A Leading Global Network Security Solution Provider

SOOSAN INT

COMPANY INTRODUCTION

SOOSAN INT

SOOSAN GROUP

ENERGY GROUP

SOOSAN INDUSTRIES
Power Plant maintenance Service

SOOSAN ENS
Nuclear power plant MMIS and
Instrumentation control

SH POWER
New renewable energy business

ICT GROUP

SOOSAN INT
Network security solutions and
ISP platform services

SOOSAN HOMETECH
Gas safety equipment manufacture
Gas Sensor/ detector/shut off device

SOOSAN ENESOL
Polymer Aluminum Solid Capacitors
Polymer Aluminum Hybrid Capacitors

HEAVY INDUSTRY GROUP

SOOSAN HEAVY INDUSTRIES
Heavy construction equipment Manufacture

SOOSAN CSM
Construction and special purpose
machinery manufacture

DOOSUNG MOTOR
Trailer, special purpose vehicle
manufacture

SOOSAN INT

A LeadingGlobal Network Security Solution Provider

COMPANY NAME	SOOSAN INT Co.,Ltd
CEO	Lee Hong Goo
ESTABLISHMENT	March 4, 1998
CAPITAL	$2,900,000
PRODUCTS	Software development and supply (Including network access control solutions)
ADDRESS	Soosan Building, 13, Bamgogae-ro 5-gil, Gangnam-gu, Seoul
CONTACT	+82-2-541-0073
	ask@soosan.co.kr / www.soosanint.com

Credit Rating A+ KOSDAQ LISTED COMPANY

Company History

2021 ~
- Launched eWalker SSL VPN
- Signed an MOU with the Korea Energy Agency to facilitate carbon neutrality and external businesses
- Launched eWalker WAF V9

2016 ~
- Launched eWalker SWG V9
- Launched ePrism SSL VA
- Changed the company name to Soosan INT and listed on KOSDAQ

2012~
- Signed the "additional terminal service" partnership agreement with LG U+
- Signed a partnership agreement with KT for "Home Wi-Fi Service"
- Signed a joint project agreement with SK Telecom for "Youth Safety Service"

2005 ~
- Won the presidential award for venture business
- Signed a joint business agreement with SK Broadband for office Internet services
- Signed a joint business agreement with KT for terminal authentication services

1998 ~
- Launched eWalker 3, an Internet use management solution for businesses
- Launched Guardian Angel 1.0, a software program designed to block harmful Internet content for individuals
- Established Plus Technology Co., Ltd.

Competitiveness of SOOSAN INT

1,400
Network security solutions provided to over 1,400 customers

3 MAJOR TELCO
Telco platform-based services for over 10 years(KT, SK, LG U+)
Established the largest know-how on traffic analysis in Korea

70%
70% of the total workforce dedicated to technology development
Talented workforce management

133 PATENTS
Patents to secure business stability and technological competitiveness

FIRST
To develop Internet traffic filtering solutions
To develop SSL decryption solutions
To supply network-based harmful content blocking services (web filtering)

ONLY
Vendor to supply shared terminal detection services together with telco companies
Vendor to supply nationwide traffic analysis services

HAVE
Capability to analyze nationwide networks
High-performance DPI engine-based traffic analysis technology
Extensive know-how on building various networks

Network Security Solutions

Based on next-generation security technology to prevent ransomware / APT attacks / Web service threats / leakage of internal information

Walker SWG

Blocks hazardous websites / controls Internet access (web filtering)

- Block hazardous websites and malware
- Network security solutions with traffic access control
- Controls HTTPS web-site/service access
- Provide the largest URL DB in Korea

Prism SSL VA

Ensure SSL traffic visibility

- SSL traffic visibility solution
- Interconnection to other network security device available without replacing or modifying network layout/device
- Ensure visibility of SSL traffic on all traffic ports
- Provides an asymmetric routing environment

Walker SSL VPN

Optimized for remote and work-from-home environment / ensure super-fast speed and stable security

- Super-fast SSL VPN solution
- Support the remote work/work-from-home SSL VPN communication environment
- Provide high speed and stable secure channels
- The only SSL VPN with its own OTP solution in the industry

Walker DLP

Prevent personal information / internal information leakage

- Prevent personal information / internal information leakage through e-mail and messenger
- Wide and intensive logging for leaked information
- Provide various e-mail, messenger and cloud service pattern for accurate logging
- Provide audit log

Walker WAF

Detect and defend against Web attacks / prevent personal information leakage

- Web application firewall solution that secure web services
- Provide real-time monitoring and alert response services
- Protect against potential hacking attacks
- Provide web application traffic analysis

Walker CLOUD

Network security in cloud environment

- SSL visibility for other cloud based service
- SasS and SECaaS (Software as a Service and Security as a Service)
- SASE (Secure Access Service Edge) for enterprise network security
- Instance autoscaling based on traffic load

Walker SWG

Harmful website blocking solution (Web filtering)

Integrated Internet access control solution designed to control non-work related websites including HTTPS and block access to harmful websites
Improve work efficiency and prevent security threats

WHY eWalker SWG?

