APPLICATION INSIGHT SWG

Specification Sheet

< Secure Web Gateway Specification Sheet >

Technical specifications

[Configuration]

- Integrated Hardware Appliance

- H/W Bypass Support for Hardware Fault Conditions

- S/W Bypass Support for Software Fault Conditions

- Support for Installation of Hardware-Based SSL/TLS Acceleration Card for Enhanced Performance

- Supports Installation Using Transparent Proxy Architecture Without Modifying Existing Network Configuration

- Support for Forward Proxy Mode Configuration Using Dedicated Agent or PAC (Proxy Auto Configuration)

- Support for In-line (Sniffing) and Out-of-Path (Mirroring) Modes Without Interfering with TCP/TLS Sessions

- Support for High Availability (HA) Configuration with Active-Active and Active-Standby Functionality

- Asynchronous Traffic Handling in Redundant or Multi-Segment Configurations

- Support for Network Interface Redundancy via Link Aggregation (Bonding Configuration)

- Support for ICAP Client and ICAP Server Modes for Integration with Third-Party Solutions

- Support for Automatic Synchronization of URL Blacklists Provided by Third-Party Solutions

- Support for NAT (Network Address Translation) Configuration within the Decryption (Active) Segment

- Health Check Function for Monitoring Interconnected System Failures and Enabling Bypass within the Decryption (Active) Segment

- Support for Multi-Segment Architecture to Accommodate Multiple Decryption (Active) Zones

- Support for Passive Decryption Traffic Mirroring on 8 or More Ports

[Web Security]

- Support for Category-Based Filtering to Identify and Detect Malicious and Non-Business Websites (with Proprietary URL Category Database Supporting Online Updates)

- Support for Access Control to Malicious Categories Based on Integration with Google Safe Browsing API

- Support for YouTube Filtering Functionality Based on Integration with YouTube API to Identify and Detect Video Categories

- Support for Application Control Functionality to Identify and Detect Network Applications such as Messenger and SNS (with Proprietary Network Application Database Supporting Online Updates)

- Support for CASB Functionality to Control Access and Feature Usage of SaaS Applications such as Google Workspace, Office 365, and Webmail (with Proprietary SaaS Database Supporting Online Updates)

- Support for Simplified Security Policy Configuration for Generative AI Services Without Specifying Endpoints (URLs) or Identifiers (Keys), Using Proprietary Generative AI Database with Online Update Capability

- Support for Country-Based IP Access Restrictions (with Proprietary Country IP Database Supporting Online Updates)

- Integrated ATP Functionality for Malicious File Analysis via Interworking with Dedicated Security Solutions

- Support for Captive Portal Functionality that Allows Web Access After User Identity Authentication

- Support for Security Policy Enforcement Based on Identification of Real Client IP Embedded in HTTP Headers

- Support for Security Policy Enforcement Based on Identification of User Identity Embedded in HTTP Headers

- Support for Blocking Access to External Open Proxies such as Malicious Proxy Servers or Anonymous VPNs

- Support for Blocking Access from Compromised Clients to Command and Control (C&C) Servers

- Support for Modifying and Forwarding HTTP Structure of Web Requests or Responses Based on Specified Conditions

- Support for Configuring Approved Browsers and Restricting Access from Unapproved Browsers During Web Access

- Support for Detecting Web Access Violating RFC and Other Web Standards

- Support for Configurable Response Control Conditions Including Malicious URL Scanning in Web Content and Attachments, as well as File Size and Extension Restrictions

- Support for Anti-Malware Functionality to Detect Malicious Code Patterns in Web Responses (e.g., Exploit Kits, Redirects, JavaScript Obfuscation)

- Support for Anti-Virus Functionality to Detect Malicious File Downloads in Web Responses

- Support for Configuring Content Size Limits in Web Responses

- Support for Integration with Cyber Threat Intelligence Platforms to Identify and Respond in Real-Time to Various Cyber Threats (e.g., Blacklisted Client IPs, C&C IPs)

- Support for Integration with Cyber Threat Intelligence Platforms to Query Reputation of Malicious URLs and Files from Stored Log Data

- (Sniffing only) Support for SNI-Based Identification to Apply Web Security Policies on HTTPS Traffic Without Performing Decryption

[Data Loss Prevention]

- Support for Attachment Archiving Functionality that Extracts and Stores Original Files for Post-Access Review

- Support for Detection and Prevention of Leakage of Eight Types of Sensitive Information (e.g., Resident Registration Numbers, Credit Card Numbers) Contained in Web Content and Attachments

- Support for Configurable Web Request Control Conditions Including Keyword or Regex Matching, File Size and Extension Restrictions on Web Content and Attachments

- Support for Configuring Content Size Limits in Web Requests

[SSL Visibility]

- Supported Encryption Protocols: SSL V3.0, TLS V1.0, TLS V1.1, TLS V1.2, TLS V1.3

- Support for HTTP/2 Protocol Decryption

- Support for Encryption and Decryption of Various SSL/TLS-Based Application Protocols Beyond HTTPS(e.g., FTPS, SMTPS, LDAPS, IMAPS)

- Support for Encryption and Decryption of TLS Upgrade Protocols such as STARTTLS

- Selective Encryption and Decryption Support for Specified TCP Port Targets

- Support for Encryption and Decryption of SSL/TLS Traffic over IPv6

- Support for Decryption Policy Enforcement Based on Client OS Identification via OS Fingerprinting

- Support for Encryption and Decryption Using ECC (Elliptic Curve Cryptography) Certificates

- Support for Automatic Identification of SNI in Encrypted Traffic Without Predefined Decryption Target Registration

- Support for Online and Offline Updates of Application Database for PKP (Public Key Pinning)

