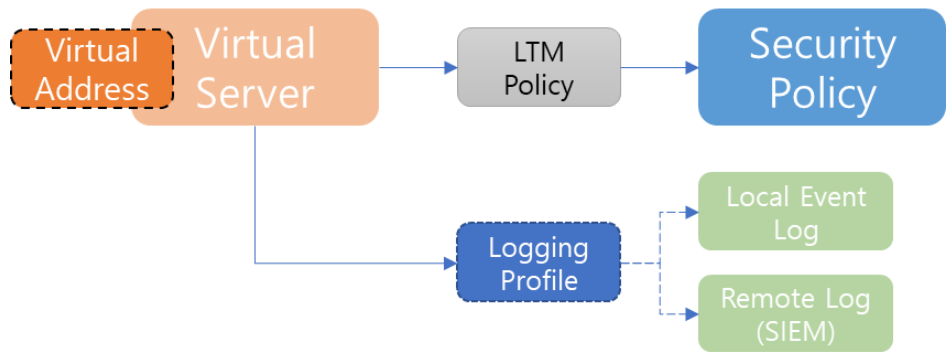


BIG-IP ASM(AWAF) 서비스 추가 방법

일반적인 In-line 구성에서 vlan-group 사용 중인 경우를 기준으로 서비스 추가 방법에 대한 가이드 문서입니다.



웹 방화벽에서 하나의 서비스를 구성하는 경우에 아래와 같은 과정을 거칩니다.

1. (장비에서 SSL 암호화 사용하는 경우) 인증서 등록 및 Client SSL Profile 작성
2. VS 와 Security Policy 연동을 위한 LTM Policy 작성 (또는 수정)
3. Virtual Address 및 Virtual Server 생성 (LTM Policy, Logging Profile 연동)
4. 서비스 확인

1 (사전 작업) 인증서 추가

BIG-IP 에서 사용하는 모든 인증서는 System - Certificate Management : Traffic Certificate Management : SSL Certificate List 메뉴에서 관리합니다.

System » Certificate Management : Traffic Certificate Management : SSL Certificate List							
Traffic Certificate Management Device Certificate Management HSM Management							
* Search Import... Create...							
<input checked="" type="checkbox"/>	Status	Name	Contents	Key Security	Common Name	Organization	Expiration
<input type="checkbox"/>		20220111_star.itian.co.kr	RSA Certificate & Key	Normal	*.itian.co.kr		Feb 4, 2023
<input type="checkbox"/>		20220111_star.itian.co.kr_chain	Certificate Bundle				Jun 1, 2023 - Nov 10, 2031
<input type="checkbox"/>		baek_test_chain	Certificate Bundle				Jan 1, 2029 - Jan 1, 2031
<input type="checkbox"/>	<input type="checkbox"/>	ca-bundle	Certificate Bundle				May 16, 2022 - Oct 6, 2046
<input type="checkbox"/>	<input type="checkbox"/>	default	RSA Certificate & Key	Normal	localhost.localdomain	MyCompany	Mar 20, 2031
<input type="checkbox"/>	<input type="checkbox"/>	f5-ca-bundle	RSA Certificate		Entrust Root Certificat...	Entrust, Inc.	Dec 8, 2030
<input type="checkbox"/>	<input type="checkbox"/>	f5-irule	RSA Certificate		support.f5.com	F5 Networks	Jul 19, 2027
<input type="checkbox"/>		sskim_test2	RSA Certificate & Key	Normal	*.kkachiandkkachi.com		May 2, 2023
<input type="checkbox"/>	<input type="checkbox"/>	yjm_test.crt	RSA Certificate & Key	Normal	www.jermy.com	IT	Mar 22, 2023
Archive... View Certificate Order Status... Delete OCSP Cache... Delete...							

리스트 우측 상단의 Import 버튼을 선택해 인증서 Key 를 업로드 합니다.

