Advanced SSL Traffic Visibility Appliance

ePrism SSL VA

Doc. No. 2018-SPA-SM0006-v1.1.0

CONTENTS

I. Introduction

- Why ePrism SSL VA is needed
- Risks associated with SSL
- Legal compliance
- ePrism SSL VA

Why ePrism SSL is Needed

Increasing Use of SSL Traffic

Of the top 50 sites,
42 use HTTPS.
(ALEXA's Top 500 Sites, Sep. 2017)

Of global web traffic,
More than 55% is SSL traffic.
(Cisco Encrypted Traffic Analytics, ETA)

Of web traffic in 2019,
Up to 80% will use SSL.
(Gartner Predicts 80% Web Encryption by 2019)

E-MAIL
- G-mail
- Outlook
- NAVER mail

CLOUD
- NAVER cloud
- Dropbox
- GOOGLE drive

WEBSITE
- Google
- NAVER
- YouTube

SNS
- Facebook
- KakaoTalk
- Twitter

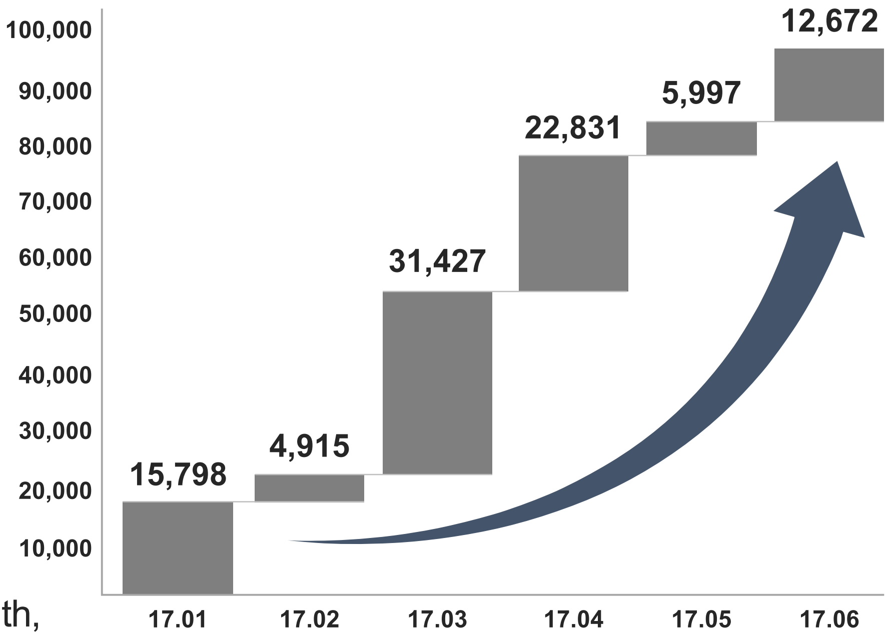
Why ePrism SSL is Needed

Upsurge in SSL-Based Security Threats

80% of recent APT attacks and 41% of hackers,
use SSL traffic.
(Traffic analysis by Zscaler Cloud, Aug. 2016 to Jan. 2017)

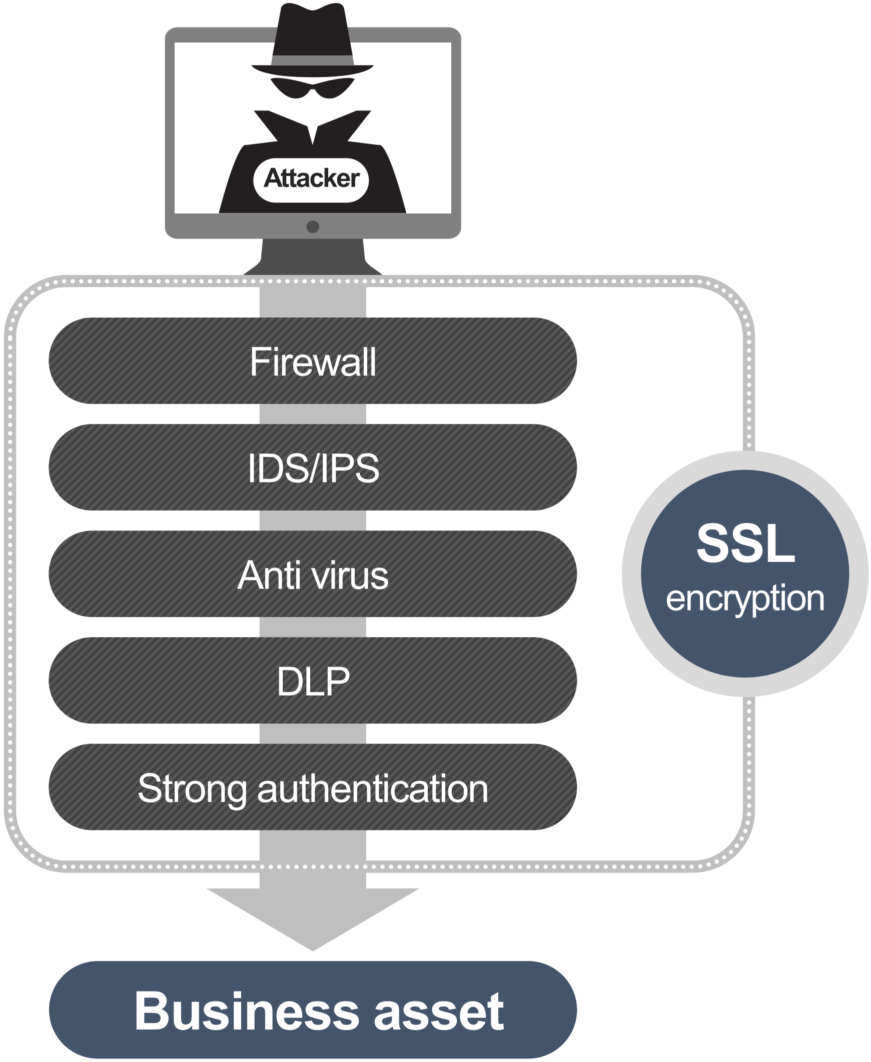
Harmful SSL-based attacks occur,
an average of 600,000 times a day.
(Traffic analysis by Zscaler Cloud. Aug. 2016 to Jan. 2017)

An average of 15,000 attacks detected per month,
of 93,000 in the first half of the year
(HTTPS-based malicious code collection by SOOSAN INT)



※ HTTPS-based malicious code collection of the first half year of 2017 by SOOSAN INT (feat.: Malwares.com/Mangoscan.com)

Why ePrism SSL is Needed



Standard internal network security

- Different security appliances protect the network against threats at each stage in the network.
- Threats that can't be blocked are left up to end point security

By design, SSL Traffic
cannot be analyzed on the network.

SSL encryption makes it impossible for standard network devices to work as designed

SSL can also be used by hackers as a "safe" path for attacks.

Risks Associated with SSL

PrismSSL VA

- Attacks that exploit SSL traffic for malicious purposes **can’t be detected or blocked with standard security appliances.**
- IDS, IPS, APT solutions, Network DLP **and other standard security appliances can be bypassed**

CASE 1

Malware transmission via an email or a messenger;

Internal data leaks

Forbes

Mar. 29, 2018

Tax Time Is W-2 Scam Time

…The IRS urged employers to limit the number of employees who have access to W-2 forms and to require additional verification procedures to validate requests before emailing W-2s.

www.ban.com/w2-email-scam-b73014451281/

The Telegraph

Jan. 19, 2018

British 15-year-old gained access to intelligence operations in Afghanistan and Iran by pretending to be head of CIA, court hears …

www.telegraph.co.uk/news/2018/01/19/british-15-year-old-gained-access-intelligence-operations-Afghanistan/

- Monitoring/analyzing/blocking attachments is impossible
- Determining the path of leaks is impossible

CASE 2

Malware distribution via Social Media

EXPRESS

Apr. 05, 2018

Facebook data breach: 40 MILLION more users’ personal info was leaked.

FACEBOOK has revealed the data of up to 87 million people using the social media may have been shared with political firm Analytical – nearly 40 million more than previously thought.…

www.express.co.uk/news/world/941701/facebook-data-breach-cambridge-analytica-us-election-mark-zuckerberg-scandal

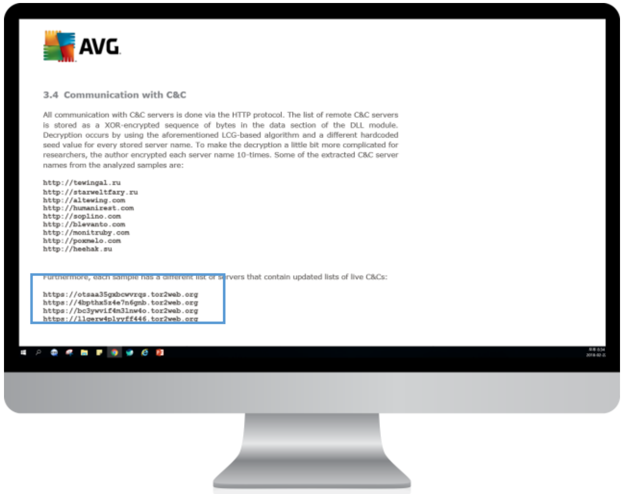
- Security threats that exploit social media features such as reliability, personal relationships, short URLs, and usability are continuously increasing.