Use of non-work related websites ➜ Decrease in work concentration

Define allowed/disallowed websites according to job characteristics to increase work concentration

Diversification of access routes for malware websites

The harmful website blocking solution enables first-layer security

FEATURES

Control access to non-work related websites

Control websites by category
Support policies based on HR DB

Block access to harmful websites

Block malware websites
Block access bypass websites
(VPNs, Browser plug-ins)

Provide SSL traffic visibility

Ensure traffic visibility for all traffic ports
Support the installation / management of SSL certificate

BENEFITS

Increase work productivity

Improve concentration during working hours by blocking non-work related websites such as stocks, shopping, and messengers
Ensure efficient control of internal traffic by blocking harmful and file-sharing websites

Improve corporate security

Block threats to information assets caused by malware proactively
Eliminate blind spots for web security by ensuring visibility of SSL encrypted traffic

Enable efficient use of resources

Allow stable Internet use due to enhanced network security
Block harmful websites to reduce social and economic costs in the event of a security-related incident

Walker SWG — Harmful website blocking solution (Web filtering)

Integrated Internet access control solution designed to control non-work related websites including HTTPS and block access to harmful websites
Improve work efficiency and prevent security threats

Mirror Mode

Client — B/B — F/W — Internet

Block harmful websites

eWalker SWG
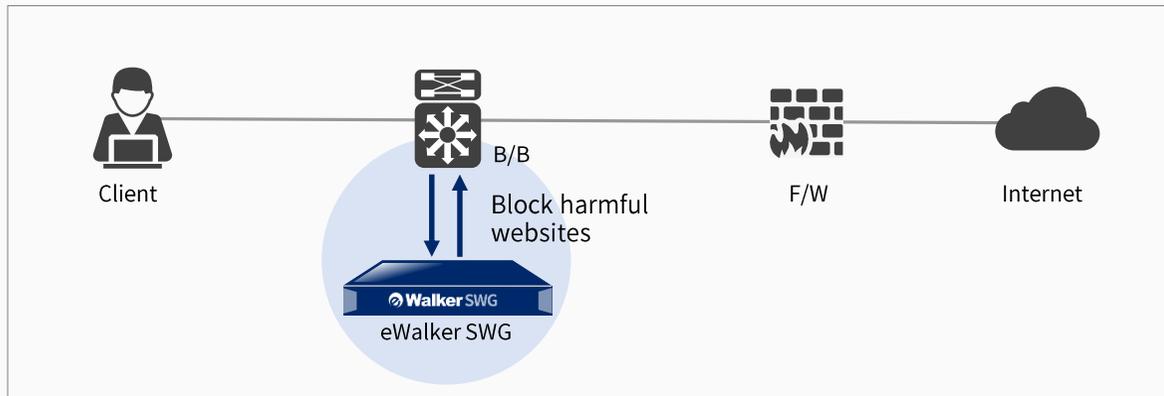
- Provide configuration without any impact on the network
- SSL traffic decryption function is disable
- Control HTTPS and harmful websites through DNS filtering
- Receive Internet access traffic of user computers through port mirroring
- Send blocking packet to user computers through blocking port connected to B/B

Inline Mode

Decrypt SSL traffic
Analyze traffic
Block harmful websites

Client — B/B — eWalker SWG — L4 SW — F/W — Internet
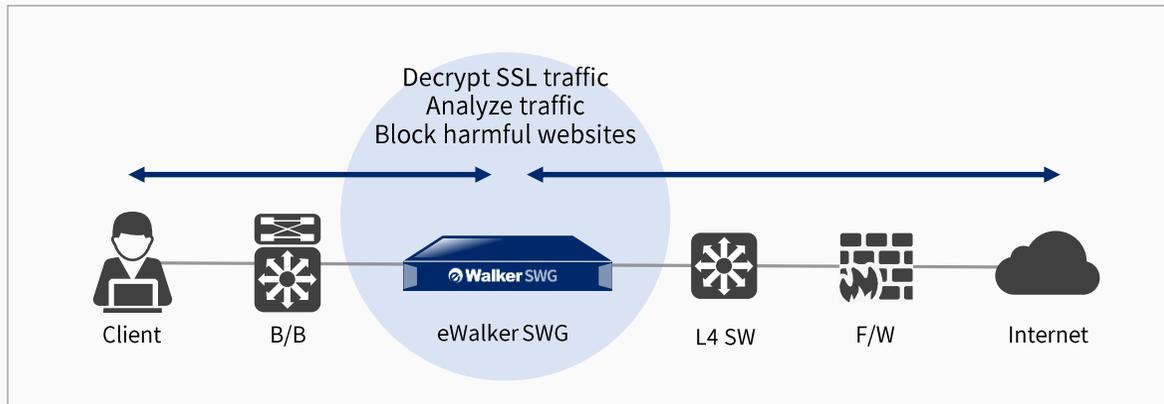
- Install the eWalker SWG product on network path (Transparency)
- Monitor all traffic and decrypt SSL traffic selectively
- Send blocking packets through the bridge interface when harmful websites are accessed
- Block the receipt/transmission of emails, block Google services selectively, block social media accounts, etc.
- Allow granular blocking of HTTPS websites

Walker SSL VA
Encrypted SSL traffic decryption solution

Its TST (TCP session transparency) high-performance engine enables transparent monitoring of all SSL traffic
SSL visibility solution functioning without any change in the network configuration, it helps existing security equipment to fully perform their functions.

