제품 소개서

Broadcom Layer7 API Gateway
(CA API Gateway)

2021.08

BROADCOM Uclick U&Ours

Layer7 Gateway 개요

Layer7 API Gateway는 client에서 API을 호출하고 그 응답을 받는 Run-time시 중요한 구성요소로, 본 프로젝트에 제안하는 Layer7 API Gateway는 그 보안성, 성능 및 안정성, 유연성에 있어 업계 최고로 인정받는 제품입니다.

◇ Layer7 Gateway 주요 기능

보안

- 대부분의 엄격한 취약점 테스트 통과:
- Common Criteria EAL4+
- FIPS 140-2 Level 3
- PCI DSS
- US Military STIG Certified
- SAML, OAuth, STS
- WS-* 호환 스택
- PKI와 HSMs의 사용 지원
- 다양한 IAM에 대한 인증 및 인가
- 서비스 모니터링 및 계측
- 알림, 트래픽 병목통제, SLA 위반에 대한 모니터링

성능/안정성

- 소프트웨어 기반의 가속기
- Layer7 API Gateway간에 클러스터링된 아키텍처로 확장
- 이중화를 위한 자동화된 failover
- XML과 JSON 메시지에 대한 어플리케이션 레벨의 트래픽 Throttling 및 우선순위화
- 변경(Transformation)
- 암호화
- 캐싱 (onboard and external)

유연성/연동

- 다양한 form factors와 배포 모델 지원 (Appliance/BareMetal/ VM/Container 등)
- 다양한 형태의 플랫폼 지원
- XML이나 JSON등 단순화된 접근 관리를 위해 어떤 계정이든 Translate할 수 있는 기능제공
- 프로토콜 중계
- Bindings Conversion
- Intelligent 또는 content기반의 라우팅
- ESB의 Content 변형

확장

- 코딩없이 커스터마이징이 가능한 매우 확장성 높은 솔루션
- Dynamic하고 새로운 기능을 추가할 수 있는 Java SDK
- 새로운 전달과 계정 제공자를 추가할 수 있는 Plug in 프레임워크
- Custom Assertion APIs

G/W 지원 스펙 및 API 관리 기능

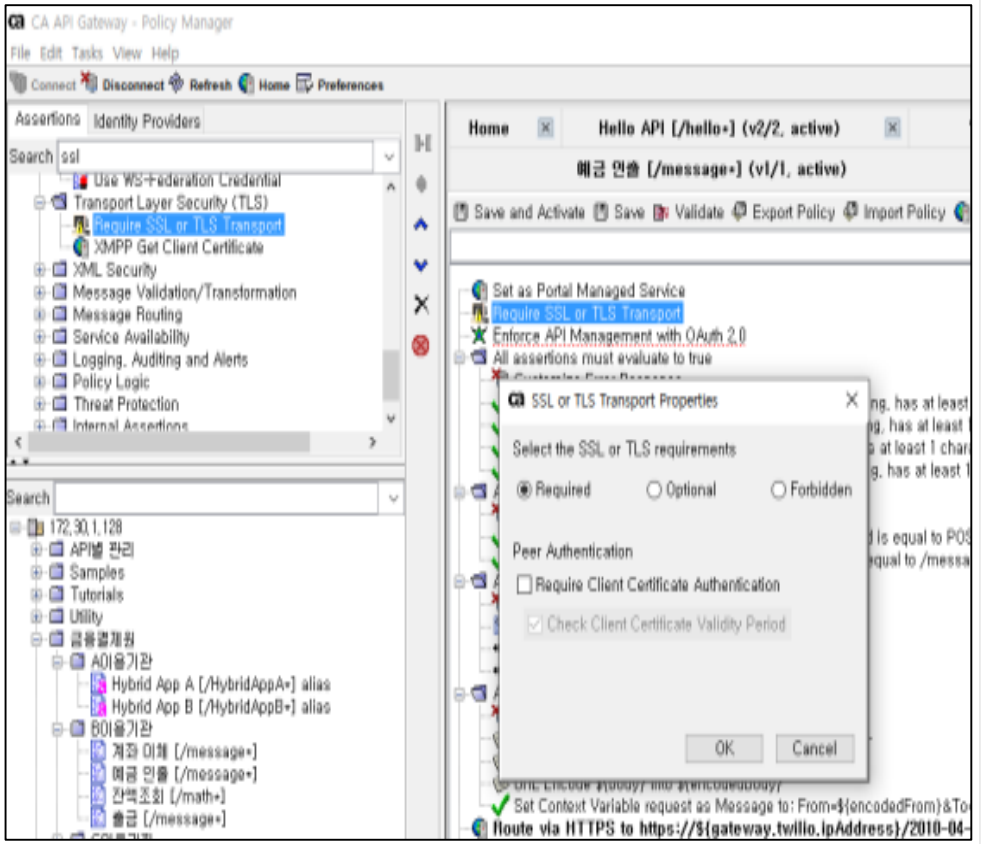
Layer7 API Gateway는 다양한 API서비스를 손쉽게 구성할 수 있는 각종 표준 및 도구를 내장하고 있습니다. 또한 API Gateway는 코딩 없이 커스터마이징이 가능한 매우 확장성 높은 기능을 제공합니다.

◇ G/W 지원 스펙 및 API 관리 기능

표준 웹 /인증 서비스 및 데이터 형식 지원

암호화/ 복호화	통신 프로토콜	Certificate	계정/ 인증관리	Global Standard 지원	
• Support for configurable cryptographic algorithms (Triple-DES, AES, SHA, RSA etc.) • Support for elliptic curve cryptography • FIPS 140-2 support in hardware • FIPS 140-2 support in software • Onboard PKI Onboard Hardware Security Module (HSM) • Support for external HSMs	• HTTP/HTTPS • WebSphere MQ • JMS • AMQP • FTP/S • SFTP • TIBCO EMS • SMTP • Raw TCP • End-to-end compression	• VMware Ready • Common Criteria • PCI-DSS certified • US STIG Vulnerability Tested • Joint DoD/IC Service Security Working Group (JSSWG) • Joint DoD/IC Enterprise Service Monitoring • HSPD12 Backend Attribute Exchange (BAE)	• Integrated STS/SAML issuer • Support for Web/browser-based SSO • Onboard identity store JSON Web Token (JWT) and JSON Web Encryption (JWE), • Integrated PKI Certificate Authority (CA) • Integrated PKI Registration Authority (RA) • OAuth support • Kerberos support, • XACML	• JSON/JSON Path • XML 1.0 • SOAP 1.2 • REST • AJAX • XPath 1.0 • XSLT 1.0 • WSDL 1.1 • JSON/XML Schema • RADIUS • LDAP 3.0 • SAML 1.1/2.0 • PKCS #10 • X.509 v3 Certificates • W3C XML Signature • W3C XML Encryption • UDDI 3.0 IPv6 • MTOM	• SSL/TLS 1.1 / 3.0 • SNMP • POP3 • IMAP4 • OAuth SAML/JWT Bearer grants • WS-Security 1.1 • WS-Trust 1.0 • WS-Federation • WS-Addressing • WS-SecureConversation • WS-MetadataExchange • WS-Policy • WS-SecurityPolicy • WS-PolicyAttachment • WS-SecureExchange • WSIL • WS-I • WS-I BSP