Risks Associated with SSL

- Malware that is unknowingly downloaded **cannot be detected or analyzed on the network.**
- If cloud apps like Google Docs are being used **blocking specific ports or IPs is impossible.**

CASE 3

C&C Communication with SSL



3.4 Communication with C&C

All communication with C&C servers is done via the HTTP protocol. The list of remote C&C servers is stored as a XOR-encrypted sequence of bytes in the data section of the DLL module. Decryption occurs by using the aforementioned LCG-based algorithm and a different hardcoded seed value for every stored server name. To make the decryption a little bit more complicated for researchers, the author encrypted each server name 10-times. Some of the extracted C&C server names from the analyzed samples are:

```
http://tewingal.ru
http://starweltfary.ru
http://altewing.com
http://humanirest.com
http://soplino.com
http://blevanto.com
http://monitruby.com
http://poxmelo.com
http://heehak.su
```

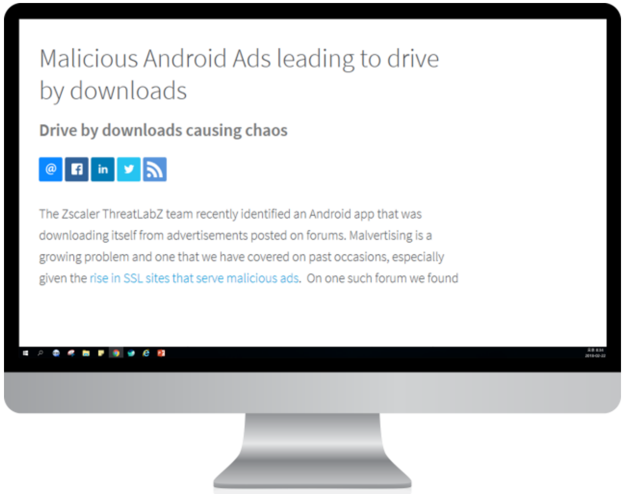
Furthermore, each sample has a different list of servers that contain updated lists of live C&Cs:

```
https://otsaa35gxbcwvrqs.tor2web.org
https://4bpthx5z4e7n6gnb.tor2web.org
https://bc3ywvif4m3lnw4o.tor2web.org
https://llgerw4plyyff446.tor2web.org
```

Analysis of Banking Trojan Vawtrak AVG Technologies, Virus Lab

CASE 4

Drive by Download with SSL



Malicious Android Ads leading to drive by downloads

Drive by downloads causing chaos

The Zscaler ThreatLabZ team recently identified an Android app that was downloading itself from advertisements posted on forums. Malvertising is a growing problem and one that we have covered on past occasions, especially given the rise in SSL sites that serve malicious ads. On one such forum we found

Zscaler (2017.06)

- Most **Malware communicates with its C&C** server using **SSL.**
- All new ransomware collected since 2016 uses SSL to communicate
- with its C&C server. (CYREN Report, 2017)

- **Drive by Download with SSL**
- Ad servers among others use SSL

Legal Compliance

The Facilitation of Communication Network Use and Information Protection Act

|Article 28| Privacy Protection Measures

<Rev. March 22, 2016>

- When Information and Communication Service providers process personal information, they must take actions technically and administratively, as listed in the following sections, to prevent the loss, theft, forgery, or alteration and to ensure the security of personal information in accordance with the Executive Order.

|Article 45| Ensuring the Stability of Information and Communications Networks

<Rev. March 22, 2016>

- Technical and physical measures such as the installation of a information protection system to prevent unauthorized access or intrusion into information and communication systems,
- Technical measures to prevent illegal leakage, falsification, tampering, and deletion of information,
- Technical and physical measures to ensure the information and communication network is always available
- Administrative safeguards regarding personnel, organization, and finances for the stability and security of the information and communication network and the and creation of related action plans.

Per the revised Act,
Using SSL is
a duty and responsibility!

For security in the world of SSL traffic,
An SSL visibility appliance is
essential!

ePrism SSL VA

ePrism SSL VA

TST-based SSL decryption allows all traffic on every port to be monitored transparently.

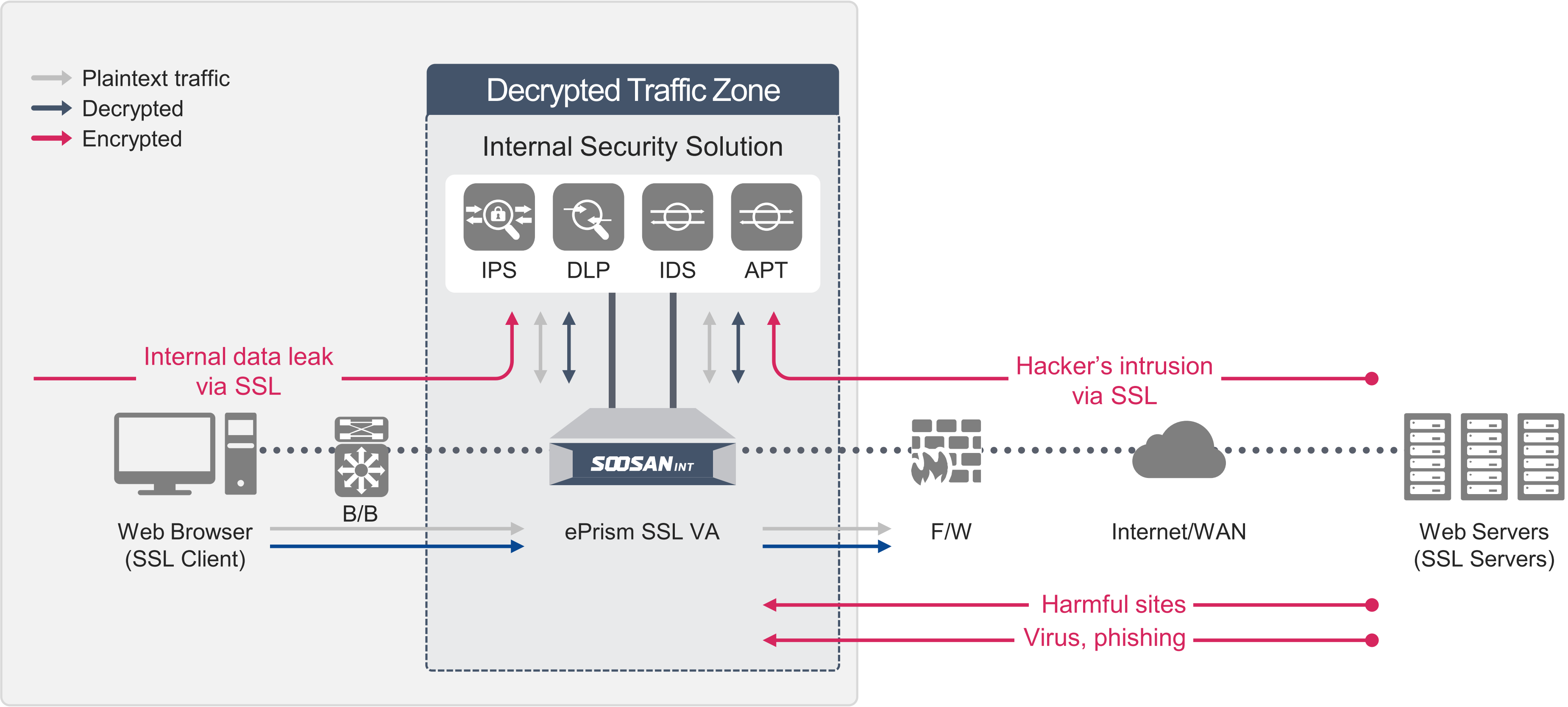
Engineered for SSL visibility, ePrism can be installed without changes to the network

- TST-based high performance session processing
- DPI-based SSL traffic analysis
- Maintains the packet 5 tuple
- Supports DTZ configuration
- Compatible with many different 3rd party devices
- Easy distribution and management of certificates
- Internet anonymizer controls
- Detailed traffic analysis and log search
- Supports various types of installation, and it's user friendly

II. Features

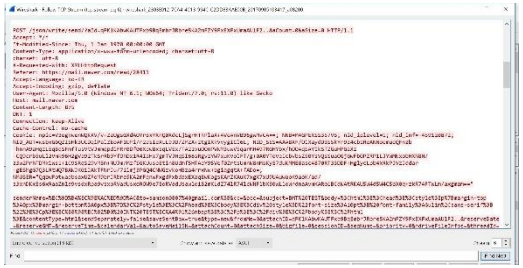
- Managing TLS/SSL with ePrism SSL
- Visibility into all SSL traffic
- TST (TCP Session Transparency) Based SSL decryption
- DTZ (Decrypted Traffic Zone)
- Compatible with a variety of network/security devices
- MPT (Message Pass Through)
- Easy certificate distribution and management
- Internet anonymizer controls
- Detailed traffic analysis and log search
- Supports many installation modes
- Enhanced usability
- Benefits

Managing TLS/SSL with ePrism SSL VA



- Decrypts SSL/TLS traffic one time, and provides the decrypted traffic to existing network security appliances (Decrypted Traffic Zone).
- Compatible with IPS, IDS, APT, SWG, and DLP appliances.
- 'One Source - Multi Use' decryption solution