System » Certificate Management : Traffic Certificate Management : SSL Certificate List » Import SSL Certificates and Keys

SSL Certificate/Key Source

Import Type	Key
Key Name	<input checked="" type="radio"/> New <input type="radio"/> Overwrite Existing kjs-testdomain.com
Key Source	<input checked="" type="radio"/> Upload File <input type="radio"/> Paste Text 파일 선택 선택된 파일 없음
Security Type	Password
Password	Normal Password
Free Space on Disk	7046 MB

Cancel Import

인증서 항목의 이름은 기존 서비스가 있으면 그 형식을 따르되, 신규 구축이라 기존 형식이 없는 경우, 아래 형식으로 생성하면 좋습니다.

구분	형식
인증서 + 키	등록일자_도메인
Chain 인증서	등록일자_도메인_Chain

Password 가 있는 경우 함께 작성합니다. 작성이 완료되면 import 버튼을 선택해 업로드합니다.

Key Import 완료 후 생성된 항목을 다시 선택해 진입합니다.

System » Certificate Management : Traffic Certificate Management : SSL Certificate List

Traffic Certificate Management Device Certificate Management HSM Management

kjs Search Reset Search Import... Create...

<input checked="" type="checkbox"/>	Status	Name	Contents	Key Security	Common Name	Organization	Expiration	Partition / Path
<input type="checkbox"/>		kjs-testdomain.com		RSA Key	Normal			Common

Archive... View Certificate Order Status... Delete OCSP Cache... Delete...

System » Certificate Management : Traffic Certificate Management : SSL Certificate List » kjs-testdomain.com

Certificate Key Certificate Signing Request Instances

General Properties

Name	kjs-testdomain.com
Partition / Path	Common
Certificate Subject(s)	No certificate

Import... Create...

Import 버튼을 선택해 인증서를 업로드합니다.

System » Certificate Management : Traffic Certificate Management : SSL Certificate List » /Common/kjs-testdomain.com

SSL Certificate/Key Source

Import Type	Certificate
Certificate Name	/Common/kjs-testdomain.com
Certificate Source	<input checked="" type="radio"/> Upload File <input type="radio"/> Paste Text 파일 선택 선택된 파일 없음
Free Space on Disk	7046 MB

Cancel Import

업로드가 완료되면 시리얼 번호와 만료일자로 인증서를 점검합니다.

Certificate Properties	
Public Key Type	RSA
Public Key Size	2048 bits
Expires	Apr 14 2023 16:45:46 KST
Version	1
Serial Number	387589546

Chain 인증서 업로드는 별도 항목, Certificate 형식으로 업로드하면 됩니다.

인증서 등록 완료 후 점검 할 항목은 Subject - Common Name(CN)과 Issuer Common Name(CN) 그리고 Subject Alternative Name(SAN) 입니다.

Serial Number	02:0f:67:5f:c1:5f:68:bd:a8:73:39:d2:53:3d:e6:a2
Fingerprint	SHA256/EC:59:45:46:32:C6:29:F7:DF:02:C1:21:1E:FE:76:D4:3C:F3:B7:A2:49:EE:E3:F3:F4:45:38:5A:4F:F7:B5:05
Subject	Common Name: *.itian.co.kr Organization: Division: Locality: State Or Province: Country:
Issuer	Common Name: RapidSSL TLS DV RSA Mixed SHA256 2020 CA-1 Organizational Unit: DigiCert Inc Division: Locality: State Or Province: Country: US
Email	
Subject Alternative Name	DNS:*.itian.co.kr, DNS:itian.co.kr

Subject - CN 과 SAN 은 인증서 사용이 가능한 도메인을 확인하는 용도, 그리고 Issuer 의 CN 은 Chain 인증서의 Subject CN 과 일치하는지 확인하는 용도입니다.

General Properties	
Name	20220111_star.itian.co.kr_chain
Partition / Path	Common
Certificate Subject(s)	RapidSSL TLS DV RSA Mixed SHA256 2020 CA-1, DigiCert Inc DigiCert Global Root CA, DigiCert Inc
Certificate Properties	
Public Key Type	RSA
Public Key Size	2048 bits
Expires	Jun 01 2023 08:59:59 KST
Version	3
Serial Number	07:98:36:03:ad:e3:99:08:21:9c:a0:0c:27:bc:8a:6c
Fingerprint	SHA256/E6:FA:48:4A:85:89:40:D1:01:97:85:55:45:4A:A4:66:53:1A:B6:C4:AB:C4:AD:2B:00:06:26:AA:AC:0D:04:F9
Subject	Common Name: RapidSSL TLS DV RSA Mixed SHA256 2020 CA-1 Organization: DigiCert Inc Division: Locality: State Or Province: Country: US
Issuer	Common Name: DigiCert Global Root CA Organizational Unit: DigiCert Inc Division: www.digicert.com Locality: State Or Province: Country: US

Chain 인증서의 Issuer 는 일반적으로 CA 인증서로 Chain 과 root CA 인증서를 같이 제공하는 곳도 있으니, 간단하게 확인하면 되겠습니다.