API G/W Manager - Assertion형식으로 API 적용



주요 기능

G/W 인증 및 권한 관리 기능

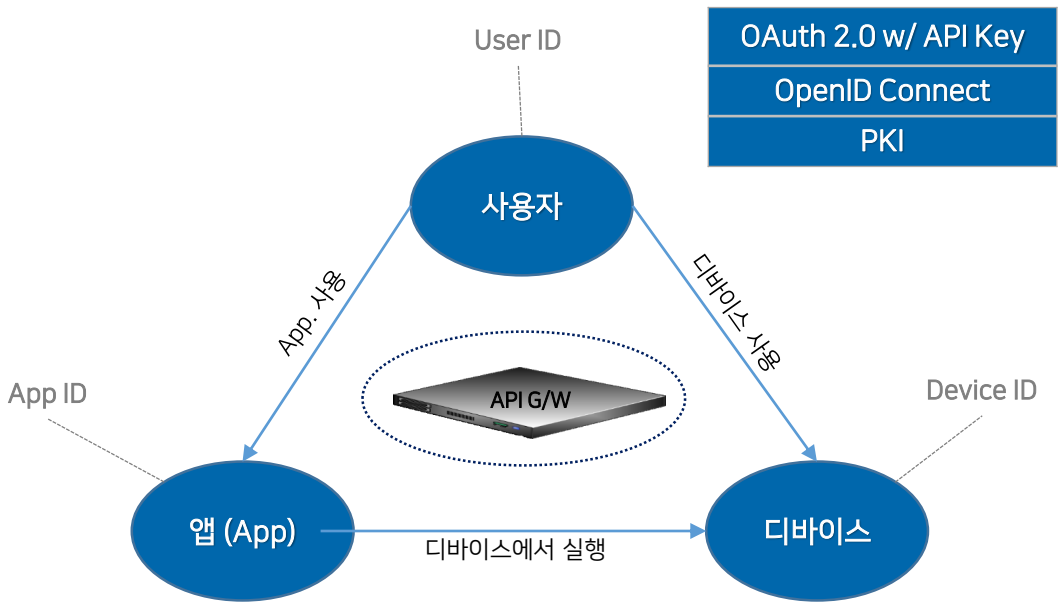
Layer7 API Gateway는 API 사용을 허가하기 위해 사용자, Application 및 Device까지 검증을 요구할 수 있습니다. 그러므로 고객사는 각 API가 처리하는 서비스의 위험도 및 데이터의 민감도에 따라 차등적으로 검증 수위를 조절할 수 있습니다.

◇ 오픈 API 사용 허가 기능을 통한 App 접근 권한 통제

API G/W에서는 하기와 같은 주요 인증 방식을 제공합니다.

- **디바이스 레벨**
  - Mutual SSL 인증
  - IP 기반 인증
- **어플리케이션 레벨**
  - API Key 인증
  - 클라이언트 방식 (OAuth 인증)
- **사용자 레벨**
  - Basic 인증
  - 제 3자 인증 (ID Federation, SSO 솔루션)
  - API Token 방식 (OAuth 인증)
- **어플리케이션 + 사용자 레벨**
  - API Token + 클라이언트 방식 (OAuth 인증)

- 3 legged 방식의 계층적 인증 보안으로 API 보안을 제공
- API G/W는 사용자, App, 디바이스의 관계를 관리



주요 기능

G/W 보안 기능

Layer7 API Gateway는 호출되는 API의 내용을 보호하기 위하여 업계 최고 수준의 다양한 보안 기능 및 정책을 OOTB(Out Of The Box)로 제공하고 있습니다.

◇ 보안기능 특징 및 취약점 대응 기능 제공

검증 모듈	내용
XML Schema 검증	• Schema 정책을 등록하여 해당 정책과 상이한 결과값의 발생을 검증
XML Structure 검증	• XML의 구조에 대한 임계치를 설정하여 해당 임계치와 상이한 결과값 발생을 검증
JSON Structure 검증	• JSON의 단계 및 전문 길이 값 등의 임계치를 설정하여 해당 임계치와 상이한 결과값 발생을 검증
TCP/IP-Based Attacks	• 다양한 routing redirect 유형의 공격 등 일반적인 TCP/IP 기반 공격에 대해 보호
Coercive Parsing and XML Bomb	• 시스템의 Processing 능력을 과부하 시키거나 악의적인 모바일 코드를 삽입하는 공격에 대해 보호
External Entity Attack	• 외부 entity 공격자가 악의적인 코드로 대체할 수 있기 때문에 신뢰할 수 없을 수 있어 Gateway는 기본적으로 외부 entity을 해석하지 않음
Schema Poisoning	• Schema Poisoning은 공격자가 스키마를 대체하거나 변조함으로써 시스템을 와해하는 시도를 포함하는데, Gateway가 비인가 된 위치로부터의 스키마 로드를 방지
WSDL Scanning	• 웹 서비스로 비인가 된 접근을 막음으로써 웹 정보 스캐닝이 차단 됨
XML Routing Detours	• 명백하게 메시지의 routing을 정의하고 routing의 덮어쓰기를 불가능하게 함
Limit Message Size Assertion	• 첨부를 포함하여 전체 메시지 사이즈의 제한을 명시하거나 메시지의 XML 부분의 사이즈를 제한
Protect Against Code Injection Assertion	• Web Service와 AJAX 어플리케이션을 포함하는 웹 어플리케이션을 목표로 하는 코드 삽입 공격을 막기 위한 기능으로 다음과 같은 위협으로 부터 보호함 - HTML/JavaScript Injection (Cross-site Scripting), Shell Injection / XPath Injection, LDAP DN Injection / LDAP Search Injection
Protect Against Cross-Site Request Forgery Assertion	• CSRF 공격을 탐지하고 방어하기 위한 기능으로 CSRF 공격을 탐지하기 위해 두 가지 메커니즘을 제공
Protect Against Document Structure Threats Assertion	• 오버사이즈 파일을 사용하는 XDoS(XML Denial of Service) 공격에 대응하기 위해, 들어오는 XML 요청의 사이즈를 제한
Protect Against Message Replay Assertion	• Gateway가 재생 공격에 대해 보호하기 위한 기능으로, SOAP 메시지가 아닌 경우 메시지 내에 특정한 ID 식별자를 지정하여 재생 공격 방지에 사용 가능 함
Protect Against SQL Attack Assertion	• Gateway가 특정하거나 일반적인 SQL 삽입 공격으로부터 Web Service을 보호
Scan Using ICAP-Enabled Antivirus Assertion	• Gateway가 McAfee, Sophos, Symantec 과 같은 ICAP 프로토콜을 지원하는 외부의 Anti-Virus 서버에 연결하여 메시지나 파일의 검사를 요청하는 기능
Validate or Change Content Type Assertion	• 목표 메시지의 Content-Type을 검증하거나 수정하기 위해 사용되는 기능
Validate OData Request Assertion	• OData 서비스에 의해 노출되는 SMD(Service Metadata Document) 를 사용하는 요청 메시지를 검증하기 위해 사용하는 기능