WHY ePrism SSL VA?

90% of Internet traffic is SSL encrypted traffic
Existing network security equipment cannot identify encrypted traffic information

Existing equipment is unable to handle the SSL traffic
ePrism SSL VA monitors all ports and traffic (not just 443 port)
Ensure visibility into SSL-encrypted traffic that existing security equipment is unable to analyze

FEATURES

Decrypt SSL traffic
Selectively separate TLS/SSL protocols only
Decrypt all encrypted traffic

Maintain session transparency
Maintain 5 Tuple session transparency

Control access bypass software
Analyze traffic sessions
Block various bypass route patterns
(VPNs, Browser plug-ins)

BENEFITS

Ensure SSL visibility to improve network security
Relay decrypted traffic to existing security equipment and help analysis, detect and response
Prevent malware and ransomware infection that exploits SSL encrypted traffic

Prevent internal information leakage
Classify L7 protocols including various bypass protocols
Prevent internal information leakage by analyzing and blocking bypass access software

Ensure stable network operation
Offer an optimized compatibility for existing network environments
Bypass feature enables stable network operations

Walker SSL VA — Encrypted SSL traffic decryption solution

Its TST (TCP session transparency) high-performance engine enables transparent monitoring of all SSL traffic
SSL visibility solution functioning without any change in the network configuration, it helps existing security equipment to fully perform their functions.
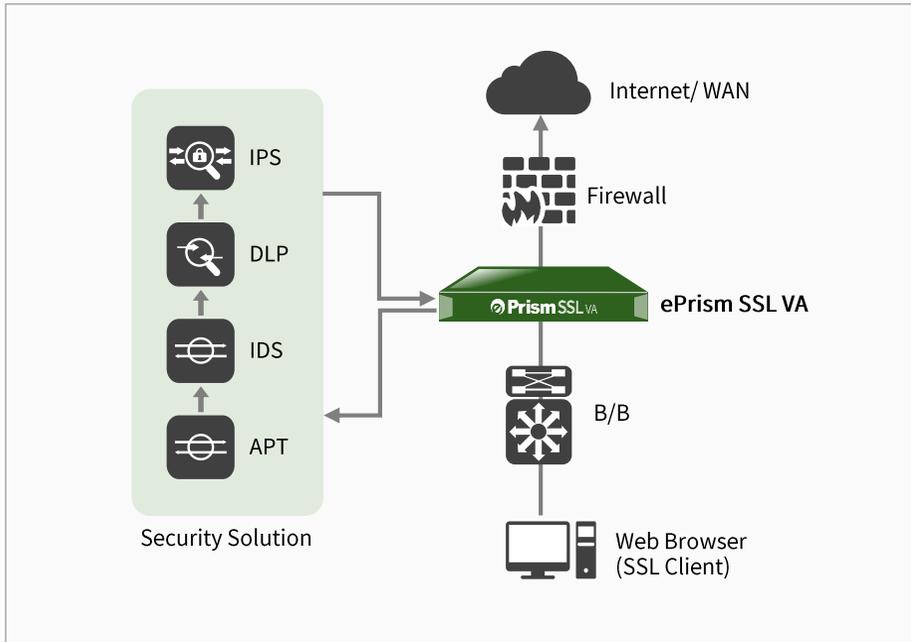
Forward Proxy

