SSL/TLS 작동 원리 및 가시성 확보 및 AISVA의 제품 구조에 대한 WHITE PAPER

- 목 차 -

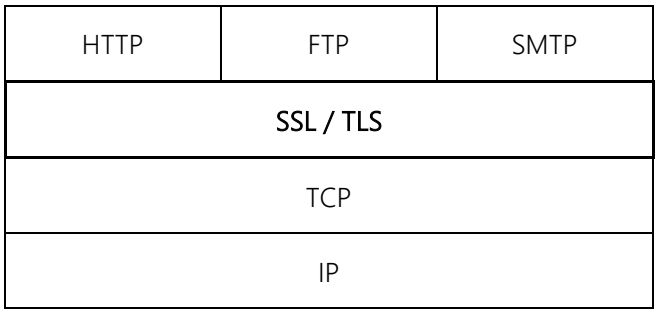
1. SSL/TLS 의 정의 및 작동 원리

인터넷 사용이 급증함에 따라 해킹이나 바이러스, 개인 정보 유출 등이 발생 빈도도 비례하여 증가하고 있다. 이에 대한 역기능들을 방어하고 통제하기 위한 Web 보안의 중요성도 함께 증대되고 있다. SSL과 TLS는 전송 레벨의 Web 보안 프로토콜로서 현재 유.무선 네트워크 환경에서 사용자의 인증, 데이터의 무결성 및 기밀성을 보장하기 위하여 보안 시스템 개발 시 그 활용도가 매우 크다. 본 WHITE PAPER 에서는 SSL과 TLS의 변화과정을 확인하고 프로토콜의 주요 동작과정 및 안정성을 분석해 본다. 또한 사용자의 익명성을 제공하기 위하여 SSL과 TLS를 확장한 SPSL(Secure and Private Socket Layer)프로토콜을 분석한다.

인터넷은 정보의 자유로운 상호 접금 및 공유를 가능하게 하였을 뿐만 아니라 금융, 주식 거래 등 다양한 웹 서비스 및 전자상거래와 같은 e-business를 창출하였다. 그러나 개방성, 공유성의 특징을 가지고 있는 인터넷은 이러한 순기능만 가지고 있는 것은 아니다. 인터넷 사용이 증가함에 따라 해킹이나 바이러스 , 개인 정보 유출 등의 발생 빈도도 비례하여 증가하고 있다. 이러한 역기능들을 방어 및 통제하기 위한 Web 보안의 중요성도 함께 증대되고 있다. 본 White Paper에서는 전송 레벨에서의 웹 보안 프로토콜인 SSL과 TLS의 변화 과정을 살펴보고, 각 프로토콜의 구조 및 동작과정 그리고 안전성을 진단한다.

1) SSL / TLS 개요

SSL(Secure Sockets Layer)은 1994년 Netscape 社에 의해서 Netscape 웹 브라우져를 통한 안전한 통신을 위하여 처음으로 제안되었으며, 1996년 Internet Engineering Task Force(IETF)에서 SSL v3.0을 제안하였다. 이후에도 SSL v3.0은 지속적으로 수정, 보안되었으며 1999년에는 TLS(Transport Layer Security)로 명칭이 바뀌어 RFC 2240(TLS v1.0)으로 표준화 되었다.



[그림 1] SSL/TLS 위치

<table>
<tr><td colspan="4">APPLICATION</td></tr>
<tr><td>SSL
Handshake
protocol</td><td>SSL Change
Cipher Spec
Protocol</td><td>SSL Alert
Protocol</td><td>Protocols secured
by SSL</td></tr>
<tr><td colspan="4">SSL Record Layer</td></tr>
</table>

