The Best Solution for Integrated Internet Access Management

eWalker SWG V9

Copyright ⓒ 2018. SOOSAN INT. All Rights Reserved.

Doc. No. 2018-SEA-SM0001-v1.0.0

CONTENTS

Ⅰ Introduction

- Why SWG is needed
- Increase of threats hidden within SSL traffic

Ⅱ Product Information

- eWalker SWG V9
- Features of eWalker SWG V9
- Detailed functions
- Deployment options
- Benefits

Ⅲ Appendix

- Function table
- Product lineup

Ⅳ Company Profile

- Company overview
- Products
- Major references

I Introduction

- Why SWG is needed
- Increase of threats hidden within SSL traffic

Why SWG is needed

Are you ready for the 'Working 52 Hours a Week' that started at 2018. 7. 1?
(The revised Labor Standards Act, Korea)

As the 'Working 52 Hours a Week' was enacted, you need to improve work efficiency further.

Revised Contents

'Working 68 hours a week' → **Reduced to 'Working 52 hours a week'.**

40 Hours					12 Hours	
Mon	Tue	Wed	Thu	Fri	Sat	Sun

When Caught for Violation,

Imprisonment for up to 2 years or fines of 20 million KRW.

Enforcement Date

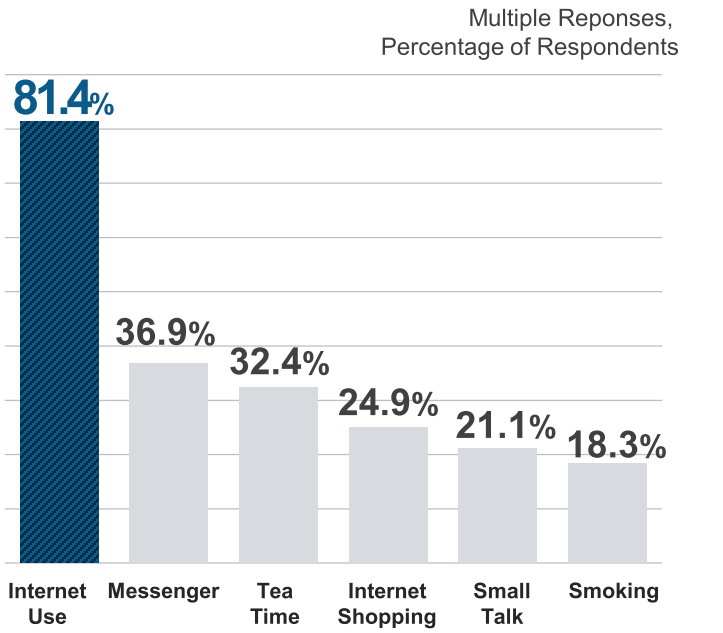
Company Size	Date
A company with 300 or more employees	Jul. 1st, 2018
A company with a number of employees between 49 and 300	Jan. 1st, 2019
A company with a number of employees between 4 and 50	Jul. 1st, 2021

Why SWG is needed

The access to Non-business site can be a main cause of decreasing work efficiency.

Nonoccupational Individual Acts

"Using Internet is ranked at top"

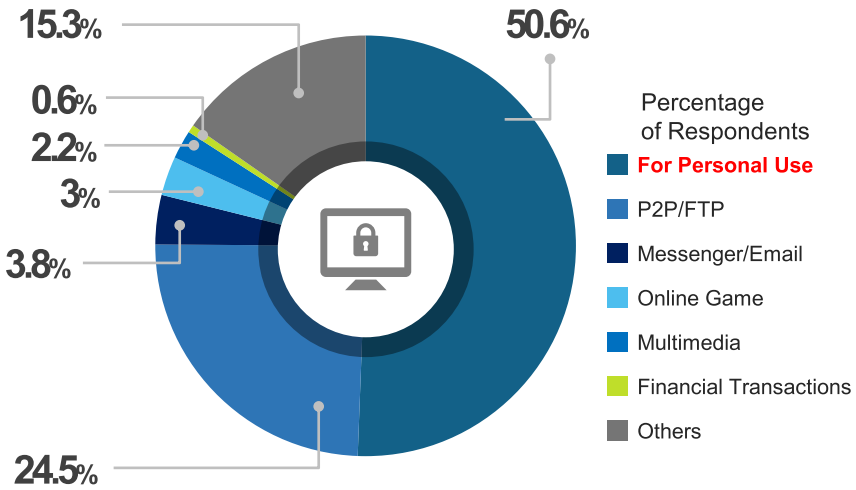


Source: Saramin, A Survey of Empty Labor at Work, 2017

Internet Usage of Many Organizations

Due to the top-ranked individual use of Internet,

"Unnecessary Increase in Traffic"



Source: NSTEK, A Survey of Internet Usage at Industries, Universities, and Public Organizations, 2016

Increase of threats hidden within SSL traffic

Bright side and Dark side of SSL traffic

Bright Side

To strengthen the data security,

" Using SSL traffic is increasing "

84% of Top 50 Sites are using SSL for communication.

Dark Side

Hidden within SSL traffic,

" Security threats are rapidly increasing "

The existing security solutions are not capable of analyzing SSL Traffic.

Increase of threats hidden within SSL traffic

Upsurge in SSL traffic

Email, SNS, and etc.
Increasing use of SSL Traffic

OUTLOOK

Facebook

Gmail

YouTube

Of web traffic in 2019,
Up to 80% will use SSL

Gartner predicted 80% of web traffic to be encrypted by 2019.

Strengthening laws of information security
Mandates to use SSL

U.S. government agencies started to use only SSL for their network communication since 2017.

The Abolition of Authentication Certificate or Active-X
Increases in using SSL

KISA

activex

Government announced the end of mandatory use.

Increase of threats hidden within SSL traffic

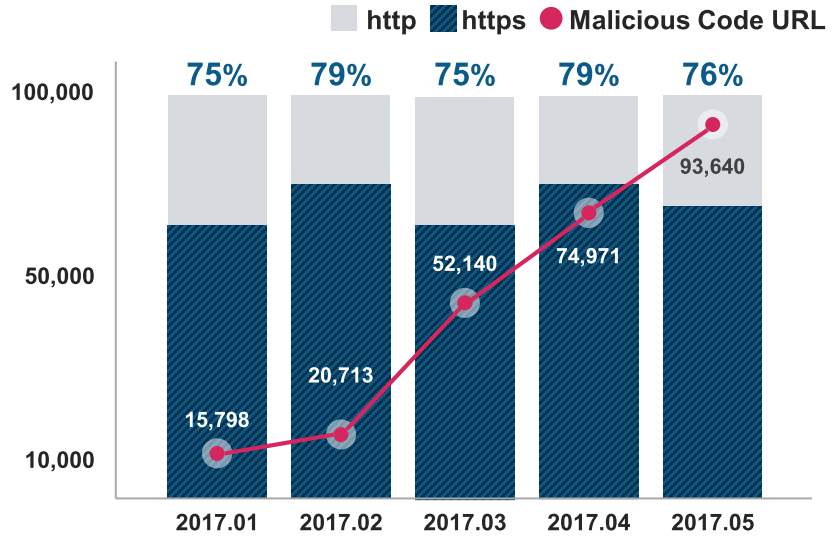
Walker SWG V9

Using Integrated Internet Access Management,

You can prevent threats hidden within SSL traffic proactively.

Increase of Malicious URLs Making Bad Use of SSL Traffic

- **More than 75% of web traffic is SSL traffic.**
- **Detected malicious URLs are rapidly increased to 90 thousand at May 2017.**



Source: Web Traffic Use Rate and Malicious Code Growth | SOOSAN INT

Detection of Malware Hidden Sites

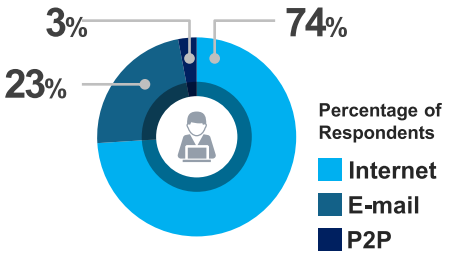
No. of stops on the intrusion routes

145% increased!