Visibility Into All SSL Traffic

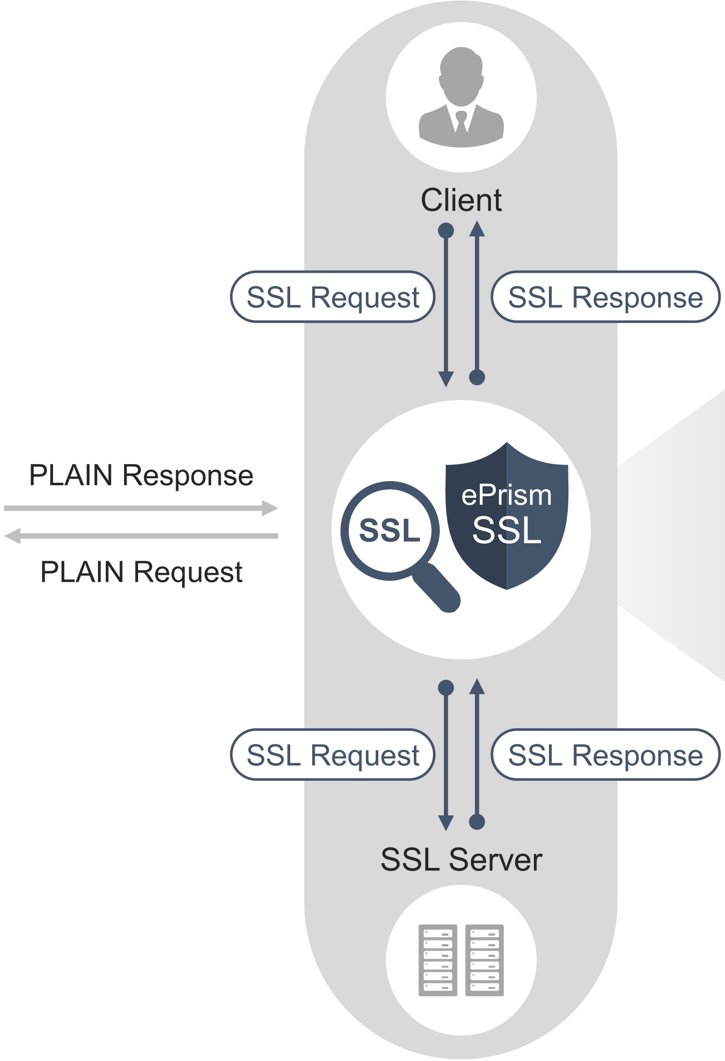


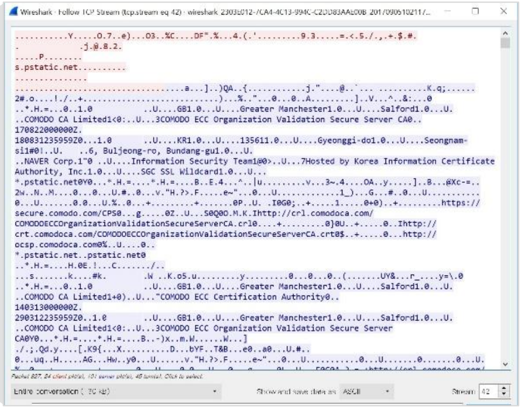
Wireshark · Follow TCP Stream (tcp.stream eq 8) · wireshark_2303E012-7CA4-4C13-994C-C2DD83AAE00B_20170905103417_a08200

```
POST /json/write/send/?aId=[illegible]&aCount=0&aSize=0 HTTP/1.1
Accept: */*
If-Modified-Since: Thu, 1 Jan 1970 00:00:00 GMT
Content-Type: application/x-www-form-urlencoded; charset=utf-8
charset: utf-8
X-Requested-With: XMLHttpRequest
Referer: https://mail.naver.com/read/28411
Accept-Language: ko-KR
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Host: mail.naver.com
Content-Length: 875
DNT: 1
Connection: Keep-Alive
Cache-Control: no-cache
Cookie: [illegible]
NPUSER=[illegible]

senderName=[illegible]&to=samson9807%40gmail.com&cc=&bcc=&subject=SMT%20TEST&body=[illegible]
%3E&contentType=html&sendSeparately=false&saveSentBox=true&type=new&fromMe=0&attachID=[illegible]&reserveDate
=&reserveGMT=&reserveTime=&calendarVal=&autoSaveMailSN=&attachCount=0&attachSize=0&bigfile=0&sessionID=&seqNums=&priority=0&driveFileInfos=&threadId=
```

Decrypted plaintext traffic





Wireshark · Follow TCP Stream (tcp.stream eq 42) · wireshark_2303E012-7CA4-4C13-994C-C2DD83AAE00B_20170905102117...

```
..........Y.....O.7..e)...O3..%C....DF".%...4.(.'........9.3.....=.<.5./.,.+.$.#.
.              .j.@.8.2.
.....P.......
s.pstatic.net..........
...............
...............................a...]..)QA..{...........j."....@..`... .........K.q;......
2#.o....!./..+...........................)...%.."...0...0..A.........]..V...^..&:...0
..*.H.=...0..1.0            ..U....GB1.0...U....Greater Manchester1.0...U....Salford1.0...U.
..COMODO CA Limited1<0:..U...3COMODO ECC Organization Validation Secure Server CA0..
170822000000Z.
180831235959Z0...1.0        ..U....KR1.0...U....135611.0...U....Gyeonggi-do1.0...U....Seongnam-
si1#0!..U.   ..6, Buljeong-ro, Bundang-gu1.0...U.
..NAVER Corp.1"0 ..U....Information Security Team1@0>..U...7Hosted by Korea Information Certificate
Authority, Inc.1.0...U....SGC SSL Wildcard1.0...U...
*.pstatic.net0Y0...*.H.=....*.H.=....B..E.4...^..|u.........v...3~.4....OA..y.....]..B...@Xc-=..
2w..N..M....0...0...U.#..0...v."H.?>.F.....e~"...0...U.............1_)...G...#..0...U..........
0...U.......0.0...U.%..0...+.........+.......0P..U. .I0G0;..+.....1.....0+0)..+.........https://
secure.comodo.com/CPS0...g.....0Z..U...S0Q0O.M.K.Ihttp://crl.comodoca.com/
COMODOECCOrganizationValidationSecureServerCA.crl0....+.........0}0U..+.....0..Ihttp://
crt.comodoca.com/COMODOECCOrganizationValidationSecureServerCA.crt0$..+.....0...http://
ocsp.comodoca.com0%..U....0..
*.pstatic.net..pstatic.net0
..*.H.=....H.0E.!...C......./..
...s.......k....#k.        .W ..K.o5.u.........y.........0...0...0..(.......UY&...r_....y=\.0
..*.H.=...0..1.0            ..U....GB1.0...U....Greater Manchester1.0...U....Salford1.0...U.
..COMODO CA Limited1+0)..U..."COMODO ECC Certification Authority0..
140313000000Z.
290312235959Z0..1.0         ..U....GB1.0...U....Greater Manchester1.0...U....Salford1.0...U.
..COMODO CA Limited1<0:..U...3COMODO ECC Organization Validation Secure Server
CA0Y0...*.H.=....*.H.=....B..-)x..m.W......W...]
./.;.Qd.y....[.K9{...X..........D...bYF..T&B...e0..a0...U.#..
0...uq..H.....AG...Hw..y0...U......v."H.?>.F.....e~"...0...U...........0...U.......0.......0...U.
```

Packet 827. 24 client pkt(s), 101 server pkt(s), 45 turn(s). Click to select.

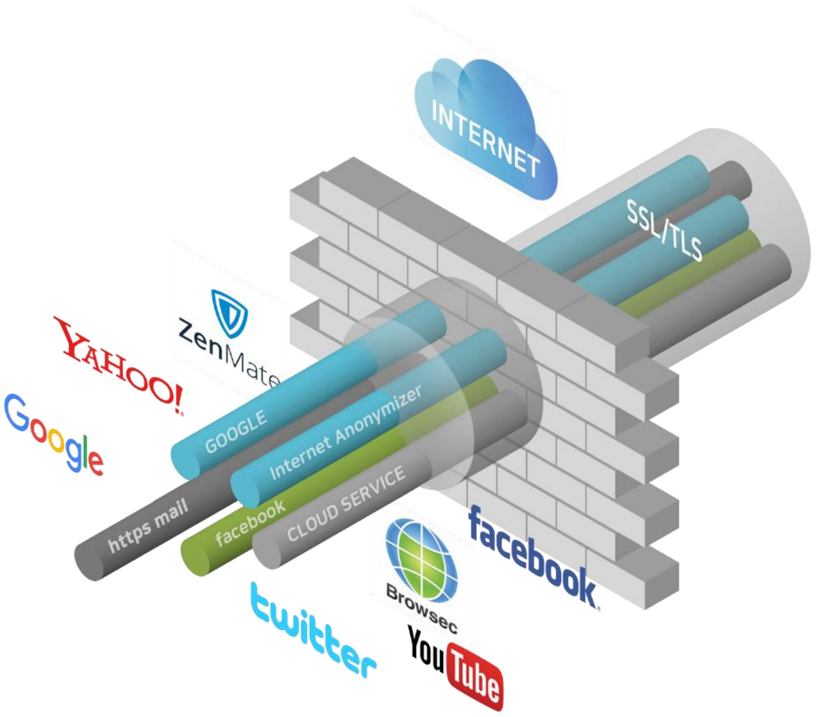
Entire conversation (30 kB) · Show and save data as: ASCII · Stream: 42

SSL encrypted traffic

TST (TCP Session Transparency) Based SSL Decryption

● TST (TCP Session Transparency)

- Using a DPI (Deep Packet Inspection) based engine, only TLS/SSL protocols are selectively separated and decrypted.
- Through analysis of each packet flow’s 5-tuple, its SSL handshake and its payload, SSL traffic is observed and decrypted



Benefits of TST

Selective decryption

- Analyzes and decrypts SSL traffic on every port

Performance and reliability

- Ensure reliable throughput without performance degradation even when processing large volume of traffic.