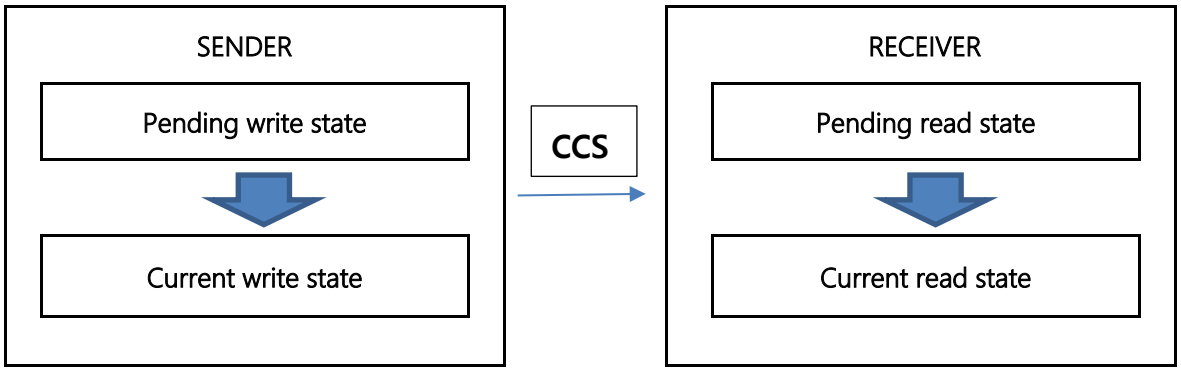
[그림 2] SSL/TLS 구조

SSL과 TLS는 [그림 1]과 같이 전송계층과 응용계층 사이에 위치함으로서 다양한 응용계층의 프로그램들과 쉽게 보안설정을 할 수 있으며, SSL/TLS는 [그림2]와 같이 레코드 레이어와 Handshake, Change Cipher spec, Alert, Application data 프로토콜로 이루어져 있다.

2) SSL/ TLS 의 동작

SSL/TLS는 크게 세션(session) 상태와 커넥션(connection)상태로 나누어서 이루어진다. 실제 통신은 하나의 세션 안에 여러개의 커넥션이 포함되는 형태로 이루어진다. 상태는 예비 상태(pending state)와 현재 상태(current state)로 나뉘어 지며, 예비 상태는 서버와 클라이언트가 통신을 수행하면서 설정된 알고리즘과 키를 임시로 저장하는 상태이며, 현재 상태는 레코드 레이어에서 실제 데이터가 처리될 때의 상태를 의미한다. 각각의 상태는 다시 read 상태와 write 상태로 이루어지며 read 상태는 상대방이 전송한 데이터를 읽기 위한 상태이며, write 상태는 상대방에게 데이터를 전송할 때 사용 되는 상태를 말한다.

Handshake 프로토콜에서는 알고리즘을 포함함 보안 파라미터(security parameters)가 설정되고, 이것은 레코드 레이어로 전달되어 키 블록을 생성하고 예비 상태로 저장된다. 저장된 예비 상태는 Change cipher spec 프로토콜에 의해 현재 상태로 옮겨진다. 이렇게 옮겨지면 예비상태는 NULL 상태로 다시 초기화 된다.



[그림 3] 상태의 변화

이 때, Change Cipher spec 메시지를 보내면 예비 write 상태가 현재 write 상태로 바뀌고, 다시 Change cihper spec 메시지를 받게 되면 예비 read 상태가 현재 read 상태로 변경된다. 위의 그림 3은 예비 상태와 현재 상태로 변화화는 과정을 나타낸 것이다.

Full Handshake에 의해 세션이 한번 생성되면 이후 통신은 Abbreviated Handshake 프로토콜에 의해 하나의 세션 상태를 공유하면서 커넥션 상태만을 재생성하여 이루어질 수 있다.

session identifier	임의의 바이트로서 세션 구분 담당
peer certificate	x. 509 v3 형식의 인증서
compression method	압축 알고리즘 명시
cipher spec	암호통신에 사용할 알고리즘 및 키 길이 명시
master secret	서버와 클라이언트가 공유하는 48 바이트의 비밀 값
is resumable	새로운 커넥션을 생성할 수 있는지를 나타내는 플래그

[표 1] SSL/TLS 세션 상태의 파라미터

server and client random	Hello 메시지에서 교환되는 서버와 클라이언트의 32 바이트의 비밀 랜덤 값
server write MAC secret	서버가 MAC 생성 시 사용할 비밀 값
client write MAC secret	클라이언트가 MAC 생성 시 사용할 비밀 값
server write key	서버의 암호화 키
client write key	클라이언트의 암호화 키
initialization vectors	블록 암호 알고리즘 사용 시 초기벡터(IV) 값
sequence numbers	Change eciper spec 메시지를 보내거나 받으면 0으로 초기화되고 메시지 마다 1씩 증가

[표 2] SSL/TLS 커넥션 상태의 파라미터

커넥션 상태는 표 2와 같은 파라미터를 포함하고 있다. 각 비밀키는 세션 상태의 master secret 과 서버와 클라이언트의 랜덤 수로 생성되므로 각 커넥션 상태는 다르게 설정된다.