Immediately after accessing, a user PC is infected with the malicious code.

Source: Web Traffic Use Rate and Malicious Code Growth | SOOSAN INT

Routes for Ransomware Intrusion, 2017



Top ranked-ransomware intrusion route in Korea,

Internet

To prevent ransomware; Internet Access Management Solution is essential.

Source: Web Traffic Use Rate and Malicious Code Growth | SOOSAN INT

Ⅱ Product Introduction

- eWalker SWG V9
- Features of eWalker SWG V9
- Detailed functions
- Deployment options
- Benefits

eWalker SWG V9,
A qualified Integrated Internet Access Management solution

Control over Harmful Sites

- Prevents security threats such as malicious code.
- Detects malicious code.

The Nation's Largest DB Provider

- Provides highly qualified/nation's largest DB.
- Runs a dedicated search program for each field with search experts.
- Manages URL and IP information through DB Update.

Internet Access Control and Integrated Management

- Blocks the access to non-business/harmful sites and integrates them to manage.
- Monitors total traffic and supports log generation.

Visibility into SSL Traffic

- Has visibility over entire network traffic.
- Eliminates blind spots within SSL traffic.

Interworking with the Existing Security Appliances

- Configures Decrypted Zone for SSL traffic.
- Provides the existing security appliances with decrypted traffic.
- Builds safe Internet network environment.

Various Supports for Rule-Based Policies

- Supports various environment for policy establishment.
- Supports for blockings, contents, exception, and logging policy.

Features of eWalker SWG V9

Control over Harmful Sites

Having partnerships with the local professionals and
a CERT team which analyzes malicious DB,

eWalker SWG V9 supports for the latest harmful/malicious DB

SK infosec

SECUDIUM INTELLIGENCE

Threat Intelligence Service reflecting the security control know-how of SK Infosec.

SOOSAN INT

A global company specialized in security solution,

SOOSAN INT creates clean and safe Internet environment using SOOSAN INT's own technological know-how.

Korea Internet & Security Agency

Healthy and safe Internet environment, leading national competitiveness.

- Nation's top security control company
- Works together with SECUDIUM, SK Infosec's security control system.
- Updates Harmful/Malware DB on a regular basis.

- Real-time response to threats
- Analyzes specific DBs to which many users access.
- Monitors and manages certain sites with history of infection persistently.

- Static analysis based on own DB
- Responses to the newest malicious attacks using dynamic analysis.
- Works together with KISA by sharing the Harmful/Malware DB.

Features of eWalker SWG V9

eWalker SWG V9

The Nation's **Largest DB** Provider

DB Update on a Regular Base

Collects **DB**. → Analyzes sites. → Structures **DB**. → **Distributes.**

- A real-time & daily update
- A frequent update of urgent & important URLs
- The KCC provides a harmful/malware DB → Applies to our own DB.
- A DB update responding to customer's request.

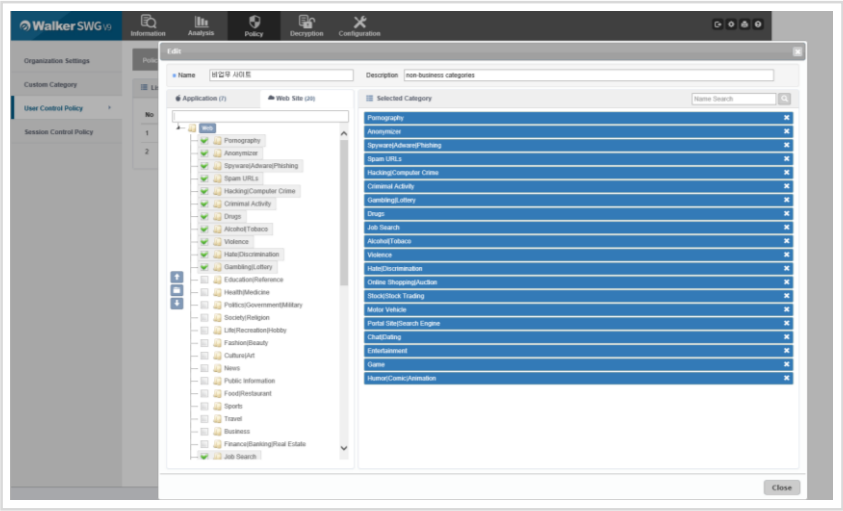
DB Collection by the Professionals **Update Process**	Collects **URL** Links.	Edits **URL**s.	Normal **URL** / Harmful **URL**	URL Distribution / Image Distribution	**URL DB**
	URLs as a result of collection	Deletes repeated URLs.	Classifies DBs.	Classifies harmful sites and verifies.	**Update**
Systematic Process Management **Verification Process**	A List of Candidates' at 1st Round	A List of Candidates' at 2nd Round	A List of Foreign Candidates	A list of Final Candidates	**A List in Operation**
	1st Verification	2nd Verification	Overseas Management System	Final Verification	**Validation**

- Operates the malicious DB collection using the professionals and updates the DB using an automatic updates system.
- Operates both KCC-supplying DB and own malicious DB simultaneously (refined DB containing more than 1,000 data).
- Provides regular updates and real-time updates due to customer requests.

Features of eWalker SWG V9

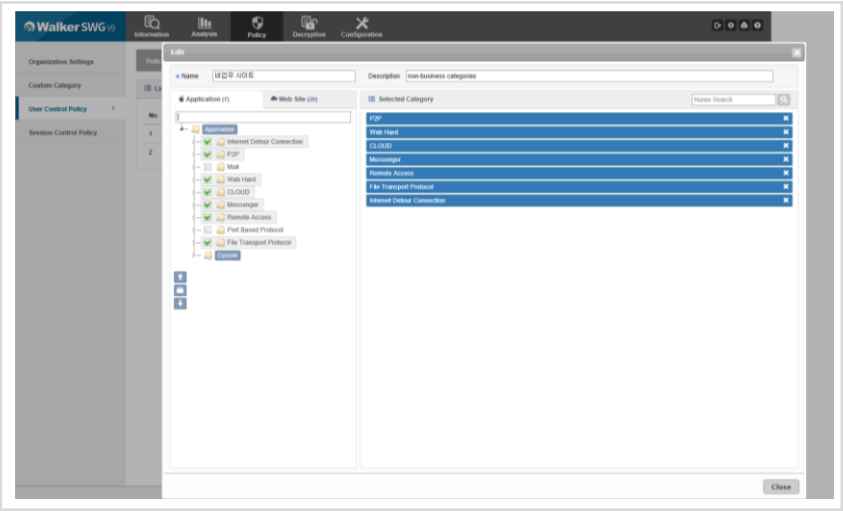
Internet Access **Control** and **Integrated Management**

Controls of Web Mail, P2P, Web Hard and Cloud



Control of Mail Receiving/Transmitting

- Performs the control process or blocking process for each category of normal mail and web mail respectively.
- Blocks entire mails or controls/blocks a mail depending on whether it is a received mail or a transmitted mail.
- Controls the process of receiving or transmitting encrypted web mails.