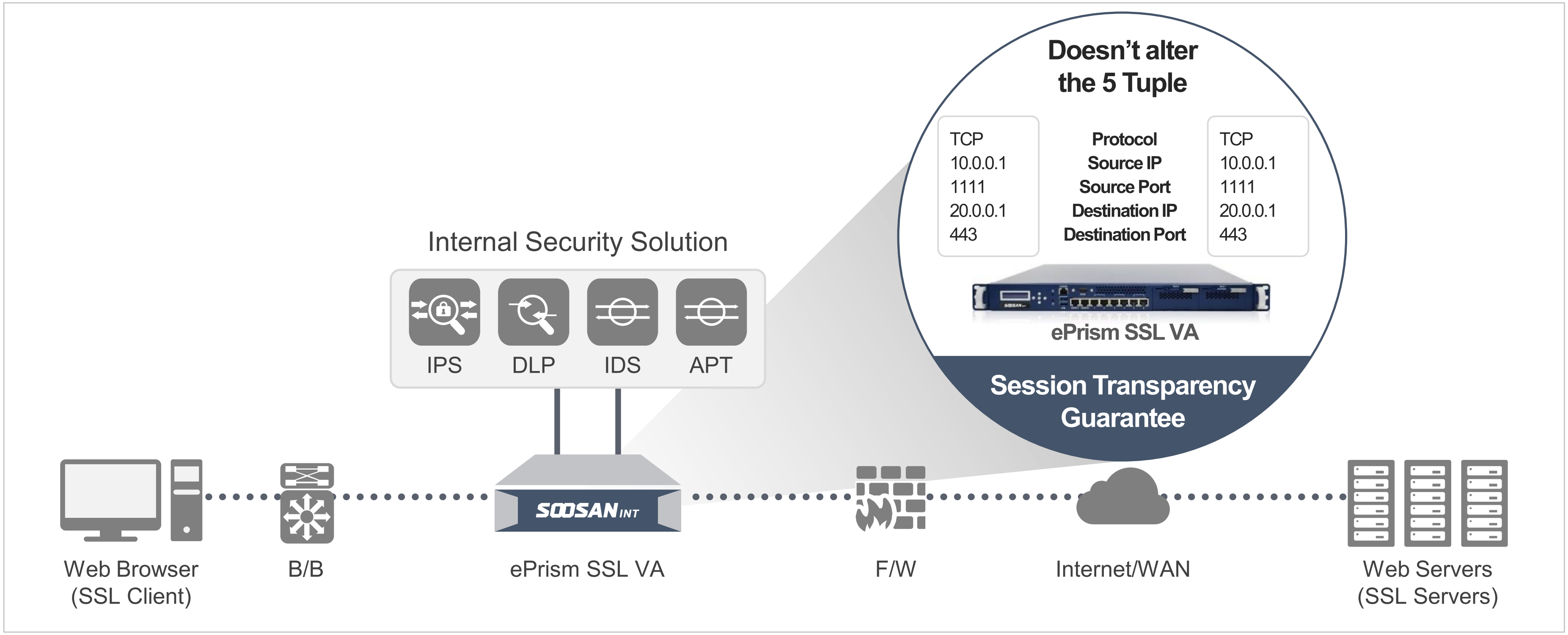
Compatibility

- Perfectly compatibility with existing security appliances, ensuring network stability.

Stability

- Installation follows the existing network configuration, reducing maintenance fees and minimizing headaches

TST (TCP Session Transparency) Based SSL Decryption



TCP	Protocol	TCP
10.0.0.1	Source IP	10.0.0.1
1111	Source Port	1111
20.0.0.1	Destination IP	20.0.0.1
443	Destination Port	443

● DPI (Deep Packet Inspection) Support

- All traffic analyzed and information relayed for blocking policies
- Maintains only the minimum number of sessions required for decryption.
- Even if a situation requiring HW bypass arises, all sessions except those being decrypted remain stable without disconnection.

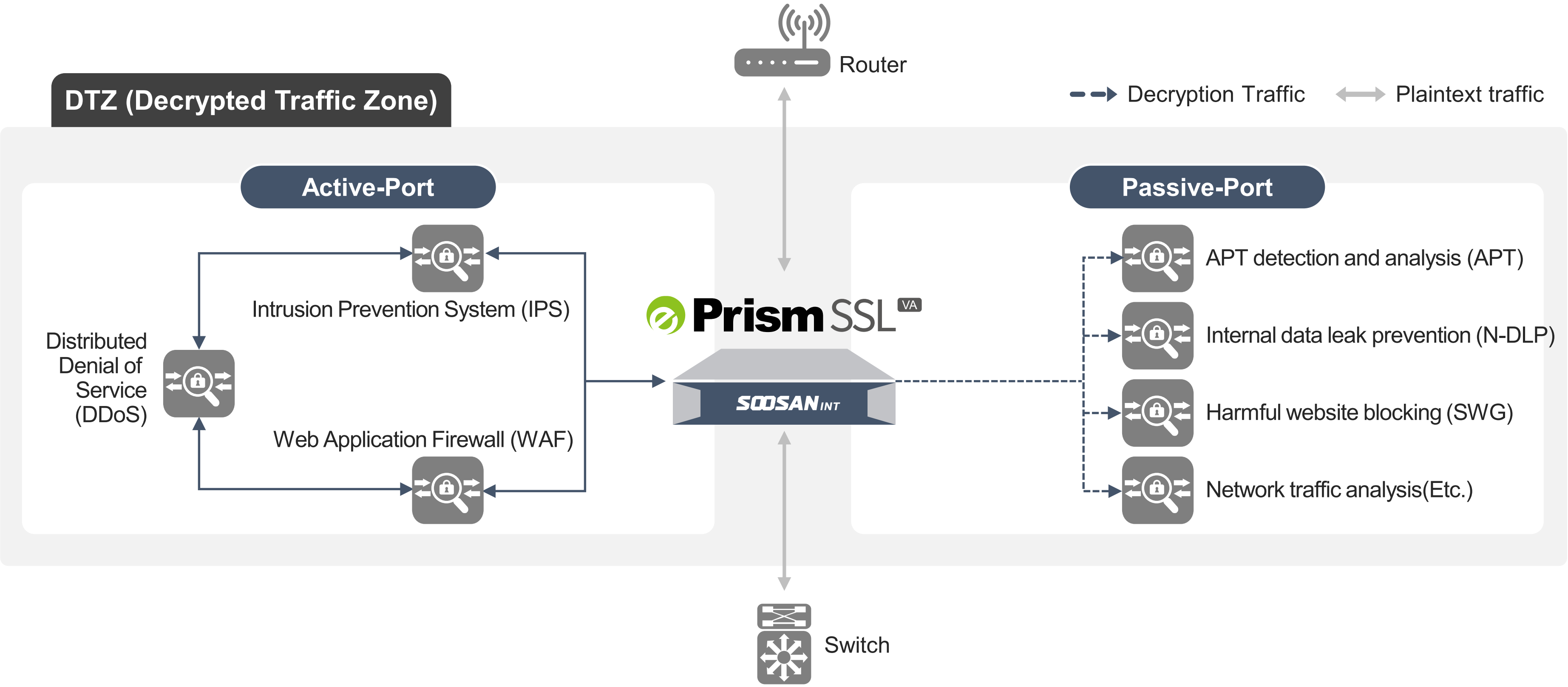
● Doesn't Change Packets' 5 Tuples

- Monitors all ports transparently without disrupting network traffic by maintaining the 5 tuple, unlike standard proxies
- Removes obstacles to non-standard traffic.
- 3rd party network appliances can be connected without the need for reconfiguration or settings changes, preventing statistical and functional errors.

DTZ (Decrypted Traffic Zone)

DTZ (Decrypted Traffic Zone)

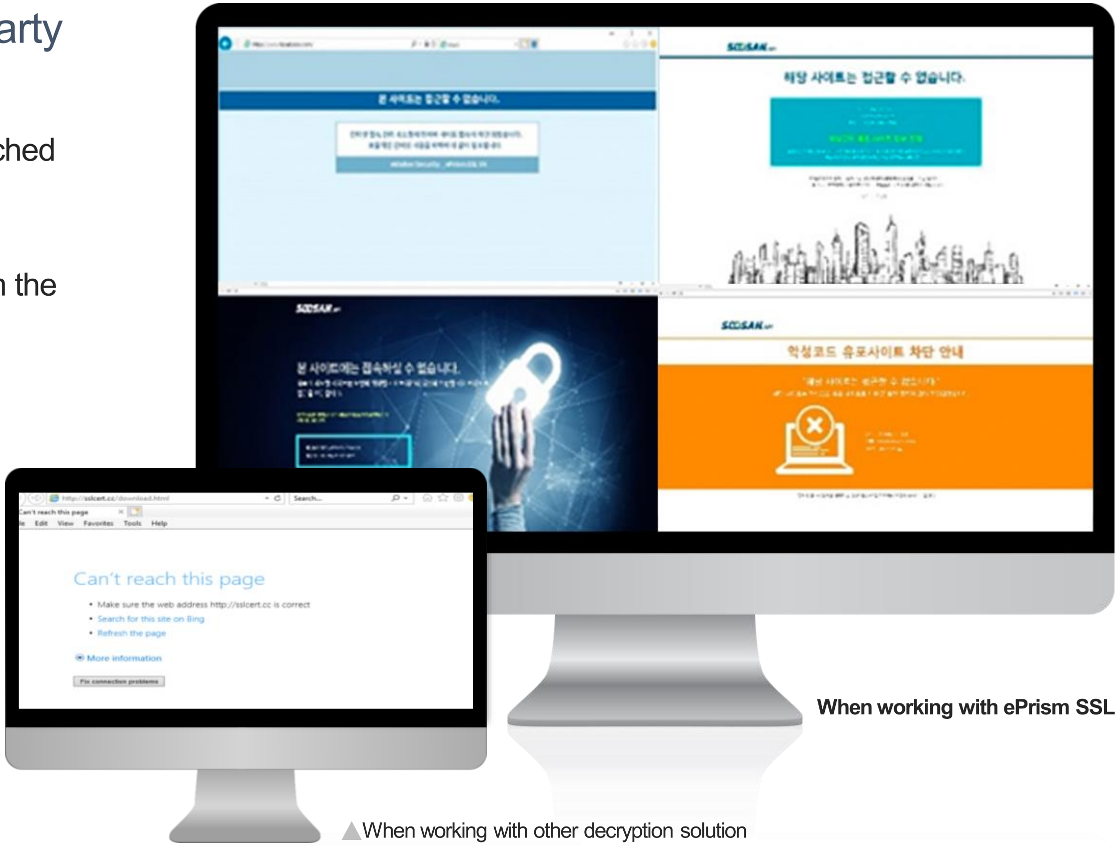
- Supplies decrypted SSL traffic to devices that can’t analyze encrypted traffic in order to allow them to function normally with SSL traffic.
- The active port (inline mode) and passive port (mirroring mode) can be used simultaneously


Router
Decryption Traffic
Plaintext traffic
DTZ (Decrypted Traffic Zone)
Active-Port
Intrusion Prevention System (IPS)
Distributed Denial of Service (DDoS)
Web Application Firewall (WAF)
Prism SSL VA
SOOSAN INT
Passive-Port
APT detection and analysis (APT)
Internal data leak prevention (N-DLP)
Harmful website blocking (SWG)
Network traffic analysis(Etc.)
Switch

MPT (Message Pass Through)

- Displays blocking messages from 3rd party devices
  - Blocking packets sent by 3rd party devices are matched to the right RST packet in the original (encrypted) session.
  - When SSL traffic is blocked, the blocking page from the 3rd party device is displayed exactly as it was sent

- User convenience
  - Users can easily find which device a security policy violation occurred on
  - Users can easily troubleshoot and configure policies when working with the majority of security devices including APTs, SWGs, and DLPs.