- Inside ➔ outside
- Ensure visibility <u>for external access</u> by internal users
- Offer the interworking function to various pieces of security equipment (IPS / ATP / DLP, etc.)
- Reinforce SSL security to prevent internal information leakage
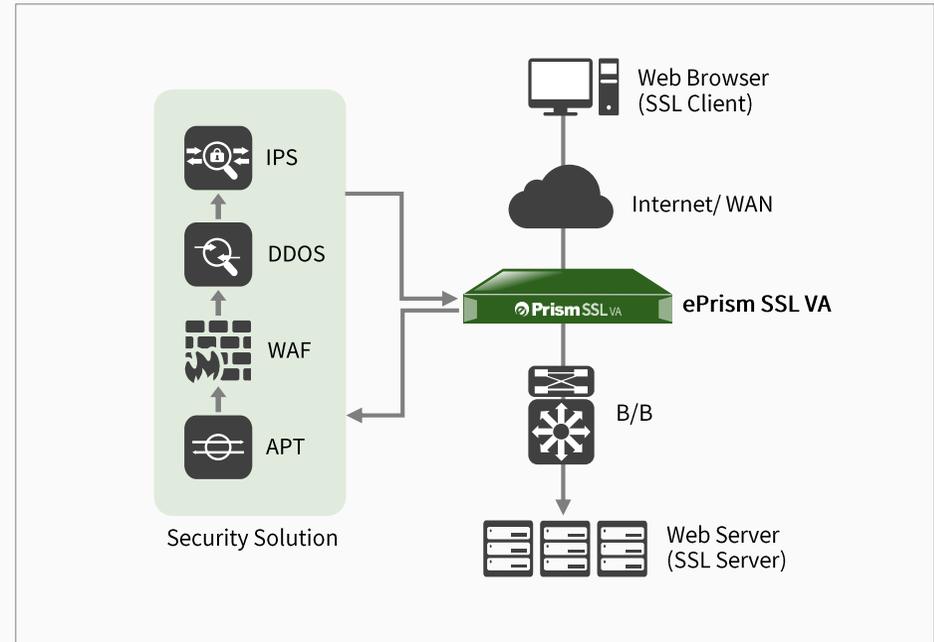
Reverse Proxy

- Outside ➔ inside
- Ensure visibility <u>for internal access</u> by external users
- Ensure SSL visibility for various pieces of security equipment (WAF / IPS, etc.)
- Reinforce SSL security for external services

Walker DLP
Network-based internal data loss prevent solution

It logs emails and outbound messages to analyze and block information from being leaked, and prevents information loss accidents due to cloud environments

WHY eWalker DLP?

94% of the loss of internal information occur through employee emails

94% of the loss of internal information occur through emails of internal/contracted employees
The loss of personal information and corporate information poses the greatest threat to the corporate security

Internal information leakage can be prevented proactively

Path of data loss has diversed such as Web mails, Messengers, Web hard, and Cloud services
Inspect any content sent to and from outside and prevent personal information/internal information leakage

FEATURES

Log inbound/outbound emails

Log illegal leakage of persoanl information/internal information via inbound/outbound emails

Log sent / received chat messages

Monitor and log chat messages include attached files

Log uploads to cloud services

Monitors file loss via Cloud and SasS service

BENEFITS

Ensure following security compliance

The Personal Information Protection Act specifies that measures must be enforced to prevent personal information from being disclosed or leaked.
DLP is a fundamental solution designed to comply with the laws on the protection of information.

Minimize economic damages caused by information leakage

Prevent damage caused by failure to protect corporate data assets such as the damage to the
reputation of the company, compensation for damages, and punishment of management, etc.

Walker DLP — Network-based internal data loss prevent solution

It logs emails and outbound messages to analyze and block information from being leaked, and prevents information loss accidents due to cloud environments
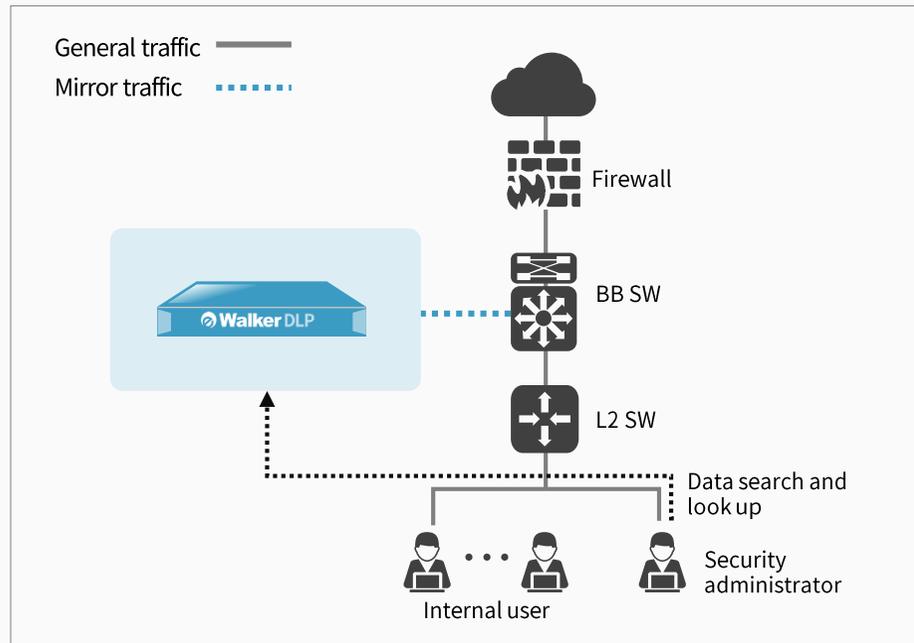
General configuration