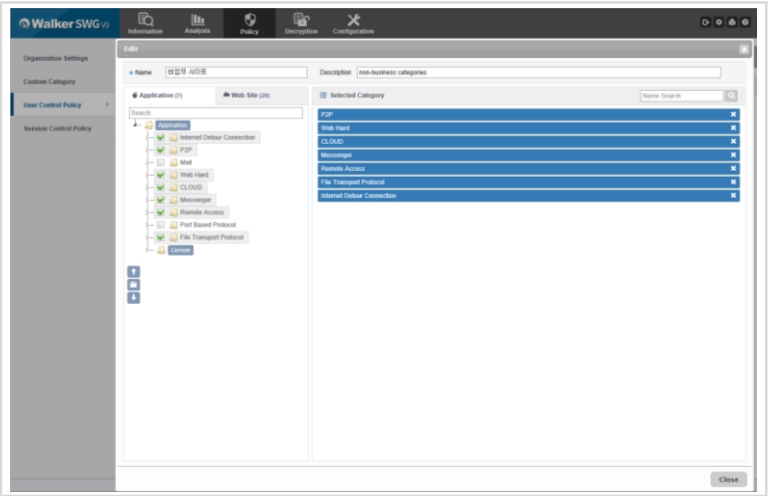
Control of P2P, Web Hard, and Cloud

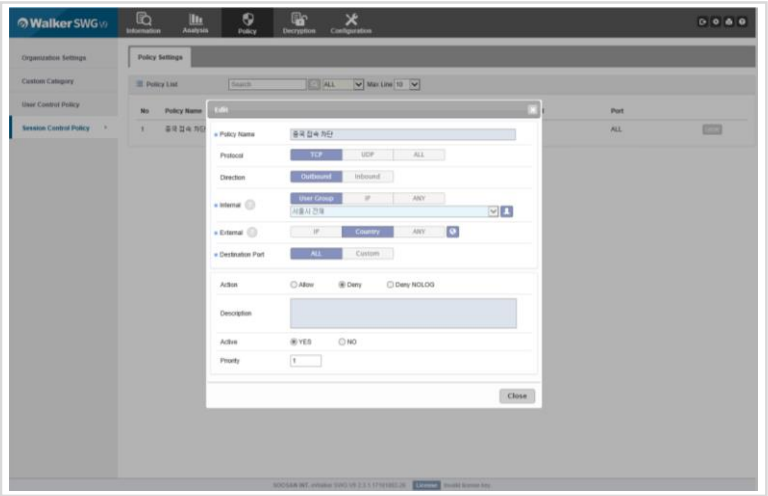
- Control over the sites such as P2P, web hard, and cloud where files are received or transmitted.
- Blocks simple URL, or controls the pattern based P2P or cloud sites.

Features of eWalker SWG V9

Internet Access **Control** and **Integrated Management**

Anonymizer Control and Session Control Policy





Anonymizers, Torrent, App Control

- By having visibility into SSL traffic, can set and use functions which wasn't effective before.
- Completely controls Anonymizers, Torrent, Messenger, stock HTS, and other Apps.

Session Control Policy

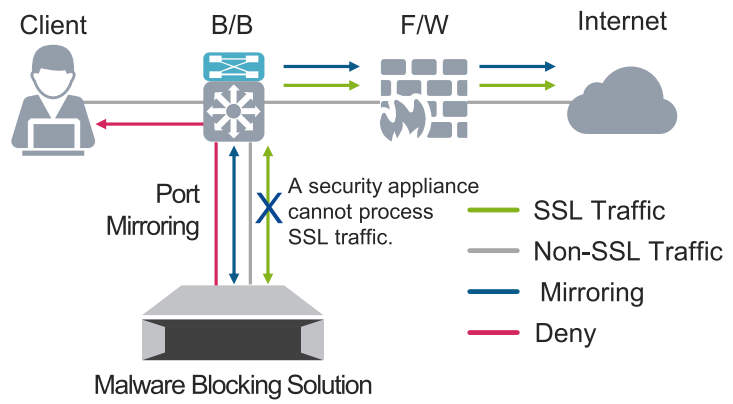
- Not just works on URLs, but controls a session for each protocol or IP.
- Is capable of setting to block the origins and the destinations, as well as options for log and access.

Features of eWalker SWG V9

Visibility into **SSL Traffic**

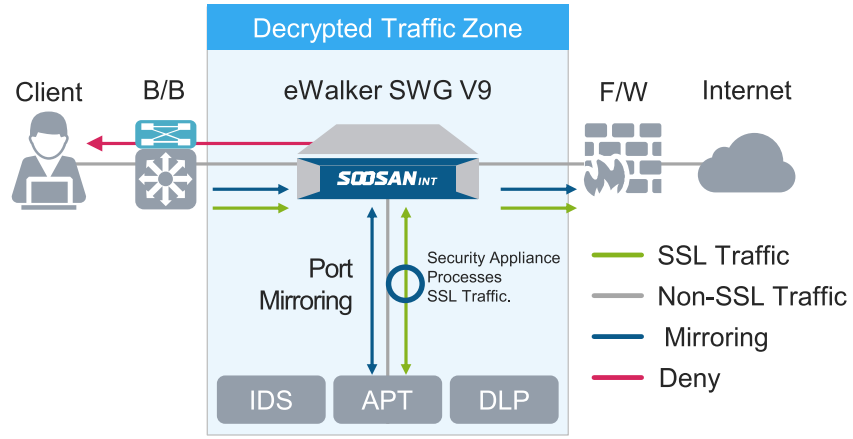
- eWalker Security V7 — Limited access control over encrypted traffic
- eWalker SWG V9 — Minimizing impact on the network, provides visibility into entire SSL traffic.
  Manages network resources systematically by blocking harmful sites and managing/controlling Internet use.

An Existing Product



DNS Blocking	IP/Port/URL Blocking
DNS Proxy Tech.	IP/Port Filtering
DNS Hijacking Tech.	URL Filtering

eWalker SWG V9

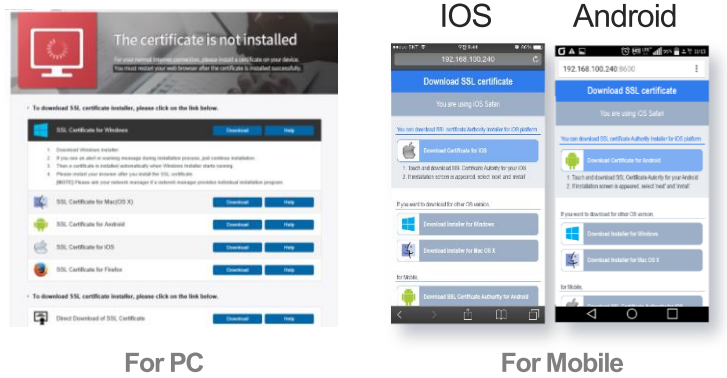


Visibility into Entire SSL Traffic
Non-business/Harmful Sites Access Control
Works with Existing Security Appliances

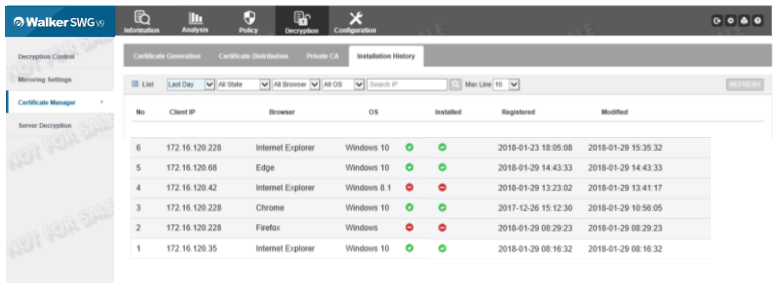
Features of eWalker SWG V9

Visibility into SSL Traffic

Certificate Installation Redirection and Status Management



Automatically redirects users to a corresponding certificate installation page for each OS.



Manages the status of certificate installation and distribution for internal users.

Redirects a Certificate Installation

- Distributes user certificates or redirects a user to a certificate installation page automatically or manually.
- Creates a certificate corresponding to a company information and distributes to a client. In addition, directly manages it.