본 사이트는 접근할 수 없습니다.

해당 사이트는 접근할 수 없습니다.

본 사이트에는 접속하실 수 없습니다.

악성코드 유포사이트 차단 안내

http://sslcert.cc/download.html

Can't reach this page

- Make sure the web address http://sslcert.cc is correct
- Search for this site on Bing
- Refresh the page

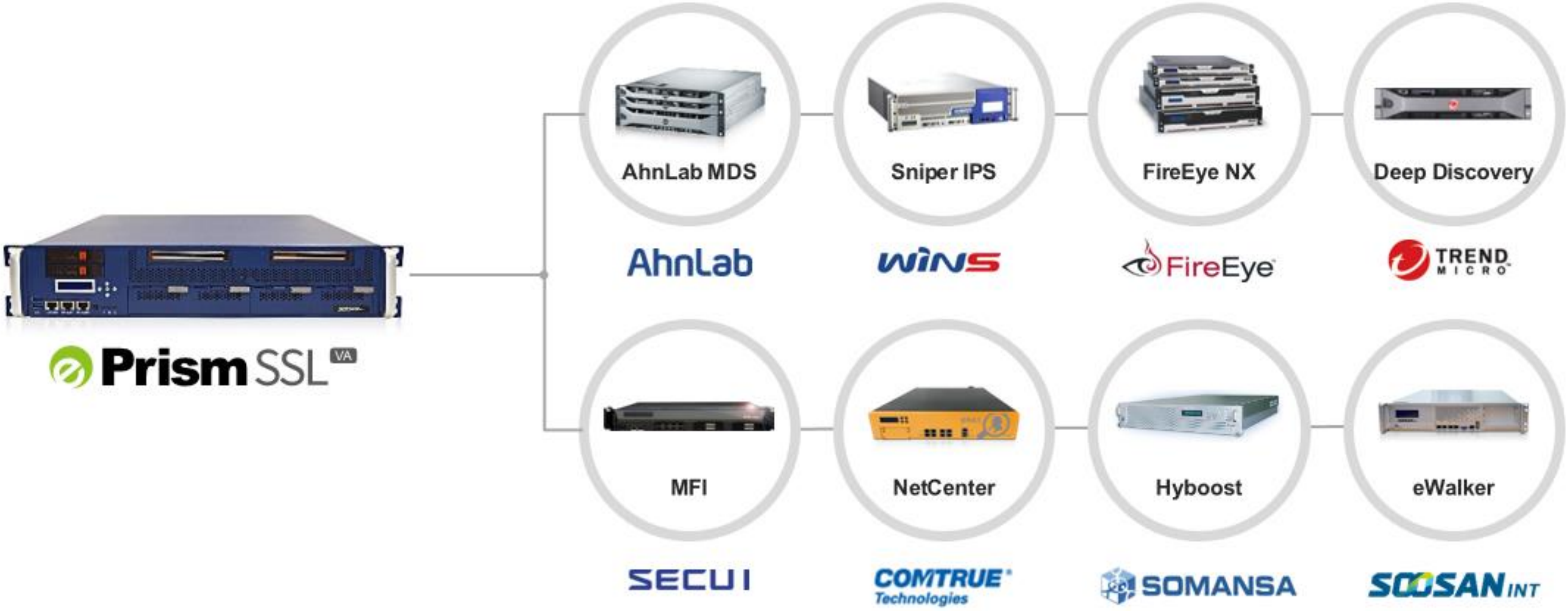
More information

Fix connection problems

When working with ePrism SSL VA ▲

▲When working with other decryption solution

Compatible With a Variety of Devices



Compatible with a wide variety of devices

- URL Filtering
- Advanced Threat Protection
- Digital Forensics
- Data Loss Prevention
- Network Email Data Loss Prevention
- Web Application Firewall

Easy Certificate Distribution and Management

● Guided certificate installation

- Provides automatic or manual CA certificate distribution and installation (for decryption).
- The GUI supports the creation of a certificate with your company's information and distribution and management on clients.

● Convenient certificate management

- Easy certification distribution for users left out of the pre-distribution by the NAC, PMS, or Active Directory.
- Easily respond to PC and/or OS changes.
- Supports Windows, Mac, Android and a variety of other operating environments.

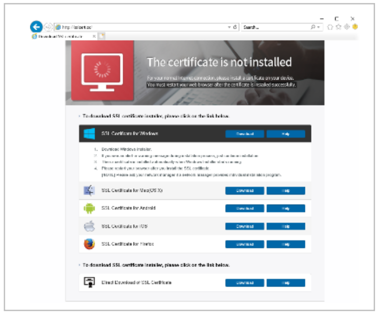
● Easily manages the installation status.

- Management for clients with personal decryption certificates
- Installation environments and SSL certificate distribution management.

Patents	A Method for Guided Private Certificate Installation
	Certificate Distribution Apparatus and Method
	Encrypted Traffic Monitoring Method and Apparatus
	Encrypted Traffic Session Processing Method and Apparatus

Automatic distribution

Automatically redirects a user to a certificate installation page of each OS.



The certificate is not installed

For your normal Internet connection, please install a certificate on your device.
You must restart your web browser after the certificate is installed successfully.

To download SSL certificate installer, please click on the link below.

SSL Certificate for Windows

1. Download Windows installer.
2. [illegible]
3. [illegible]
4. Please restart your browser after you install the SSL certificate.
[NOTE] Please ask your network manager if a network manager provides individual installation program.

SSL Certificate for Mac(OS X)

SSL Certificate for Android

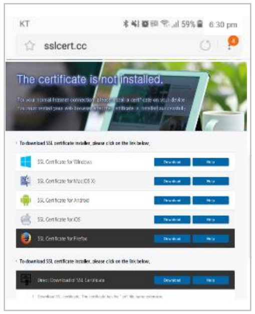
SSL Certificate for iOS

SSL Certificate for Firefox

To download SSL certificate installer, please click on the link below.

Direct Download of SSL Certificate

On a PC



The certificate is not installed.

For your normal Internet connection, please install a certificate on your device.
You must restart your web browser after the certificate is installed successfully.

To download SSL certificate installer, please click on the link below.

SSL Certificate for Windows

SSL Certificate for Mac(OS X)

SSL Certificate for Android

SSL Certificate for iOS

SSL Certificate for Firefox

To download SSL certificate installer, please click on the link below.

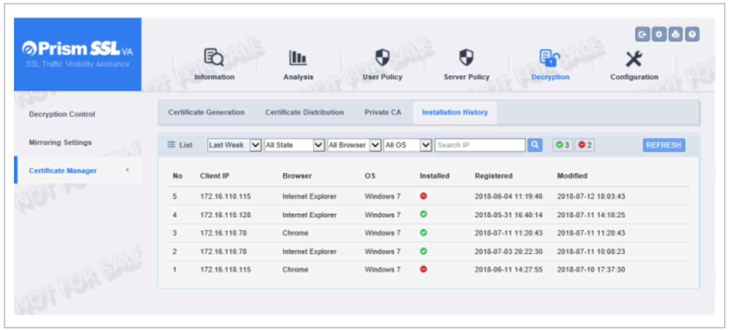
Direct Download of SSL Certificate

1. Download SSL certificate. [illegible]

On a Mobile

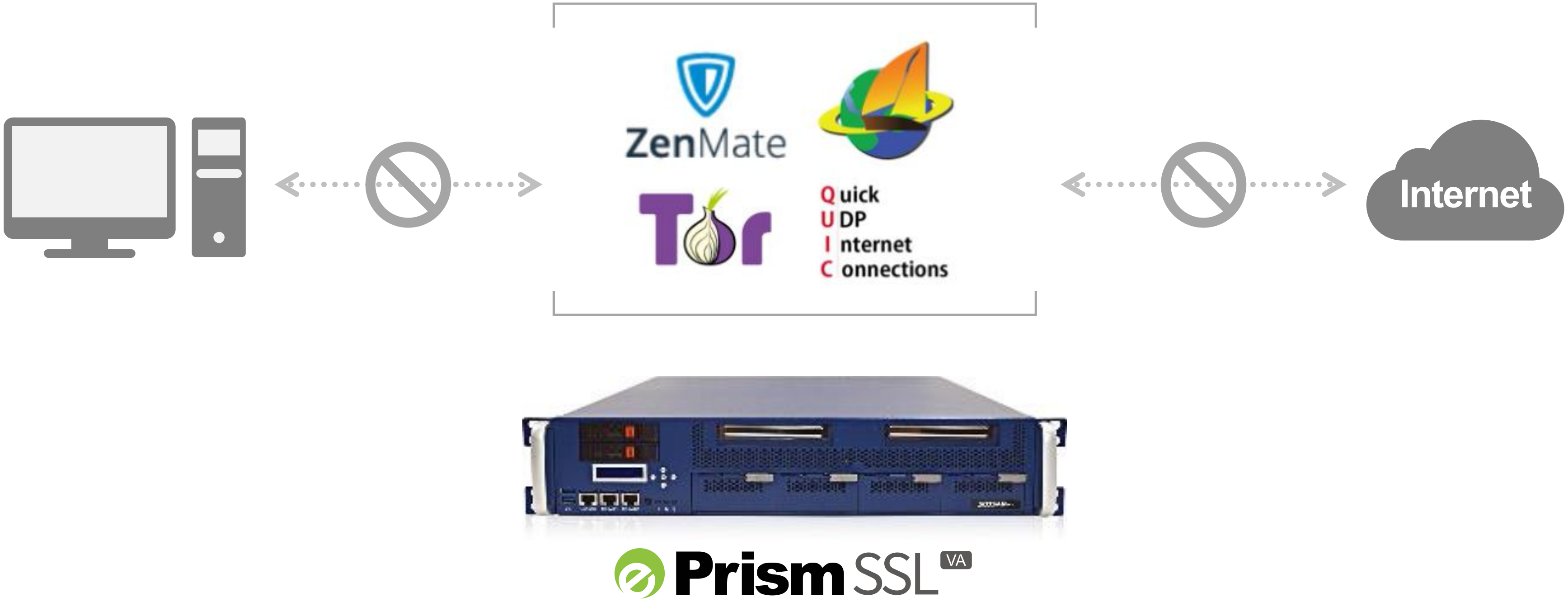
Certificate management

Manages the certificate installation and distribution for internal users.