- No impact on the existing network, simple configuration
- Enable monitoring of e-mail, messenger, social media, and file transfers that contain personal information (resident registration number, credit card information, etc.) and internal information (keywords, sizes, etc.)
- Logging of HTTPS traffic requires a link to the sPrism SSL VA product. (SSL visibility solutioin)
- Enables Inline configuration (with bypass card designed to assure network availability)
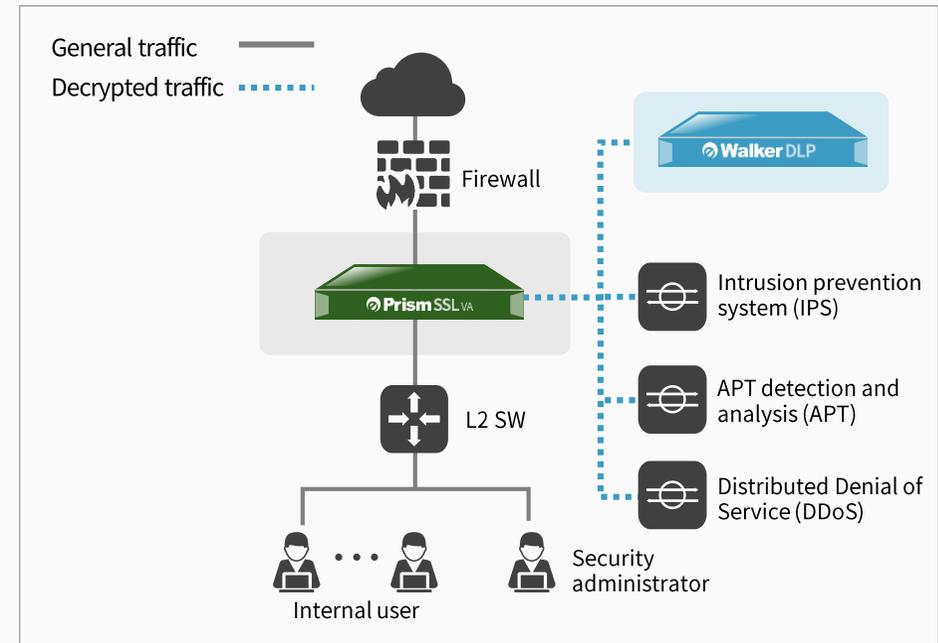
SSL decryption and filter configuration

- Proposed layout offers an integrated system designed to SSL visibility, block hazardous websites, and detect loss of internal information (including personal information).
- SSL visibility and block harmful HTTPS websites
- Monitors e-mail, messenger, social media, and file transfers that contain personal information (resident registration number, credit card number, etc.) and internal information (keywords, sizes, etc.)
- Enable SSL traffic visibility (decryption) traffic to various security devices
- Require separate purchase of ePrism SSL VA

Walker WAF — Next-generation web application firewall

Its real time white URL technology dramatically reduces false positive rates and processing time to ensure safety for web services and actively defends against malware.

WHY eWalker WAF?

Increased attacks/security-related incidents against web services

When a potential vulnerability of the web server is exploited, existing network security solutions such as IPS, IDS, and firewall are unable to detect the attack.

Implementing secure web services

The traffic analysis for various web services enables defense against Web attacks → server protection, and implementation of secure web services.

FEATURES

Detect and defend against Web attacks

Counter the latest automated / intelligent Web attacks
Counter HTTP(S) brute-force and HTTP2.0 web attacks

Prevent personal information leakage

Automatically block intentional / accidental leakage of personal information

Anti Web DoS

Detect and block HTTP Get Flood and more in real-time

BENEFITS

Enable secure web service operations

Allow normal web service requests and detect and block attacks on web servers to ensure safety

Assure highly effective security through convenient security control

Provide various features for convenient security management
Ensure user convenience in terms of real-time monitoring and policy setting
Improve security against threats such as the latest web attacks and new DOS attacks
Analyze and reflect vulnerabilities referring to OWASP, SANS, and the Office of the Director of National Intelligence, etc.

Walker WAF Next-generation web application firewall

Its real time white URL technology dramatically reduces false positive rates and processing time to ensure safety for web services and actively defends against malware.

Web traffic control

Internet   F/W   IDS / IPS   eWalker WAF V9   L4 SW   Web Server
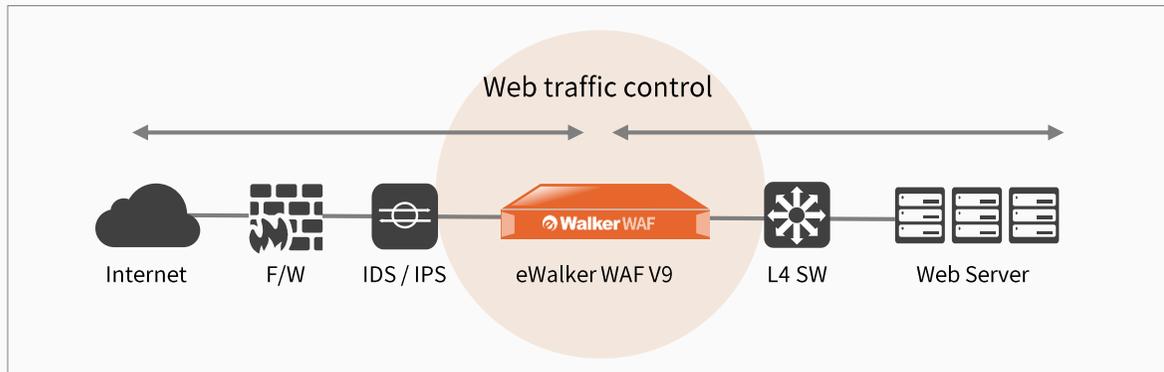
Inline Mode