Provides the Convenience of Certificate Operation and Management

- Easy distribution of a certificate for a user who was left off the pre-distribution by NAC, PMS, or Active Directory.
- Quick response against PC change or OS format which you may encounter during operation.
- Supports for various operating environment such as Windows, Mac, Android, iOS, and others.

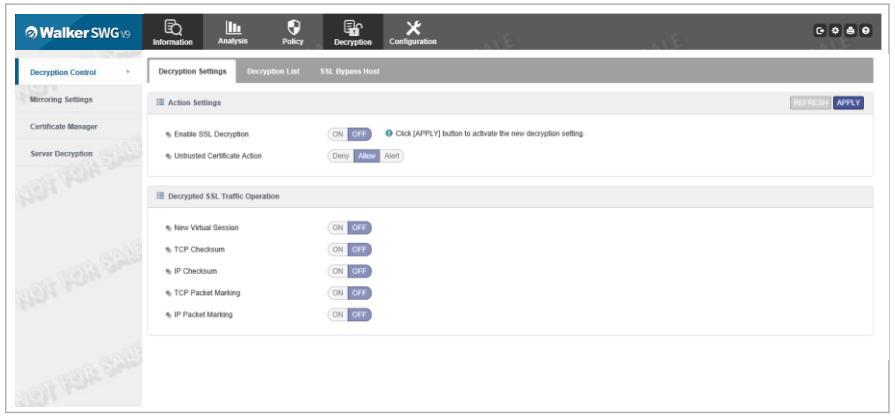
Provides Easy Management of Installation Status

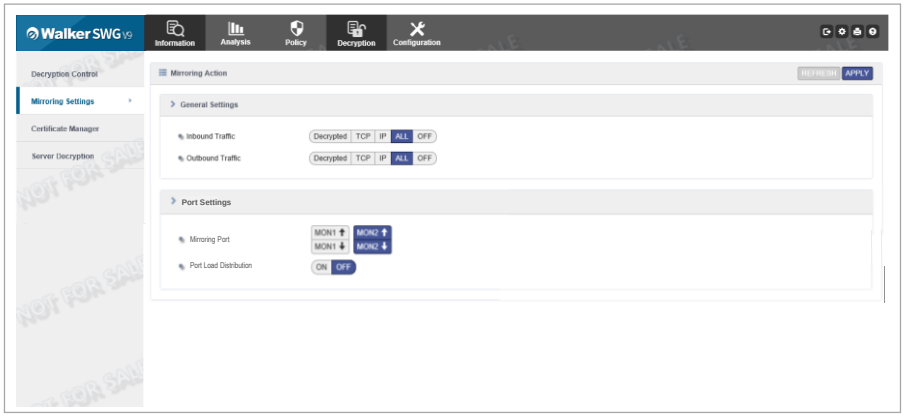
- Client information management who installed a private certificate for SSL decryption.
- Information management of installation environment and distribution of a SSL certificate.

Features of eWalker SWG V9

Interworking with the Existing Security Appliances

Settings for the process of 'interworking with other appliances'





Sets Options for the Process of 'Interworking with Other Appliances'

- Allows to set the decryption options for the process of 'interworking with other security appliances' in accordance with each appliance's feature.
- Allows to interwork with other security appliances without any change of network architecture (cost effective).

Various Methods to Interwork

- Supports two modes of interworking:
  - Active (In-line) mode
  - Passive (Mirror)
- Supports for setting options for Active mode and Passive mode to connect with 3rd party security appliances.

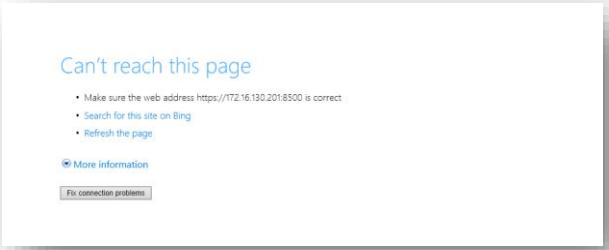
Features of eWalker SWG V9

Interworking with the Existing Security Appliances

M.P.T (Message Pass Through) allowing to check the original Blocking Message

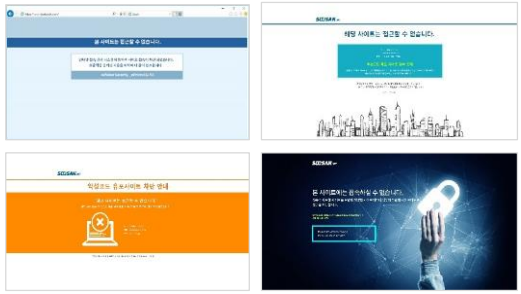
Other Decryption Solutions

Cannot Display their Blocking Page!



eWalker SWG V9

Can Display Various Blocking Pages!



Displays the Blocking Messages Transmitted from Other Security Appliances

- Provides a RST packet to match to an original session after modifying a blocking packet (RST packet) sent by a connected security appliance.
- Displays an original blocking message sent by a 3rd party security appliance when a certain site (HTTPS site) is blocked to be accessed.

Provides Management Convenience for a User

- A user can recognize an appliance to which the security policy the user violated belongs.
- A user can easily troubleshoot and configure policies when working with 3rd party appliances such as APT, SWG, and DLP.

Features of eWalker SWG V9

Interworking with the Existing Security Appliances

Interworking with many different network appliances in various successful projects!

Walker SWG

AhnLab MDS

AhnLab

Sniper IPS

WINS

FireEye NX

FireEye

Deep Discovery

TREND MICRO

MFI

SECUI

NetCenter

COMTRUE Technologies

Hyboost

SOMANSA

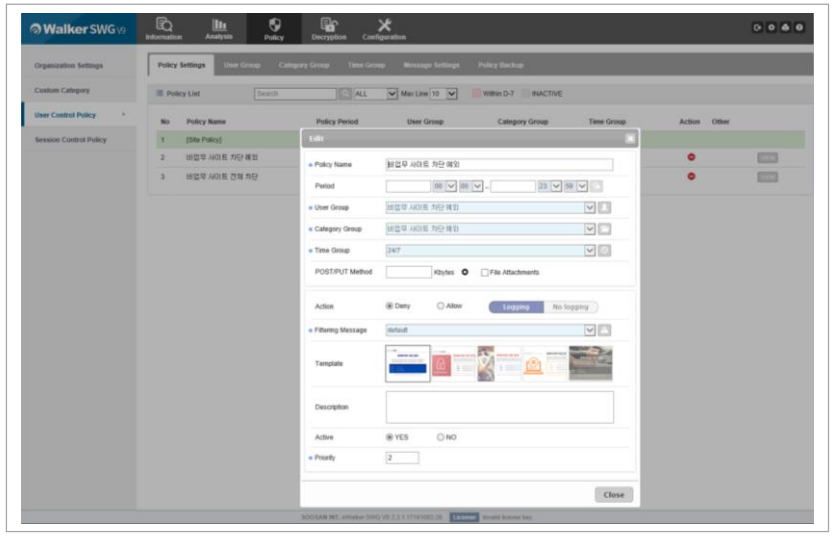
eWalker

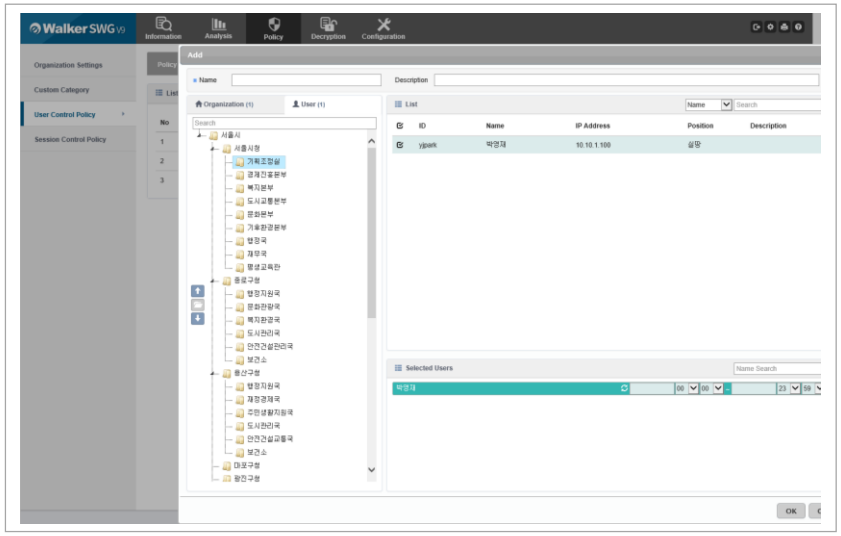
SOOSAN INT

Features of eWalker SWG V9

Various Supports for **Rule-Based** Policies

Various Blocking Policies and User Settings





Blocking Policies

- Controls and blocks Web Sites for each category.
- Sets up object sites, blocking time, and policy valid period for each user group.
- Applies effective blocking policies with 10 million URLs of Refined DB and 148 categories.