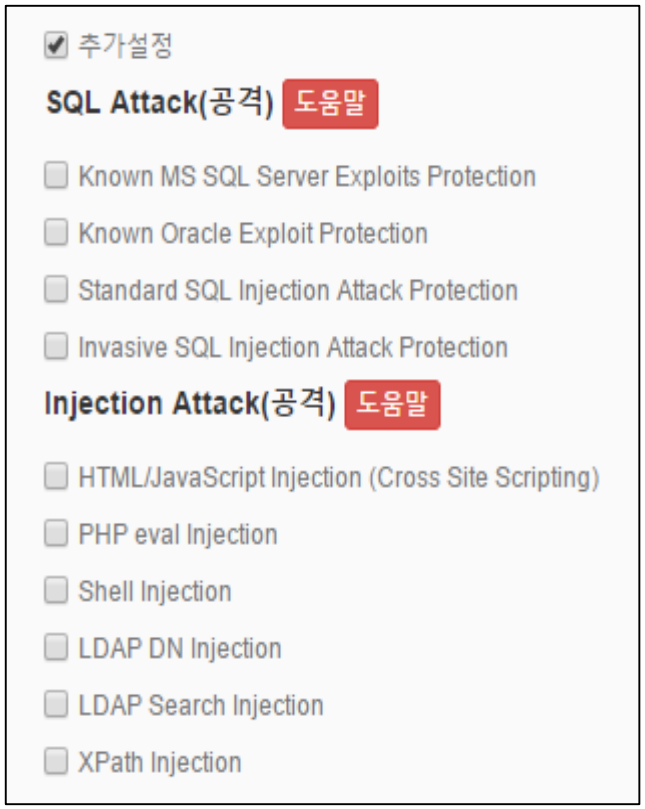
주요 기능

G/W 보안 기능

Layer7 API Gateway는 API 등록 시 이상거래 및 취약점 유형에 대응하는 설정을 할 수 있는 기능을 제공하며, 이상거래 및 취약점정책을 관리 할 수 있는 기능을 제공합니다.

◇ G/W 지원 메시지 무결성 및 기밀성 보장 기능

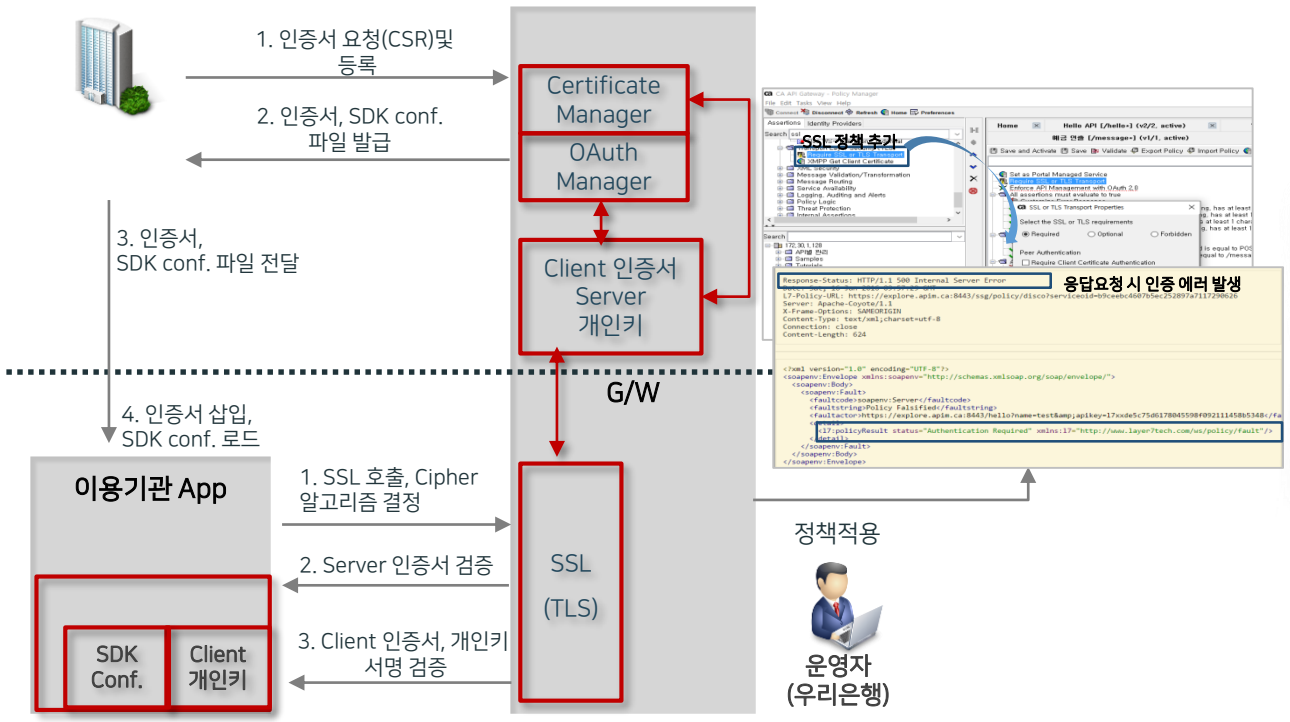
공격방식	설정 가이드
SQL Attack	DB쿼리를 수행하는 API서비스에 대하여 이 설정을 권장한다. 일반적으로 DB 종류에 따라 1~3을 선택할 수 있다. 1. MS SQL Server Exploits Protection (DB가 MSSQL인 경우) 2. Oracle Exploits Protection (DB가 Oracle인 경우) 3. Standard SQL Injection Attack Protection(그 밖의 RDB인 경우) 특별히, 엄격한 기준이 요구되는 민감한 서비스의 경우는 4. Invasive SQL Injection Attack Protection을 선택할 수 있다.
Injection Attack	일반적으로 다음과 같은 경우에 이 설정을 사용할 수 있다. 1. HTML/JavaScript Injection - API 서비스가 HTML/JavaScript 언어로 개발된 경우 2. PHP eval Injection - API 서비스가 PHP 언어로 개발된 경우 3. Shell Injection - API 서비스가 CMS나 Shell을 이용하여 직접 파일을 핸들링하는 경우 4. LDAP DN Injection - API 서비스가 JNDI를 사용하여 직접 LDAP에 쿼리를 하는 경우 5. LDAP Search Injection - API 서비스가 JNDI를 사용하여 직접 LDAP에 쿼리를 하는 경우 6. XPath Injection - API 서비스가 XPath쿼리로 클라이언트 요청을 파싱하거나 내부적으로 프로세싱하는 경우



G/W 보안 기능

Layer7 API Gateway는 SSL 3.0/TLS 1.2 최신의 전송구간 암호화 모듈을 내장하여 Client와 API G/W 구간의 통신 안전성을 제공합니다.