- Installs the eWalker WAF V9 on network path (Transparency)
- Monitor Web traffic and encrypt/decrypt SSL traffic
- Send blocking packets through the bridge interface in the event of web attacks
- Bypass function provide uninterrupted web service in the event of service failure

Active ➡ Standby or Active ▪▪▪▪▶

Internet   F/W   IDS / IPS   eWalker WAF V9   L4 SW   Web Server
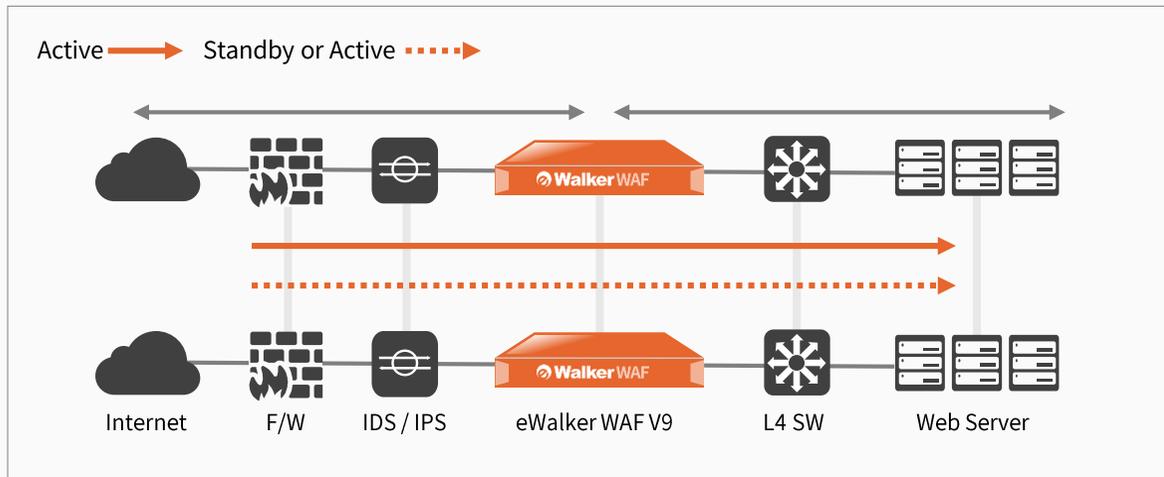
HA Mode

- Install the eWalker WAF V9 product on the network path (HA A-S, A-A)
- Monitor Web traffic and encrypt/decrypt SSL traffic
- Send blocking packets through the bridge interface in the event of web attacks
- Provide stable web security services through HA (A-S, A-A) in the event of a network failure

eWalker SSL VPN

High-performance virtual private network solution

Its real time white URL technology dramatically reduces false positive rates and processing time to ensure safety for web services and actively defends against malware.

WHY eWalker SSL VPN?

Increace of remote work/work-from-home ➜ Expand SSL VPN application

Use cases such as work-from-home, remote learning, IoT, M2M service
highlight the importance of SSL VPN

Provide thorough security

Self-built OTP solution for personal information protection, real-time monitoring and over 5 multi-authentication processes to provide thorough security

FEATURES

Support the remote work/work-from-home SSL VPN communication environment

Support various user OS environments
Control access to IP/Port by server

Solution specialized for SSL VPN

Equipped with its own OTP solution
Support more than 5 strong multi-authentication processes

Fast, reliable, and secure channel

Super-fast SSL VPN
Access settings for each user/group
Limit user access by period

## BENEFITS

Enhance the corporate network security

Use internal infrastructure through encryption even outside the company
Ensure high level corporate network security by reinforcing the authentication process
Collect encrypted remote data

Save costs and ensure convenient deployment with one-click

Replace the existing IPSec-based VPN (using SSL method)
Reduce VPN TCO
Easy implement VPN