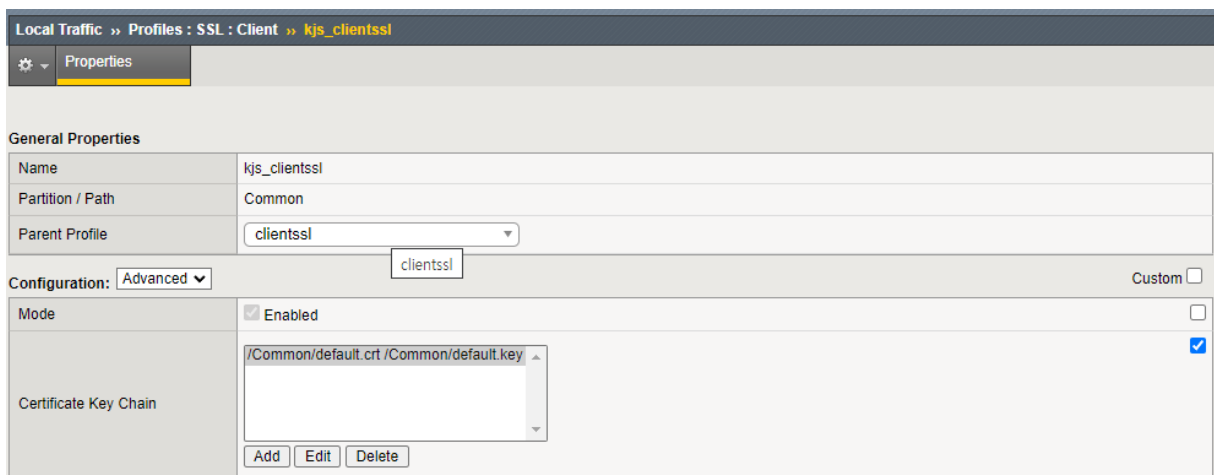
2 (사전 작업) Client SSL Profile 생성

Local Traffic >> Profiles : SSL : Client 메뉴에서 Create 버튼을 선택해 신규 Client SSL Profile 생성화면으로 진입합니다.

- 서비스를 신규 생성하는 경우, 서비스 도메인에 맞춰 Client SSL Profile 이름을 Domain 으로만 작성하는 것이 좋습니다. 작성일자나 만료일자로 작성하면 추후 인증서 교체에 매번 Profile 을 신규 생성해야 하는 불편함이 있습니다.
- 하나의 Virtual Server(Destination IP/Port)에서 둘 이상의 Domain 을 서비스하는 경우, Multi SSL Profile 를 등록해줘야 하는데, 이 때 SSL Profile 내에 SNI 설정에 주의해야 합니다.
- Star(*) 인증서와 혼용하는 경우, Star(*) 인증서를 Default SSL Profile 로 설정해야 합니다.

Server Name	<input type="text"/>
Default SSL Profile for SNI	<input type="checkbox"/>

Certificate Key Chain 항목에서 기존 인증서 항목을 선택, Add 버튼을 선택합니다.



세부 설정 화면에서 1 번 과정에서 업로드한 인증서, 키 (필요시 Chain 인증서)를 선택하고, 패스워드가 있는 경우, 패스워드 작성 후 OK 버튼을 선택합니다.

Edit SSL Certificate Key Chain	
Certificate	<input type="text" value="default.crt"/>
Key	<input type="text" value="default.key"/>
Chain	<input type="text" value="None"/>
Passphrase	<input type="password"/>
<input type="button" value="OK"/> <input type="button" value="Cancel"/>	

화면 최하단에서 Finished 버튼을 선택해 Client SSL Profile 생성을 완료합니다.