3) SSL과 TLS의 차이점

TLS는 SSL에서 여러 사항을 고려하여 수정과 보안이 이루어졌다. 우선, 키생성 과정에서 SSL은 해쉬 함수를 직접 이용하나, TLS에서는 의사 난수 함수(PRF)를 이용하여 생성한다. 또한 SSL에서는 총 12개의 error 메시지가 존재하나 TLS에서는 SSL에서의 no-certificate 메시지를 제외한 12가지가 추가 되었다. Certificate Request 은 기존 TLS에서는 rsa_ephemeral_dh,

dss_emhemeral_dh, fortezza 방식이 제외되었다. Cipher suite 관련 TLS에서는 Fortezza 알고리즘이 제외되었다.

2. SSL/TLS 가시성 확보의 필요성

1) SSL/TLS이용한 보안 위협 증가

최근 몇 년간의 주요 보안 이슈는 DDoS 와 APT 라 할 수 있다. 특히, APT 의 경우, 사실상 그동안의 보안 위협들이 다양한 방식으로 혼합되어 일어나기 때문에 이를 방어하기 위해서는 다양한 애플리케이션에 대해 다양한 방법으로 대처해야만 한다.

그런데, APT 를 비롯한 다양한 보안 위협들에 대해서는 다양한 솔루션이 등장하고 있으며, 전통적인 보안 솔루션에서도 이를 방어하기 위한 다양한 기능 개선들을 추가하고 있는데 반해, 새로운 보안의 위협으로 대두되고 있는 것이 있다. 바로 SSL(Secure Socket Layer) 또는 TLS(Transport Layer Security) 라고 불리는 암호 규약이다.

TLS 는 클라이언트/서버 응용 프로그램이 네트워크로 통신을 하는 과정에서 도청, 간섭, 위조를 방지하기 위해서 설계되었으며, 암호화를 통해 최종단간의 인증, 통신 기밀성을 유지시켜준다. 그런데, 암호화 통신으로 인해 보안 솔루션이 이를 해독하고 분석 및 방어하는 것을 방해하는 현상이 발생하게 되었다. 보안을 강화하기 위한 방식이 오히려 보안 솔루션을 무력하게 되는 상황을 만들게 된 것이다.

최근의 추세는 개인정보, 거래정보와 같은 중요한 정보는 암호화하여 전송하도록 하고 있으며, 주요 웹 사이트에서도 HTTP 가 아니라 HTTPS 를 사용하는 경우가 많아졌다. 특히 구글, 페이스북, 아마존 등의 해외주요 웹사이트의 경우, 전면적으로 HTTPS 를 사용하고 있다. 문제는 APT 를 이용한 다양한 공격들에서 HTTPS 를 적극 활용하고 있으며, 이를 통한 악성코드 유포 등에 대한 분석 및 차단이 점점 어려워지고, 암호화된 트래픽은 지속적으로 늘어나고 있다는 것이다.

물론, 최근의 보안 솔루션들 – 대표적으로 웹 애플리케이션 방화벽, 침입방지솔루션, 차세대 방화벽 등 – 은 SSL/TLS 에 대한 보안 기능들을 지원하고 있으나, 평문 형태의 데이터 처리 성능에 비해서 암호화된 데이터에 대한 처리 성능이 현저하게 낮기 때문에 증가하고 있는 암호화 트래픽에 대해서 효과적으로 대응하기는 어려운 상황이며, 지속적으로 증가하고 있는 SSL 트래픽에 대하여 대응 방법이 제한적이라는 것이다.

2) APT 공격에서의 SSL 활용 사례

APT 공격에서 가장 흔히 사용되는 방식이 Drive by download 방식이며, Watering Hole 유형의 기법을 통해 감염된 사이트에 방문과 동시에 악성코드를 다운로드 하도록 하는 방식을 많이 사용한다. 보안 솔루션은 해당 사이트 자체를 미리 인지하여 차단하는 방식을 사용하거나, 실시간 해당 사이트의 응답데이터를 분석하여 악성여부를 판단한다. 또는 다운로드 된 악성 파일을 검사하는 정적 분석 또는 동적 분석을 통하여 파일 자체를 차단하기로 한다. 그런데 최근 공격자들은 악성파일을 감염시키는 과정에서 보안솔루션의 방어를 회피하기 위하여, SSL 로 암호화된 사이트를 이용하는 경우가 증가하고 있으며, 이런 경우 기존의 보안 솔루션으로 방어하는 것이 어려운 경우가 많이 있다. 이미 감염된 PC 를 원격으로 제어하거나, 감염 PC로부터 정보를 유출할 때 노출을 최소화하기 위하여 SSL로 암호화한 통신을 사용하기도 하기도 한다.