User Settings, an object of a policy

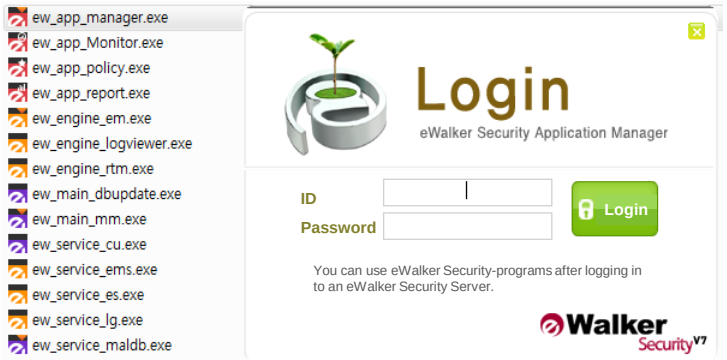
- Sets a user as an object of a URL blocking policy.
- Sets a user as a group, a team, an individual, or a special user.
- Classifies a user in accordance with a personnel DB of a company.

Features of eWalker SWG V9

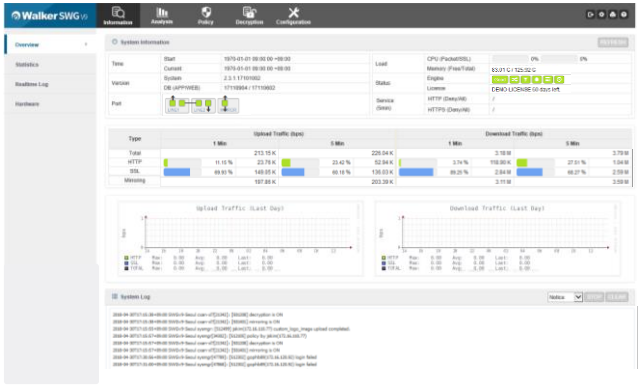
Web-based **Management Page**

Enhanced convenience of management by changing the existing management methods

Existing Products – App Management Tools



eWalker SWG V9 – Web Management Page



Changed an Operation System

- Changes the operation system from Windows Server-based to Linux-based, and increased the log search speed.
- Puts less weight on licenses of existing OS and DBMS.

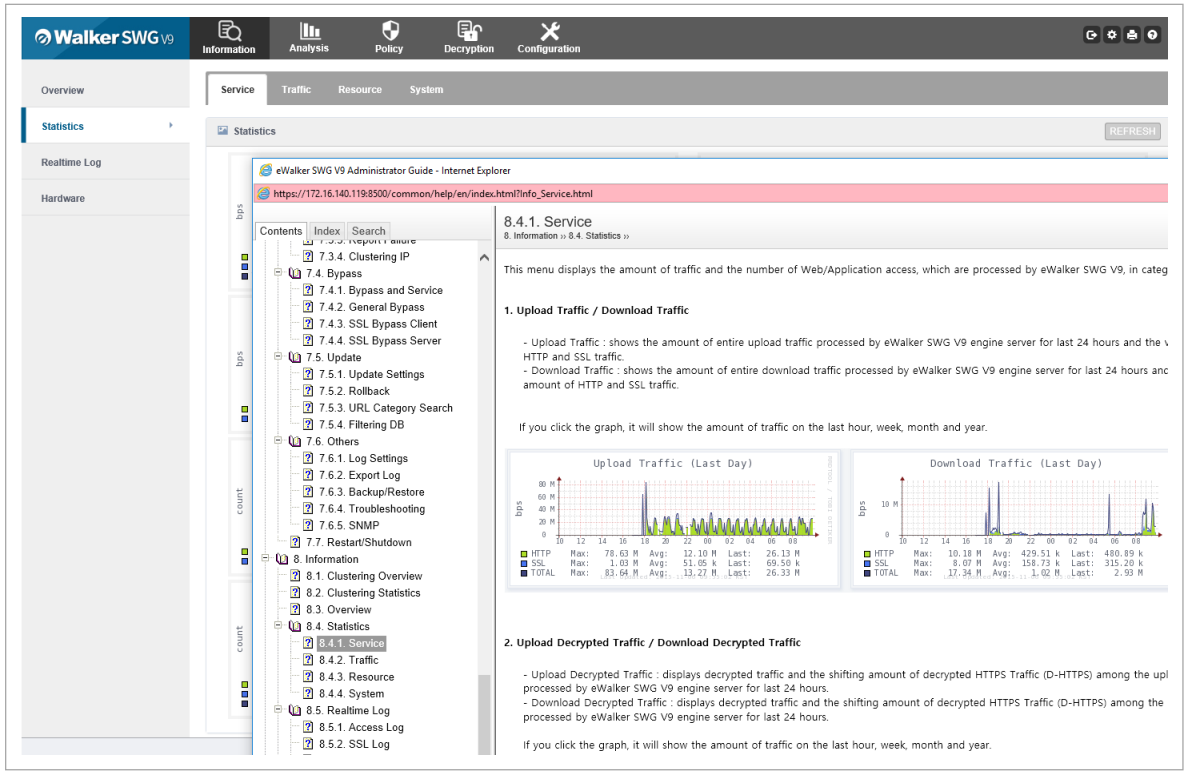
Changed a Management Method: App-based ➡ Web-based

- Enhances a convenience of an administrator with a web-based management page.
- Provides reliable control and management without any impact of an administrator's PC environment.

Features of eWalker SWG V9

Online Help

Immediate help with Online Help



Online Help

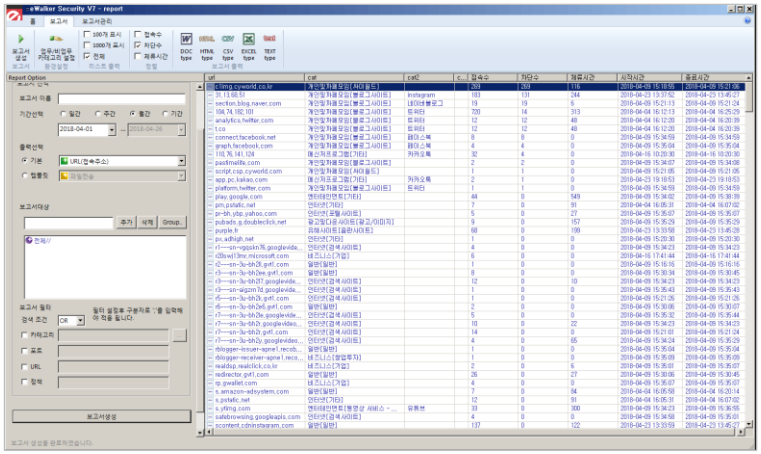
- Allows to check immediately using Online Help, when an administrator needs help for operation.
- Our Online Help displays automatically a help page corresponding to a menu which an administrator is currently viewing.