No	Client IP	Browser	OS	Installed	Registered	Modified
5	172.16.110.115	Internet Explorer	Windows 7	●	2018-06-04 11:19:46	2018-07-12 18:03:43
4	172.16.110.128	Internet Explorer	Windows 7	✓	2018-05-31 16:40:14	2018-07-11 14:18:25
3	172.16.110.78	Chrome	Windows 7	✓	2018-07-11 11:20:43	2018-07-11 11:20:43
2	172.16.110.78	Internet Explorer	Windows 7	✓	2018-07-03 20:22:30	2018-07-11 10:08:23
1	172.16.110.115	Chrome	Windows 7	●	2018-06-11 14:27:55	2018-07-10 17:37:30

Internet Anonymizer Controls



● ePrism SSL Features:

- Analyzes plaintext and SSL sessions, and classifies L7 protocols including various Internet anonymizers.
- Maintains the latest protocol definitions with regular updates from the SOOSAN INT DB server.
- Through the combination of ePrism SSL VA policies, create a wide variety of traffic controls

Detailed Traffic Analysis and Log Search

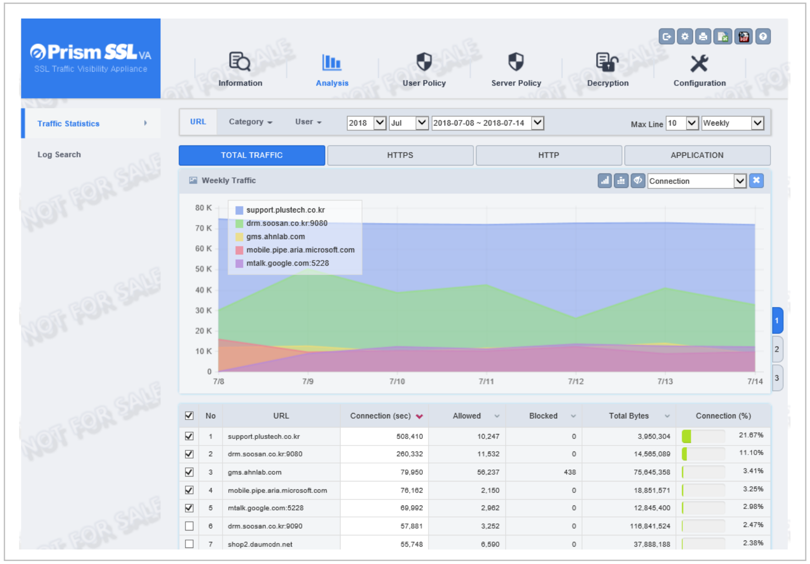
● SSL session monitoring

- Provides real time SSL traffic session monitoring.
- Analyzes SSL traffic to provide a wide variety of statistics and reports including up/down stream traffic and more
- Easily check whether SSL sessions were successfully established in order to process and manage exceptions

● Traffic state management

- Provides reports on SSL traffic, all traffic (encrypted and plaintext) and more through detailed traffic analysis.
- Provides detailed, printable reports in PDF or Excel format
- Search the included SSL log and all traffic log by various fields for traffic management

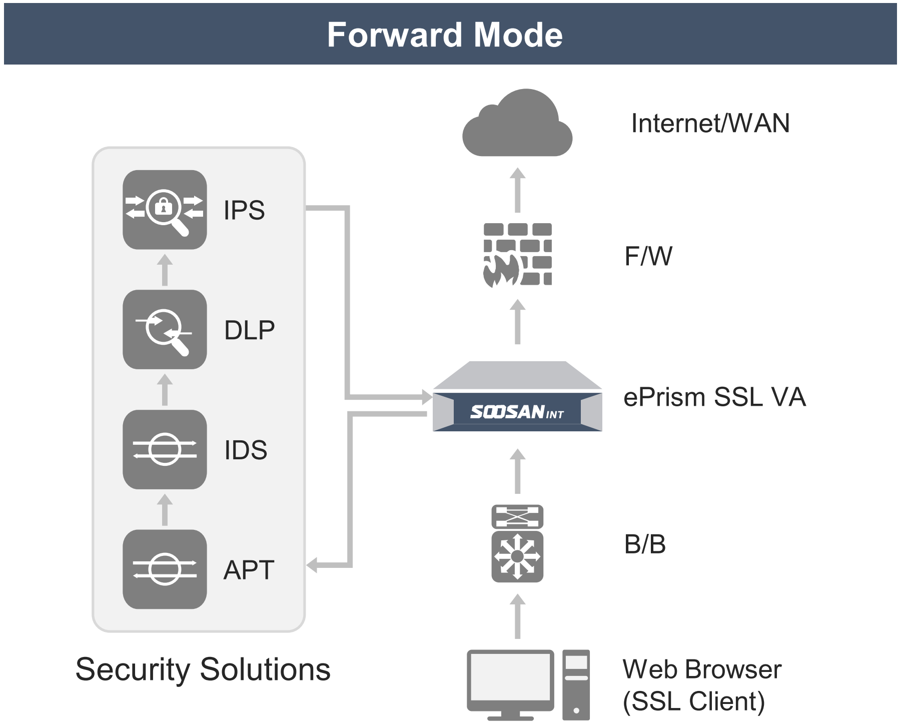
SSL session monitoring and traffic status management

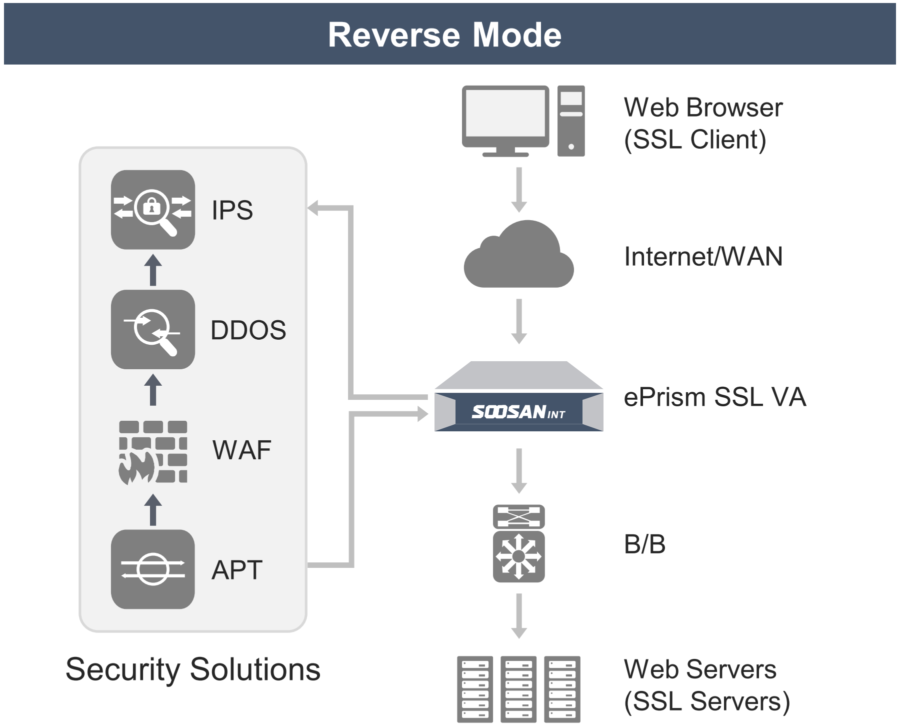


2018 | Jul | 2018-07-08 ~ 2018-07-14 | Max Line 10 | Weekly | Connection

☑	No	URL	Connection (sec)	Allowed	Blocked	Total Bytes	Connection (%)
☑	1	support.plustech.co.kr	508,410	10,247	0	3,950,304	21.67%
☑	2	drm.soosan.co.kr:9080	260,332	11,532	0	14,565,089	11.10%
☑	3	gms.ahnlab.com	79,950	56,237	438	75,645,358	3.41%
☑	4	mobile.pipe.aria.microsoft.com	76,162	2,150	0	18,851,571	3.25%
☑	5	mtalk.google.com:5228	69,992	2,962	0	12,845,400	2.98%
□	6	drm.soosan.co.kr:9090	57,881	3,252	0	116,841,524	2.47%
□	7	shop2.daumcdn.net	55,748	6,590	0	37,888,188	2.38%

Supports Many Installation Modes





Forward Proxy

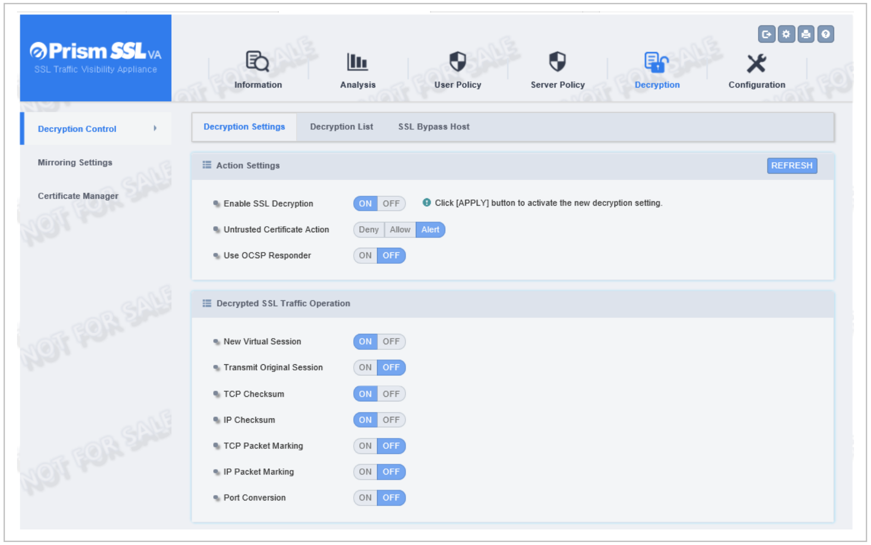
- Inside ➡ Outside
- ePrism SSL provides visibility when internal users access **external devices**.
- ePrism SSL works with many security appliances (IPS, ATP, DLP, and etc.).
- ePrism enhances SSL security to prevent internal data leaks.