3) SSL 로 보호된 웹 사이트의 보안 공백

많은 웹 서버로 유입되는 다양한 공격들을 침입방지시스템 및 웹 애플리케이션 방화벽 등의 보안솔루션을 통하여 방어하고 있다. 현재의 대부분의 보안 제품들은 SSL 에 대한 보안 기능을 지원하고 있지만, SSL 처리 시에 발생하는 성능 문제를 안고 있으며, 증가하는 SSL 트래픽에 대응하기 위해서는 장비 증설이 필요한 경우가 많다. 또한 평문 통신에 비해 암호화된 통신을 처리하는 성능 10% 내외 수준인 경우가 대부분이다.

따라서 SSL 처리를 위해서는 보안 장비의 증설하거나, 증설이 어려운 경우는 해당 트래픽을 그냥 통과시킬 수 밖에 없는 상황이다. 이러한 경우, 통신 보안을 위해 도입한 SSL 로 인하여 보안의 공백이 발생하는 경우가 발생한다.

4) SSL 가시성을 제공하는 방식

SSL 가시성을 제공하는 방식은 여러 가지 방식이 있지만, 크게 2가지 형태로 나눌 수 있다. 네트워크 상에서 인라인으로 설치된 보안 장비에게 복호화 된 트래픽을 전달하는 방식과 미러링으로 설치된 보안 장비에게 복호화 트래픽을 전달하는 방식이다.

첫 번째로, 인라인 형태의 보안 솔루션 – 방화벽, IPS, DLP 등 - 에게 가시성을 제공하기 위해서는 다음과 같은 순서로 트래픽을 처리한다.

① Client 에서 Server 로 접속하는 SSL 접속을 가시성 장비에서 연결 처리
② 가시성 장비에서 복호화한 트래픽을 보안 장비로 전달
③ 보안 장비에서는 보안 기능 수행 후, 가시성 장비로 트래픽 전달
④ 가기성 장비는 암호화한 트래픽을 다시 서버로 전달

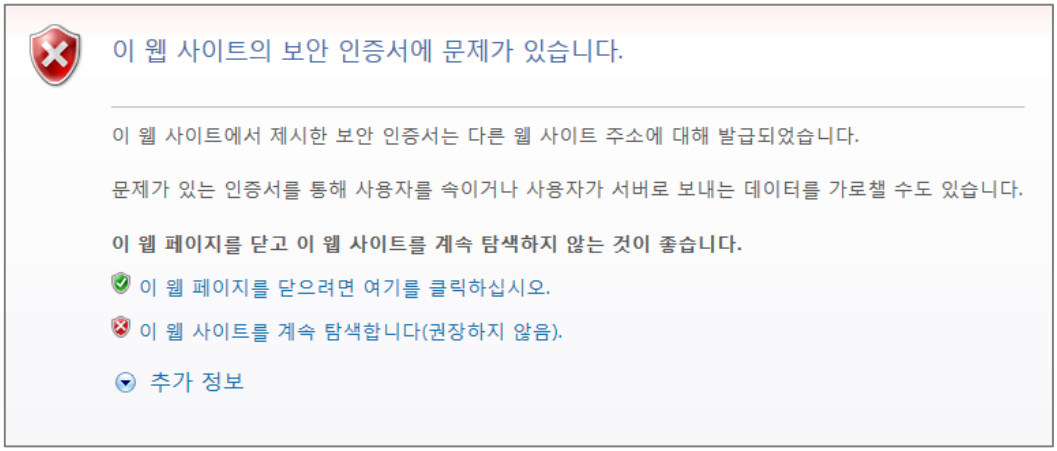
전통적인 방식의 네트워크 기반의 보안 솔루션에 제공하는 방식으로, 보안 장비의 SSL 처리를 위한 성능 감소를 제거하여 효과적인 망 운영을 할 수 있도록 지원하며, SSL 암복호화 처리가 애초에 불가능한 보안 제품이라 하더라도 완전한 보안 기능을 사용할 수 있도록 지원한다.

두 번째로, 미러링 형태로 연결된 보안 솔루션 – IDS, 로그분석 솔루션, 포렌식 솔루션 등 – 에게 가시성을 제공하기 위해서는 복호화된 트래픽을 복사해서 전달한다. 두 가지 방식의 차이점은 보안 장비에게 단순히 전달만 하느냐, 보안 장비를 통과한 트래픽을 서버로 다시 전달하느냐의 차이만 존재한다. 최근 APT 방어나 이상 징후 분석 등을 위한 보안 솔루션을 위해 적합한 방식이라 할 수 있다.