Detailed functions

Reports and Statistics

Big Data-based, various Traffic Analysis Reports and Statistics

Existing Products – App Management Tools



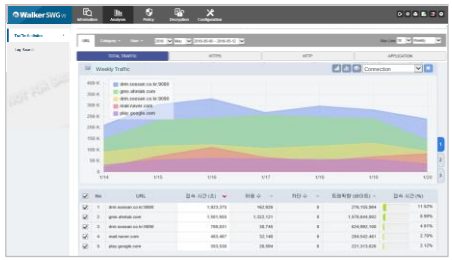
Application Based,

- Provides a function of search or statistics allowing various options in accordance with the analysis of the Internet contents supplied to a user.

Standard

Bid Data

eWalker SWG V9 – Reports and Statistics



Web Based,

- A function of search or statistics allowing various options.
- A function of analysis and statistics of decrypted traffic.

Elastic Search Based,

- A function of fast search or statistics allowing various options.
- A function of analysis and statistics of decrypted traffic.
- Large volume of data processing and real-time analysis processing.

Detailed functions

Reports and Statistics

Customizing the DB Sharing;

Automatic Updates using the Personnel Information

Sharing the Personnel Information

ID No.

Name

Position

IP

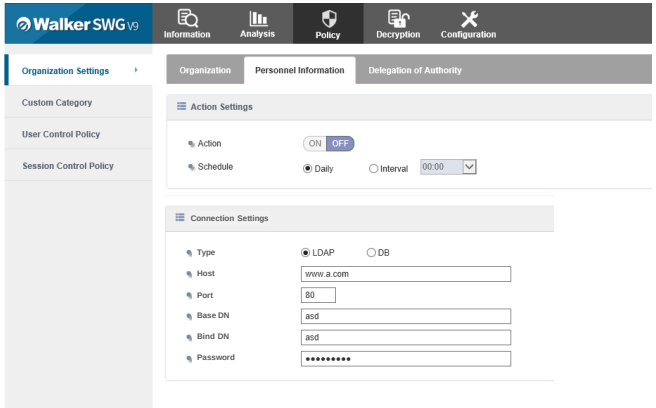
Group

Duty

- Shares Personnel DB: Group, user, position, and etc.
- Interworks with NAC System: IP, user information
- Uses LDAP (Lightweight Directory Access Protocol) for a process of interworking.
- Configures to block all unauthorized users from accessing to Internet sites.

Collects Shared Information

Update and Application



- Classifies/registers clients automatically.
- Updates by using the personnel information when adding users or changing group or IP.
- Applies the same policy for the blocking process or the exception process without initialization.
- Checks system condition and operating condition in real-time.

Detailed functions

eWalker SWG V9 Special Features

A proven solution for Integrated Internet Access Management, which provides SSL visibility

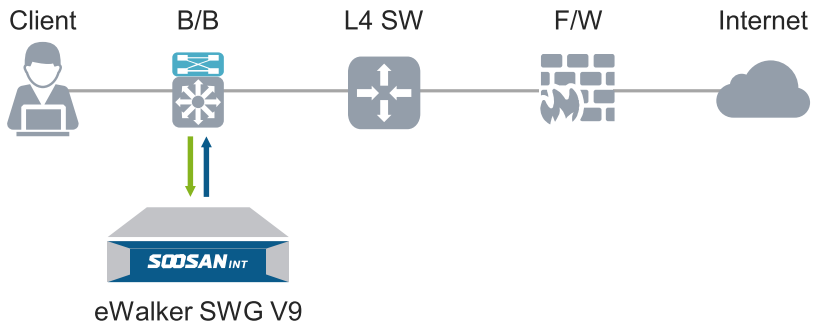
Walker SWG V9

Harmful SNS **Contents Filtering**	Malicious Code's Spread and Origin **Access Blockings**	Private Certificate **Creating and Maintaining**	The Newest URL Category **Automatic Update**
External Security Appliances **Blocking a Message Transfer**	Certificate Automatically/Manually **Distribution**	Category, Keyword, etc. **Detailed Blocking Functions**	Encrypted Traffic Decryption **Provides Visibility**

Deployment options

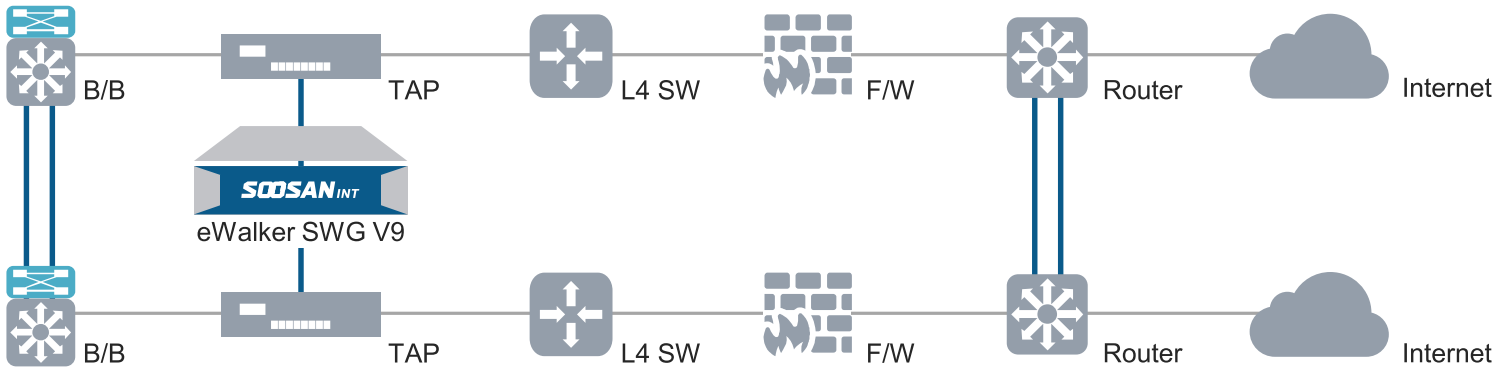
Various Deployment Modes - **Mirror Mode**

Mirror Mode



- Supports for a deployment that doesn't have any impact of the network.
- Controls HTTPS or harmful sites by blocking specific DNS.
- Receives Internet access traffic of a user PC through Mirror Port.
- Transmits Blocking Packets to a user PC through a blocking Port connected to B/B.
- SSL decryption is not available.

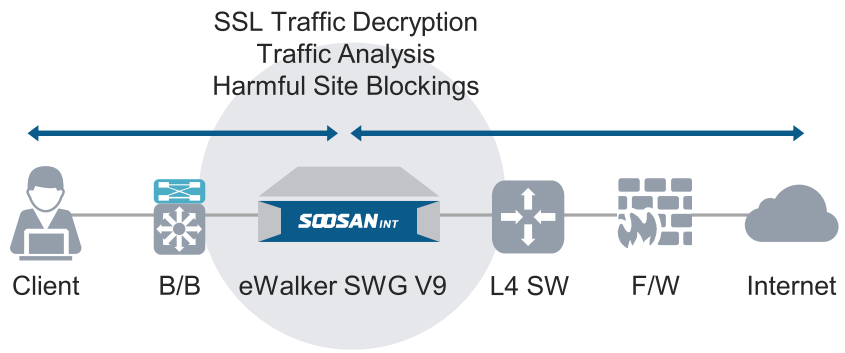
Case Study
(Construction Company H)