◇ G/W 보안통신 프로토콜(SSL,TLS)을 통한 암호화 통신기능



구현 내용

- API G/W 내부적으로 보안통신 프로토콜 보유
- 운영자는 필요한 API 서비스에 대하여 이미 정의된 정책 적용만으로 통신암호화 구현
- SSL Cipher 알고리즘 선택 지원, 신뢰된 인증서 선택 지원

기대 효과

- 클라이언트 인증서를 인증하는 Mutual SSL 지원으로 안정적인 인증
- SDK 제공으로 개발자 편의성 증대
- Mobile SDK는 CA Site 혹은 Github에서 다운로드 가능 (Open Source)

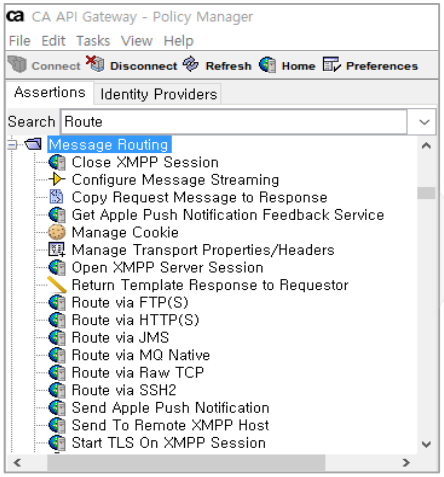
사용량 제어 기능

Layer7 API Gateway는 다양한 알고리즘에 의한 부하분산 기능이 있으며 특정 API 서버의 장애 시 Failover 정책에 따라 서비스의 높은 안정성을 높일 수 있습니다. 뿐만 아니라 다양한 기준으로 사용량 제어 (rate limit) 을 설정할 수 있습니다.

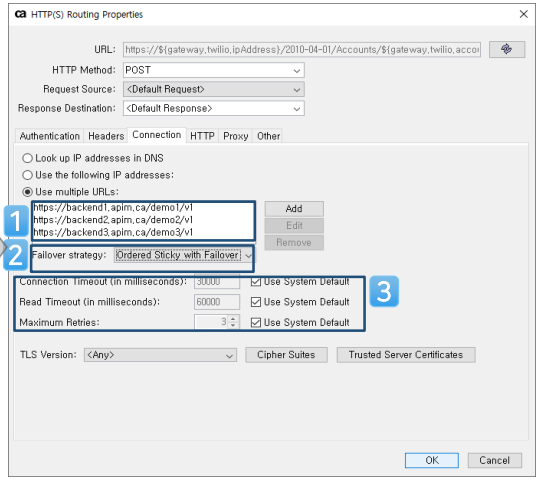
◇ G/W 메시지 라우팅·부하 분산, 사용량 제어 기능

메시지 라우팅/부하분산

Policy manager

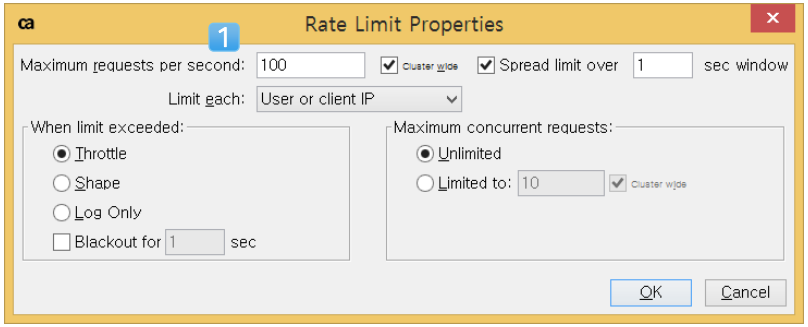


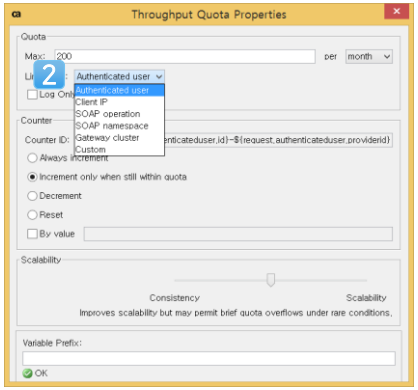
HTTP(S) Routing Properties (Routing)



1 API G/W가 로드 분배할 API서버
2 Load Balancing & Failover 전략(Ordered Sticky, Random Sticky, Round-Robin Sticky)
3 API서버의 Parameter 설정(Connection Timeout, Read Timeout, 재시도 횟수)

사용량 제어 기능





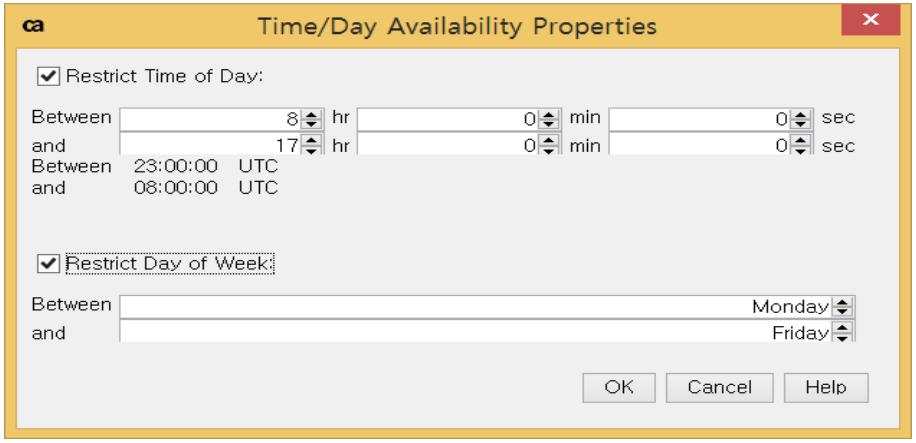
1 각 API에 Rate Limit 설정 (초당 호출 수)
2 각 API에 Throughput Quota 설정 (월, 일, 시, 분, 초 단위 사용 제한)

API 접근 제한 기능

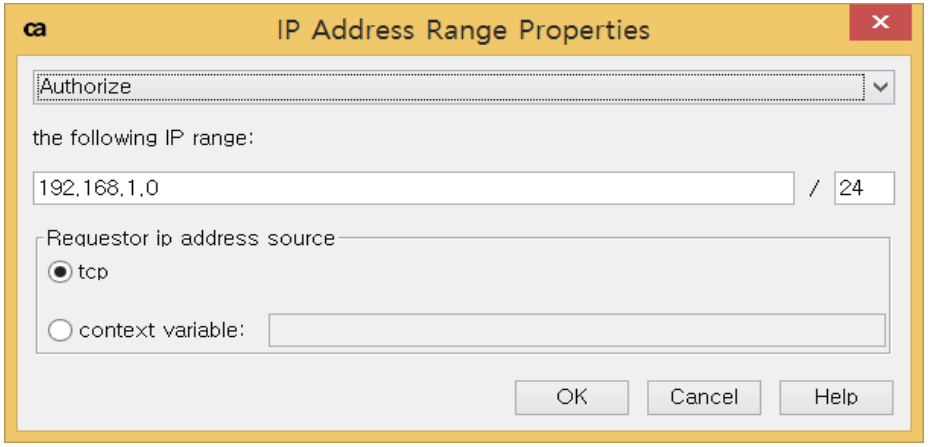
Layer7 API Gateway는 사용자, 시간대, IP등 다양한 기준으로 API 호출에 대한 접근을 제어합니다. 또한 특별히 요구되는 접근제한은 관리자 콘솔 하면에서 간단한 조작을 통해 수정하여 바로 적용 가능합니다.