5) 트래픽 방향성에 따른 SSL 처리 방식

가시성 장비는 기본적으로 SSL 프록시의 구조를 가지고 있으며, 클라이언트의 SSL 접속을 처리하기 위해서는 반드시 필요한 요소가 있다. 인증서와 개인키가 바로 그것이다. SSL 인증서와 개인키가 없다면, 어떠한 SSL 에 대한 처리도 불가능하다.

단순히, SSL 암복호화를 하기 위해서라면, 실제 서버와는 무관한 인증서/개인키를 등록할 수도 있겠지만, 유효하지 않은 인증서를 사용했을 경우에는 사용자는 항상 에러 페이지를 보게 될 것이다.



인증서/개인키를 처리하는 방식도 보통 2가지 방식으로 처리된다.

내부 웹 서버를 보호하기 위해서 가시성 장비를 활용할 때는 실제 웹 서버의 인증서/개인키를 추출하여 그대로 등록하는 방식을 사용한다. 웹 애플이케이션 방화벽을 포함한 대부분의 프록시 장비에서 사용하는 방식이다. 가시성 장비가 마치 웹 서버인 것처럼 동일한 인증서/개인키를 이용하여 SSL 접속을 처리하고, 복호화한 평문 데이터를 보안 솔루션으로 전달하는 방식이다.

내부 웹 서버가 아니라, 인터넷에 있는 불특정 다수의 웹 서버로 접속하는 SSL 통신에 대해서는 첫 번째 방식을 사용할 수가 없다. SSL 통신을 처리하기 위해서는 인증서와 개인키가 반드시 필요한데, 개인키는 다른 말로는 비밀키라고도 부르는 것으로 외부에 노출될 경우 모든 보안이 무력화될 수 있기 때문에 절대 공개되지 않아야 한다. 다시 말해, 인터넷 상에 존재하는 외부 서버의 개인키를 등록하는 것을 불가능하다.

그래서, 가시성 장비는 인증서와 개인키를 자동으로 생성하는 방식을 사용한다.

가시성 장비에서는 사설 CA(Certificate Authority) 를 설치하고, SSL 트래픽이 발생할 때마다 해당 도메인에 적합한 인증서와 개인키를 자동으로 생성하여, 클라이언트와 SSL 통신을 수행한다. 이 때에도 생성된 인증서는 신뢰된 인증 기관에서 발행된 것을 아니므로, 클라이언트에서는 인증서 오류 메시지가 발생할 수 있다. 오류 없이 처리하기 위해서는 가시성 장비에서 사용하는 사설 CA 인증서를 클라이언트에 신뢰된 인증 기관으로 등록하는 절차가 필요하다.

사설 CA 인증서를 등록하는 절차는 웹 브라우저에서 몇 번의 클릭을 통해 가능하며, 일반 사용자에게 편이성을 제공하기 위해 별도의 프로그램을 한 번 실행하는 것으로 대신하기도 한다.

6) SSL 가시성 장비 선정에서의 주요 체크포인트

SSL 가시성 장비는 암복호화에 관련된 기능을 대행하여 다른 보안 솔루션에게 SSL 처리에 대한 부담을 줄여 본연의 보안 기능에 충실하도록 가시성을 제공하는 것이다. 본연의 기능으로만 볼 때는 매우 단순한 구조로 되어 있으므로, 도입 검토 시에 기능적 요소는 크게 중요하지 않는 것처럼 보인다. 그러나, 실제로 어떤 방식으로 또는 어떤 보안 장비에게 가시성을 제공할 것이냐에 따라 검토해야 할 중요한 몇 가지 요소가 있다.

가장 핵심적인 요소는 성능이다. 다른 보안 솔루션에게 충분한 수준의 성능으로 가시성을 제공하느냐이다. 현재 시장에 출시된 가시성 장비는 그리 많지는 않지만, SSL 처리 성능에 대한 수치를 볼 때 중요한 요소가 있다. 바로 인증서의 공개 키 길이이다. 과거에는 SSL 성능에 대한 테스트에서 주목되지 않은 항목이라 1024Bits 의 사설 인증서로 테스트되는 경우가 많았지만, 현재 대부분의 웹사이트에서 사용하는 인증서는 2048 Bits 로 구성되어 있다. 발표 기관에 따라 차이가 나기는 하지만, 대부분의 기업, 기관에서 공개된 문서에 따르면, 1024 Bits 와 2048 Bits 의 키 길이 차이에 따라 성능이 3~4배까지 차이가 나는 것으로 알려져 있다. 따라서 단순히 성능 수치를 볼 것이 아니라 공개키 길이가 얼마일 때의 성능인지를 반드시 확인할 필요가 있다.