Reverse Proxy

- Outside ➡ Inside
- ePrism SSL provides visibility when external users access **internal devices.**
- ePrism SSL provides many different security appliances (such as WAF and IPS) with SSL visibility.
- ePrism SSL enhances SSL security for external services.

Enhanced Usability

Decryption Management and Configuration



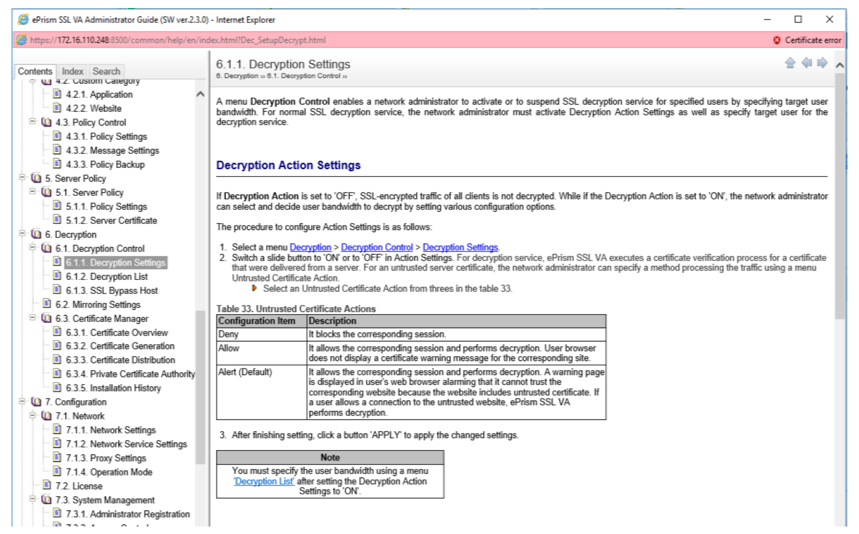
Action Settings

- Enable SSL Decryption [✓ ON] OFF — Click [APPLY] button to activate the new decryption setting.
- Untrusted Certificate Action Deny Allow [✓ Alert]
- Use OCSP Responder ON [✓ OFF]

Decrypted SSL Traffic Operation

- New Virtual Session [✓ ON] OFF
- Transmit Original Session ON [✓ OFF]
- TCP Checksum [✓ ON] OFF
- IP Checksum [✓ ON] OFF
- TCP Packet Marking ON [✓ OFF]
- IP Packet Marking ON [✓ OFF]
- Port Conversion ON [✓ OFF]

Online Help



6.1.1. Decryption Settings

6. Decryption » 6.1. Decryption Control »

A menu **Decryption Control** enables a network administrator to activate or to suspend SSL decryption service for specified users by specifying target user bandwidth. For normal SSL decryption service, the network administrator must activate Decryption Action Settings as well as specify target user for the decryption service.

Decryption Action Settings

If **Decryption Action** is set to 'OFF', SSL-encrypted traffic of all clients is not decrypted. While if the Decryption Action is set to 'ON', the network administrator can select and decide user bandwidth to decrypt by setting various configuration options.

The procedure to configure Action Settings is as follows:

1. Select a menu Decryption > Decryption Control > Decryption Settings.
2. Switch a slide button to 'ON' or to 'OFF' in Action Settings. For decryption service, ePrism SSL VA executes a certificate verification process for a certificate that were delivered from a server. For an untrusted server certificate, the network administrator can specify a method processing the traffic using a menu Untrusted Certificate Action.
   - Select an Untrusted Certificate Action from threes in the table 33.

Table 33. Untrusted Certificate Actions

Configuration Item	Description
Deny	It blocks the corresponding session.
Allow	It allows the corresponding session and performs decryption. User browser does not display a certificate warning message for the corresponding site.
Alert (Default)	It allows the corresponding session and performs decryption. A warning page is displayed in user's web browser alarming that it cannot trust the corresponding website because the website includes untrusted certificate. If a user allows a connection to the untrusted website, ePrism SSL VA performs decryption.

3. After finishing setting, click a button 'APPLY' to apply the changed settings.

Note
You must specify the user bandwidth using a menu 'Decryption List' after setting the Decryption Action Settings to 'ON'.

● Decryption Forwarding Settings

- Includes connection decryption settings to match the features of any security device
- Supports inline and other configurations to connect with 3rd party network appliances
- Changes to your network architecture are not needed (cost effective)

● Online Help

- Online help provided to aid administrators in operating ePrism SSL
- When help is running, help tips are automatically displayed with the corresponding menus.

Benefits

SSL Traffic Visibility

- With SSL visibility, **prevent web security threats**
- **Avoid** malware and ransomware **infection before it occurs.**
- **Create a** Decrypted Traffic Zone for SSL traffic, and feed **decrypted traffic to** current security devices

Internal Data Leak Prevention

- Analyze and block Internet anonymizers.
- **Classify L7 protocols** including many different anonymization/bypass protocols.
- **Protocol DB updates** on a regular base.

Look forward to…

Verified-System Reliability

- **Highest compatibility** with standard networks.
- **Supports network reliability** with several bypass modes.
- **Reliability verified** by many public/financial enterprises.
- Has around 80 **references** and has completed **field verification.**

Raise Enterprise Security Level

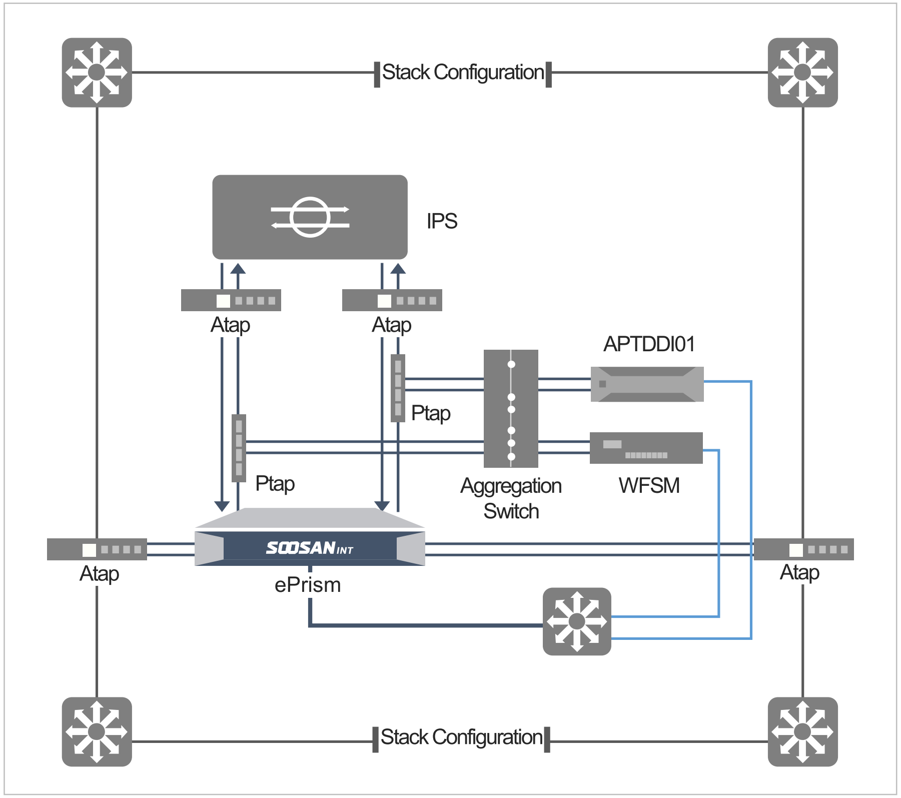
- **Understand and prevent** potential threat factors **in advance.**
- **Enhance public image and customer confidence** by deploying **powerful** security solutions.
- **Meet security compliance** reguluations, strengthened every year.
- **Reduce the social and economic cost** when security incidents occur.

III. Case Studies and Product Specs

- Case studies
- Product Lineup
- Specifications

Case Study 1

Client	Installation Environment
A Broadcasting Company	▪ Broadcasting companies are very sensitive to service availability by nature. For a quick recovery from potential service failures, additional bypass taps were installed in each section. ▪ Inline: An IPS device (manufactured by W) was connected. ▪ Mirroring: An APT device (manufactured by T) and a harmful site SWG (manufactured by SOOSAN INT) were connected.



Background

Issues with company F's product

- Not compatible with devices that block connections
- IPS devices cannot be connected inline

Issues with company B's product

- Not compatible with devices that block connections

ePrism Installation

Connected Blocking Devices

- If T's device sends a blocking packet for a decrypted packet, ePrism places a custom header on the blocking packet and checks where to send it in order support the process.