Deployment options

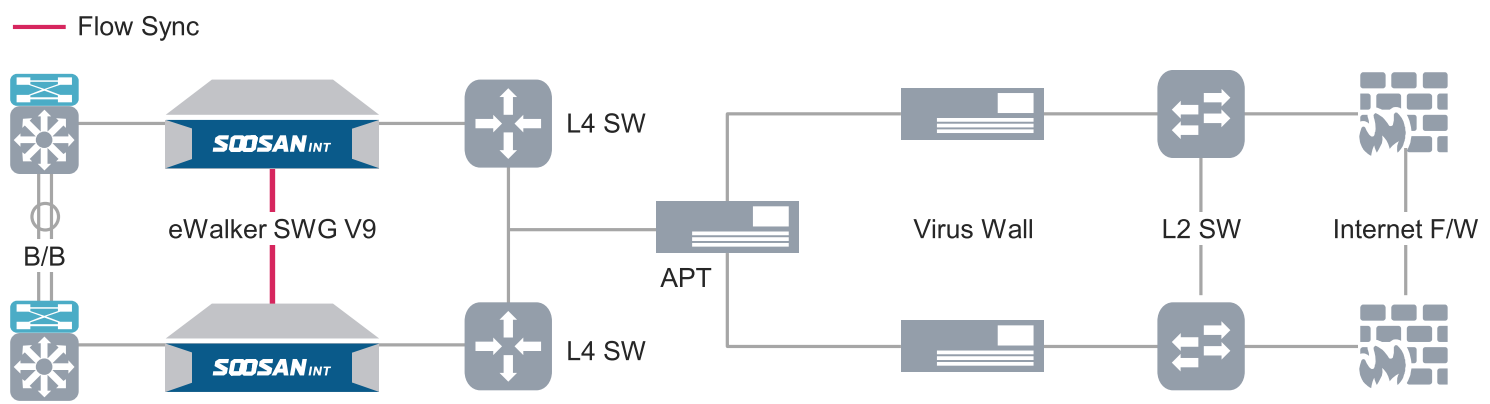
Various Deployment Modes – **Inline Mode**

Inline Mode
(Transparent Mode)



- Installs eWalker SWG V9 (Transparency) on a network path.
- Monitors all ports and decrypts SSL traffic selectively.
- Transmits Blocking Packets through Bridge Interface, if a client accesses to a harmful site.
- Blocks detailed issues of HTTPS sites such as Rx/Tx of Web mail, selective Google services, specific SNS accounts, and etc.

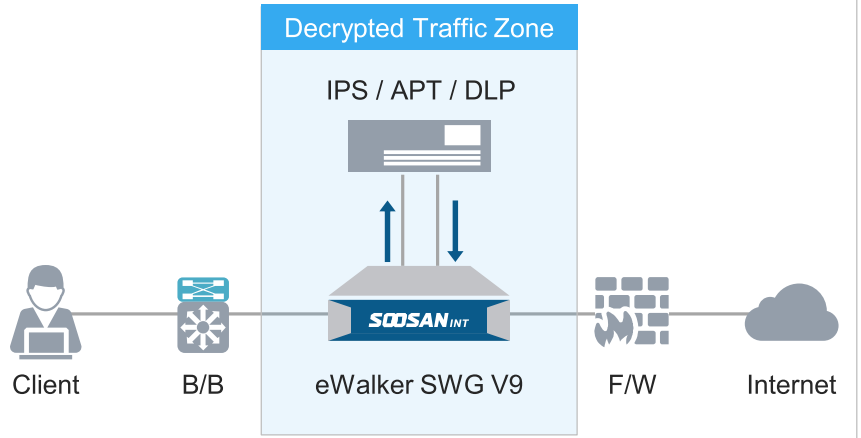
Case Study
(Financial Company A))



Deployment options

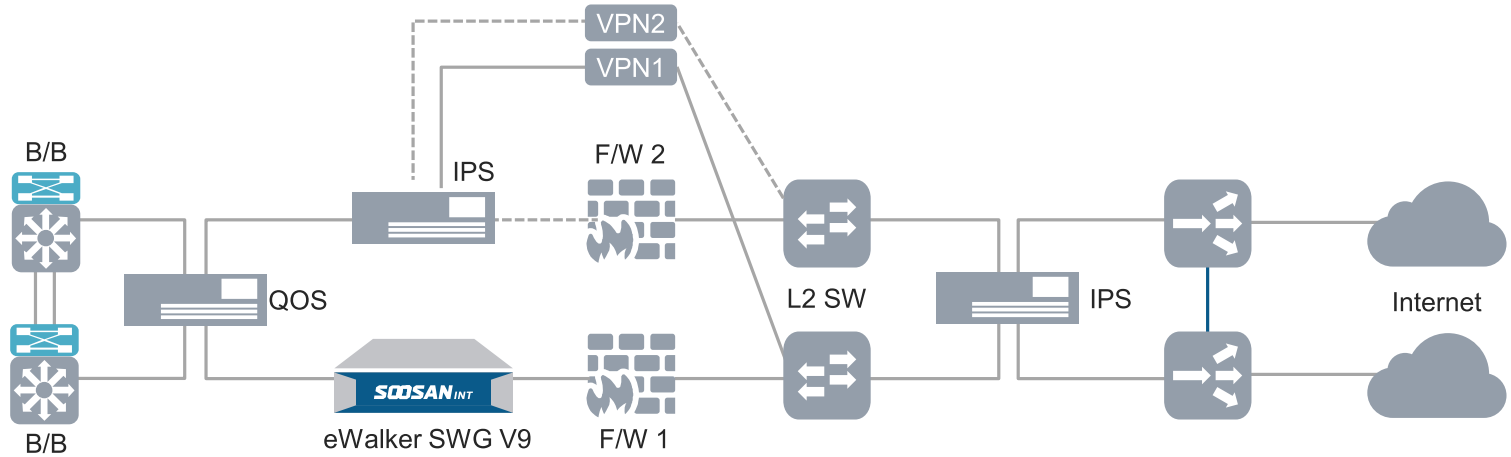
Various Deployment Modes – **Inline Mode**

Inline Mode
(Transparent and DTZ Mode)



- Installs eWalker SWG V9 (Transparency) on a network path.
- Monitors all ports and decrypts SSL traffic selectively.
- Provides decrypted data for other security appliances passing through DTZ (Decrypted Traffic Zone).
- Transmits Blocking Packets through Bridge Interface, if a client accesses to a harmful site.
- Blocks detailed issues of HTTPS sites such as Rx/Tx of Web mail, selective Google services, specific SNS accounts, and etc.
- Interworks with other security appliances (IPS, APT, DLP, etc.)

Case Study
(Manufacturer S)



Benefits

Benefits of Integrated Internet Access Management

Proven-System Reliability

- Offers the optimum reliability for a base system.
- Allows to operate reliable network by providing immediate technical support.
- Has been proven and received excellent marks in the field of network security by many public/financial enterprises.
- Helps in providing reliable services with the nation's largest DB.

SSL Traffic Visibility

- Prevents web security threats in advance by having visibility into encryption traffic.
- Avoids infection with malicious code or ransomware.
- Perfectly responds to the encrypted traffic by interworking with existing security appliances.
- Provides Internet users with reliability by strengthening security over the network.

Work Efficiency Enhancement

- Blocks non-business sites regarding stock trading, Internet shopping, Messenger, and etc.
- Blocks harmful sites and file sharing sites.
- Distributes internal traffic efficiently and enhances resource utilization due to the decrease of unnecessary traffic.

Enterprise Security Level Enhancement

- Understands and prevents potential factors of threats against data assets.
- Enhances public images and customer confidence by building information security solutions.
- Complies with security compliances tightened up every year.
- Reduces social and economic cost resulted from damage of a security accident.