두 번째로는 SSL 을 처리하는 방식 또는 순서와 관련된 것이다. 인라인(In-Line) 형태의 보안 솔루션에 가시성을 제공하는 경우를 보면, 클라이언트와 가시성 장비 사이의 SSL 세션, 가시성 장비와 보안 솔루션 사이의 평문 세션, 그리고 가시성 장비와 서버 사이의 SSL 세션으로 구성된다. 그리고, 보안 솔루션이 프록시 방식이라면, 가시성 장비와 보안 솔루션 사이에도 클라이언트 사이드 세션과 서버 사이드 세션으로 2개로 나누어진다.

① 클라이언트 – 가시성 장비 (SSL)
② 가시성 장비 – 보안 솔루션 (평문)
③ 보안솔루션 – 가시성 장비 (평문)
④ 가시성 장비 – 서버 (SSL, 평문)

보안 솔루션 특성에 따라 클라이언트의 요청 데이터 또는 서버의 응답 데이터가 보안 솔루션을 지나면서 차단되거나 변경되는 경우도 있으며, 패킷의 전송 흐름도 독립적으로 일어나는 경우가 있다. 따라서 가시성 장비에서도 최대 4개의 세션을 독립적이면서도 연관되게 처리해

야 한다. 그렇지 않을 경우, 세션에 단절이 발생하거나, 정상적으로 암복호화가 수행되지 않는 경우도 있다. 따라서 실제로 구성하고자 하는 보안 솔루션과의 연동 테스트는 필수적이다.

그 밖의 요소로는 네트워크 구성과 관련해서 투명 프록시 형태로 구성이 가능해야 하며, 장애 시에는 선택적으로 바이패스 하는 형태로 대비책을 가지고 있어야 하며, 부가적인 기능이 어느 정도로 지원하느냐를 검토해야 할 것이다. 단순히 다양한 기능을 지원하는 것보다는 운영 환경에 얼마나 적합하냐는 것이 더 중요하다.

7) SSL 가시성 장비를 통한 보안 수준 향상

SSL로 암호화된 서비스의 증가는 필연적이며, 보안 솔루션의 SSL에 대한 지원도 필수적이라 할 수 있다. 전체 트래픽에서 SSL 에 대한 비중이 극히 적은 경우에는 기존 솔루션에서 SSL 보안 기능을 추가하는 것으로 대신할 수 있겠지만, 지속적으로 증가하는 SSL 트래픽에 대응을 하기에는 어려움이 있을 것이다. 기존 보안 솔루션의 증설만으로는 목표 달성이 어려울 수 있으며, SSL 가시성 장비에 대한 검토 또는 도입을 통해 SSL 통신에 대한 보안 공백을 해소하는 계기로 만드는 것이 필요한 시점이 왔다.

3. APPLICATION INSIGHT SVA 소개

APPLICATION INSIGHT SVA(SSL Visibility Appliance)는 SSL Traffic에 대한 복호화 및 암호화를 제공함으로써 기존 보안 장비에서 암호화된 트래픽에 대해서도 강력한 보안정책이 적용 될 수 있도록 SSL 트래픽에 대한 가시성을 제공하는 전용 어플라이언스 제품입니다.

1. 제품 구성도

1.1. 구성 모드

AISVA 제품은 Active Inline 과 Passive Inline 을 동시적으로 지원하여 다양한 보안 제품들과 연동이 가능하도록 설계되어 있습니다.

- eth 1 ~ eth 4 : Active Inline Port (For IPS, FW, WAF 등의 인라인 장비)
- eth 5 ~ eth 16 : Passive Inline Port (Option NIC, For IDS, TMS 등의 미러링 장비)

[AISVA 구성모드]

1.2. Session Flow

AISVA는 Inbound 및 Outbound SSL 트래픽에 대해서 동시적으로 암복호화가 가능합니다.

즉, 외부에서 내부 SSL 서버로의 통신 / 내부에서 외부 SSL 서버로의 통신에 대해서 동시적인 암복호화가 가능합니다. 복호화 Session Flow 과정은 다음과 같습니다.

- **Active-Inline (인라인 장비)**

  ① AISVA가 Proxy로 작동하여 클라이언트와 직접 세션을 맺고 SSL 통신을 한다.

  ✓ AISVA에 내부 SSL 서버의 IP, Port, 사용중인 SSL 인증서를 등록해야 한다.

  ② AISVA는 암호화되어 있던 SSL 트래픽을 복호화하여 eth2번 포트로 전송한다.

