of **cluster nodes**, and seamless policy replication.

About Cybersecurity Center of Excellence

The Cybersecurity Center of Excellence (CCoE) is a joint initiative of the Government of Telangana and Data Security Council of India (DSCI) to accelerate the cybersecurity momentum and create a conducive cybersecurity ecosystem that nurtures innovation, entrepreneurship and capability building. CCoE works with all industry organisations, government agencies, academia and R&D centers and user groups and collaborates with other industry bodies, incubators and accelerators to accomplish its mission. DSCI is a not-for-profit, industry body on data protection in India, set up by NASSCOM®, committed to making the cyberspace safe, secure and trusted by establishing best practices, standards and initiatives in cyber security and privacy. DSCI is the apex industry body for Cybersecurity in India.

https:/ccoe.dsci.in   ccoe.hyd   ccoe_hyd   cybersecurity-ceo-telengana   ccoeofficial

About SafeSquid Labs

Pioneering enterprise web security, SafeSquid Labs specialises in Layer 7 perimeter security innovations to safeguard government establishments, and large organisations globally. Our solutions defend internet users, cloud infrastructures, and web applications from the most sophisticated internal and external cyberattacks. High performance, innovative features, and unparalleled scalability are the hallmarks of our offerings.

Telefonica O2, Batelco, Safran Defense Industries, Bell Canada, Government of Aruba, Defence Ministry of Netherlands, Bhabha Atomic Research Centre, Nuclear Fuel Complex of India, are among the more recognizable beneficiaries.

https://www.safesquid.com/   SafeSquid   safesquid   SafeSquid SWG

CYBERSECURITY CENTER OF EXCELLENCE

Cybersecurity Centre of Excellence, (DSCI)
4th Floor, Pioneer Towers, Inorbit Mall Road,
Hi-tech City,Hyderabad, India-500081

FOR ANY QUERIES:

P: +91 98711 74349
E: marketing.ccoe@dsci.in

SAFESQUID LABS

304, 3rd Floor, A wing, Neelkanth Business Park,
Nausena Vihar, Road, VidyaVihar West,
Mumbai 86

FOR ANY QUERIES:

P: +91 90824 22590
E: vk@safesquid.net

FORTIFY THE INTRINSIC SECURITY QUOTIENT OF YOUR ENTERPRISE TO DEFEND AGAINST ZERO - DAY WEB - BASED THREATS

CYBERSECURITY
CENTRE *of* EXCELLENCE
A joint initiative of DSCI & Government of Telangana

FOR ANY QUERIES:

P: +91 98711 74349

E: marketing.ccoe@dsci.in