◇ G/W API 접근 제한 기능

시간 기반 접근통제



IP 기반 접근통제 (IP대역)

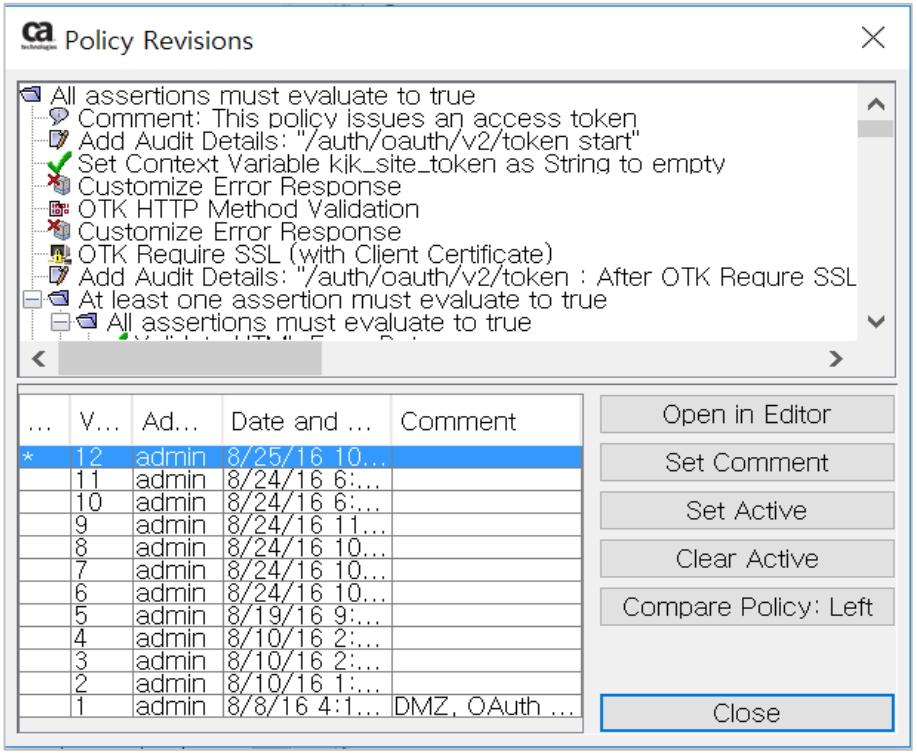


제한 정책	내용
사용자 인증 정책	• 사용자 인증 정책에 대응한 인증 - Internal 정책 : G/W 내부 데이터베이스에서 사용자를 인증 - Federated 정책 : X509와 SAML과 같은 ID 통합 Provider로부터 인증 - LDAP 정책 : 외부 LDAP 서버에서 사용자 인증
시간 기반의 접근통제	• 특정 시간, 특정요일 별 통제
IP기반의 접근 통제	• 특정 IP, 특정 IP 대역 통제

API 버전 관리 기능

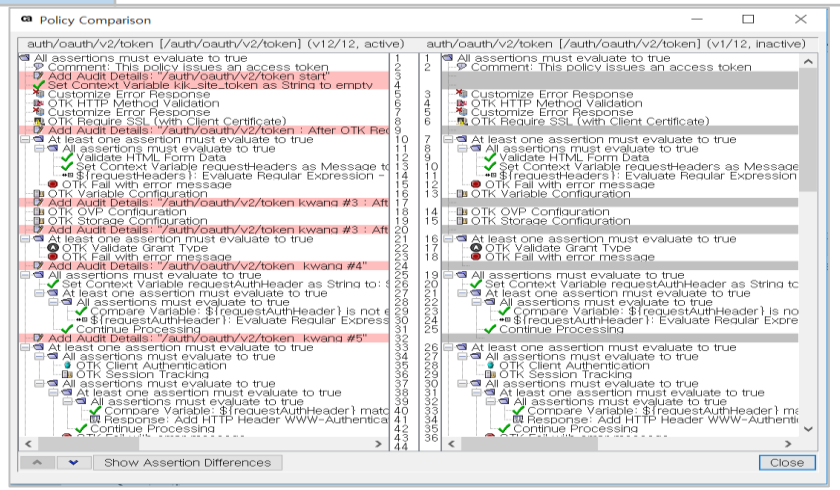
Layer7 API Gateway는 API 정책에 대하여 자동 버전관리를 제공하며, Policy Manager라는 관리 Tool 을 통해 버전 간의 비교와 Rollback 등을 지원함으로써 정책의 버전 업 시 API Developer Portal의 버전 관리 기능과 연동하여 기존 제휴서비스 영향도를 최소화하는 것이 가능합니다.

◇ G/W API 버전 관리 기능



[API Revision 기능]

형상관리 (Revision 관리)	
Set Active	해당되는 API변경 이력 중에 원하는 Version으로 활성화
Compare Policy	API 의 버전 별 수정된 부분에 대한 내용을 확인할 수 있는 기능

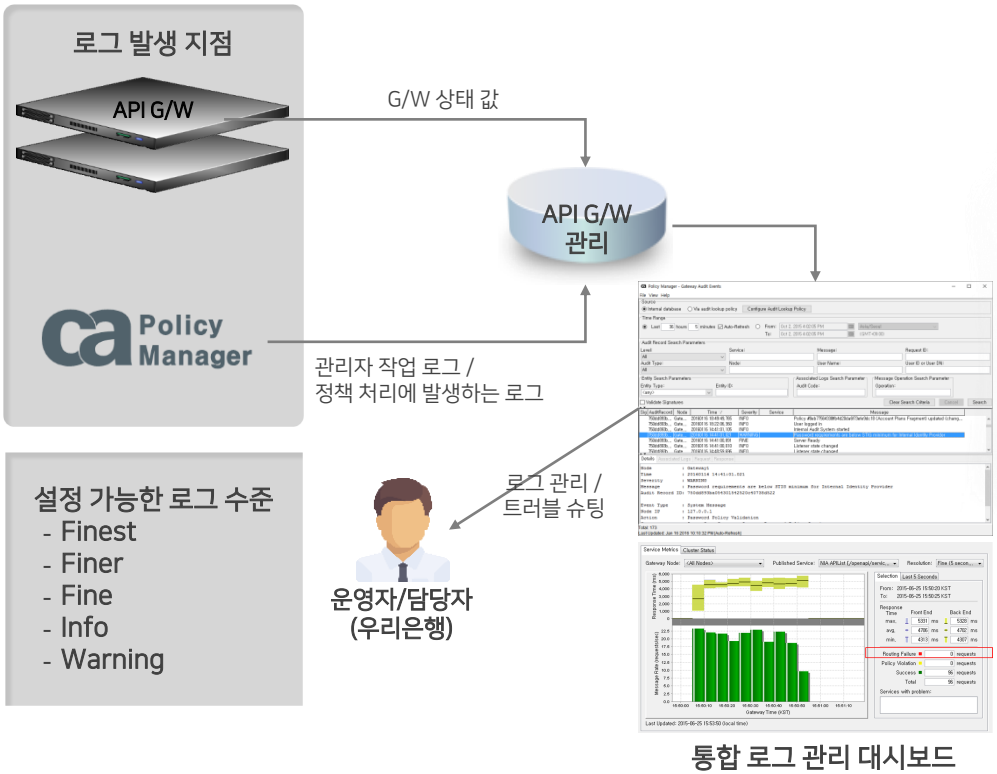


[Version별 Compare 기능]

로그 처리 및 이력관리 기능

Layer7 API Gateway는 Gateway 내에서 발생하는 여러 이벤트에 대한 로그 및 설정한 정책과 관련하여 발생한 로그를 단일 메뉴에서 통합 관리할 수 있는 기능을 제공할 뿐만 아니라, OOTB로 제공되는 Dashboard을 통해서는 API Transaction에 대한 기본적인 시각화 기능을 제공합니다.