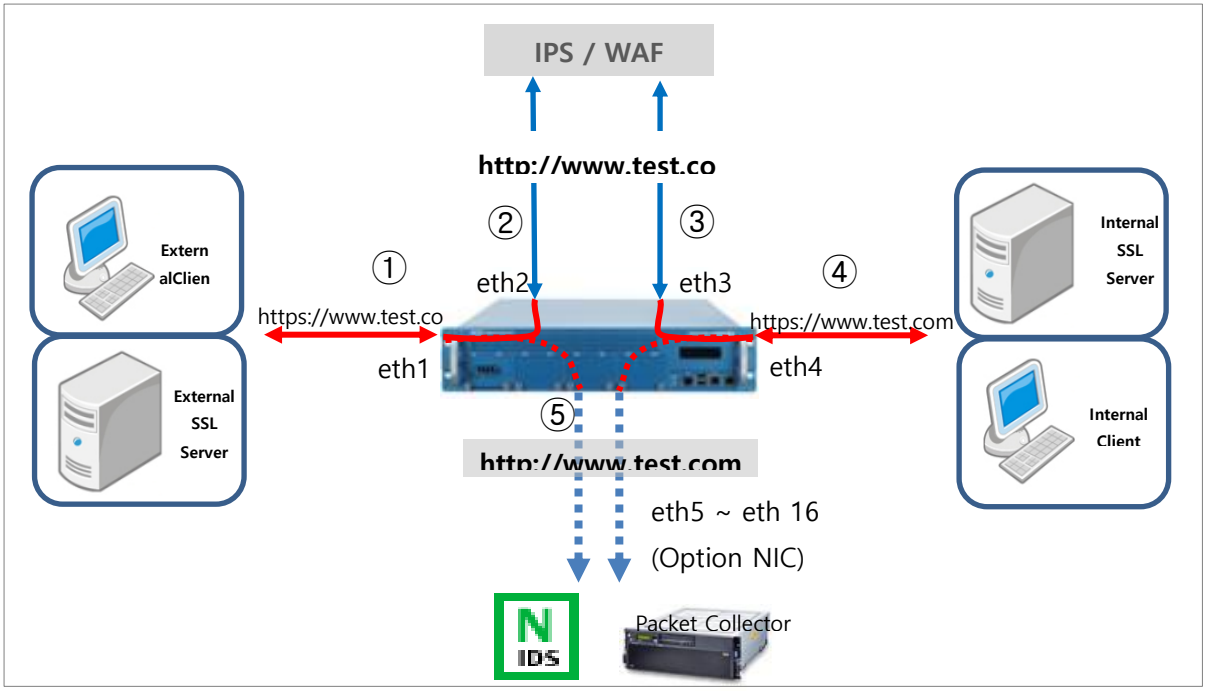
  이때 eth1 번을 통해 유입된 None-SSL 트래픽도 함께 전송한다.

  ③ 복호화된 SSL 트래픽은 IPS/WAF등과 같은 In-Line 보안 장비를 통과한 후 eth3 포트를 통해 재 유입된다.

  ④ AISVA는 eth3번을 통해 유입된 트래픽을 다시 암호화하여 eth4번으로 전송한다.

- **Passive-Inline (미러링 장비)**

  ⑤ ②번 단계에서 eth 2번을 통과하는 트래픽을 Passive Inline Port(eth 5 ~ eth 16)에 동시적으로 복사하여 준다.



[AISVA Session Flow]

1.3. Outbound SSL 인증서

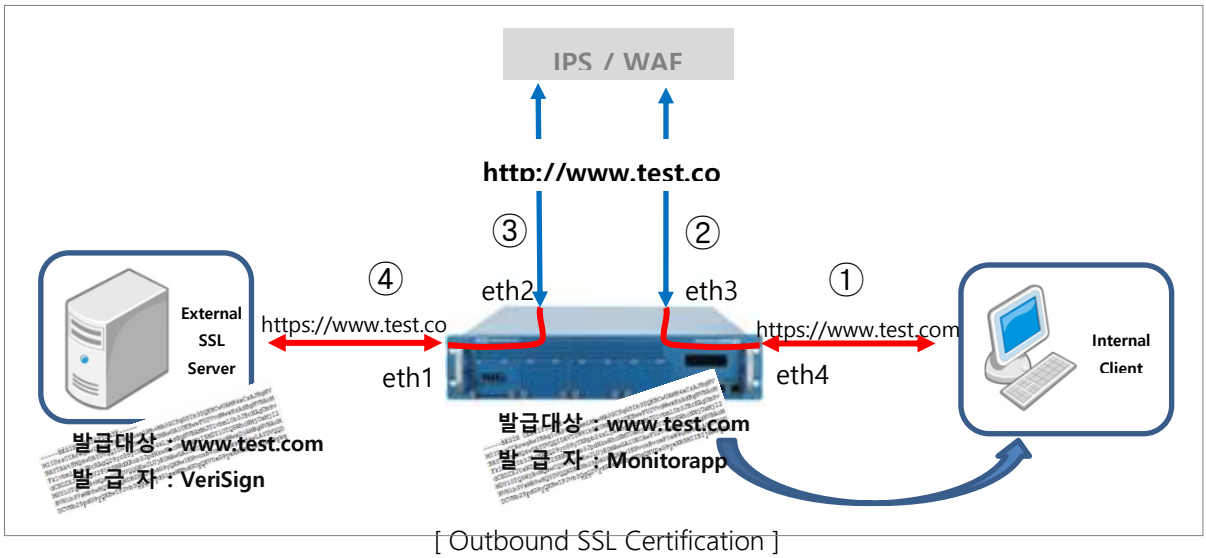
AISVA는 외부(인터넷)의 SSL 서버와의 통신에 대해서도 암복호화가 가능합니다.