3 (사전 작업) Security Policy 준비

- 기존 default_policy 가 있다면 해당 Policy Clone 을 통해 복제하면 간단합니다.

- 기존의 서비스와 같은 Policy 로 묶을 수 있는지 여부를 담당자와 확인하여, Security Policy 가 과도하게 늘어나지 않도록 (관리가 어렵지 않도록) 하면 좋습니다. (예를 들어, service.domain.com / dev-service.domain.com 같은 경우)

4 (사전 작업) LTM Policy 준비

Local Traffic >> Policies : Policy List 메뉴에서 LTM Policy 를 작성합니다.

- LTM Policy 적용에는 두 가지 방법이 있습니다.
- Virtual Server 의 Security 탭에서 Application Security Policy 를 직접 선택하여, LTM Policy 가 자동 생성되도록 하는 방법과 LTM Policy 를 직접 생성하여 Rule 에서 작성한 조건에 따라 Security Policy 에 연동되도록 하는 방법입니다.
- 기존 장비에 서비스만 추가하는 것이라면 기존 방식을 유지하는 것이 좋으나, 신규 구축인 경우, 고객 담당자와 협의가 필요합니다. 특히, 하나의 Virtual Server 에서 여러 도메인을 서비스하는 경우, LTM Policy 를 직접 생성하여 Rule 을 설정하는 것이 필수이므로, 확인이 필요합니다.

일반적인 서비스 Security Policy 적용을 위한 LTM Policy 설정은 Host header 기준으로 Security Policy 를 연동하고, Default 동작으로 Last_Policy 에 연동되도록 설정하는 형식입니다.

또는 기존 LTM Policy 의 default 동작을 참조하여 LTM Policy Draft 를 생성, Publish 까지 완료합니다.

5 (사전 작업) Virtual Address 생성 준비(tmsh command)

서비스 추가 대상 Virtual Server 의 Destination IP/Port 를 확인합니다.

- Vlan-group 을 사용한 구성에서 Virtual Address 는 ARP Disable, ICMP Echo Disable 옵션이 반드시 설정되어야 하기 때문에 미리 Virtual Address 를 확인해야 합니다.

기존에 등록되어 있는 Virtual Address 가 아닌 신규 Virtual Address 는 CLI 에서 생성합니다.
(GUI 에서는 Virtual Server 생성시 Virtual Address 자동 생성 외 별도 생성 방법이 없습니다.)
아래 명령어를 참고하여 생성하면 됩니다.

TMSH 명령어 샘플	<code>create ltm virtual-address 10.10.10.1 address 10.10.10.1 arp disabled icmp-echo disabled description service.domain.com</code>
-------------	--

6 (본 작업) Virtual Server 생성

Virtual Server 생성시 되도록이면 기존 설정을 따르되, 신규 구축인 경우 아래 설정 값을 참조하면 좋습니다.

옵션	설정 값
Name	V_(IP)_(PORT) 양식 또는 기존 설정 참조
Description	(필요에 따라 작성)
Destination Address	(Service IP)
Service Port	(Service Port)
Protocol Profile (Client)	f5-tcp-lan
HTTP Profile	http
SSL Profile (Client)	(사전 생성한 Client SSL Profile)
SSL Profile (Server)	serverssl 또는 serverssl-insecure-compatible
Websocket Profile	Websocket
VLAN and Tunnel Traffic	(기존 설정 참조) All VLANs and Tunnels or ex
Address Translation	<u>Disabled</u>
Port Translation	<u>Disabled</u>
iRule	(기존 설정 참조)
Policies	생성한 LTM Policy
Security – Log Profile	기존 사용중인 Logging Profile 또는 Log illegal Requests 선택

7 (작업 후) 결과 모니터링

CLI 에서 Destination IP / Port tcpdump 및 실제 트래픽 발생을 통해 Virtual Server 및 서비스 정상 여부를 확인합니다.

실제로 서비스 접근이 가능한 환경이라면 간단한 공격 Request 를 통해 Event Log 확인을 통해 Security Policy 적용 여부를 확인할 수 있습니다.