- Support for Automatic Learning of TLS Connection Failures (IP/URL) and List-Based Bypass Execution

- Support for Service Port Conversion and Forwarding of Decrypted Packets

- Support for Detailed Configuration of Passive Mirroring Conditions for Decrypted Packets (IP, Port, Packet Direction)

- Support for Automatic Certificate Distribution by Redirecting Users Without Installed Certificates to a Certificate Provisioning Page upon Web Access

- Support for Integration with 3rd Party Solutions to Automatically Update Internal Users' Root CA Certificate Installation Status

- Support for Detection and Blocking of Invalid SSL Certificates

[Remote Browser Isolation]

- Support for Unified Web Security Functionality that Applies SWG Policies Even to Isolated Traffic

- Support for Granular Web Isolation Policy Configuration Based on User Identity and Destination

- Support for Configurable Web Isolation Targets Including Host, IP, URL Categories, and SaaS Application Lists

- Support for Configurable Control of File Upload and Download in Remote Browser Environments

- Support for Secure File Download in Remote Browser Environments through Malware Detection (Anti-Virus) and Content Disarm & Reconstruction (CDR)

- Support for Clipboard Control Functionality in Remote Browser Environments

- Support for Print Control Functionality in Remote Browser Environments

- Support for Watermark Display Functionality in Remote Browser Environments

- Support for Configurable Rendering Modes in Remote Browser Environments Including Video Streaming and Image Rendering

- Support for RBI Portal Functionality that Displays a List of Accessible Servers Based on the Logged-in User’s Access Permissions

[Operation & Convenience]

- Ensures Service Availability Without Downtime During Pattern Updates and Policy Changes

- Provision of Web-Based GUI Management Console Page Without Requiring Additional Program or Active-X Installation

– Support for Encrypted Communication Protocols (SSH, HTTPS) During Remote Access

– Support for Two-Factor Authentication (2FA) Using One-Time Password (OTP) for Administrator Login

- Support for Configurable Password Management Policies for Administrator Accounts Including Expiration Dates and Restrictions on Reusing Previous Passwords

- Support for Role-Based Access Control with Granular Permission Settings per Management Menu for Administrator Accounts

- Provision of Customizable Statistical Report Items Across Various Categories

- Support for Automatic Generation and Email Delivery of Traffic, System, and Report Data

- Support for Configurable Grouping Based on User, IP, URL, Host, and URL Categories

- Support for Unified Policy Lookup Across Users, IP Addresses, URLs, and Groups

- Support for Bulk Query of Web Security Policies with No Detection History During a Specified Period

- Support for One-Click Exception Handling to Reclassify URL Categories During Log Review

- Support for Configurable Bypass Conditions Including IP, Host, PKP Lists, HTTP Headers, and File Extensions

- Support for Real-Time Policy Synchronization Between Systems and Peer Authentication for Policy Sync Operations

- Support for Periodic Backup and Restoration of System Policy and Configuration Settings

- Support for Automatic Backup and Restoration of Policy Change History

- Support for Customizable Block Pages per Web Security Policy

- Support for Configurable Block Pages that Offer User Override Options with Accountability Tracking

- Support for Integrated UI Allowing Internal Users to Request URL Category Changes from Block Pages and Administrators to Process Them

- Support for Integrated UI Allowing Administrators to Request URL Category Reclassification Directly from the Vendor and Monitor Results in Real Time

- Support for Policy Testing Functionality that Performs Self-Validation Using Web Request and Response Data to Immediately Verify the Behavior of Generated Web Security Rules

- Support for Web Acceleration via Caching and Provision of Dedicated UI for Cache Status Monitoring

- Support for Multiple Email Integration Types Including SMTP, SMTPS, and AWS SES for Audit Log Delivery Upon System Anomalies

- Support for Integration with General-Purpose Messengers such as Telegram, Slack, and Discord for Audit Log Delivery Upon System Anomalies

- Support for Real-Time Monitoring of System Resources and Temperature with Threshold Alerts

- Support for SNMP GET and SNMP TRAP Configuration for Versions v2 and v3

- Provision of Operational Convenience via Open Web API Based on REST Architecture

- Provision of Various Troubleshooting Features Including TCPDUMP, Debugging, and Automatic System Recovery via User Interface

[Department & User Management]

- Support for Multi-Tenant Functionality Enabling Department-Specific Independent Security Policy Configuration

- Support for Unregistered Department Functionality to Apply Web Security Policies to Unregistered Users

- Support for Department and User Integration via CSV File Upload, Database, and LDAP Connectivity

- Support for User-Specific Expiration Date Assignment and Automatic Deletion Functionality

[Log Management]

- Support for Real-Time Logging and Querying of Web Access Records for All Users

- Support for Real-Time Logging and Querying of Decrypted Plaintext Data (Request/Response)

- Support for Visibility Enhancement by Highlighting Detection Evidence within Decrypted Plaintext Data in Detection Logs

- Support for Real-Time Logging and Querying of TLS Session Encryption and Decryption Processes

- Support for Real-Time Logging and Querying of IP, Port, and SNI Information for Bypassed Encrypted Traffic

- Support for Real-Time Audit Logging and Querying of System Operation History and Configuration Changes

- Support for Log Transmission and Customizable Format Settings for Integration with SIEM/SOAR Systems

- Support for Various Log Transmission Protocols (UDP, TCP, SSL, etc.) for Integration with SIEM/SOAR Systems

- Support for Configuring Distinct Log Formats for Each SIEM/SOAR System Integration

- Support for Detailed Policy Configuration for Automated Log Management and Data Protection Compliance, Including Retention Period Settings, Backup Path Designation, and Deletion Conditions