Walker SSL VPN — High-performance virtual private network solution

Its real time white URL technology dramatically reduces false positive rates and processing time to ensure safety for web services and actively defends against malware.
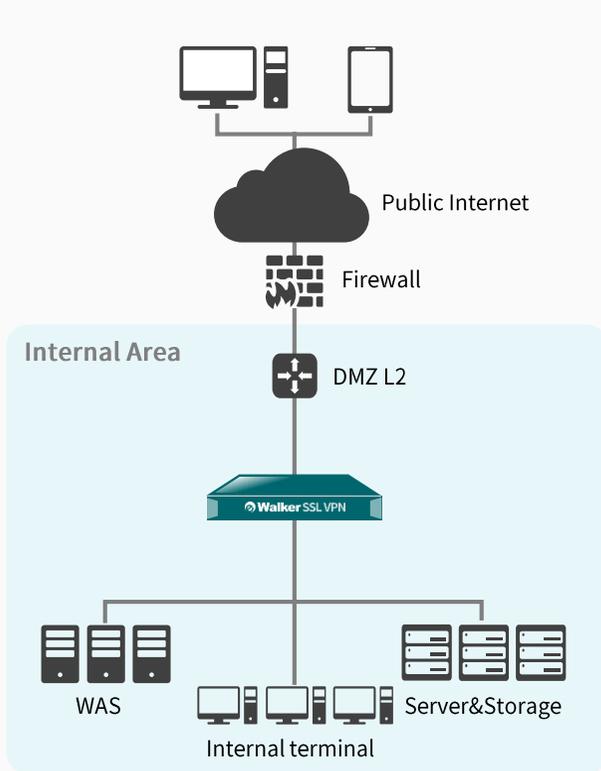
General configuration (single)
- Behind Firewall DMZ location (controls unnecessary traffic)
- Reinforcement of security through firewall security policy setting
- Only allows SSL VPN service port in the firewall
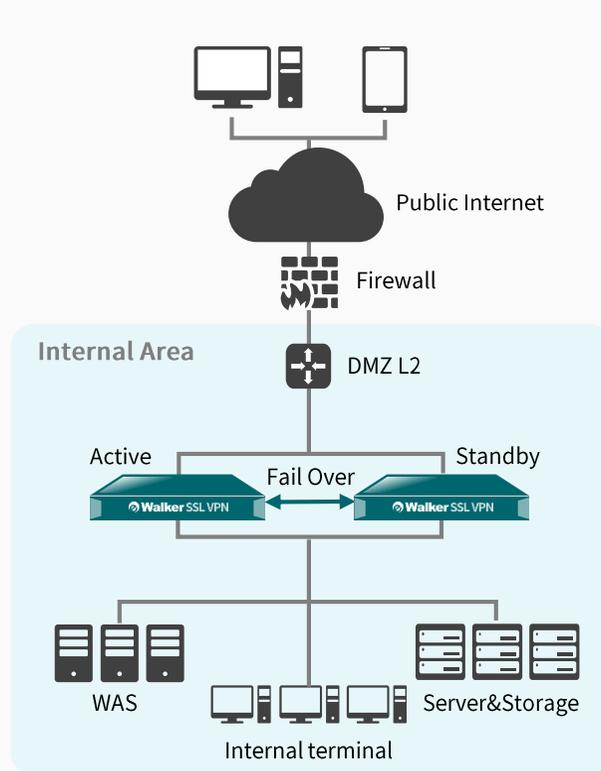
Redundant configuration (Active-Standby)
- HA configuration with two physical device which are applied in real-time in the form of failover when failure occurs
- VRRP applied inside and outside the redundant configuration, respectively
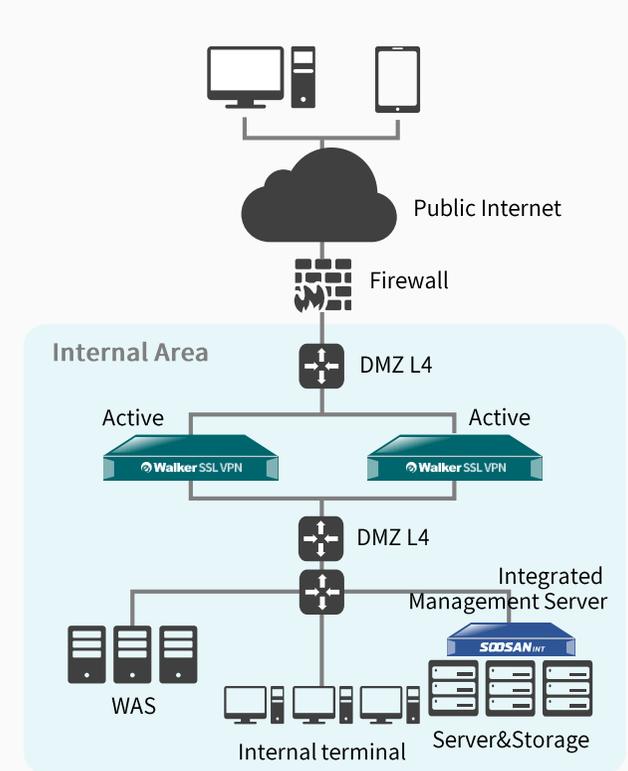
Redundant configuration (Active-Active)
- Traffic load balancing with internal L4 switchs
- Provide user account management through Policy Server
- VPN policy setting, integrated monitoring and statistical report