단, Outbound SSL 암복호화 기능은 선택사항으로 불필요할 경우에는 사용하지 않아도 무방합니다.

Outbound SSL 설정은 Inbound SSL 설정과 다르게 SSL 인증서를 등록하지 않아도 됩니다.

AISVA가 아웃바운드 트래픽의 TCP 세션에서 SSL 세션을 자동으로 추출하고 내부 사용자의 앞단에서 Proxy로 작동하여 해당 SSL 통신의 인증서를 자동 생성하여 복호화가 진행됩니다.

그러나, AISVA의 Root CA를 이용하여 인증서를 발급하게 되어 내부 클라이언트의 브라우저에서 신뢰할 수 없는 인증서로 경고나 오류가 발생하게 됩니다. 그래서 AISVA의 Root CA 인증서를 내부 클라이언트의 PC에 신뢰할 수 있는 인증서로 등록해야 합니다.



[Outbound SSL Certification]

1.4. SSL Offload

AISVA는 웹서버의 부하를 줄이기 위하여 SSL 통신의 SSL Offload를 지원합니다.

클라이언트와 AISVA는 기존 그대로 SSL 통신을 하고, AISVA와 웹서버는 일반 평문 통신을 하게 됩니다.

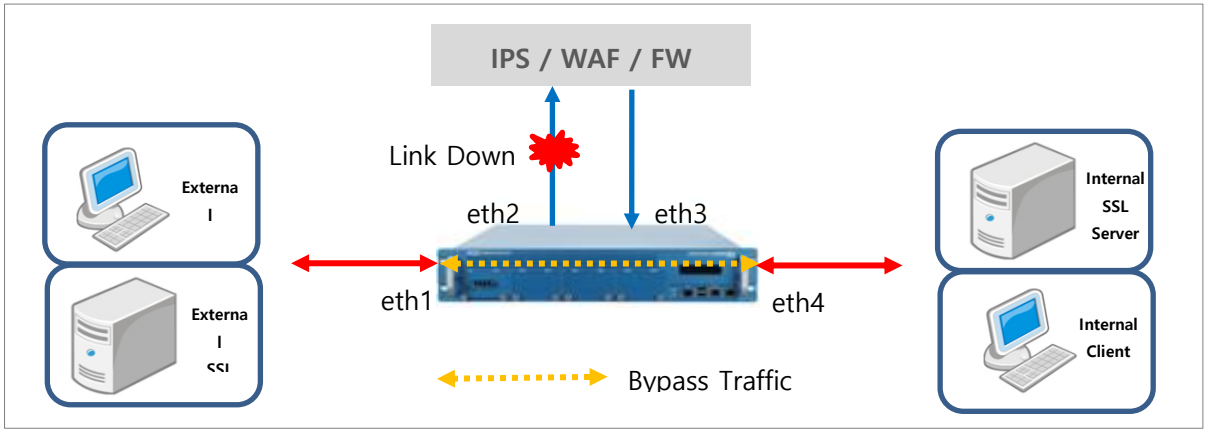
SSL Offload 기능은 기능 변경 이후 eth1 / eth2 번만을 Inline으로 연결하여 사용 가능합니다.

[SSL Offload]

1.5. Bypass

AISVA는 장애 상황에 맞게 대처하기 위해 아래와 같이 Bypass를 지원합니다.

- eth2 / eth3 Link Down : eth1 ←→ eth4 다이렉트 통신



- Software Fail / Hardware Fail / Power Off : eth1 ←→ eth2, eth3 ←→ eth4 통신