◇ G/W 로그 처리 및 이력관리 기능



로그 정책	내용
System Audit Log	• G/W의 Internal 상태에 관한 로그 (예>라이선스 업데이트, 서비스 재시작 등) • 로그 Level과는 별개로 로그에 기록됨
Administrator Audit Log	• API G/W 관리 활동에 대한 작업 로그 (예>Audit로그 검색、Policy 변경、Policy Manager에 로그인 등) • 기본적으로 로그 Level이 Info 이상으로 기록됨
Massage Audit Log	• API에 적용된 정책처리에 발생하는 로그 (예> Assertion 처리, Assertion 오류 등) • 기본적으로 로그 Level이 Warning 이상으로 기록됨

주요 기능

OAuth 기능 지원

Layer7 API Gateway는 OAuth 인가 서버를 내장하고 있어, OAuth 토큰 제공자와 토큰 소비자의 역할을 모두 수행 가능하여 제휴사를 위한 오픈API 플랫폼에 안전한 인증/인가 환경을 제공합니다. 뿐만 아니라 CA API Gateway는 표준 OAuth Grant Type 외 확장 Grant Type까지 지원하고 있습니다.

◇ G/W OAuth 기능 지원

	장점	단점
Authorization Code	• 클라이언트와 리소스 소유자의 사이의 중간단계에서 각각을 인증 하는 보안 이점 • 엑세스 토큰을 리소스 사용자에게 직접 주는 대신 클라이언트에 제공하는 보안적인 이점	• 토큰 발급 과정이 다소 복잡하고, 클라이언트의 인증 플로우 구현이 필요
Implicit	• JavaScript 와 같은 스크립트 언어를 사용하는 브라우저에 클라이언트 수정 없이 적용 가능하도록 최적화 됨	• 중간단계의 Credential 검증 없이 클라이언트가 바로 엑세스 토큰을 취득하는 문제
Client Credentials	• 클라이언트 Credential 로 간편하게 엑세스 토큰을 발급 받을 수 있음	• Authorization Scope 이 이전에 할당된 리소스로 제한되는 경우에만 권장됨 • 클라이언트 Credential 만을 가지고 엑세스 토큰을 발급하므로 신뢰된 클라이언트에 의해서만 사용하도록 권장되며 주로 서버간 인증에만 사용을 권고
Resource owner password credentials	• 사용자 이름과 비밀번호로 간편하게 엑세스 토큰을 발급 받을 수 있음	• 클라이언트가 사용자 Credential을 요구하므로, 리소스 소유자와 클라이언트 사이에 확실한 신뢰관계가 있을때만 권장됨
지원되는 확장 Grant Type : SAML 2.0 Bearer Assertion Profile (RFC7522), JSON Web Token Profile (RFC7523),		

구현 내용

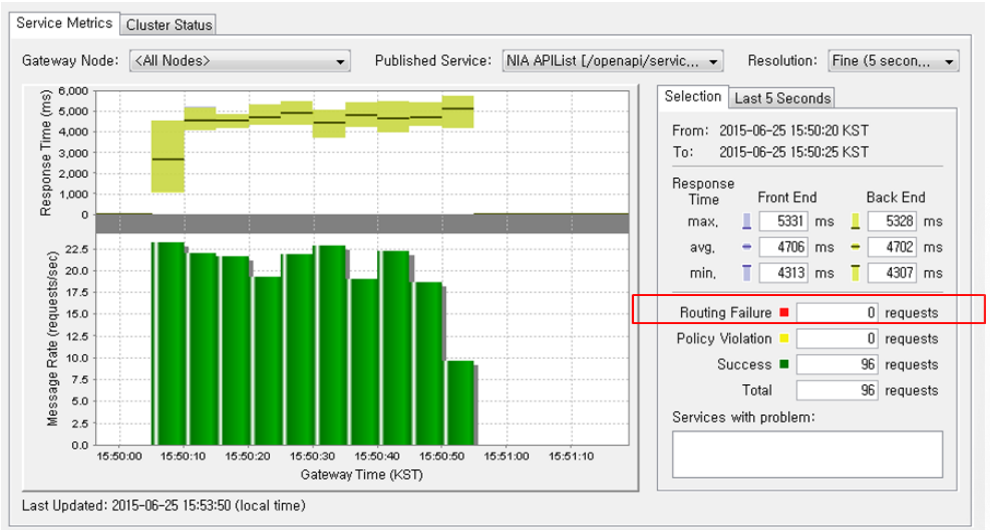
- 금융권에 요구되는 High Level 보안 수준 만족을 위한 최선의 선택
- 오픈 된 환경에서 다수의 사용자와 어플리케이션을 각각 인증한 후 인증 연동을 할 필요성
- 향후 증가할 이용기관의 어플리케이션을 각각 식별하고 검증해 할 필요성
- Gateway 솔루션이 제공하는 모바일 SDK 에 포함된 OAuth 인가 기능을 통해, 클라이언트 개발과정은 단순화 하면서 보안성은 높이는 것이 가능한 이점

모니터링 기능

Layer7 API Gateway는 자체적으로 서비스 및 API 사용량에 대해서 다양한 관점에 대한 모니터링을 위한 리포팅, 일림 설정 등의 기능을 제공함으로써, 장애 발생 시 경보 기능을 발생시켜 운영관리에 효율성을 증대시킵니다.