Ⅲ Appendix

- Function table
- Product lineup

Function table

eWalker SWG V9 Detailed Functions

Decryption

- Control over encrypted traffic (decryption, blockings, mirroring, logging, etc.)
- Blockings of Internet anonymizers
- Decryption Bypass for specific users
- 5 tuple maintaining to provide encrypted traffic transparency
- Private certificate for re-encryption
- Automatic/Manual distribution of a certificate
- Installation of a private certificate using multiple browsers
- Interworking process with other security appliances by converting decrypted traffic into plaintext.
- Display of an original blocking message which was generated by an 3rd party appliance
- Supports for TLS 1.0, TLS 1.1, TLS 1.2, and SSL 3 Encryption
- Supports for RSA/DH public key algorithms
- Supports for AES/3DES/DES/RC4 symmetric key
- Supports for 2048/4096/8192bits RSA keys
- Supports for IPv6/VLAN Tagging (802.1Q)
- Supports for POP3S/SMTPS/FTPS/IMAPS/HSTS/QUIC
- Above protocols are available both for default ports and unknown ports

Configuration and H/W

- Duplex deployment of equipment & bypass (including S/W bypass)
  - ✓ Duplex deployment of equipment power
- A single equipment can be deployed in an Active (In-line) mode or a Passive (Mirror) mode.
- LLCF & ideal switching to the backup line when failure occurs.
- Packets are transmitted to the security system which is connected in inline configuration even in Bypass condition.

DB

- Has 10 Millions of URL DB lists & more than 148 categories
- Supports for the public key- based license information input module which is required for update server denial prevention.

Blockings

- Keyword blockings
- Internet anonymizers blockings
- Selective blockings of receiving/transmitting web mail
- Selective controls of service or App such as stock-HTS, Torrent, Messenger, video, game, web hard, P2P, remote control, etc.
- Selective controls of HTTPS service such as Google's Gmail, Docs, and Drive.
- Blockings of malicious code's distribution, and stops on the paths.
- Blockings of trolling by Korea Communications Standards Commission
- Blockings for a country (provides for a selective country).
- Blocking-bypass policy

Management and Reporting

- Client registration using an automatic function of searching PC information.
- Permission settings for each account, administrator audit
- Account lock-out for 5 consecutive failures of login attempts
- Encryption and storage of important system information
- Rule-based policy
- Exception policy for each client
- Detailed reports
- Supports for various output of a report such as in Excel, CSV, PDF, or etc.

Monitoring

- Check of real-time server condition which is displayed on a real-time monitoring screen (server condition: CPU, Memory, HDD Usage, Network Traffic).
- Real-time monitoring of entire traffic, encrypted traffic, decrypted traffic
- Monitoring of hardware condition, NIC, and external appliances' interworking mode

Product lineup - eWalker

Product Lineup

Network Type Appliance (Support NIC Type 1G/10G)

As an Internet Access Control System passed through SOOSAN INT's own Performance Test and Reliability Test,

All-In-One Hardware System without Any Change of the Network Architecture.

Small Scale Network | **Medium Scale Network** | **Large Scale Network**

IV Company Profile

- Company overview
- Products
- Major references

Company overview

Walker SWG V9

“ Delivering Innovative Security Solutions and Service ”

Security Solutions

- No. 1 seller in the public organization market!
- The network security solution chosen by 1,000 client companies
- Offering network and data security solutions

Platform Business

- Has been providing platform-based Device Authentication Service for Korea’s 4 major telecoms for over 10 years.
- Value creation though big data analysis on standard infrastructure
- Most traffic analysis know-how in Korea

2018
SOOSAN INT
Credit Rating

March 2018
SOOSAN INT
Patents Holding

Company Name	SOOSAN INT Co., Ltd.
Date of Est.	March 4th, 1998
C.E.O.	Chung Suk Hyun, Lee Sung Kwon
Capital	KRW 3.37 billion
Employees	101 (as of March 2018)
Business Area	Software development and supply (Network access management solution, etc.)
Affiliates	SOOSAN Industries Co., Ltd. SOOSAN Heavy Industries Co., Ltd. SOOSAN ENS Co., Ltd. SOOSAN Hometech Co., Ltd.

HQ Seoul Korea

3rd Fl., Suseo Hyundai Venture-ville, 10, Bamgogae-ro 1-gil, Gangnam-gu, Seoul, Korea 06349

Tell 82. 2. 541. 0073 | Fax 82. 2. 541. 0204
E-mail gb@soosan.co.kr | HP http://www.soosanint.com

R&D Center Hanoi, Vietnam

Keangnam Hanoi Landmark Tower,
Mễ Trì, Từ Liêm District, Hanoi

Products

Walker SWG V9

SOOSAN INT

Walker SWG V9

Integrated Internet Access Management Solution

- A business efficiency solution.
- Controls access to HTTPS sites.
- Has visibility into SSL traffic.
- Includes the nation's largest URL DB.

Prism SSL VA

SSL Visibility Solution

- TST-based visibility into TLS/SSL traffic at all ports.
- Since 5-tuples are not modified, can be installed in existing networks without changes to the network architecture

ReD HYPERVISOR SECURITY

Virtualization-based Next Generation Security Solution

- 1st application of VMI in Korea
- Next Generation Hypervisor Security Solution
- Data security solution applicable across industries

Walker Security V7

Non-business Sites Blocking Solution

- The highest share in the Korean government sector.
- Chosen by over 1,000 clients
- Korea's largest DB
- Controls access to non-business/harmful sites, with integrated management.

Major references

Walker SWG V9

Industrial Sector

- Hyundai
- Hyundai Engineering & Construction
- Hyundai Department Store Group
- KIA
- SsangYong
- Korean Air
- Woongjin
- Coway
- Kyowon 교원
- MBC
- EBS
- Hankook
- KCC
- Hanjin Heavy Industries & Construction Co., Ltd.
- Iljin
- Kumho Petrochemical
- HDC Hyundai Development Company
- kt telecop

Financial Sector

- KDB Bank
- KEB Hana Bank
- Korea Eximbank
- Mirae Asset Securities
- Mirae Asset Life Insurance
- Hyundai Marine & Fire Insurance
- Hyundai Capital
- Hyundai Card
- Hyundai Life
- Allianz
- KB Insurance
- Hanwha Life
- NongHyup Life Insurance
- 신협
- LIG 투자증권
- Kyobo Life
- IBK Capital
- MG Non-Life Insurance

Government Sector

- Cheong Wa Dae
- 국회사무처
- Supreme Court of Korea
- 검찰 Prosecution Service
- 대한민국 육군 Republic of Korea Army
- 대한민국해군 Republic of Korea Navy
- 서울특별시의회 Seoul Metropolitan Council
- Ministry of Oceans and Fisheries
- Ministry of Foreign Affairs
- Ministry of the Interior and Safety
- Ministry of Health and Welfare
- Korea Communications Commission
- Gangwon Province
- 광주광역시 Gwangju City
- Korea Financial Investment Association

Public/ Medical Sector

- KEPCO KPS
- K water
- KHNP
- kotra
- Seoul Metro
- KoROAD 도로교통공단
- HUG Korea Housing & Urban Guarantee Corporation
- SH 에스에이치공사
- 대구광역시시설관리공단
- 한국철도시설공단 Korea Rail Network Authority
- The-K 한국교직원공제회
- 서울특별시농수산식품공사 Seoul Agro-Fisheries & Food Corporation
- 서울아산병원 Asan Medical Center
- 인제대학교상계백병원
- 연세대학교 의료원 Yonsei University Health System
- 원주세브란스기독병원
- 부산대학교병원

Education Sector

- 강원도교육청 Gangwon-do Office of Education
- 전라북도교육청
- Daegu Metropolitan Office of Education
- Hankuk University
- Korea University
- Kongju National University
- 국립중앙도서관 National Library of Korea
- 국립세종도서관 National Library of Korea, Sejong
- 국회도서관 National Assembly Library
- 육군사관학교 Korea Military Academy
- 서울시립대학교 University of Seoul
- 부천대학교 Bucheon University

Walker SWG V9

SOOSAN INT

SOOSAN INT Co., Ltd. | gb@soosan.co.kr