Connections to inline devices

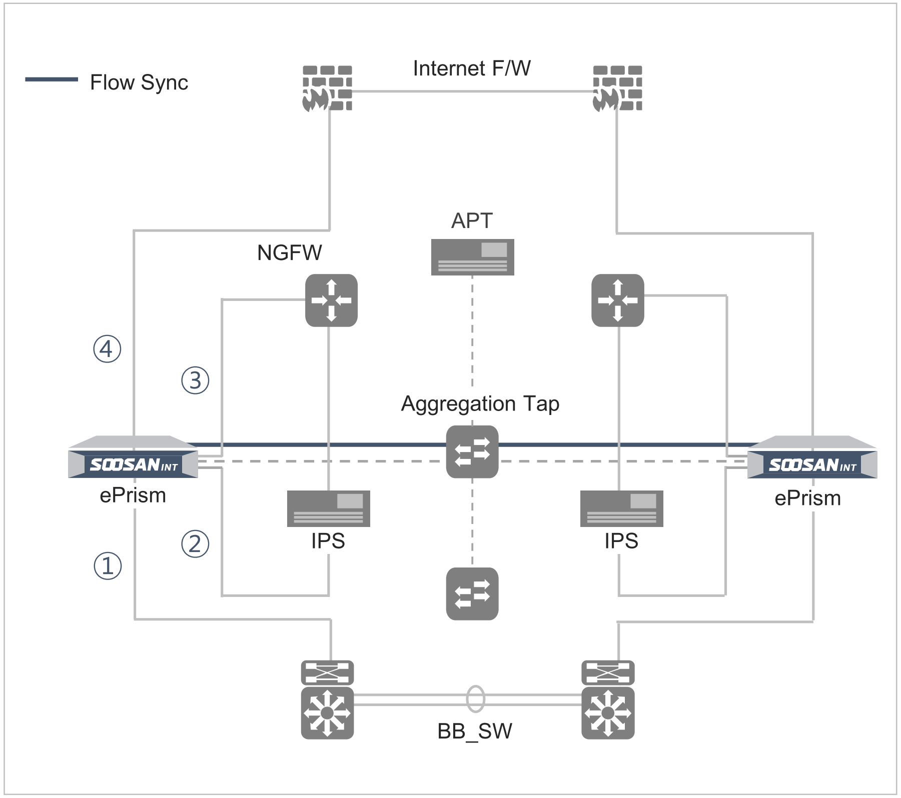
- ePrism can be connected to an inline devices by activating the Real In-Line mode.

Bypass speed on appliance failure (fail safe protection)

- Less than 2 sec.

Case Study 2

Client	Installation Environment
A Financial Company	▪ This client has been using company S' product as a harmful site blocking solution ▪ Network environment: Active/Standby ▪ Inline connections: NGFW (manufactured by P), IPS product (manufactured by W) ▪ Mirroring connections: APT (manufactured by F), harmful site blocking device (manufactured by S)



Background

Poor performance with standard harmful site blocking solutions

- F's device failed the connection test (Couldn't isolate/block and connect).
- Even with connected to the company's own products issues arose due to the use of ICAP

ePrism Installation

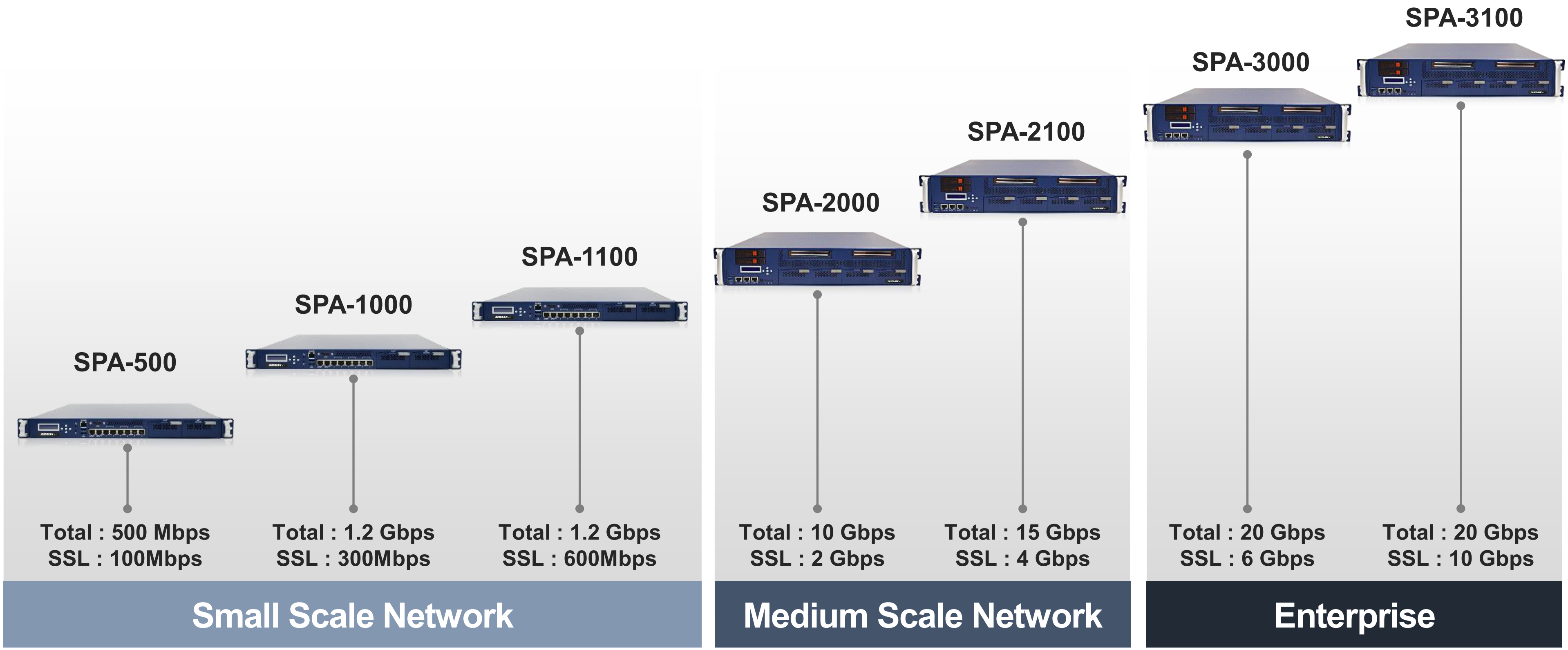
ePrism received good marks in compatibility with 3rd party devices during the PoC

Connections and blockings

- Checked that there were no issues connecting to S' device
  - ✓ Verified normal IP/website blocking worked
  - ✓ Verified that the blocking message was displayed even for HTTPS blocking
- Compatible with F's device
- Also provides compatibility with F's NX

Product Lineup

Prism SSL VA
Product Lineup



SPA-500
Total : 500 Mbps
SSL : 100Mbps

SPA-1000
Total : 1.2 Gbps
SSL : 300Mbps

SPA-1100
Total : 1.2 Gbps
SSL : 600Mbps

Small Scale Network

SPA-2000
Total : 10 Gbps
SSL : 2 Gbps

SPA-2100
Total : 15 Gbps
SSL : 4 Gbps

Medium Scale Network

SPA-3000
Total : 20 Gbps
SSL : 6 Gbps

SPA-3100
Total : 20 Gbps
SSL : 10 Gbps

Enterprise

Specifications

		SPA-500	SPA-1000	SPA-1100	SPA-2000	SPA-2100	SPA-3000	SPA-3100
Performance	Total throughput	500Mbps	1.2Gbps	1.2Gbps	10Gbps	15Gbps	20Gbps	20Gbps
	SSL intercept throughput	100Mbps	300Mbps	600Mbps	2Gbps	4Gbps	6Gbps	10Gbps
	No. of SSL sessions for new handshake (CPS)	700/sec	1,500/sec	2,500/sec	4,500/sec	6,000/sec	8,000/sec	35,000/sec
	No. of SSL flows (concurrent processes)	25,000	50,000	100,000	220,000	350,000	500,000	1,000,000
SSL Visibility	Session management mapping	Supported						
	Traffic analysis/monitoring							
	Multi-dimensional analysis & report (category/user/time)							
	Certificate distribution tool							
Filtering (*SSL /Non-SSL)	DB-based malicious code blocking	Supported						
	Internet anonymizer control							
	Filtering policy (category/user/time)							
Etc.	Network interface	Fixed 8 x 1Gbps Copper (additional 8 ports available for expanding)			Max. 16 ports available (1G/10G and no. of ports can be varied depending on client's environment)			
	Operation mode	Inline mode (Hardware Bypass available)						
	SSL management transparency	TCP session transparency maintaining via Certification Resigning (5-Tuple)						
	Encryption protocol	TLS 1.0, TLS 1.1, TLS 1.2, SSL v3						
	Public key algorithm	RSA, DHE, ECDHE						
	Symmetric key algorithm	AES,AES-GCM,3DES,SEED,ARIA,CAMELLIA,DES,RC4						
	Hash algorithm	MD5, SHA-1, SHA-2						
	RSA key	1024 to 8192 bits						

IV. Company Profile

- Company Overview
- Product Lineup

Company Overview

PrismSSL VA

“ 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

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.

V. Appendix

- Major References

Major References

Industrial Sector

- MBC
- HOYA
- SK bioland
- KCC
- Huvis
- eduwill
- Humanizing Genomics macrogen
- HS Ad
- woongjin
- BGFretail
- SSANGYONG

Financial Sector

- KDB Bank
- KDB Bank affiliate KDB Life
- KB Insurance
- MIRAE ASSET Life Insurance
- NongHyup Life Insurance
- SBI Savings Bank
- Welcome WELCOME FINANCE, INC.
- Danal

Public/ Education Sector

- Keit 한국산업기술평가관리원 Korea Evaluation Institute of Industrial Technology
- Korea Financial Investment Association
- KDIC Korea Deposit Insurance Corporation
- kamco KOREA ASSET MANAGEMENT CORPORATION
- Committee for the Five northern Korean Provinces
- Ministry of Oceans and Fisheries
- KEPCO KPS
- Gyeonggido Job Foundation 경기도일자리재단
- KIER KOREA INSTITUTE OF ENERGY RESEARCH
- 한국한의학연구원 KOREA INSTITUTE OF ORIENTAL MEDICINE
- KRICT 한국화학연구원 Korea Research Institute of Chemical Technology
- MAPO 마포중앙도서관
- 강원도교육청 Gangwon-do Office of Education
- 부천대학교 BUCHEON UNIVERSITY
- 4·16세월호참사 특별조사위원회

Prism SSL VA

SOOSAN INT

SOOSAN INT Co., Ltd.

✉ gb@soosan.co.kr