◇ G/W 모니터링 기능

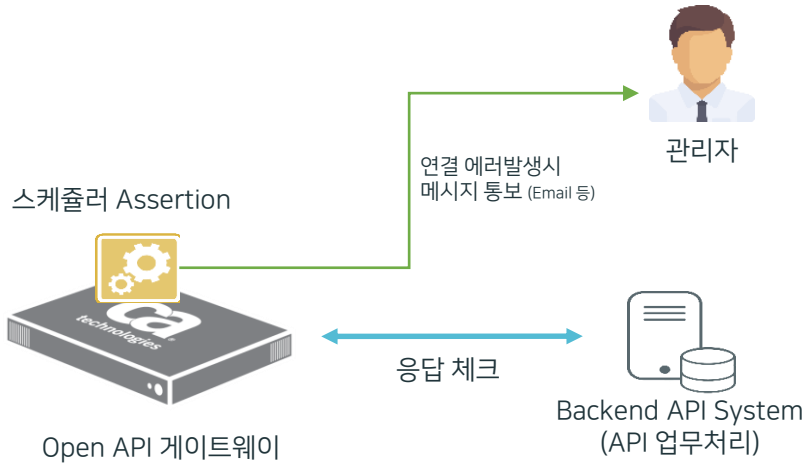
API G/W DashBoard (Policy Manager 내 기능)



대시보드 모니터링

- API G/W 대시보드 정보를 이용하여 서비스 상태 및 연계기관 접속 상태 모니터링
  - 서비스 Frontend/Backend Response Max치를 이용한 비정상 감지
  - Routing Failure 및 policy violation 발생시 원인 파악 후 비정상 유무 판단
  - 그 외 비정상 상태의 원인이 API G/W가 아닐 경우 담당자에게 통보

G/W 내장 스케줄러 서비스를 통해 API 서비스 연결 에러 발생시 통보 기능 제공

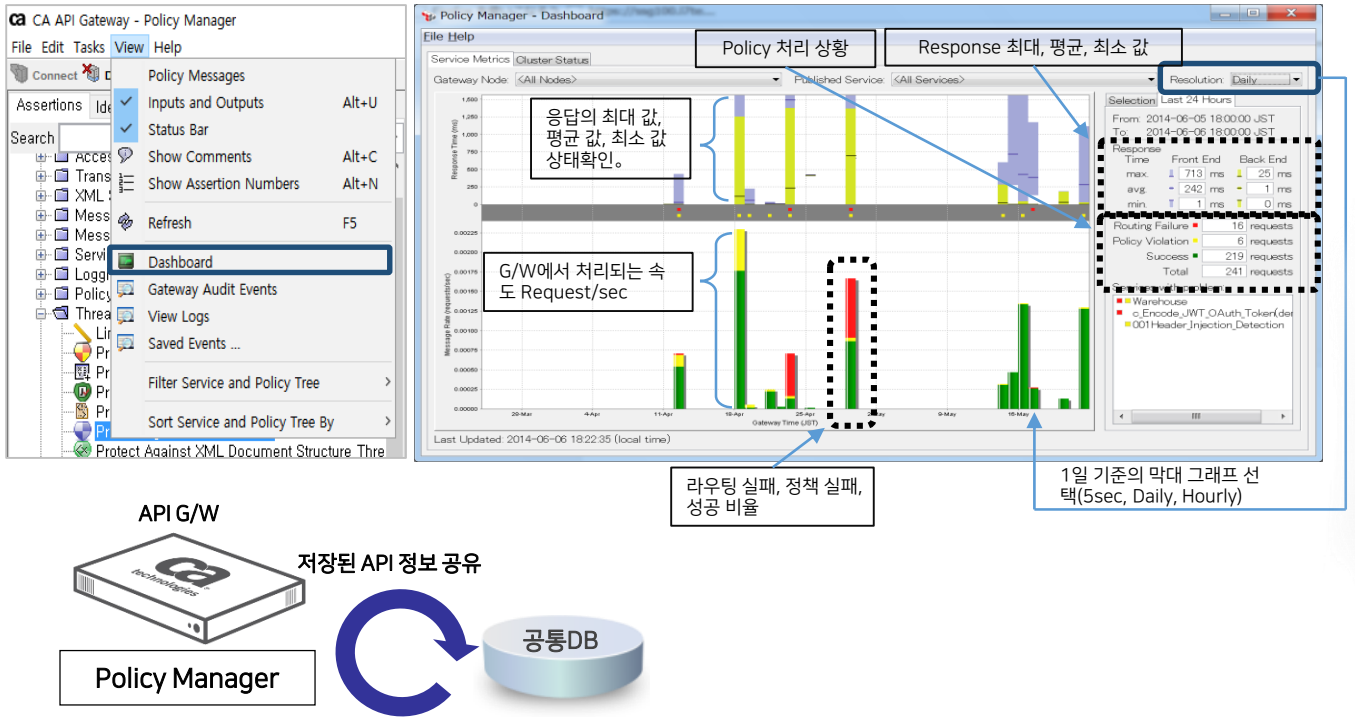


서비스 상태 관리 기능

Layer7 API Gateway는 수행된 API 서비스에 대한 상태 값을 보유하고 있으며 Policy Manager에서 가시성 있는 대시보드를 제공합니다.