Telco platform service

As a nationwide backbone infrastructure service that has created new value-added services for telecommunication companies
The "Device identification technology" is the first additional service model built for new revenue generation

An Value-added internet service for customers with multiple devices

Services provided for over 10 years

Provide services for three telecommunication companies

Operate services nationwide

Internet   ISP Backbone   Router

SOOSAN INT

Device authentication system

Authentication (OK)

Authentication (OK)

Block Internet and induce authentication

Block Internet and induce authentication
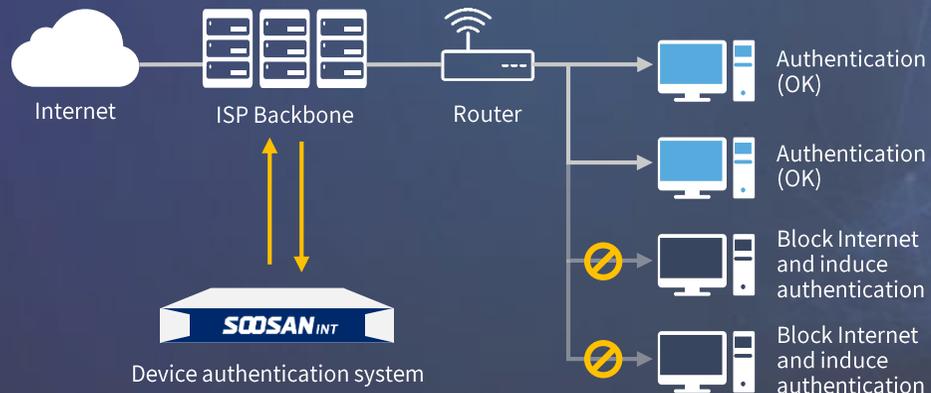
Key References

Corporation		Finance		Public Sector		Healthcare / Education	
SAMSUNG	kt	SHINHAN BANK	kakaobank	Ministry of Land, Infrastructure and Transport	Ministry of Oceans and Fisheries	Asan Medical Center	GangNeung Asan Hospital
HYUNDAI MOTOR GROUP	LG U+	Korea Eximbank	BANK OF KOREA	Ministry of Education	Ministry of Unification	SEVERANCE HOSPITAL	NHIS Ilsan Hospital
POSCO	KOREAN AIR	toss	koscom	Ministry of Health and Welfare	Ministry of Foreign Affairs	HANIL GENERAL HOSPITAL	ULSAN UNIVERSITY HOSPITAL
SK chemicals	SK broadband	HANYANG SECURITIES	HYUNDAI MOTOR SECURITIES	Ministry of Environment	Ministry of Agriculture, Food and Rural Affairs	KNUH	CHUNG-ANG UNIVERSITY HOSPITAL
CJ ENM	HANCOM Inc.	KDB Bank affiliate KDB Life	Hanwha Life	Culture Heritage Administration	Korean Intellectual Property Office	Gyeongsangbuk-do Office of Education	GYEONGSANGNAMDO OFFICE OF EDUCATION
HYUNDAI ENGINEERING & CONSTRUCTION	HJSC	TONGYANG LIFE INSURANCE	KFTC	SUPREME COURT OF KOREA	PROSECUTION SERVICE	INCHEON METROPOLITAN CITY OFFICE OF EDUCATION	Jeju Special Governing Provincial Office of Education
mall	LOTTE HIMART	Hyundai Marine & Fire Insurance	MG Non-Life Insurance	Ministry of the Interior and Safety National Information Resources Service	KNPA KOREAN NATIONAL POLICE AGENCY	DAEJEON METROPOLITAN OFFICE OF EDUCATION	Ulsan Metropolitan Office of Education

Certification

Best SME Awards on the Internet-based Network SW category (2000)
Prime Ministerial Prize at the Information Culture Awards (2002)
Grand Prize in the Intelligent Application category at the Intelligence Awards (2010)
Presidential Citation for its promotion at the Startup Awards (2011)
Award certificate for invention promotion from the Korea Invention Promotion Association (2011)
Korea Licensing Association President's Prize at the Electronic IT Industry Patent Management Awards (2012)
Award certificate for the development of ICT SMEs and startups (2014)
Bronze award at the Electronic ICT Industry Patent Management Awards (2014)
Grand Prize at the New SW Product Awards (2019)

CC (Common Criteria) certification
eWalker DLP V9, Walker SWG V9, eWalker SWG V8, eWalker Security V7M, eWalker Security V7, eWalker WAF V9
GS (Good Software) certification
eWalker SSL VA V3, eWalker DLP V9, eWalker SWG V9, eRed Virtual Shield S1, ME.Guard V1.0, eWalker SSL V1.0, eWalker Security V7, ClassWa V1.0, eWalker 3 SQL V5.1

AWARD

CERTIFICATIONS

SOOSAN *INT* Thank you