◇ G/W 모니터링 기능

API Gateway 대시보드



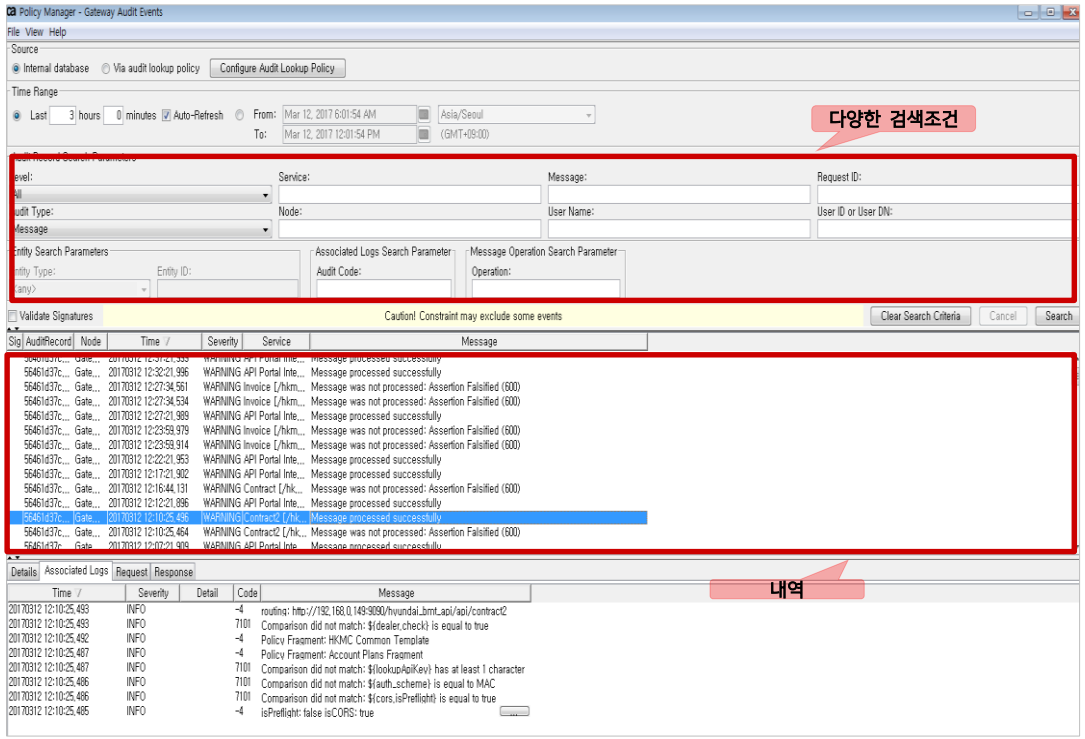
모니터링 기능

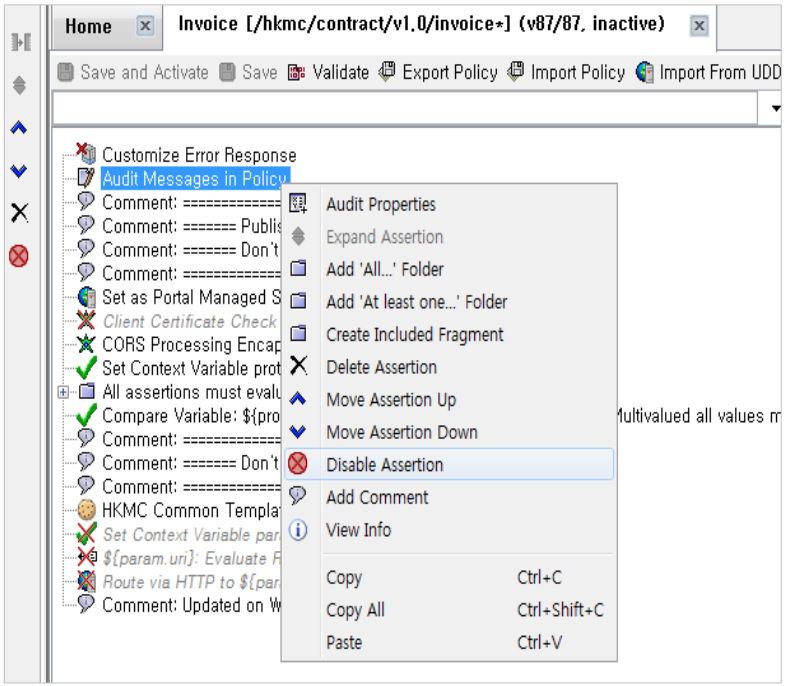
- API G/W 대시보드를 이용하여 API서비스 처리 상황 및 API G/W Cluster 상태 관리
- API 처리 상황 파악
  - API 요청에 대한 최대, 최소, 평균 응답(Frontend, Backend)
  - Backend 라우팅(전송) 실패 횟수
  - 정책처리에 실패한 횟수(요청에 대한 처리 오류 횟수)
  - 정책처리에 성공한 횟수
  - 전체 API 또는 특정 API별 조회가능

내역 관리 기능

Layer7 API Gateway는 수행된 API 서비스에 대한 상태 값을 보유하고 있으며 Policy Manager에서 가시성 있는 대시보드를 제공합니다.

◇ G/W 내역 관리 기능

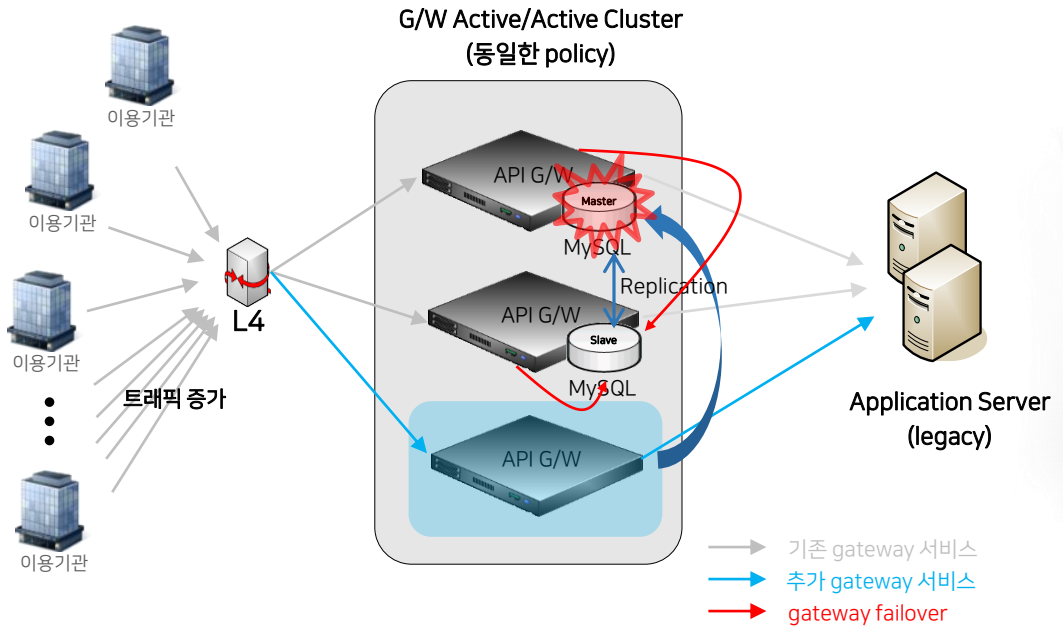




G/W 지원 스펙 및 API 관리 기능

Layer7 API Gateway로 구성된 API 플랫폼은 Application Layer의 멀티 클러스터 환경 구축을 지원합니다. 또한, 외부 L4 에 의해 Routing 된 Message를 처리하고 Sticky Session mode 를 지원하여, 불필요한 센터간 실시간 정보공유 영향도를 최소화하도록 구성할 수 있습니다.

◇ G/W 부하 처리 방안



구현 내용

- L4를 이용한 G/W Active/Active 구성
- G/W가 관리하는 API 개수 제한 없음
- 관리 API 개수 증가 시 조직 별 관리 UI 제공
- 클러스터 아키텍처 구성으로 API G/W를 추가 설치하면 기존 환경 DB에 policy를 참조하여 동일하게 운영 가능
- 가용성 증대 (Auto Failover)

보안 인증 사항

Layer7 API Gateway는 CC인증을 보유하고 있습니다.

◇ G/W 보안 인증 사항

COMMUNICATIONS SECURITY ESTABLISHMENT

Certificate of Product Evaluation

CA Technologies CA API Gateway v9.2

Access Control Devices and Systems

CA Technologies

This is to certify that the named product has been evaluated under the terms and conditions of the Canadian Common Criteria Scheme and complies with the requirements for Common Criteria Recognition Agreement (CCRA).

Conformance Claim:	Standard Protection Profile for Enterprise Security Management Policy Management, v2.1, 24 October 2013 and Standard Protection Profile for Enterprise Security Management Access Control, v2.1, 24 October 2013
CC Evaluation Facility:	EWA-Canada
Date Issued:	10 October 2017

The IT product identified in this certificate has been evaluated at an approved evaluation facility established under the Canadian Common Criteria Scheme using the Common Methodology for IT Security Evaluation, Version 3.1 Revision 5, for conformance to the Common Criteria for IT Security Evaluation, Version 3.1 Revision 5. This certificate applies only to the specific version and release of the product in its evaluated configuration and in conjunction with the complete certification report. The evaluation has been conducted in accordance with the provisions of the Canadian Common Criteria Scheme and the conclusions of the evaluation facility in the evaluation report are consistent with the evidence adduced. This certificate is not an endorsement of the IT product by CSE or by any other organization that recognizes or gives effect to this certificate, and no warranty of the IT product by CSE or by any other organization that recognizes or gives effect to this certificate, is expressed or implied.

ORIGINAL SIGNED **383-4-417**

Manager COTS Assurance Programs

Canada

"CC인증 인증서"

요청 시 별도 제출

감사합니다.